Pravni vidiki preiskovanja in dokazovanja kaznivih dejanj s pomočjo informacijskih in komunikacijskih tehnologij

Nathan Klasinc

Namen prispevka:
Namen prispevka je prikazati preiskovanje kibernetskega kriminala iz vidika organov pregona s poudarkom na pravnem vidiku. V prispevku sem se osredotočil na problematiko s katero se morajo spopadati organi pregona in tožilstvo.

Metode:
Uporabljena metoda za prispevek je bila analiza slovenskih zakonodajnih aktov, strokovnih člankov in prispevkov konference.

Ugotovitve:
Glede na hiter razvoj informacijskih in komunikacijskih tehnologih se Slovenija dokaj uspešno prilagaja temu razvoju vendar ne bo smela razvoja zakonodaje in tehnik preiskovanja opustiti.

Izvirnost/pomembnost:
V prispevku je na kratek in razumljiv način predstavljena problematika s katero se srečujejo organi pregona in zakonodajna veja oblasti.

Ključne besede:
Kibernetična kriminaliteta, Zakon o kazenskem postopku, Kazenski zakonik, informacijsko komunikacijska tehnologija, računalniška kriminaliteta

1 Uvod

V 21. stoletju se tehnologija razvija hitreje kot to lahko to dojemajo ljudje, ki jo razvijajo. Kar je danes novo in predstavlja višek moderne tehnologije bo čez pol leta že korak zadaj. Po Moorovem zakonu se moč procesorjev podvoji približno vsaki dve leti. Bolj natančno vsakih dvajset mesecev. Sicer so strokovnjaki napovedali, da se bo ta trend končal ali vsaj upočasnil od leta 2014 vendar bo tehnologija še vedno prodirala naprej (Kanellos, 2003).

Z razvojem tehnologije se je povečala tudi navezanost in odvisnost od tehnologije. V skoraj vsakem gospodinjstvu najdemo vsaj en računalnik. Večina študentov ga že nujno potrebuje, za delo v poslovnem svetu so pa tako in tako obvezni. Podobno se dogaja pri razvoju mobilne telefonije. Če smo nekoč imeli mobilni telefon, da smo na hitro nekoga poklicali, smo v 21. Stoletju prešli čez to navidezno mejo in mobilni telefoni so veliko več kot samo telefoni. Če primerjamo tehnologijo izpred 50 ali 60 let nazaj lahko zamislimo kaj smo imeli tedaj in kaj imamo sedaj. Elektronska voščilnica, ki nam zaigra Vse najboljše in jo prejmemo preko navadne pošte vsebuje čip, ki premore več moči in računalniških zmogljivosti kot vsi računalniki zavezniških sil leta 1945. Pametni telefoni prekašajo vse računalniške zmožnosti Nase (National Aeronautics and Space Administration) leta 1969, ko so poslali na Luno človeško posadko.

Playstation igralna konzola, ki stane približno 300€ je močnejši in hitrejši kot so bili superračunalniki konec 20. Stoletja in so stali več milijonov € (Kaku, 2011).

Če razvoju elektronskih naprav prištejemo še razvoj interneta, ki je postal glavna sila medijev in prevladujoč način komunikacije se znajdemo v situaciji, ko tehnologija omogoča nove načine izvršitve kaznivih dejanj in razvoj novih kaznivih dejanj na tako hiter način, da organi pregona zaostajajo pri pregonu, zakonodajno delo pa tudi ne more slediti vsem novostim in temu ustrezno prilagajati zakonodajo.

V sledečem članku smo si zastavili vprašanje s kakšnimi težavami se spopadajo organi pregona pri preiskovanju kaznivih dejanj storjenih s pomočjo informacijsko komunikacijskih tehnologij. Težave se pojavljajo tako na strani policije in ostalih preiskovalnih organov, kot na področju tožilstva in sodstva. Razvoj informacijsko komunikacijskih tehnologij eksponentno narašča. Trenutno je slovenska zakonodaja v skladu s tehnologijo vendar so spremembe na področju zakonodaje pogosto počasnejše kot pa na področju tehnologije, zaradi tega bo nujno potrebno hitrejše prilagajanje zakonodajne veje oblasti pri sprejemanju in spreminjanju zakonov ter njihovi implementaciji za kar je odločilnega pomena usposobljenost preiskovalnih organov.

