# KONVENCIJA O KIBERNETSKI KRIMINALITETI
# "Budimpeštanska konvencija"

Andrej Rupnik

**Povzetek** — Konvencija Sveta Evrope iz leta 2001 je prvi mednarodni pravni akt, ki sodobno kibernetsko kriminaliteto obravnava z vidika priporočil, ki naj jih podpisnice upoštevajo pri oblikovanju in reformi svojega notranjega prava. Zakonodajne spremembe bodo potrebne predvsem v kazenskem materialnem in procesnem pravu, spremeniti ali dopolniti pa bo potrebno tudi predpise, ki urejajo telekomunikacije. Konvencija določa tudi splošen okvir mednarodnega sodelovanja preiskovalcev, saj kibernetski kriminal pogosto presega meje nacionalnih jurisdikcij.

**Ključne besede** — kibernetska kriminaliteta, kazensko pravo, mednarodno sodelovanje, Svet Evrope

**Abstract —** Cybercrime Convention of 2001 is the first international legal act with recommendations to the national legislators, which shall be considered in the process of defining and reforming the national law of signing state. Changes will have to be made in the substantive and procedural criminal law, as well the ones considering the telecommunication regulations. Convention also defines a general framework for the international co-operation of investigative authorities, as the cyber-crime tends to exceed the borders of national jurisdictions.

**Keywords —** cyber-crime, criminal law, international co-operation, Council of Europe

## I. EKSPERTNA SKUPINA SVETA EVROPE (PC-CY)

Pod okriljem Sveta Evrope oziroma njegovega Komiteja za probleme kriminalitete, je bila v letu 1997 oblikovana skupina strokovnjakov (označena s kratico PC-CY) iz držav članic z nalogo, da pripravi tako imenovano »cyber crime« konvencijo, ki bo določila mednarodne pravne standarde na področju boja proti z računalništvom povezani kriminaliteti. V rednem delu skupine je sodelovalo relativno omejeno število strokovnjakov članic Sveta Evrope, predvsem iz držav z bogatimi izkušnjami na področju kiber kriminala, zelo aktivno pa so pri pripravi kovencije sodelovali predstavniki držav opazovalk - ZDA, Kanade, Južnoafriške Republike in Japonske.

V decembru 2000 je Svet Evrope povabil k zasedanju, na katerem je delovna skupina obravnavala že 25. verzijo osnutka konvencije, tudi vse ostale članice, saj je šlo za zadnje zasedanje, po katerem so se v osnutek konvencije vnesli le še edicijski popravki, besedilo pa se je uvrstilo v redno obravnavo v organih Sveta Evrope oziroma na zasedanje odbora ministrov. Države, ki pri pripravi besedila niso sodelovale, so bile na zadnje zasedanje PC-CY vabljene predvsem z namenom, da se seznanijo z opravljenim delom in vsebino konvencije.

V okviru diskusij odbora ministrov 21.septembra 2001 o nujni pospešitvi podpisovanja in ratifikacij konvencij Sveta Evrope s področja boja proti terorizmu, je bila med konvencije, katerih sprejem je potrebno pospešiti, uvrščena tudi kovencija Sveta Evrope o kibernetski kriminaliteti (Cyber Crime Convention). Temu je sledila formalna potrditev na Komiteju ministrov Sveta Evrope 8. novembra 2001. Naglico gre pripisati znanim »enajsto septembrskim« dogodkom v ZDA in s tem povezanimi mednarodnimi ukrepi, ministri pa so svojo odločitev sprejeli v prepričanju, da lahko tudi nova konvencija v precejšnji meri pripomore k boju proti terorizmu, saj le-ta posega tudi v kibernetski prostor, bodisi, da ga uporablja kot orodje ali pa kot objekt napada. S tem so nastale varnostne in politične okoliščine, ki so znatno prispevale k dejstvu, da je predmetna konvencija »rekordna« kar po nekaj kriterijih: v zgodovini Sveta Evrope še nobena konvencija ni bila podpisana v tako kratkem času po zaključku ekspertnega dela, redke konvencije so doživele tako široko podporo, rekordno pa je bilo tudi število držav, ki so jo bile pripravljene podpisati ob formalni razglasitvi. Istočasno je konvencija postala tudi predmet zelo širokih diskusij, saj je prenekatera interesna skupina smatrala, da gre za preširoko pooblaščanje organov pregona za vstop v sfero zasebnosti ljudi, na drugi strani pa so tudi ponudniki internet in drugih kibernetskih storitev nasprotovali novim obvezam, ki jim jih konvencija nalaga (hramba podatkov o prometu ne zgolj za sistem obračunavanja storitev, temveč tudi za dokazovanje ilegalnih aktivnosti, obvezno sodelovanje z organi pregona itd.), saj zanje pomenijo nove, predvsem finančne obremenitve.

