**ЗВОНИМИР М. ИВАНОВИЋ**[*]
**ОЛИВЕР ЛАЈИЋ**
Криминалистичко-полицијска академија
Београд

УДК 343.533::004(4-12)
ИД БРОЈ 192627980
Монографска студија
Примљен: 27.03.2012
Одобрен: 11.05.2012

# УПОРЕДНОПРАВНА АНАЛИЗА МЕРА СУПРОТСТАВЉАЊА ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ[**]

***Сажетак:*** Упоредноправна анализа одређених правних института три државе на простору југоисточне Европе (овом анализом су обухваћене Албанија, Турска и Хрватска) дата је у тексту који следи. Анализа се односи на поједине материјалне и процесне кривичноправне области, с посебним акцентом на проблематику високотехнолошког криминала. Ова анализа има за циљ упоређивање правно-техничких решења различитих културолошких, социолошких и религијских средина и спровођење, у тим условима, одређених института Конвенције Савета Европе о високотехнолошком криминалу (ВТК), као што су мере обезбеђења података о комуникацијама, мере хитне заштите, задржавања података, хитног очувања и делимичног чињења доступним података о саобраћају, као и инкриминисање појединих понашања која до сада нису била уврштена у национална законодавства. Анализом је обухваћен низ специфичности националних законодавстава, уз усредсређивање на кривична материјална и кривична процесна законодавства наведених држава. Од посебног значаја су на основу анализе добијени предлози за примену добрих практичних решења и правно-техничких облика примене појединих института и мера које

[*] zvonimir.ivanovic@kpa.edu.rs

[**] Овај рад је резултат реализовања научноистраживачког пројекта под називом „Развој институционалних капацитета, стандарда и процедура за супротстављање организованом криминалу и тероризму у условима међународних интеграција". Пројекат финансира Министарство науке и технолошког развоја Републике Србије (број 179045), а реализује Криминалистичко-полицијска академија у Београду (2011−2014). Руководилац пројекта је проф. др Саша Мијалковић.

предвиђа та Конвенција, а њихова једноставност и прагматичност могу бити од велике користи и нашем правном систему.

***Кључне речи:*** високотехнолошки криминал, Конвенција о високотехнолошком криминалу (ВТК),Савет Европе, мере против ВТК, анализа законодавстава и мера против ВТК

## Увод

У савременом окружењу, које подразумева брзу и тренутну комуникацију, од изузетног је значаја временски опсег за остваривање сарадње с најудаљенијим местима на Земљи, с циљем спречавања и сузбијања високотехнолошког криминала. У том смислу, веома је важна анализа кривичноправног и кривичног процесног стања законодавства у земљи која треба да буде субјекат те сарадње. Таквом анализом као резултат се може добити простор за сарадњу, као и утврђивање постојања разлика у националним законодавствима у материјалном и формалном смислу, које у одређеним случајевима не могу бити препрека тој сарадњи, али је могу значајно успорити или отежати[1]. Претходно изнето, наравно, није усамљени резултат анализе. На тај начин и таквим анализама може се уочити боља пракса појединих држава у тој области и доћи до закључака и могућих утицаја на наше законодавство. Као предмет анализе у овом случају узете су три земље које репрезентативно приказују стање на Балканском полуострву. Једна од њих је с простора бивше СФРЈ - Хрватска, с веома занимљивим решењима која имају доста сличности са српским, али опет и великих разлика. Друга је Албанија која није имала додирних тачака с легислативом бивше СФРЈ, али је из бившег, социјалистичког блока, те стога може заслуживати одређену пажњу. На крају је Турска с веома специфичним легислативним и географским окружењем, које је од изузетног значаја за неку врсту неутралне анализе с могућим позитивним решењима и за српско законодавство.

[1] Више о томе видети у: Васић, Александра (2011): Liability of internet service providers based on the American law and the law of the EU, *NBP*, *16*(3), 99–109.

## Албанија[2]

У оквиру надлежности полиције и тужилаштва у Албанији у току 2009. и 2010. године најчешће су се дешавала кривична дела везана за ВТК, која се могу груписати у пет основних области[3]:

- интернет преваре, укључујући постављање и злоупотребу преварених сајтова с циљем противправног прибављања личних и финансијских података;
- преваре с платним и кредитним картицама, израда и употреба платних фалсификованих картица прибављених скримингом и продаја противправно прибављених података у вези с кредитним картицама на интернету;
- фалсификовање везано за компјутере, углавном посредством социјалних мрежа, противправним приступом и представљањем за друго лице, с циљем прибављања противправне имовинске користи. Посебна категорија је нуђење противправно умноженог софтвера;
- неовлашћен приступ усмерен против јавних и приватних правних лица, са сврхом ометања њиховог нормалног функционисања или наношења штете. Такође је усмерен и на приватне кориснике, с циљем противправног прибављања личних и финансијских података;
- нуђење и растурање дечјег порнографског материјала на интернету.

