STRUČNI RAD (PROFESSIONAL PAPER)
UDK: 343.232(497.6):004
343.137(094.5)(497.6)

Mr Olivije Zimonja
Uprava kriminalističke policije, Ministarstvo unutrašnjih poslova Republike Srpske
e-mail: olivije.zimonja@mup.vladars.net

Mr Dragana Vujić
Uprava kriminalističke policije, Ministarstvo unutrašnjih poslova Republike Srpske

# IMPLEMENTACIJA PROCESNIH ODREDBI KONVENCIJE O KIBERNETIČKOM KRIMINALU U ZKP-u REPUBLIKE SRPSKE

*Apstrakt*

*Konvencija o kibernetičkom kriminalu potpisana je u Budimpešti 23. novembra 2001. godine i predstavlja oblik međunarodnog ugovora. Konvencija o kibernetičkom kriminalu spada u krug takozvanih okvirnih konvencija, što znači da njene odredbe nisu direktno primjenjive već je neophodno da svaka država nakon ratifikacije izvrši implementaciju ove konvencije u vlastito zakonodavstvo. Cilj ovog rada jeste da ukaže na stepen implementacije procesnih odredbi koje predlaže Konvencija o kibernetičkom kriminalu u Zakonu o krivičnom postupku Republike Srpske, te da se ukaže na načine njihove primjene a sve u cilju unapređenja postupaka koji se sprovode prilikom dokazivanja krivičnih djela kompjuterskog kriminala.*
*Ključne riječi: Konvencija, kibernetika, kompjuteski kriminalitet, implementacija.*

## 1. UVODNE NAPOMENE

Republika Srpska je na polju zaštite od kibernetičkog kriminaliteta načinila značajne korake usmjerene prevashodno ka izgradnji pravnog okvira (2011. godine usvojen Zakon o informacionoj bezbjednosti te odgovarajući podzakonski akti, različiti vidovi i oblici sajber kriminaliteta regulisani su u glavi XXXII Krivičnog zakonika Republike Srpske pod nazivom Krivična

djela protiv bezbjednosti kompjuterskih podataka), strateškog pristupa (Vlada Republike Srpske je oformila Radnu grupu zaduženu za izradu prijedloga strategije RS za borbu protiv sajber kriminaliteta, kao i Radnu grupu za izradu Strategije sajber bezbjednosti Republike Srpske. Usvajanje navedenih strategija predviđeno je Planom rada Vlade RS za 2017. godinu) te odgovarajućih operativnih mehanizama (u pogledu operativnih mehanizama, Republika Srpska ima Odjeljenje za visokotehnološki kriminalitet pri Upravi kriminalističke policije u MUP-u Republike Srpske dok Zakon o informacionoj bezbjednosti predviđa osnivanje CERT-a (Computer Emergency Response Team) kao posebne organizacione jedinice za djelovanje u hitnim slučajevima sa zadatkom koordinacije prevencije i zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema organa i drugih fizičkih i pravnih lica pri Agenciji za informaciono društvo Republike Srpske). Potpisivanjem Konvencije o kibernetičkom kriminalitetu od strane BiH 2006. godine, Republika Srpska je preuzela obaveze za krivična djela iz oblasti kibernetičkog kriminaliteta te izvršila djelimično usklađivanje normi krivičnog materijalnog i procesnog prava sa navedenom konvencijom. Iako su nacionalnim zakonodavstvom preciznije određena krivična djela koja čine sajber kriminalitet u smislu poglavlja XXXII Krivičnog zakonika Republike Srpske, ne treba izgubiti iz vida da značajan udio u strukturi krivičnih djela u ukupnom sajber kriminalitetu čine i klasična krivična djela počinjena uz pomoć kompjutera, odnosno, putem interneta. Tako je u nacionalnom zakonodavstvu pitanje seksualnog zlostavljanja djece putem interneta regulisano u poglavlju XV Krivičnog zakonika Republike Srpske pod naslovom „Krivična djela protiv polnog integriteta“ u okviru čega se ističu dva krivična djela i to iskorištavanje djece i maloljetnih lica za pornografiju i upoznavanje djece sa pornografijom.

Dakle, navedena djela ne spadaju u kompjuterski kriminalitet, već se radi o klasičnim krivičnim djelima koja su izvršena uz pomoć kompjutera, odnosno, intereneta, pa se zbog navedenog istražuju pod okriljem sajber krimialiteta. Sa sve većom digitalizacijom društva koja predstoji, uključujući i e-servise državne uprave i integrisane baze podataka građana, e-zdravstvo, povezivanje kritične infrastrukture i industrije i integrisane digitalne sisteme finansijskog sektora i banaka, rizici od sajber kriminaliteta postaju sve veći zbog čega je nezahvalno govoriti o bezbjednosti u sajber prostoru uopšte upravo zbog činjenice da kompjuterski kriminalitet karakteriše velika dinamika i izuzetna šarolikost pojavnih oblika, formi i vidova ispoljavanja te da štete koje sa sobom nosi mogu biti zaista ogromne.

## 2. KONVENCIJA O KIBERNETIČKOM KRIMINALU I NJENA IMPLEMENTACIJA U ZAKONODAVSTVU BOSNE I HERCEGOVINE

Konvencija o kibernetičkom kriminalu (Convention on Cybercrime) donesena je od strane Vijeća Evrope 2001. godine[2] i predstavlja oblik medjunarodnog ugovora kao važnog izvora međunarodnog prava kojim se uređuju međusobni odnosi između subjekata međunarodnog prava. Konvencija spada u krug takozvanih okvirnih konvencija što znači da njene odredbe nisu direktno primjenjive već ih svaka država potpisnica treba implementirati u svoje zakonodavstvo. Naziv konvencije je preveden kao Konvencija o kibernetičkom kriminalitetu, iako se u naučnoj i stručnoj literaruri mogu pročitati i mišljenja da je prevod neadekvatan iz razloga što riječ kibernetika, engl. cybernetics ne označava isto što i riječ cyber. Kibernetika se najčešće definiše kao sistemsko proučavanje komunikacije i upravljanje u organizacijama svih vrsta dok za termin cyber još ne postoji precizna definicija mada se u Rječniku stranih riječi navodi da se pojmom cyber označava sve što je vezano uz svijet prividne stvarnosti koji nastaje uz pomoć kompjutera (Vojković, Štambuk-Sunjić, 2006: 124).