## II. SPREJEM IN PODPIS

Svet Evrope je organiziral podpisovanje konvencije v Budimpešti 23. novembra 2001, dan pred tem pa je skupaj z madžarsko vlado organiziral še enodnevno konferenco, ki je bila praktično v celoti posvečena vsebini konvencije. K podpisovanju konvencije so povabili vse članice Sveta Evrope in opazovalke, na dan sprejetja pa jo je podpisalo, kot že rečeno, rekordnih 30 držav. Zanimivo je tudi, da je konvencijo podpisala tudi vrsta držav, v katerih se s problemi računalniškega kriminala ne ukvarjajo kaj dosti niti s kazensko pravnih vidikov (odsotnost ustreznih materialnih in procesnih določb in zakonodaje o varstvu osebnih podatkov), še manj pa s policijsko - preiskovalnih. V tem oziru, izhajajoč seveda iz primerjalnih mednarodno pravnih izhodišč, Slovenija spada med relativno urejene države, saj naša materialna kazenska zakonodaja vsebuje večino inkriminacij (ne pa vseh), ki jih pozna konvencija, relativno dobro pa so urejeni tudi nekateri instituti kazenskega procesnega prava. Primerjalno je konvencija sicer širša od naših nacionalnih določb, kar pomeni, da bodo potrebne spremembe v nekaterih zakonih (kazenski zakonik, zakon o kazenskem postopku, zakon o telekomunikacijah). Uvesti bo potrebno nekatere nove pravne institute in na novo urediti druge, sicer že obstoječe določbe, predvsem v smislu dikcijskih sprememb. Slovenska primerjalna prednost je tudi v tem, da spadamo v ne ravno veliko skupino držav, ki ima v organizacijski strukturi policije posebno enoto za boj proti računalniški kriminaliteti, ki deluje tudi v resnici in ne zgolj na papirju.

Vlada Republike Slovenije je najprej oblikovala medresorsko strokovno skupino, ki so jo sestavljali predstavniki ministrstev za notranje zadeve, informacijsko družbo, zunanje zadeve in pravosodje, pripravila pa je interdisciplinarno verificiran prevod konvencije. Republika Slovenija je konvencijo podpisala 24. julija 2002. Trenutno čaka na ratifikacijski postopek v Državnem zboru, postala pa je tudi del tako imenovanega »evropskega prava« (acquis communautaire). Medresorska delovna skupina že pripravlja dopolnitve in popravke slovenskega kazenskega zakonika in zakona o kazenskem postopku, s čimer bo naš notranji pravni red usklajen z določili konvencije.

## III. VSEBINA KONVENCIJE

Konvencija ima preambulo in štiri poglavja. V prvem definira uporabljene izraze, v drugem ukrepe, ki jih je treba sprejeti na državni ravni, v tretjem mednarodno sodelovanje, četrto poglavje pa vsebuje končne določbe.