2 Opredelitev kaznivih dejanj na področju informacijskih in komunikacijskih tehnologij

Zaradi nenehnega in razvoja Informacijskih in komunikacijskih tehnologij (v nadaljevanju IKT) je v pravnem pogledu skoraj nemogoče uskladiti zakonodaje za čisto vsako izvedeno dejanje. Gledano iz pravnega vidika težave nastanejo že pri sami opredelitvi kaznivega dejanja in imena kako se bo uporabljalo v zakonu. Kajti, če v zakonu ne bodo zajete vse možnosti lahko sledi posledica, da določeno dejanje ne bo sankcionirano ter zanj ne bo mogoče uvesti kazenskega postopka. Pojem kot je računalniška kriminaliteta je pogosto uporabljen vendar ni vedno primeren. Računalniki so samo eno izmed orodji IKT in po navedbah nekaterih strokovnjakov že morda nekoliko zastareli. Poleg računalnikov na področje IKT spadajo še mobilni telefoni (t.i. pametni telefoni), tablični računalniki, itd. zato je računalniška kriminaliteta zelo ozko področje kriminalitete. Bolj širši pojem je kibernetska oz. kibernetična kriminaliteta, ki se vse bolj uporablja kot osnovni termin kriminalitete, ki nastane s pomočjo IKT. (Završnik, 2007)

Glede nato, da med dvema ali več IKT napravami nastane povezava oz. t.i. mreža lahko govorimo tudi o kriminaliteti IKT, ki pa je nadpomenka kibernetske kriminalitete. Pri opredeljevanju sfere kibernetske kriminalitete se moramo spoznati tudi z več vrstami ustvarjanja mrežnih povezav in dostopanja do medmrežja. Na grobo lahko povezave delimo na žične in brezžične. Bolj podrobno jih pa razdelimo na (Završnik, 2007):

- ISDN (integrated services digital network)
- ADSL(asymetric digital subscriber line)
- Širokopasovne (broadband) povezave
- kabelske povezave
- LAN(local area network).
- WAP (wireless application protocol)
- UMTS (universal mobile telecommunicationssystem),
- Bluetooth
- WLAN (wireless local areanetwork)

2.1 Zakonodaja v ožjem pogledu

Glede na spremembe tehnologije se je morala spreminjati tudi zakonodaja, da lahko organi pregona uspešno opravljajo svoje delo. V Kazenskem zakoniku (v nadaljevanju KZ-1) je naštetih precej kaznivih dejanj, ki jih moč posredno ali neposredno izvajati v okviru kibernetične kriminalitete. (Kazenski zakonik (KZ - 1), 2011)
Neupravičeno prisluškovanje in zvočno snemanje (137. člen KZ)

- Neupravičeno slikovno snemanje (138. člen KZ)
- Kršitev tajnosti občil (2. odstavek 139. člena KZ);
- Nedovoljena objava zasebnih pisanj (140. člen KZ);
- Zloraba osebnih podatkov (143. člena KZ);
- Kršitev moralnih avtorskih pravic (147. člena KZ);
- Kršitev materialnih avtorskih pravic (148. člen KZ)
- Kršitev avtorskih sorodnih pravic (149. člen KZ)
- Napad na informacijski sistem (221. člen KZ)
- Zloraba informacijskega sistema (237. Člen KZ)
- Izdelovanje ali pridobivanje orožja in pripomočkov namenjenih za kaznivo dejanje – pripomočke za vdor ali neupravičen vstop v informacijski sistem (3. odstavek 306. člena KZ)

Naveden zakoni in njegovi členi so že poželi val kritik in argumentov zakaj je zakon slab. Kot navaja vir sta najbolj sporna 1. odstavek 148. člen in 1. odstavek 221. Člen. (Zakon o Kazenskem Postopku (ZKP-UPB8), 2009):