Naime, termin „kibernetički“ kriminalitet je širi pojam od pojma „kompjuterski“ kriminalitet te se na ovaj način konvencijom obuhvataju problemi vezani za prenos informacija i podataka preko informacionih i telekomunikacionih sistema. Upravo zato, smatra se da je i opravdan naziv Konvencija o kibernetičkom a ne kompjuterskom kriminalitetu. Naime, sve brže integrisanje informatičke i telekomunikacione tehnologije i njihova međusobna povezanost dovode i do povezanosti njihove zloupotrebe, te samim tim termin „kompjuterski“ postaje preuzak i zamjenjuje se terminom „kibernetički“. Iako je termin „kibernetički“ opšteprihvaćen, zakonodavstva u BiH ne koriste navedeni termin niti samim tim određuje definiciju istog. Bosna i Hercegovina je 2006. godine ratifikovala[3] Konvenciju o kibernetičkom kriminalu[4] („Službeni glasnik BiH – Međunarodni ugovori“, br. 6/06) kao i Dodatni protokol Konvenciji o kibernetičkom kriminalu, a u vezi s kažnjavanjem djela rasističke i ksenofobske prirode počinjenih putem računarskih sistema (Službeni glasnik BiH – Međunarodni ugovori“, br. 6/06) 2006. godine.

Važnost Konvencije o kibernetičkom kriminalu ogleda se upravo u obavezama država potpisnica da stvore normativne pretpostavke za uvođenje dodatnih procedura i ovlaštenja, kako bi se omogućilo efikasno otkrivanje

2 Stupila je na snagu 2004. godine.

3 Pristanak države da bude vezana međunarodnim ugovorom može se izraziti na različite načina kao što su potpisivanje, ratifikacija, odobrenje, prihvatanje ili na način kako se države potpisnice dogovore. Po pravilu, najveći broj međunarodnih ugovora prolazi kroz faze potpisivanja i ratifikacije gdje potpisivanje predstavlja fazu koja slijedi nakon obavljenih pregovora i donošenja konačnog teksta ugovora dok ratifikacia, shodno naučnom tumačenju predstavlja konačan pristanak države da bude vezana ugovorom.

4 Strukturalno gledano, Konvencija o kibernetičkom kriminalu, pored preambule sadrži četiri osnovna dijela i to određenje osnovnih pojmova; mjera koje države potpisnice treba da preduzmu na nacionalnim nivoima a koje su razvrstane kroz dvije ključne oblasti i to kroz krivično materijalno pravo i procesno pravo; opštih načela, postupaka i mjera međunarodne saradnje te završnih odredbi.

i procesuiranje slučajeva kompjuterskog kriminala (Selimović, 2015).

Kada je u pitanju implementacija Konvencije u krivične zakone u BiH, treba napomenuti da se u Bosni i Hercegovini primjenjuju četiri krivična zakona s obzirom na podijeljenu nadležnost u propisivanju krivičnih djela između države i entiteta. Krivični zakon Bosne i Hercegovine („Službeni glasnik BiH“, br. 3/03, 32/03, 37/03, 54/04, 61/04, 30/05, 53/06, 55/06, 32/07, 8/10, 47/14, 22/15, 40/15) sadrži krivična djela kojima se štite vrijednosti čija zaštita je u isključivoj nadležnosti države, dok su u krivičnim zakonima entiteta i Brčko distrikta propisana sva ostala krivična djela uključujući i krivična djela iz domena kibernetičkog kriminala. U BiH izvršena je djelimična implementacija krivičnih djela predviđenih Konvencijom, tj. krivičnih djela iz domena kibernetičkog kriminala i to u oblasti krivično materijalnog prava u predmetnim krivičnim zakonima što je prikazano u Tabeli br. 1.

Tabela br. 1. Implementacija krivičnih djela predviđenih Konvencijom (krivično materijalno pravo)[5].

| ***Odredbe Konvencije*** | ***KZ FBIH*** | ***KZ RS*** | ***KZ BD*** |
|---|---|---|---|
| **Član 2 – Nedozvoljeni pristup** | Član 397 | Član 411. | Član 391 |
| **Član 3 – Nezakonito presretanje** | Član 393 stav (2) | Član 411. | Član 387 stav (2) |
| **Član 4 – Povreda integriteta podataka** | Član 393 stav (1) | Član 407. | Član 387 stav (1) |
| **Član 5 – Povreda integriteta sistema** | Član 396 | Član 413. | Član 390 |
| **Član 6 – Zloupotreba uređaja** | Član 393 stav (5) i (6) | Član 409. | Član 387 stav (4) i (5) |
| **Član 7 – Kompjutersko falsifikovanje** | Član 394 stav (1) | Član 408. | Član 388 stav (1) |
| **Član 8 – Kompjuterska prevara** | Član 395 | Član 410. | Član 389 |
| **Član 9 – Krivična djela koja se odnose na dječiju pornografiju** | Član 211 | Članovi 175., 176., 177. i 178. | Član 186 stav (3), 208 i 209 |

5 Legenda: BD (Brčko distrikt), FBIH (Federacija Bosne i Hercegovine), KZ (Krivični zakon), RS (Republika Srpska).

| | | | |
|---|---|---|---|
| **Član 10 – Krivična djela u vezi sa napadom na intelektualnu svojinu i odnosna prava** | - | - | Član 256 i 257 |
| **Član 11 – Pokušaj i saučesništvo** | Član 28 i 31 | Član 37., 38. i 39. | - |
| **Član 12 – Odgovornost pravnih lica** | Glava 14 | Glava X | - |
| **Član 13 – Sankcije i mjere** | - | - | - |

Takođe, Zakoni o krivičnom postupku, kojih je u BiH četiri, kao i krivični zakoni, donekle su usklađeni sa krivično procesnim odredbama iz Konvencije što je prikazano u Tabeli br.2.