### *Preambula*

V preambuli konvencija določa svoj širši mednarodno pravni kontekst, v katerem se zlasti sklicuje na Konvencijo Sveta Evrope o varstvu človekovih pravic in temeljnih svoboščin iz leta 1950, Mednarodni pakt Združenih narodov o državljanskih in političnih pravicah iz leta 1966, Konvencijo Sveta Evrope o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov iz leta 1981, Konvencijo Združenih narodov o otrokovih pravicah iz leta 1989, Konvencijo Mednarodne organizacije dela o prepovedi najhujših oblik dela otrok in takojšnjem ukrepanju za njihovo odpravo iz leta 1999, obstoječe konvencije Sveta Evrope o sodelovanju na kaznovalnem področju, podobne obstoječe pogodbe med državami članicami Sveta Evrope in drugimi državami, ter nenazadnje, na pravni red Evropske unije. Konvencija upošteva dosedanji mednarodno pravni okvir, ki ga dopolnjuje in ga v ničemer ne omejuje.

### *1. poglavje: Pomen izrazov*

V prvem poglavju najdemo definicije posameznih izrazov, ki jih uporablja konvencija, saj je enotno razumevanje uporabljenih pojmov za uspešno mednarodno sodelovanje in skupno kriminalitetno politiko več kot nujno. Konvencija na dovolj jasen način definira pojme: računalniški sistem, računalniški podatki, ponudniki storitev in podatki o prometu.

### *2. poglavje: Kazensko materialno in procesno pravo ter sodna pristojnost*

V drugem poglavju konvencija nalaga podpisnicam ukrepe, ki jih morajo le-te sprejeti na državni ravni na področjih kazenskega materialnega prava, kazenskega procesnega prava in jurisdikcije.

V **kazensko materialnem delu** vsebuje več naslovov s členi, ki definirajo inkriminacije po vrstah, glede na *predmet napada* in na *način storitve*. V prvo skupino spadajo *kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov*, posamične inkriminacije pa zajemajo protipraven dostop (sem spadajo predvsem vdori v sisteme, tako imenovani hacking), protipravno prestrezanje (prestrezanje tokov podatkov, prestrezanje elektronskih emisij itd.), motenje podatkov (na primer širjenje računalniških virusov in internetnih črvov), motenje sistemov (onemogočanje delovanja strežnikov, poplavljanje z velikim številom elektronskih sporočil – tako imenovani floading itd.) in zlorabo naprav (strojne in programske opreme, ki omogoča izvedbo prej naštetih dejanj). V drugi skupini najdemo dejanji, ki sta *povezani z računalniki* – to sta računalniško ponarejanje in računalniška goljufija, nanašata pa se seveda na digitalne podatke, vsebovane v računalniških

sistemih (s tem se dejanji, izvršeni v kibernetskem prostoru, razlikujeta od klasičnega ponarejanja in goljufije, ki se nanašata na fizičen, oprijemljiv svet). Tretja skupina vsebuje kaznivi dejanji, *povezani z vsebino digitalnega zapisa*. Sem spadajo kazniva dejanja, povezana z otroško pornografijo (na primer prikazovanje na svetovnem spletu) in kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic (prevladujoče v tej skupini je softversko piratstvo). V sklop materialnega dela so uvrščena tudi pravila za ugotavljanje odgovornosti udeležencev pri kaznivih dejanjih (poskus, pomoč, napeljevanje, odgovornost pravnih oseb) in kazenske sankcije.