- 148.člen – »(1)*Kdor neupravičeno uporabi eno ali več avtorskih del ali njihovih primerkov, katerih skupna tržna cena pomeni večjo premoženjsko vrednost, se kaznuje z zaporom do treh let*.«
  Kritiki v tem izpostavljajo, da bo na podlagi takšnega zakona vsak, ki ima na računalniku naložene nekaj nelegalne programske opreme (operacijski sistem, urejevalnik besedil,…) ter zajetno količino grafičnih in zvočnih datotek v skupni vrednosti pet tisoč evrov jih bo moč zakonsko preganjati za kaznivo dejanje Kršitev materialnih avtorskih pravic. (Računalniške novice, 2011) Strokovnjaki sicer izpostavljajo v tem primeru, da je za kaznivost potreben namen prodaje. Pri tem se moramo vprašati kdo bo ugotavljal namen prodaje? Ali bo to policist na samem kraju dejanja in bo prepuščeno njegovi presoji ali pa bo to sodišče? (Šepec, Spremembe in novosti s področja, 2010)
- 221. člen – »(1) Kdor neupravičeno vstopi ali vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.«

Kritiki se pri tem členu sprašujejo, če se bo sankcioniralo tudi »vdore« v nezaščitena Wi-Fi omrežja? Problematika je v tem, ker imajo računalniki, tablični računalniki in mobilni telefoni možnost samodejnega vklopa na Wi-Fi omrežje, če je to nezaščiteno in se za vklop v omrežje ne potrebuje gesla in uporabniškega imena. Stroka v tem primeru še ni konkretno odzvala na kritike. Menimo lahko, da tudi v tem primeru bi se moral ugotavljati namen vstopa in storilčev naklep. Vsekakor vdor ne more biti naključen, ker v primeru vdora mora storilec preiti nek varnostni mehanizem. (Računalniške novice, 2011)

Poleg klasifikacije kaznivih dejanj in njihove umestitve v KZ je še bolj pomembno kako je zakonodajna veja uredila Zakon o kazenskem postopku (v nadaljevanju ZKP). Pridobivanje elektronskih podatkov iz IKT nima nobene smisla, če niso te pridobljeni na podlagi veljavnega ZKP. V kolikor niso pravilno pridobljeni za njih velja enako kot za vse nelegitimno pridobljene dokaze in sicer, da so podvrženi eksluziji dokazov. Slovenski ZKP ureja vsebine glede

elektronskih dokazov v 219. a in 223. a členu. Ta dva urejata sledeče vsebine (Kastelic & Škraba, 2012):

- Zaseg elektronske naprave zaradi odprave preiskave te naprave oziroma iskanja podatkov v njej
- Zavarovanje podatkov v elektronski obliki (elektronski podatki se shranijo na drug nosilec podatkov ali se pa izdela kopija celotne nosilca podatkov)
- Preiskavo elektronske naprave (obsega pridobivanje podatkov iz elektronskih naprav, pod to štejemo vsebinski pregled in pridobivanje podatkov v elektronski napravi)

Omenjena člena urejata posege v komunikacijsko in elektronsko zasebnost imetnika ter drugih uporabnikov. Na podlagi teh dveh členov lahko organi pregona posegajo v ustavno zavarovane pravice posameznika do komunikacijske zasebnosti. Člena prav tako določata, da je na njuni podlagi moč pridobiti vse podatke, ki so v elektronski obliki in vsebujejo pomembne informacije za kazenski postopek. (Kastelic & Škraba, 2012)

2.2 Digitalni dokazi

Glede na porast kibernetične kriminalitete se je morala praksa spopasti tudi s tem kaj se lahko opredeli kot digitalni dokaz. Definicij, ki opredeljujejo digitalne dokaze je več, ki pa imajo med seboj podobnosti. Ena izmed njih navaja, da so digitalni dokazi informacije ali podatki, ki so pridobljeni, ko se zbira podatke ali fizično zaseže napravo za preiskavo. Informacije morajo biti shranjene, ustvarjenje ali posredovanje s pomočjo elektronske naprave (Dimc & Dobovšek, 2012). Malo drugačna definicija pa opredeljuje digitalne dokaze kot informacijo, ki je bila ustvarjena ali shranjena v digitalni obliki. Seveda se mora navezovati in biti pomembna za neko pravno zadevo oziroma dogodek (Šepec, 2013). Omeniti moramo tudi definicijo in opredelitve, ki je zapisana v slovenski zakonodaji. Poleg že omenjenih členov ZKP in KZ-1 se moramo osredotočiti tudi na peti odstavek 99. člena ZKP, ki navaja, da je *listina vsako pisanje, nosilec podatkov ali drug predmet, primeren in namenjen za dokaz kakšnega dejstva, ki ima vrednost za pravna razmerja*. Tako, da v to kategorijo nosilcev podatkov spada več ali manj vsaka elektronska naprava, ki ima možnost zapisa. Sicer pa digitalne dokaze lahko razdelimo na tri vrste