Tabela br. 2. Implementacija krivičnih djela predviđenih Konvencijom (procesno pravo)

| Odredbe Konvencije | ZKP BIH | ZKP FBIH | ZKP RS |
|---|---|---|---|
| **Član 16 – Brza zaštita pohranjenih kompjuterskih podataka** | - | - | - |
| **Član 17 – Zaštita i brza distribucija podataka u vezi prometa** | - | - | - |
| **Član 18 – Nalog za dostavu podataka** | Član 72a | Član 86a | Član 129 i Član 137 |
| **Član 19 – Pretraživanje i pljenidba pohranjenih kompjuterskih podataka** | - | Član 65 | Član 115 |
| **Član 20 – Prikupljanje u realnom vremenu podataka u vezi sa prometom** | Član 65 stav (6) | Član 130 | - |
| **Član 21 – Presretanje podataka u vezi sa sadržajem*** | Član 116 | Član 130 | Glava 17 |

* Zakonito presretanje u Bosni i Hercegovini je regulisano Odlukom Savjeta ministara Bosne i Hercegovine o posebnim obavezama pravnih i fizičkih osoba koje pružaju telekomunikacijske usluge, administriraju telekomunikacijske mreže i vrše telekomunikacijske djelatnosti, u pogledu osiguranja i održavanja kapaciteta koji će omogućiti ovlaštenim agencijama da vrše zakonito presretanje telekomunikacija, kao i kapaciteta za čuvanje i osiguravanje telekomunikacijskih podataka („Službeni glasnik BiH“, br. 104/06).

U Tabelama broj 1 i 2 je korišćena metodologija i sistematika Saveta Evrope u okviru IPA SEE (Octopus Cybercrime Community) o implementaciji odredaba Konvencije o kibernetičkom kriminalu u nacionalno zakonodavstvo Bosne i Hercegovine.

Kada je u pitanju implementacija odredbi međunarodne saradnje propisanih Konvencijom, ista se vrši u skladu sa pozitivnim pravnim propisima implementiranim kroz nadležne zakone o krivičnim postupcima u Bosni i Hercegovini i drugim relevantnim zakonima u Bosni i Hercegovini, te se koriste instrumenti saradnje sa drugim međunarodnim subjektima putem zvaničnih kanala INTERPOL-a, EUROPOL-a, instituta međunarodne pravne pomoći i specijalnih direktnih veza koje odgovarajuće institucije u Bosni i Hercegovini imaju pravo da ostvaruju kroz potpisivanje sporazuma o saradnji. U dijelu koji se odnosi na međunarodnu saradnju, odnosno, mogućnosti razmjene informacija i dokaza kroz mehanizme konvencije, osvrnućemo se samo na jedan od najznačajnijih mehanizama konvencije iz ovog dijela, a to je komunikacija putem kontakt tačke "24/7" te na činjenicu kako je ovo pitanje riješeno u BiH.

Naime, Ministarstvo unutrašnjih poslova Republike Srpske (u daljnjem tekstu: MUP RS) veoma često prikuplja i razmjenjuje elektronske dokaze, ali u svom radu ne koristi mehanizam kontakt tačke 24/7 s obzirom na to da je kontakt tačka smještena u Direkciju za koordinaciju policijskih tijela BiH a MUP RS i Direkcija instutucionalno nemaju uređene procedure razmjene informacija po principima budimpeštanske konvencije. MUP Republike Srpske prikuplja i razmjenjuje elektronske dokaze kroz direktnu korespondenciju kako sa domaćim tako i sa stranim servis provajderima, te sa domaćim i stranim institucijama za sprovođenje zakona MUP RS ima veoma pozitivna iskustva. Intencije su da MUP Republike Srpske u budućnosti ima vlastitu kontakt tačku 24/7 za budimpeštansku konvenciju iz razloga što postoje opravdana mišljenja da je potrebno da kontakt tačka bude stručno osposobljeno, ovlašteno službeno lice koje posjeduje adekvatan nivo pravne, tehničke i kriminalističke obučenosti za sajber kriminalitet. Takođe, intencija je da kontakt tačka 24/7 treba da bude smještena u jedinicu koja se bavi sajber kriminalitetom s obzirom na to da je potrebno da osobe koje su određene kao kontakt tačke treba da poznaju pravila i procedure i načine prikupljanja, čuvanja, distribucije i rukovanja sa elektronskim dokazima iz razloga što su su elektronski dokazi veoma osjetljivi te da se nestručnim rukovanjem veoma lako mogu unuštiti, te da često zbog nestručnosti dolazi do gubitka vremena u prikupljanju podataka i prikupljanja pogrešnih podataka.