У националном законодавству Албаније, Кривични законик (АКЗ) који датира још из 1995. године (Закон број 7895 од 27. јануара 1995)[4] морао је претрпети структуралне измене како би се увеле измене садржане у поменутим конвенцијама Савета Европе. Закони којима је то учињено су Закон број 10023 од 27. новембра 2008. године, који је дао основне материјалне законске елементе, и Закон број 9859 од 20. јануара 2008. године,[5] којим се инкриминишу производња и дистрибуција дечје порнографије на интернету. Доношењем Закона број 9380 у априлу 2005. године, ауторска и сродна права (уопште права интелектуалне својине) испуњавају услове из члана 10 ЦЕТС 185. Неки, посебни аспекти

[2] Албанија је потписала Конвенцију о ВТК (ЦЕТС 185) Савета Европе (СЕ) 23. новембра 2001. године, а исту ратификовала 20. јуна 2002. године. Целокупни инструментаријум је ступио на снагу у Албанији 1. јула 2005. године, а допуњен је потписивањем додатног протокола 26. маја 2003. године и његовом ратификацијом (ЦЕТС 189) 26. новембра 2005. године. Албанија је 19. децембра 2008. године потписала и Конвенцију о заштити деце од сексуалне експлоатације и сексуалног злостављања (ЦЕТС 201) и ратификовала је 14. априла 2009. године. Ступила је на снагу 1. јула 2010. године.

[3] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Albania%20_15%20May%2007_En.pdf последњи пут приступљено 9. 5. 2012. године.

[4] Сви извори националних законодавстава коришћени у овом тексту доступни су на енглеском језику на сајту: http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp, последњи пут приступљено 05.05.2012.год.

[5] Којим је уведен додатни параграф у члану 117.

права интелектуалне својине су уређени Законом број 9947 од 7. јула 2007. године (у погледу права индустријске својине), Законом број 9188 од 12. фебруара 2004. године, изменама и допунама КЗ (у погледу повреда права интелектуалне својине) и Законом број 9918 од 15. маја 2008. године (у вези с електронским комуникацијама).

У материјалном смислу, ЦЕТС 185 је примењена у АКЗ у члану 192/б, који комбинује њена два елемента члана 2, прописујући као дело неовлашћено приступање рачунарском систему, као и приступање кршењем безбедносних мера. Тежи облик постоји када су у питању посебни рачунарски системи (нпр., војни, националне безбедности, јавне безбедности, цивилне заштите, здравствене заштите или други системи од јавног значаја). Чл. 3, 4 и 5 ЦЕТС 185 (неовлашћено пресретање, неовлашћен приступ електронској обради података и неовлашћен приступ заштићеном рачунару, рачунарској мрежи ) предвиђени су у члану 293/а, 293/б и 293/ц АКЗ, при чему је израз „неовлашћено" преведен у „незаконито", што не одражава исту суштину и што се квалитативно разликује, посебно због тога што је у другим прописаним облицима поново коришћен израз „неовлашћено". Члан 6 ЦЕТС 185, под називом Злоупотреба уређаја, унет је у члан 293/д АКЗ, али поседовање таквих уређаја, прибављених с намером злоупотребе, није инкриминисано. Рачунарско фалсификовање (фалсификовање у вези с рачунарима) из члана 7 ЦЕТС 185 је преписано у члану 186а АКЗ, док је тежи облик формулисан у виду одређивања специфичног субјекта као извршиоца дела, у облику „лица које је задужено за задржавање и администрирање рачунарских података у питању". Није дефинисано ни шта значи бесправно, нити је потпуније прецизирано шта се подразумева под лицем описаним у претходној реченици. Такође, члан 8 Конвенције (рачунарска превара) копиран је у члану 143/б АКЗ, прописујући тежи облик алтернативно: када је дело извршено на организован начин, више од једном, или када је нанета штета већих размера или је делом оштећено више лица. Члан 9 Конвенције је примењен у члану 117 АКЗ, инкриминишући приказивање порнографског материјала малолетнику, док у другом одељку није инкриминисано стварање таквог материјала уз злоупотребу малолетника, као ни његова дистрибуција на интернету на различите начине[6]. Ту су у питању изрази „нуђење, чињење доступним и пренос", за које албански законодавац сматра да се могу садржати у изразу „дистрибуција".