V **kazensko procesnem delu** konvencija uvaja institut takojšnjega zavarovanja in shranitve računalniških podatkov in delno razkritje podatkov o prometu. Ker je kibernetski prostor izjemno dinamična kategorija, obstaja velika verjetnost, da bodo podatki v strežniških datotekah, ki se avtomatsko generirajo in opisujejo, kaj se je v sistemu dogajalo (kdo, kdaj, kako, od kod, kaj je počel…) izgubljeni še preden se bo pričela formalna preiskava, zato je ukrep zavarovanja podatkov, ki lahko vsebujejo dokaze o kriminalni aktivnosti, nujen in racionalen, izvesti pa ga morajo ponudniki omrežnih storitev ali skrbniki sistemov. Organi pregona jim lahko s tako imenovano *odredbo za pripravo* naložijo, da zavarovane podatke in podatke o uporabnikih storitev izročijo za namen kazenske preiskave. V nadaljnjih določbah najdemo še pravila, ki urejajo pogoje in način zasega shranjenih računalniških podatkov, zbiranje podatkov o prometu v dejanskem času (gre za tehnične podatke o telekomunikacijah, brez vpogleda v samo vsebino podatkov ali sporočil, postopek pa poteka sočasno s komunikacijo samo) in prestrezanje vsebinskih podatkov (v tem primeru preiskovalci dobijo neposreden in takojšen vpogled v vsebino posredovanih podatkov ali informacij).

V delu, ki se ukvarja s **sodno pristojnostjo**, najdemo pravila o izključni sodni pristojnosti (na lastnem ozemlju, ladji, letalu, ali nad svojim državljanom), o odstopu od izključne pristojnosti, pristojnosti v primeru, ko ni možna izročitev storilca, o prednosti nacionalnega prava pred mednarodnim in o posvetovalnem postopku v primeru multilateralne pristojnosti.

### *3. poglavje: Mednarodno sodelovanje*

Poleg splošnih načel, povezanih z mednarodnim sodelovanjem, vsebuje to poglavje še načela za izročitev storilcev, splošna načela, povezana z medsebojno pomočjo, ureja pošiljanje informacij brez zaprosila (samoiniciativno ravnanje še pred prejemom formalnega zaprosila), postopke v zvezi z zaprosili za medsebojno pomoč, kadar ni veljavnih mednarodnih pogodb in določbe o zaupnosti (vsi v preiskovanje vpleteni organi morajo ohraniti zaupnost podatkov) in omejeni uporabi (zgolj za postopke, navedene v zaprosilu). Konvencija ureja še pravila o medsebojni pomoči, kadar se izvajajo nujni začasni ukrepi (sem spadata takojšnje zavarovanje shranjenih računalniških podatkov in takojšnje razkritje zavarovanih podatkov o prometu) in o medsebojni pomoči pri izvajanju preiskovalnih pooblastil (pomoč pri dostopu do shranjenih računalniških podatkov, čezmejni dostop do shranjenih računalniških podatkov s soglasjem ali kadar so podatki javno dostopni, pomoč pri zbiranju podatkov o prometu v dejanskem času, pomoč pri prestrezanju vsebinskih podatkov). Kibernetski kriminal je globalen pojav, ki ne upošteva geografskih, političnih, jurisdikcijskih, kulturnih ali kakih drugih meja. Zaradi učinkov globalizacije so preiskave pogosto izjemno kompleksne, saj lahko zajemajo večje število držav, v katerih so bile bodisi izvršene posamezne sekvence protipravnega delovanja, ali pa so na njenem ozemlju nastale škodljive posledice. Takim razmeram se morajo prilagoditi tudi organi pregona, zato je mednarodno pravna ureditev te sfere na način, ki bo zagotavljal takojšen, hiter in učinkovit odziv, več kot nujna, k temu pa organe pregona nenazadnje zavezuje tudi določba konvencije, po kateri morajo podpisnice zagotoviti vključitev domačih organov pregona v mednarodno mrežo, ki se bo lahko v primeru incidenta nemudoma odzvala, saj mora vsak njen člen delovati 24 ur na dan in 7 dni v tednu.

### *4. poglavje: Končne določbe*

V tem poglavju so vsebovane tehnične določbe o postopku podpisovanja konvencije, začetku njene veljavnosti, postopku naknadnega pristopa h konvenciji, vsebuje pa še določila o (omejeni ali neomejeni) teritorialni uporabi konvencije, o njenih učinkih (glede na druge multilateralne in bilateralne mednarodne pogodbe), o izjavah glede dovoljenih posebnih modalitet (strožjih pogojih, pod katerimi bo podpisnica štela določeno ravnanje kot kaznivo), o zvezni klavzuli (za federalno urejene države, kot so na primer ZDA), uveljavljanju pridržkov, stanju in umiku pridržkov, postopku spreminjanja konvencije, reševanju sporov, posvetovanju pogodbenic, odpovedi in postopku uradnega obveščanja (o podpisih, ratifikacijah, sprejetjih, odobritvah, pristopih itd.).