Prethodno navedeno ima svoje utemeljenje u sljedećim odredbama Konvencije:

- Član 27 u tački a) precizira da će svaka strana odrediti jedan ili više centralnih organa nadležnih za slanje i odgovore na zahtjeve za uzajamnom

pomoći, za izvršavanje tih zahtjeva ili njihovo prosleđivanje organima nadležnim za njihovo izvršavanje. Predmetnim je ostavljena mogućnost formiranja više kontakt tačaka u jednoj zemlji.
- Član 28 - tajnost i ograničenje korištenja.
- Član 29 - Hitna zaštita pohranjenih kompjuterskih podataka.
- Član 35 - Mreža 24/7 gdje se između ostalog navodi da je uloga kontakt tačke davanje tehničkih savjeta, zaštita podataka u skladu sa članovima 29. i 30. te prikupljanje dokaza, davanje pravnih informacija i lociranje osumnjičenih što je isključivo domen rada i nadležnost specijalizovanih jedinica za sajber kriminalitet.

U nadležnim policijskim agencijama na entitetskom nivou, tj. Federalna uprava policije i Ministarstvo unutrašnjih poslova Republike Srpske, uspostavljene su specijalizirane jedinice za borbu protiv kibernetičkog kriminala, koje se bave krivičnim djelima u visokotehnološkom, tj. kompjuterskom okruženju i te obavljaju digitalnu forenziku. Digitalna forenzika računara i mobilnih telefona se osim u navedenim institucijama obavlja i u Državnoj agenciji za istrage i zaštitu, Graničnoj policiji Bosne i Hercegovine, Agenciji za forenzička ispitivanja i vještačenja, i Policiji Brčko Distrikta.

## 3. IMPLEMENTACIJA PROCESNIH ODREDBI KONVENCIJE O KIBERNETIČKOM KRIMINALU U ZKP-u REPUBLIKE SRPSKE

Konvencija o kibernetičkom kriminalu u Odjeljku 2, pod nazivom „Procesno pravo“, predlaže ovlaštenja i procedure koje države potpisnice konvencije trebaju usvojiti u cilju provođenja posebnih istraga ili krivičnih procesa za krivična djela predviđena konvencijom, odnosno kompjuterska krivična djela, ali i na sva druga krivična djela počinjena kompjuterskim sistemom i na prikupljanje elektronskih dokaza kod svih ostalih krivičnih djela (Selimović, 2015).

Konvencija takođe predviđa da svaka država potpisnica treba da vodi računa o tome da uvođenje, pokretanje i primjena ovlaštenja i procesa predviđenih u ovom odjeljku budu podvrgnuti predviđenim uslovima i zaštitama u internom pravu svake države potpisnice, koji treba da osiguraju adekvatnu zaštitu prava i sloboda čovjeka, a naročito prava utvrđenih shodno obavezama koje je ta strana potpisala u primjeni Konvencije o zaštiti osnovnih ljudskih prava i sloboda Vijeća Evrope (1950) i Međunarodnog pakta u vezi građanskih i političkih prava Ujedinjenih naroda (1966) ili drugih međunarodnih instrumenata koji se primjenjuju na prava čovjeka a koji moraju integrisati princip proporcionalnosti.[6] Mjere, odnosno ovlaštenja i procedure, koje predviđa konvencija su: brza zaštita pohranjenih kompjuterskih podataka, zaštita i brza distribucija

6 Konvencija o kibernetičkom kriminalu (Službeni glasnik BiH – Međunarodni ugovori, br. 6/06).

podataka u vezi sa prometom, nalog za dostavu podataka, pretraživanje i pljenidba pohranjenih kompjuterskih podataka, prikupljanje u realnom vremenu podataka o prometu i presretanje podataka u vezi sa sadržajem. U Tabeli br. 3 prikazane su mjere, odnosno, ovlašćenja i procedure koje predviđa Konvencija o kibernetičkom kriminalu i njihova implementacija u ZKP RS.

Tabela br.3. Mjere, odnosno, ovlaštenja i procedure koje predviđa Konvencija o kibernetičkom kriminalu i njihova implementacija u ZKP RS.

| ***Odredbe Konvencije*** | ***ZKP RS*** |
|---|---|
| Član 16 – Brza zaštita pohranjenih kompjuterskih podataka<br>1. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi njeni nadležni organi mogli naložiti, ili na drugi način postići, hitnu zaštitu određenih kompjuterskih podataka, uključujući i podatke o prometu, koji su pohranjeni pomoću kompjuterskog sistema, a naročito onda kada postoje razlozi da se smatra da su ti kompjuterski podaci naročito podložni gubitku ili mijenjanju.<br>2. Kada strana provodi zaštitu iz stava 1. ovog člana izdavanjem naloga nekoj osobi da zaštiti odreñene pohranjene kompjuterske podatke koji se nalaze u njenom posjedu ili pod njenim nadzorom, ta strana će usvojiti zakonske i druge mjere potrebne da se ta osoba obaveže da će te kompjuterske podatke zaštititi i sačuvati njihovu cjelovitost u periodu koliko je to potrebno, a najviše 90 dana, kako bi se nadležnim organima omogućilo da traže njihovo otkrivanje. Strana može predvidjeti mogućnost kasnijeg obnavljanja takvog naloga.<br>3. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi se obavezao skrbnik ili druga osoba koja treba čuvati kompjuterske podatke da drži u tajnosti poduzimanje takvih postupaka tokom vremenskog perioda koji je predviñen domaćim pravom strane.<br>4. Ovlaštenja i postupci navedeni u ovom članu bit će u skladu sa članovima 14. i 15. | |

| | |
|---|---|
| Član 17 – Zaštita i brza distribucija podataka u vezi prometa<br>1. Svaka strana će, u pogledu podataka o prometu koje je potrebno zaštititi prema članu 16., usvojiti zakonske i druge mjere potrebne kako bi se osiguralo: a) da takva hitna zaštita podataka o prometu bude moguća bez obzira da li je u prenos te komunikacije bio uključen jedan ili više pružalaca usluga; b) hitno otkrivanje nadležnom organu strane ili osobi koju taj organ odredi, dovoljne količine podataka o prometu kako bi se mogli identificirati pružaoci usluga i put kojim je komunikacija prenesena. 10<br>2. Ovlaštenja i postupci navedeni u ovom članu bit će u skladu sa članovima 14. i 15. | |