- Nelegalne informacije (kopije avtorskih del, gesla, številke kreditnih kartic,…)
- Sredstva za kazniva dejanja (programska hekerska orodja, ponarejene listine,…)
- Informacije kot dokaz (video datoteke, zvočne datoteke, elektronska pošta,…)

Seveda pa en dokaz ni omejen na eno zvrst. Tako je lahko npr. nezakonito pridobljeno geslo nelegalna informacija ter prav tako sredstvo za storitev kaznivega dejanja. Pri preiskovanju kaznivih dejanj v predkazenskem postopku se najbolj pogosto preiskujejo digitalni dokazi kot npr: el. Pošta, razne datoteke (zvočne, grafične, video,…), skripte, zapisi s forumov, socialnih omrežji, klepetalnic, finančni podatki,… (Kastelic & Škraba, 2012)

Na analizo digitalnih dokazov in uspešnost preiskave pa vpliva še nekaj drugih značilnosti digitalnih dokazov (Kastelic & Škraba, 2012):

- Prikritost (kje se podatki nahajajo in kako jih poiskati)
- Občutljivost (na podatke lahko namerno ali nenamerno vplivamo; uničenje in spreminjanje)
- Prenosljivost (podatke so lahko preneseni ali kopirani)
- Razmerje med količino in površino (mediji so vse manjši in lahko vsebujejo vse več podatkov)
- Nedosegljivost (podatke je potrebno pridobit, ki pa so lahko šifrirani ali kriptirani)

2.3 Pridobivanja elektronskih dokazov v teoriji po ZKP

Nova zakonodaja navaja kako morajo organi pregona postopa v primeru zasega elektronske naprave. ZKP pravi, da mora odredba vsebovati čim več podatkov o elektronski napravi, ki je navedena za preiskavo. Odredba mora prav tako vsebovati utemeljitev razlogov za preiskavo, opredelitev vsebine podatkov, ki se iščejo poleg tega morajo navesti še ostale okoliščine, ki bi lahko vplivale oziroma se navezujejo na preiskovalno dejanje. Pravna stroka se tukaj sprašuje kako natančno mora biti opisana elektronska naprava, ki je navedena v odredbi. Minimalen opis je lahko npr. mobilni telefon, prenosni računalnik,… Vendar bi bilo v odredbo napisati čim več identifikacijskih podatkov. Kot takšne podatke lahko upoštevamo znamko naprave, določene tehnične karakteristike ali kakšne druge posebne lastnosti. Kot primer se tukaj navaja, da se mora navesti tudi spominsko kartico v mobilnem telefonu. (Selinšek, 2012)

Tako se poraja vprašanje ali spominska kartica, ki je v mobilnem telefonu in se na njo zapisujejo podatki in vendar ni navedena v odredbi, lahko predmet preiskave? Spominska kartica ni ključni element mobilnega telefona, ki lahko deluje tudi brez spominske kartice. Zagotovo je najbolje, da je v odredbi napisanih čim več podatkov o napravah kajti s tem se olajša delo preiskovalcem in postopek je lažje opravljen korektno in lahko poteka v nadaljevanju kazenskega postopka brez morebitnih zapletov in eksluzije.

Pri preiskavi strežnikov je lahko malo bolj zakompliciran postopek. Odredba lahko navede en strežnik in vse strežnike, ki so z njim povezani. Zakon pravi, da v odredbi mora biti navedeno ali gre to samo za en strežnik ali jih gre za več, ki so med sabo povezani. V kolikor se lahko preiščejo tudi povezani strežniki potem stroka v tem primeru ne vidi težav, da se pregledajo ostali strežniki tudi, če se fizično nahajajo na drugem kraju ali državi. Glede nato, da se podatki nahajajo na svetovnem spletu v katerem ni meja se smatra tudi, da so podatki »brezmejni« in zaradi tega ni potrebe po mednarodni pravni pomoči, da bi preiskovalci lahko preiskali tudi te naprave pa čeprav iz druge lokacije ali države. (Selinšek, 2012)