## IV. PROTOKOL O RASIZMU IN KSENOFOBIJI

Zaradi nasprotovanja nekaterih držav, ki so sodelovale pri njeni pripravi, konvencija ne vsebuje določb o rasizmu in ksenofobiji v kibernetskem prostoru. Glavno nasprotovanje v tej zvezi so izrazile ZDA zaradi svoje tradicionalne ureditve svobode govora in izražanja. Ker je bilo pripravljavcem veliko do tega, da konvencijo podpišejo tudi ZDA, kot tehnološko in kibernetsko najbolj razvita država na

svetu, so pritiskom podlegli, problem pa rešili tako, da je Svet Evrope v letu 2001 formiral novo skupino strokovnjakov iz držav članic in opazovalk z nalogo, da pripravi Protokol o boju proti rasizmu in ksenofobiji na računalniških sistemih (PC-RX delovna skupina), ki bo smiselno dopolnil konvencijo. Skupina je svoje delo opravila in protokol je pripravljen za podpis, podpisala pa ga bo tudi Republika Slovenija.

## ZAKLJUČEK

S pojavom prvih osebnih računalnikov v zgodnjih osemdesetih letih, predvsem pa z njihovim povezovanjem v omrežja, ki so s pojavom interenta postala eno samo globalno omrežje, se je odprla tudi nova fronta boja proti kriminaliteti, ki se, kot še nikoli prej v tolikšni meri, razlikuje od sveta, ki so ga vajeni preiskovalci. Kriminalci so vstopili tudi v kiber prostor, v katerega smo, če to hočemo ali ne, vsaj posredno vključeni vsi, s tem pa smo vsi tudi potencialne žrtve. Čas je, da v ta svet bolj organizirano in učinkovito vstopijo tudi varuhi zakonitosti.

## VIRI


http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm

http://www2.gov.si/mid/mid.nsf/V/K165AC0770D1A9BF1C1256C53003B6D1C/$file/Konvencija_CyberCrime.pdf



**Andrej Rupnik** je državni podsekretar v Ministrstvu za notranje zadeve – Policiji, nekdanji vodja enote za računalniško kriminaliteto, sedaj pa vodi enoto za mednarodno sodelovanje.

Je univerzitetni diplomirani pravnik, sicer karierni policist, ki je v štiriindvajsetih letih opravljal vrsto različnih nalog v slovenski policiji, med ostalim pa je se izpopolnjeval tudi na ameriški FBI akedemiji. Strokovna pot ga je vodila od delovnega mesta uniformiranega policista na policijski postaji, kjer je začel svojo kariero, bil je predavatelj v policijski šoli, opravljal je različne naloge v kriminalistični policiji, v zadnjih letih pa dela na najbolj odgovornih vodstvenih mestih. Po prihodu v kriminalistično policijo je bil sprva zadolžen za razvoj kriminalističnega informacijskega sistema in kriminalistične analitike, v tem okviru pa je vodil ali sodeloval pri ključnih razvojnih projektih, obenem pa sodeloval v nekaterih najbolj odmevnih preiskavah. S pojavom kibernetskega kriminala je s sodelavci opravil prve, pionirske korake preiskovanja te vrste kaznivih dejanj. Sodeloval je na številnih mednarodnih seminarjih s področja računalniške kriminalitete in kriminalistične analitike, pogosto tudi kot predavatelj. Bil je slovenski predstavnik v zaključnem delu PC-CY pri Svetu Evrope, sodeloval pa je pri pripravi notranje pravnega postopka za pristop Republike Slovenije h konvenciji.