| | |
|---|---|
| Član 18 – Nalog za dostavu podataka<br>1. Svaka strana će usvojiti zakonske i druge mjere su potrebne kako bi njeni nadležni organi bili ovlaštena da nalože: a) osobi koja se nalazi na njenoj teritoriji da dostavi odreñene kompjuterske podatke, koji su u posjedu ili pod nadzorom te osobe i koji su pohranjeni u kompjuterskom sistemu ili na mediju za pohranjivanje kompjuterskih podataka; i b) pružaocu usluga koji nudi svoje usluge na teritoriji strane da dostavi podatke o pretplatnicima koji se odnose na te usluge, a koje ima u posjedu ili pod nadzorom;<br>2. Ovlaštenja i postupci navedeni u ovom članu bit će u skladu sa članovima 14 i 15.<br>3. U smislu ovog člana, izraz „podaci o pretplatnicima“ označava sve informacije u obliku kompjuterskih podataka ili u bilo kojem drugom obliku, koje ima pružalac usluga, a koje se tiču pretplatnika na njegove usluge, osim podataka o prometu ili sadržaju, putem kojih se može utvrditi: a) vrsta komunikacijske usluge koja je korištena, tehničke mjere koje su poduzete i period pružanja usluge; b) identitet, poštanska ili geografska adresa i broj telefona pretplatnika, kao i svaki drugi pristupni broj, te podaci u vezi fakturisanja i plaćanja, koji su raspoloživi na osnovu ugovora ili sporazuma o pružanju usluga; c) sve druge informacije o mjestu gdje je komunikacijska oprema instalirana, koje su raspoloživa na osnovu ugovora ili sporazuma o pružanju usluga. | Naredba za oduzimanje predmeta (Član 129)<br><br>1) Predmeti koji se po Krivičnom zakoniku treba da oduzmu ili koji mogu poslužiti kao dokaz u krivičnom postupku privremeno će se oduzeti i na osnovu sudske odluke će se obezbijediti njihovo čuvanje.<br>(2) Naredbu za oduzimanje predmeta izdaje sudija na prijedlog tužioca ili ovlašćenog službenog lica koje je dobilo odobrenje od tužioca.<br>(3) Naredba za privremeno oduzimanje predmeta sadrži: naziv suda, pravni osnov za privremeno oduzimanje predmeta, naznaku predmeta za oduzimanje, ime lica od kojeg se oduzimaju predmeti, mjesto oduzimanja predmeta i rok za oduzimanje predmeta.<br>(4) Na osnovu izdate naredbe ovlašćeno službeno lice vrši oduzimanje predmeta.<br>(5) Ko drži takve predmete dužan je da ih preda po naredbi suda. Lice koje odbije da ih preda može se kazniti do 50.000 KM, a u slučaju daljeg odbijanja - može se zatvoriti. Zatvor traje do predaje predmeta ili do završetka krivičnog postupka, a najduže 90 dana. Na isti način postupiće se prema službenom ili odgovornom licu u državnom organu ili pravnom licu.<br>(6) Odredbe stava 5. ovog člana odnose se i na podatke pohranjene u kompjuteru ili sličnim uređajima za automatsku obradu podataka. Pri njihovom pribavljanju posebno će se brinuti o propisima koji se odnose na čuvanje tajnosti određenih podataka.<br>(7) O žalbi protiv rješenja kojim je izrečena novčana kazna ili je određen zatvor odlučuje vijeće iz člana 24. stav 5. Žalba ne zadržava izvršenje rješenja.<br>(8) Pri oduzimanju predmeta naznačiće se gdje su pronađeni i opisaće se, a po potrebi i na drugi način obezbijediće utvrđivanje njihove istovjetnosti. Za oduzete predmete izdaće se potvrda.<br>(9) Mjere iz stava 5. ovog člana ne mogu se primijeniti prema osumnjičenom, odnosno optuženom niti licima koja su oslobođena dužnosti svjedočenja.<br><br>Naredba opereteru telekomunikacija (Član 137) |