Pregled strežnika, ki se ne nahaja v Sloveniji je nekoliko sporen. Vendar glede na trend razvijanja IKT, ki zadnja leta stremi k uporabi t.i. Oblakov pri katerih je osnovna karakteristika, da se velika večina dokumentov razen operacijskega sistema nahaja na oddaljeni lokaciji lahko rečemo, da je slovenska zakonodaja smiselno uredila postopek in ne bo potrebne takojšne prenove zakonov. Po drugi strani v primeru, da preiskovalci želijo preiskati strežnik na drugi lokaciji preko medmrežja se pa poraja vprašanje kaj preprečuje osumljencu ali tretji osebi povezani s postopkom, da strežnika preprosto ne izklopi?

Preiskava elektronske naprave je v nekaterih pogledih podobna hišni preiskave. Lahko se izvaja tudi med samo hišno preiskavo. Tako nam tudi narekuje 219.a člen ZKP. V kolikor je preiskava elektronske naprave navedena v odredbi za hišno preiskavo se jo naj bi opravljalo kot samostojno dejanje (223.a člen ZKP). Kadar se preiskovanje elektronske naprave opravlja brez hišne preiskave se uporablja malo drugačen postopek. V preiskovanju elektronskih naprav ni potrebna prisotnost dveh solenitetnih prič tudi takrat ne, ko se opravlja v sklopu hišne preiskave. Vendar za zakon ne prepoveduje prisotnosti dveh solenitetnih prič pri zasegu elektronske naprave ter zavarovanju podatkov. Poleg tega, da ima lahko osumljenec prisotni dve priči ga morajo organi pregona prav tako obvestiti o njegovi pravici do odvetnika in IT strokovnjaka. To pravico ima tudi imetnik naprave, ki ni nujno, da je osumljenec v kazenski zadevi. V kolikor je prisoten odvetnik, osumljencu ni onemogočeno, da nebi bil prisoten tudi IT strokovnjak. Gre namreč zato kaj kdo ponuja. Odvetnik ponuja pravno pomoč IT strokovnjak pa ponuja tehnično pomoč zato je njuna prisotnost kumulativna. Vendar pa ZKP nikjer ne navaja, da mora imetnik naprave biti prisoten pri preiskavi. Po drugi strani pa njegova prisotnost ni

izključujoča. V primeru, da se preiskava elektronske naprave odvija v sklopu hišne preiskave je seveda mogoče, da je imetnik navzoč pri preiskavi ampak ne more v preiskavi aktivno sodelovati. V primeru odsotnosti imetnika, ki bi zavrnil svojo prisotnost ali prisotnost IT strokovnjaka ali odvetnik se lahko na podlagi 223 a. člena zavarovanje podatkov vseeno naredi. Enako prav tako velja kadar je imetnik naprave neznan. Smotrno je tudi počakati na imetnika v kolikor lahko ta pride v razumnem času. (Selinšek, 2012)

2.4 Pridobivanja elektronskih dokazov v praksi – digitalna forenzika

Vedi, ki se ukvarja s preučevanjem digitalnih dokazov rečemo tudi digitalna forenzika. Slovenska policija je tudi v leto 2009 uvedla enoto za računalniško preiskovanje, ki se imenuje Oddelek za računalniško preiskovanje. S tem bi se radi povečali učinkovitost boja proti naraščajoči kibernetski grožnji. Pod njihovo delo spada preiskovanje kaznivih dejanj računalniške kriminalitete in izvajanje postopkov digitalne forenzike. V to spada zavarovanje podatkov in njihova preiskava. Prav tako pa tudi nudijo pomoč ostalim policijskim enotam, ki za tovrstno preiskovanje nimajo primerne opreme in znanja. (Kastelic & Škraba, 2012)
Pridobivanje digitalnih podatkov je delikaten postopek, ki je opredeljen v ZKP. ZKP navaja kako poteka zaseg elektronske naprave, zavarovanje naprave in preiskava naprave. Preiskovalci se morajo držati določenega zaporedja vendar jim ZKP omogoča tudi prilagajanje v kazenskem postopku. Na podlagi ZKP je policija sestavila metodologijo za preiskovanje elektronskih naprav. (Kastelic & Škraba, 2012)