| | |
|---|---|
| Član 19 – Pretraživanje i pljenidba pohranjenih kompjuterskih podataka<br>1. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi njeni nadležni organi bili ovlašteni da izvrše pretresanje ili na sličan način imali pristup:<br>a) kompjuterskom sistemu ili njegovom dijelu, kao i kompjuterskim podacima koji su u njemu pohranjeni i b) mediju za pohranjivanje kompjuterskih podataka u kojem kompjuterski podaci mogu biti pohranjeni na njenoj teritoriji.<br>2. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi se osiguralo da, u slučajevima kada njeni organi pretresaju ili na sličan način pristupaju određenom kompjuterskom sistemu ili njegovom dijelu, u skladu sa stavom 1.a), a imaju razloga da smatraju da su traženi podaci pohranjeni u drugom kompjuterskom sistemu ili njegovom dijelu na njenoj teritoriji, i da se tim podacima može zakonito pristupiti iz prvog sistema ili su njemu dostupni, navedeni organi budu u mogućnosti da hitno prošire pretresanje ili slično pristupanje i tom drugom sistemu.<br>3. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi ovlastila svoje nadležne organe da oduzmu ili na sličan način osiguraju kompjuterske podatke kojima je pristupljeno u skladu s odredbama stavova 1. ili 2. Te mjere će uključivati davanje ovlaštenja organima da: a) oduzmu ili na sličan način osiguraju kompjuterski sistem, njegov dio ili medij za pohranjivanje kompjuterskih podataka; b) izrade i zadrže kopiju tih kompjuterskih podataka; c) održe cjelovitost relevantnih pohranjenih kompjuterskih podataka i d) učine nedostupnim ili uklone te kompjuterske podatke iz kompjuterskog sistema u koji je ostvaren pristup.<br>4. Svaka strana će usvojiti zakonske i druge mjere potrebne kako bi ovlastila svoje nadležne organe da narede svakoj osobi koja ima saznanja o funkcioniranju kompjuterskog sistema ili o mjerama koje su primijenjene radi zaštite kompjuterskih podataka u njemu da pruži informacije koje su razumno potrebne kako bi se omogućilo poduzimanje mjera navedenih u stavovima 1. i 2.<br>5. Ovlaštenja i postupci navedeni u ovom članu bit će u skladu sa članovima 14. i 15. | (1) Ako postoje osnovi sumnje da je neko lice počinilo krivično djelo, sud može na osnovu prijedloga tužioca ili na prijedlog ovlašćenih službenih lica koja su dobila odobrenje od tužioca narediti da operater telekomunikacija ili drugo pravno lice koje vrši pružanje telekomunikacionih usluga dostavi podatke o korišćenju telekomunikacionih usluga tog lica, ako bi takvi podaci mogli da budu dokaz u krivičnom postupku ili da posluže za prikupljanje informacija koje mogu da budu od koristi u krivičnom postupku.<br>(2) U hitnim slučajevima tužilac može da naredi radnje iz stava 1. ovog člana i dobijeni podaci će se zapečatiti dok ne bude izdata sudska naredba. O preduzetim mjerama tužilac odmah obavještava sudiju za prethodni postupak, koji može u roku od 72 časa izdati naredbu. U slučaju da sudija za prethodni postupak ne izda naredbu, tužilac će podatke vratiti bez prethodnog otvaranja.<br>(3) Radnje iz stava 1. ovog člana mogu se odrediti i prema licu za koje postoje osnovi sumnje da učiniocu, odnosno od učinioca prenosi informacije u vezi sa krivičnim djelom, odnosno da učinilac koristi njegovo sredstvo telekomunikacije.<br>(4) Operateri telekomunikacija ili druga pravna lica koji pružaju telekomunikacione usluge dužni su da tužiocu i policijskim organima omoguće sprovođenje mjera iz stava 1. ovog člana.<br>Pretresanje stana, ostalih prostorija i pokretnih stvari (Član 115)<br><br>(1) Pretresanje stana i ostalih prostorija osumnjičenog, odnosno optuženog i drugih lica, kao i njihovih pokretnih stvari van stana može se preduzeti samo onda ako ima dovoljno osnova za sumnju da se kod njih nalaze učinilac, saučesnik, tragovi krivičnog djela ili predmeti važni za postupak.<br>(2) Pretresanje pokretnih stvari u smislu odredbe stava 1. ovog člana obuhvata i pretresanje kompjuterskih sistema, uređaja za pohranjivanje kompjuterskih i elektronskih podataka, kao i mobilnih telefonskih aparata. Lica koja se koriste ovim uređajima dužna su da omoguće pristup, predaju medij na kome su pohranjeni podaci, te pruže potrebna obavještenja za upotrebu tih uređaja. Lice koje odbije njihovu predaju može se kazniti prema odredbi člana 129. stav 5. ovog zakona.<br>(3) Pretresanje kompjutera i sličnih uređaja iz stava 2. ovog člana će se obaviti uz pomoć stručnog lica. |

| | |
|---|---|
| Član 20 – Prikupljanje u realnom vremenu podataka u vezi prometa | - |
| Član 21 – Presretanje podataka u vezi sadržaja* | Posebne istražne radnje (Član 234. stav 2)<br>a) nadzor i tehničko snimanje telekomunikacija,<br>b) pristup kompjuterskim sistemima i kompjutersko sravnjenje podataka,<br>v) nadzor i tehničko snimanje prostorija,<br>g) tajno praćenje i tehničko snimanje lica, transportnih sredstava i predmeta koji su u vezi sa njima,<br>d) korišćenje prikrivenih istražilaca i korišćenje informatora,<br>đ) simulovani i kontrolisani otkup predmeta i simulovano davanje potkupnine i<br>e) nadzirani prevoz i isporuka predmeta. |

* Zakonito presretanje u Bosni i Hercegovini je regulisano Odlukom Savjeta ministara Bosne i Hercegovine o posebnim obavezama pravnih i fizičkih osoba koje pružaju telekomunikacijske usluge, administriraju telekomunikacijske mreže i vrše telekomunikacijske djelatnosti, u pogledu osiguranja i održavanja kapaciteta koji će omogućiti ovlaštenim agencijama da vrše zakonito presretanje telekomunikacija, kao i kapaciteta za čuvanje i osiguravanje telekomunikacijskih podataka („Službeni glasnik BiH“, br. 104/06).

Iz predočenog tabelarnog prikaza je vidljivo da zakonodavac nije u potpunosti implementirao predložene mjere i ovlaštewa Konvencije o kibernetičkom kriminalitetu, te da postojeća zakonska rješenja pružaju solidnu osnovu za suprotstavljanje ovom vidu kriminaliteta.

U prilog navedenom izdvajamo sljedeće:

- Mjere odnosno ovlaštenja i procedure predviđene Konvencijiom su sljedeće: 1) brza zaštita pohranjenih kompjuterskih podataka; 2) zaštita i brza distribucija podataka u vezi prometa; 3) nalog za dostavu podataka; 4) pretraživanje i pljenidba pohranjenih kompjuterskih podataka; 5) prikupljanje u realnom vremenu podataka o prometu i 6) presretanje podataka u vezi sadržaja.
- Od ukupno šest mjera odnosno ovlašćenja, u krivičnoprocesnom zakonodavstvu Republike srpske samo tri ovlašćenja su implementirana kroz odredbe ZKP RS i to: 1. nalog za dostavu podataka (Implementacijom ove mjere države potpisnice konvencije bi omogućile svojim organima da izdaju naredbe svim osobama za dostavu posebnih (određenih) kompjuterskih podatak, koje posjeduju ili su pod njihovom kontrolom i svim davaocima usluga za dostavu podataka o pretplatnicima na njihove usluge, a koje podatke posjeduju ili nad kojima imaju kontrolu. U tabeli je predočeno da navedena mjera odgovara radnji dokazivanja propisanoj u ZKP RS koja nosi naziv Privremeno oduzimanje predmeta te u okviru iste posebno izdvojeno Naredba operateru telekomunikacija, koja se teorijeski svrstava u posebne slučajeve privremenog oduzimanja predmeta. Deskripcija zakonodavnih rješenja vezanih za navedenu radnju dokazivanja

predočena je u tabeli. Ovdje je važno istaći da bi se ova radnja dokazivanja mogla podrobnije regulisati kako bi se izbjegle greške kod zumačenje iste, i to u smislu da je zakonodavac u zakonsku normu trebao dodati da se pod predmetima podrezumijevaju i podaci koji su pohranjeni u kompjuterima i sa njima povezanim uređajima i drugim meijima koji služe za pohranjivanje podataka. Kroz poseban slučaj privremenog oduzimanja predmeta Naredbu operateru telekomunikacija zakonodavac je u potpunosti implementirao odrebu Konvencija - svim davaocima usluga za dostavu podataka o pretplatnicima na njihove usluge, a koje podatke posjeduju ili nad kojima imaju kontrolu). 2. pretraživanje i pljenidba pohranjenih kompjuterskih podataka ( Ovom mjerom se daju ovlašćenja nadležnim organima za pretres i pljenidbu kompjuterskih sistema ili nekog od njegovih dijelova, kompjuterskih podataka pohranjenih u kompjuterskom sistemu, uređaju ili drugom mediju, kao i ovlašćenje da navedeni mogu, ukoliko rapsolažu osnovanom sumnjom da su traženi podaci pohranjeni u drugom kompjuterskom sistemu mogu hitno produžiti pretres i na taj drugi kompjutreski sistem (ovdje se radi o mrežnom pretraživanju sistema). Pored pretresanja ova mjera se odnosi i na zapljenu ili neki drugi sličan način osiguranje kompjuterskih sistema i njihovih podataka, kao i ovlaštenje da nadležni organi prilikom preduzimanje ove mjere mogu narediti svakom licu koje poznaje funkcionisanje kompjutreskog sistema ili mjerama vezanim za zaštitu kompjuterskih podataka, da pruži informacije nadležnim organima o istom. Prethodno navedeno implementirano je u krivičnoprocesno zakonodavstvo RS u vidu radnje dokazivanja Pretresanje stana, ostalih prostorija i lica. U pogledu navedene mjere, zakonodavac nije u potpunosti implementira sva ovlašćenja koja predviđa ova mjera i to: nije predvidio mogućnost da se pretres može produžiti na povezani kompjuterski sistem, načine i zadržavanje kopije kompjuterskih podataka kao i mogućnost da se učine nepristupačnim ili odstrane kompjuterske podatke iz kompjuterskog sistema kome je pristupljeno). 3. presretanje podataka u vezi sadržaja (S obzirom da se ovom mjerom vrši, na način kako je to definisano Konvencije, uvid u sam sadržaj određene komunikacije, čime se ovom mjerom zadira u osnovna ljudska prava i slobode, gdje se prevashodno misli na pravo na privatnost i poštovanje privatnog života, ova mjera je, upravo zbog toga limitirana samo za određena, teška krivična djela. Poštujući navedeno, Konvencija ovom mjerom daje mogućnost nadležnim organima da prikupljaju ili snimaju tehničkim sredstvima podatke u vezi sadržaja, prenesenog kompjuterskim sistemom u vezi određene komunikacije na svom području, pri čemu ovu mjeru mogu izvršiti nadležni organi sami ukoliko posjeduju odgovarajuću tehniku, može biti naložena davaocu usluga da je on izvrši ili jednostavno da sarađuje i pruži pomoć nadležnim organima u realizaciji iste. U krivičnoprocesnom zakonodavstvu Republike Srpske je navedena mjera u potpunosti implementirana u Glav XVII Posebne istražne radnje.
- Komparativni pokazatelji zakonodavnih rješenja na nivou Republike

Srpske, Federacije BiH kao i Brčko Distrikta BiH pokazuju da je situacija u pogledu implementacije mjera odnosno ovlašćenja predviđenih Konvencijom identična u sva tri krivično procesna zakonodavstva.
- U zakonodavnim rješenjima na nivou Republike Srpske, Federacije BiH kao i Brčko Distrikta BiH ne mogu se naći ovlaštenja i procedure koje odgovaraju trima mjerama i to: brza zaštita pohranjenih kompjuterskih podataka; zaštita i brza distribucija podataka u vezi prometa; prikupljanje u realnom vremenu podataka o prometu.