Ko je dosežen dovolj velik dokazni standard za preiskavo se lahko preiskovalci lotijo operacijskih postopkov. Postopki so enaki za vse elektronske naprave. Prva faza vsebuje zaseg naprave, ki je lahko izvedena pri hišni preiskavi, osebni preiskavi na kraju dejanja,… Glede na podatke policije se večino zasegov elektronskih naprav zgodi pri hišnih preiskavah na domu ali pri preiskovanju poslovnih prostorov. Pri zasegu je pomembno, da se napravo temeljito označi in zapečati. Na ta način se zagotavlja istovetnost ter integriteto podatkov oziroma zasežene naprave. Po zasegu sledi zavarovanje podatkov kar vključuje izdelavo identične kopije nosilca podatkov. V celotnem postopku je to najpomembnejši del. Poleg tega, da morajo biti podatki pravilno zavarovani, se je treba držati zakonskih določil in načel digitalne forenzike. Nato sledi analiza in obdelava zaseženih podatkov. Pri tem delu faze preiskave morajo preiskovalci uporabljati ustrezno opremo s katero ne bo prišlo do nezaželenih sprememb podatkov ali nosilca podatkov. Na koncu se naredi še zaključek v obliki zapisnika in arhiviranja podatkov. (Kastelic & Škraba, 2012)

2.5 Problematika policije

Klub urejeni zakonodaji in urejenih preiskovalnih postopkov digitalnih forenzikov se policija pri svojem delu vseeno spopada z nekaterimi težavami. Težave lahko nastanejo zaradi napačne interpretacije ZKP ali iz strani policije ker je na tem področju še dokaj neizkušena in ji primanjkuje prakse.

Pogost problem se pojavlja, ko sodišče sprva zahteva od uporabnika, da ta sam privoli in izroči podatke. V primeru, da se to ne zgodi lahko šele policija zaprosi za izdajo odredbe. Vendar v določenih primerih policija ne more tako posredovati, ker lahko pride do uničenja podatkov. V primeru, ko gre za elektronsko pošto ali podobne storitve, kjer lahko uporabnik podatke izbriše iz skoraj, da katerekoli elektronske komunikacijske naprave ali v primerih, ko ima več ljudi dostop do strežnikov. V takšnih primerih je pridobitev dovoljenja uporabnikov brezpredmetno

in nesmiselno. Do enakega problema lahko pride tudi takrat, ko je odredba izročena pred pričetkom preiskave. Ponovno lahko uporabnik ali nekdo drug podatke uniči.

V mnogih primerih se lahko zgodi, da določena elektronska naprava ni bila zasežena pri preiskavi oziroma z odredbo temveč je bila najdena na kraju kaznivega dejanja ali pa jo je našel občan. Skratka policija ne ve kdo je lastnik naprave ali pa ta ni dosegljiv. Organi pregona v tem primeru niso seznanjeni ali se je potrebno ravnati v skladu z 219 a. in 223 a. členom ZKP. (Kastelic & Škraba, 2012)

Kadar se izvaja hišna preiskava na podlagi odredbe je težko verjetno, da bodo na odredbi vsi identifikacijski podatki elektronske naprave katero mora policija zaseči in preiskati. Lahko se zgodi, da je zaradi tega odredba zavrnjena s strani tožilstva oziroma sodišča.

ZKP določa, da je uporabnik elektronske naprave lahko prisoten pri zavarovanju naprave vendar ne pri preiskave elektronske naprave. Vendar lahko odredba tako narekuje in v tem primeru policija vidi težavo kjer so mnenja, da je lahko imetnik naprave prisoten pri preiskave samo takrat kadar je to izrecno potrebno in lahko s svojo prisotnostjo olajša delo preiskovalcev. Sicer pa policija meni, da bi o prisotnosti imetnika elektronska naprave morala odločati samo policija. (Kastelic & Škraba, 2012)

Težave lahko tudi nastanejo pri sodnih odredbah, če imajo le-te predpisane nekatere omejitve. Omejitev se morajo upoštevati lahko jih je pa tudi več v eni odredbi. Pod najbolj pogoste omejitve spadajo (Kastelic & Škraba, 2012):