## 4. ZAKLJUČAK

S obzirom na činjenicu da je sajber prostor dio svakodnevice današnjeg društva kroz komunikacije, poslovanje, trgovinu, obrazovanje, kulturu, zdravstvo, diplomatiju, sistem bezbjednosti, kritičnu infrastrukturu, saobraćaj, ali i zabavu i društvenu interakciju, tako je i sajber kriminalitet sve češće dio svakodnevnog iskustva kako građana tako i institucija. Takođe, činjenica je da je sajber kriminal posljednjih godina u porastu i da za posljedicu ima kako velike finansijske gubitke tako i uništavanja imovine i gubitke života te je upravo zbog toga potrebno stalno praćenje promjena u ovoj oblasti. Ratifikacija Konvencije o kibernetičkom kriminalu u BiH predstavlja značajan korak u suprotstavljanju ovom obliku kriminaliteta. Međutim, zakonodavstvo u BiH je izvršilo djelimičnu implementaciju odredbi ove konvencija u svoje interne zakonske propise gdje se misli kako na odredbe krivičnog materijalnog prava, tako i na odredbe procesnog prava i međunarodne saradnje. Naučna i stručna javnost u BiH koja je upoznata sa odredbama konvencija te koja u svom radu ima dodira sa kompjuterskim kriminalitetom, ističe da se pažnja zakonodavaca uglavnom fokusira na odredbe materijalnog prava te njihovu uskladjenost sa odredbama konvencije, nego na ostale odredbe.

Analiza implementacije procesnih odredbi Konvencije o kibernetičkom kriminalu u ZKP-u Republike Srpske pokazala je da postojeća zakonska rješenja pružaju neophodnu osnovu za suprotstavljanje ovom vidu kriminaliteta iako zakonodavac u potpunosti ne implementira predložene odredbe i ovlašćenja iz ove oblasti. Iz predočene tabele u kojoj je prikazana usklađenost odredbi procesnog dijela između Konvencije i ZKP RS, vidljivo je da organi zaduženi za suprostavljanje ovom vidu kriminaliteta imaju na raspolaganju mjere i ovlašćenja koja omogućavaju npr. oduzimanje kompjuterskih podataka koji obuhvataju i podatke o pretplatnicima na telekomunikacijske usluge, pretres i oduzimanje kompjutera i uređaja za pohranjivanje i kompjuterskih i elektronskih podataka, izvrše presretanje podataka u vezi sa sadržajem i sl. a koja se realizuju kroz radnje dokazivanja i posebne istražne radnje.

U cilju potpunije implementacije odredaba konvencije u nacionalno zakonodavstvo a istovremeno imajući u vidu i efikasnije suprotstavljanje ovom

vidu kriminaliteta, smatramo da je potrebno izvršiti izmjene i dopune postojećeg ZKP RS te u isti uvrstiti ovlaštenja koja trenutno ne sadrži krivičnoprocesno zakonodavstvo a koja su predviđena konvencijom kao i da je potrebno mjere i ovlašćenja koja su predviđena i uslađena sa konvencijom dodatno razraditi i proširiti jer su ista djelimično usklađena sa odredbama koje propisuje konvencija.

## 5. LITERATURA

1. Selimović, M. (2015). Implementacija procesnih odredbi Konvencije o kibernetičkom kriminalu u Zakonu o krivičnom postupku Federacije BiH, Časopis za kriminalistiku, kriminologiju i sigurnosne studije Godište XV, Broj 1-2, Univerzitet u Sarajevu.
2. Sijerčić-Čolić, H., Hadžiomeragić, M., Jurčević, M., Kaurinović, D. i Simović, M. (2005). Komentari zakona o krivičnom/kaznenom postupku u Bosni i Hercegovini. Sarjevo: Savjet/Vijeće Evrope, Evropska komisija.
3. Vojković. G., Štambuk-Sunjić, M. (2006). Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, Zbornik radova Pravnog fakulteta u Splitu, Vol.43 No.1.
4. Council of Europe (2015). Convention on Cybercrime. Preuzeto sa: http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.
5. Konvencija o kibernetičkom kriminalu, Službeni glasnik Bosne i Hercegovine – međunarodni ugovori, broj 6/2006.
6. Krivični zakon BiH, Službeni glasnik BiH broj 3/2003, 32/2003 - ispr., 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 8/2010, 47/2014, 22/2015, 40/2015 i 35/2018).
7. Krivični zakonik Republike Srpske, Službeni glasnik Republike Srpske broj 64/17.
8. Krivični zakon Fedaracije BiH, Službene novine FbiH broj 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14 i 76/14.
9. Krivični zakon Brčko distrikta Bosne i Hercegovine, Službeni glasnik Brčko distrikta BiH, broj 10/03, 6/05, 21/10 i 9/13.
10. Zakon o krivičnom postupku BIH, Službeni glasnik Bosne i Hercegovine br. 3/03, br. 32/03, 36/03, 26/04, br. 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, br. 58/08, br. 12/09, 16/09, 93/09, 72/13..
11. Zakon o krivičnom postupku Republike Srpske, Službeni glasnik Republike Srpske broj 53/12, 91/17 i 66/18.
12. Zakon o krivičnom postupku FBIH, Službene novine FBiH, 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 i 59/14.
13. Legislativni profil Bosne i Hercegovine o implementaciji odredaba Konvencije o kibernetičkom kriminalu u nacionalno zakonodavstvo, Savet Evrope u okviru IPA SEE (Octopus Cybercrime Community) https://www.coe.int/fr/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/

## IMPLEMENTING THE PROCEDURAL PROVISIONS OF THE CONVENTION ON CYBERCRIME IN THE CRIMINAL PROCEDURE LAW OF THE FEDERATION OF REPUBLIC OF SRPSKA

*Abstract*

*The Convention on Cybercrime was signed in Budapest on November 23, 2001 and represents a form of international treaty. The Convention on Cybercrime belongs to the so-called framework conventions, which means that its provisions are not directly applicable, but it is necessary that each state after the ratification implement the implementation of this convention in its own legislation. The aim of this paper is to point out the degree of implementation of the procedural provisions proposed by the Convention on Cybercrime in the Criminal Procedure Code of the Republic of Srpska and to point out the ways in which they are applied in order to improve the procedures that are being implemented in proving criminal offenses of computer crime.*

*Keywords: convention, cybernetics, computer crime, implementation.*