- Ime datoteke - v odredbi je navedeno, da se lahko iščejo datoteke samo določenega tipa
    - Omenjena omejitev je zelo nesmiselna kajti eno ali več datotek se lahko zelo hitro preimenuje ali spremeni končnico.
- Tip datoteke – v tem primeru se omejitev nanaša na končnico datoteke npr. policija lahko pregleda datoteke samo tipe .mp3
    - Kot v prejšnji omejitvi tudi tukaj velja, da se lahko končnico zelo hitro spremeni, s tem se pa vsebina datoteke ne spremeni. Takoj, ko datoteki vrnemo »pravilno« končnico se jo lahko normalno uporablja naprej.
- Čas datoteke – odredba lahko narekuje, da se sme pregledati samo datoteke, ki so nastale v določenem času
    - Ponovno gre za dokaj nesmiselno omejitev kajti sistemski čas in s tem čas nastanka datotek se brez težav spremeni. Za spreminjanje časa nastanka datotek se lahko uporabnik poslužuje tudi drugih programov, ki to omogočajo.
- Vsebina datoteke – v kolikor v odredbi piše, da se sme preiskovati samo datoteke z določeno vsebino tako ponovno ovirajo ali onemogočajo preiskavo.
    - Nekatere tipe datotek se lahko pregleda samo takrat, ko se jih predhodno obdela z določenim programski orodjem.
- Veljavnost odredbe – odredba lahko prav tako predpisuje datumsko do kdaj mora biti preiskava elektronske naprave narejena.
    - V kolikor se zaseže več elektronskih naprav lahko čas, ki ga predpisuje 223 a. člen preseže kjer so organi pregona vezani na čas treh mesecev. Vendar po 219 a. členu nimajo nobene časovne omejitve.
- Izvajalci preiskave – odredba lahko specificira katera enota policije bo izvajala preiskavo

- Ponovno prihaja do vmešavanja v delo policije. Policija namreč meni, da mora biti njim prepuščena taktika dela ter, da lahko sami določajo katera enota iz policije bo sodelovala v postopku

2.6 Problematika tožilstva

Tožilstvo je izpostavilo problematiko kriptiranih podatkov in programov za kriptiranje. Kot težavo izpostavlja dostop do kriptirnih programov, ki omogočajo kriptiranje na najvišjem nivoju. Vsekakor takšni programi niso in ne morejo biti prepovedani. Pojavljajo se tudi v množični uporabi saj se marsikdo želi zavarovati svoje podatke in takšen program lahko dobi brez težav na svetovnem spletu. Poleg tega, da so »fizično« lahko dosegljivi so cenovno zelo ugodni ali celo zastonj (t.i. open source). Računalniški kriptirni program, ki uporablja 256 bitni kriptirni ključ je praktično nezlomljiv. Algoritmi, ki so uporabljeni jih je dejansko nemogoče odpreti brez ključa (zaščitnega gesla) in so na najvišjem nivoju kriptiranja. (Krumpak, 2012)

Elektronski dokazi, ki so pridobljeni in kriptirani na tak način z razlogom, da jih organi pregona ne morejo pridobiti veljajo kot uničen dokaz. Omenjeni programi so zmožni tudi oblikovanja skrite particije na trdem disku. Bolj laično to pomeni, da se trdi disk razdeli na dva ali več delov od katerega je en del skrit oziroma neviden in na tem neviden trdem disku se lahko namesti operacijski sistem (npr. Windows). V kolikor uporabnik uporablja neviden del trdega diska se bo vsaka operacija izvajala na nevidnem delu in bo tako vsaka informacija avtomatsko kriptirana 256 bitnim ključem. (Krumpak, 2012)

Boj proti takšnim sredstvom lahko organi pregona izvajajo s prikritimi preiskovalnimi ukrepi. Poleg tega je skoraj nujno, da se pri pregledu elektronskih naprav storilca loči od elektronske naprave zelo hitro tudi s silo, če je to potrebno za izvedbo preiskave. Drugače lahko osumljenec zelo hitro napravo ugasne ali zažene kriptirne programe itd. Omenjen pristop je pogojno določen tudi v ZKP.

Stroka primerja tudi slovensko zakonodajo ter zakonodajo Velike Britanije. V slovenski zakonodaji je sicer določeno, da imetnik elektronske naprave omogoči organom pregona dostop do podatkov tudi, če so ti kriptirani. Se pravi jim predloži kriptirno geslo. Vendar praksa je pokazala, da so elektronske naprave, ki so zasežene približno v 90 % v lasti oseb, ki imajo status osumljenca. Zakon jim pa dovoljuje nesodelovanje z organi pregona. V takšnem primeru lahko policija ostane brez dokaznega gradiva. V Veliki Britaniji so to problematiko rešili z Zakonom o ureditvi preiskovalnih pooblastil. Po njihovi zakonodaji je ne sodelovanje z organi pregona samostojno kaznivo dejanje, ki se ga sankcionira z denarno kaznijo ali zaporom do dveh let. Stroka še navaja, da takšna zakonska ureditev nebi bila mogoča v slovenski ustavnopravni ureditvi. (Krumpak, 2012)

3 Zaključek

Vsekakor lahko vidimo, da je slovenska zakonodaja dokaj dobro pripravljena na kibernetsko kriminaliteto. Vprašanje se pojavlja, če so organi pregona dovolj dobro izurjeni in, če bodo lahko dobro sodelovali med sabo tako organi pregona kot policija. Posebna enota, ki jo je sestavila policija je vsekakor korak v pravo smer. Porast kibernetskega kriminala prav tako predstavlja težavo saj se glede na podatke kazniva dejanja s področja kibernetske kriminalitete drastično dvigujejo. Drugo vprašanje, ki se pojavlja je koliko časa bo zakonodaja zdržala glede na spremembe IKT, ki se razvija z veliko hitrostjo. Če karikiram mislim, da bo zakonodajna veja

oblasti morala spreminjati in dodajati predpise in odločbe tako hitro kot razvijalci programske opreme nadgrajujejo verzije programske opreme.

Literatura

Dimc, M., & Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi.* Ljubljana: Fakulteta za varnostne vede, Univerza v Mariboru.

Kaku, M. (2011). *Phsysics of the Future.* Doubleday.

Kanellos, M. (2. februar 2003). *CNET.* Prevzeto 31. marec 2013 iz Moore's Law to roll on for another decade: http://news.cnet.com/2100-1001-984051.html

Kastelic, T., & Škraba, M. (2012). Digitalni dokazi - metode in izkušnje policije. *Digitalni dokazi* (str. 29-44). Ljubljana: Univerza v Mariboru, Faulteta za varnostne vede in Pravna fakulteta.

Kazenski zakonik (KZ - 1). (2011). *Uradni list RS, 55/2008, 66/2008 - popr., 39/2009, 55/2009 - Odl. US, 91/2011*.

Krumpak, I. (2012). Državno tožilstvo vidik problematike digitalnih dokazov. *Digitalni dokazi* (str. 45-58). Ljubljana: Univerza v Mariboru, Faulteta za varnostne vede in Pravna fakulteta.

Računalniške novice. (6. junij 2011). *Slovenska vlada brezglavo nad spletno piratstvo in računalniški kriminal.* Prevzeto 1. april 2013 iz http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/slovenska-vlada-z-vsemi-topovi-nad-spletno-piratstvo-in-racunalniski-kriminal.html

Selinšek, L. (2012). Pravno-teoretični vidiki preiskave elektronskih naprav - nekaj odrtih vprašanj. *Digitalni dokazi* (str. 7-16). Ljubljana: Univerza v Mariboru, Faulteta za varnostne vede in Pravna fakulteta.

Šepec, M. (2010). Spremembe in novosti s področja. *11. Slovenski dnevi varstvoslovja.* Ljubljana.

Šepec, M. (2013). Privilegij zoper samoobtožbo in nezakoniti digitalni dokazi. *Preiskovanje in dokazne prepovedi* (str. 127-144). Ljubljana: Univerza v Mariboru, Fakulteta za varnostne vede.

Zakon o Kazenskem Postopku (ZKP-UPB8). (2009). *Uradni list RS, 32/2012*.

Završnik, A. (2007). Kibernetičan kriminaliteta: (kiber)kriminološke in (kiber)vikitmološke posebnosti "informacijske avtoceste". *Revija za kriminalistiko in kriminologijo, 3*, 248-260.