Примена Додатног протокола о инкриминацији ксенофобије и расизма образложена је у изменама и допунама (у предлогу) Закона од 27.

[6] Реч је о избору албанског законодавца да резерве одређене конвенцијом у вези с тим кривичним делом примени као минимум стандарда.

новембра 2008. године, али је занимљиво да није утврђен члан 2 тог додатног протокола (о дефиницији те врсте материјала), већ се његово значење подразумева као ноторна чињеница. Растурање расистичког и ксенофобичног материјала посредством рачунарских система из члана 3 је потпуно примењено (у члану 119/а), док су расистичка и ксенофобична увреда (члан 5 ЦЕТС 189) обухваћене чланом 119/б, расистичка и ксенофобична претња (члан 4) чланом 84/а АКЗ, а злоупотреба уређаја (члан 6) је копирана у члану 74/а. Члан 10 Конвенције, у вези са злоупотребом права интелектуалне својине, унет је у чл. 148 и 149 АКЗ.

Албански Законик о кривичном поступку (АЗКП) такође датира из 1995. године (Закон број 7905 од 21. марта 1995) и њим су унете одредбе које се тичу мера хитног очувања похрањених рачунарских података (предвиђене чланом 16 ЦЕТС 185) и то у члану 299/а АЗКП. Овлашћено лице за предузимање те мере је ЈТ, а основ представљају основи сумње да такви подаци могу бити изгубљени, оштећени или измењени, што су нешто шири оквири од ЦЕТС 185 (која говори о довољним основима за веровање). Оно што не одговара члану 16 јесте формулација у АЗКП „да пронађе и учини доступним" описане податке, о чему се у ЦЕТС 185 не говори. Време за које се ти подаци похрањују је 90 дана, иако је ЦЕТС предвидео да та мера траје до 90, а не тачно 90 дана, што, наравно, може направити проблеме у случајевима занављања захтева. Да забуна буде још већа, постојеће образложење у предлогу измена ЗКП је одређивало максимум од 180 дана у том случају, што значи да је могуће занављање и уз укупно важење од 180 дана, али је то из текста АЗКП тешко закључити. Члан 17 ЦЕТС 185, у вези с хитним очувањем и делимичним чињењем доступних података о саобраћају, преписан је у члану 299/б АЗКП, а проблем се јавља у случају када схватимо да је систем заокружен применом Закона број 9918, посебно члана 101 2ц, и односом тог члана и члана АЗКП.

Члан 18 ЦЕТС предвиђа наредбу за прибављање података, док се у АЗКП тиме бави члан 191/а, који у ставу 1 даје овлашћење суду (у случајевима кривичних дела у вези с информационим технологијама) да нареди предају података лицу које их контролише или их има у држави-ни, с тим што се такође наводи да то може захтевати и оптужени (окривљени). Став 2 омогућава суду и да нареди предају података о кориснику. Став 3 омогућава ЈТ да нареди чињење доступним података, док упоредо обавештава и суд, у случајевима и времену када постоји опасност да би непоступање у том смислу озбиљно угрозило поступак и његово вођење, а суд мора преиспитати ту одлуку у року од 48 часова.

Тако широко овлашћење ЈТ даје могућност да се та мера злоупотребљава и да она буде правило, а став 1 изузетак.

Претрага и привремено одузимање похрањених података (члан 19 ЦЕТС) прописани су чланом 208/а АЗКП на сличан начин као и у Конвенцији. Тај члан садржи четири става у којима стоји „претрази и на сличан начин остваreном приступу подацима", док је Конвенција то одредила као „привремено одузимање", што би обухватило оба појма кумулативно, а не алтернативно. За претраживање рачунара и привремено одузимање података (копирање) с њега у виду умножавања неопходно је да их одобри суд својом одлуком, којом суд може и ограничити примену тих овлашћења. Важно је истаћи да та овлашћења суд може ограничити алтернативно на једно од оба прописана. Дакле, могуће је да суд одреди само претрагу а не и привремено одузимање (копирање) података. У том смислу, парадокс је што за овлашћење претраге рачунара подносилац захтева мора дати спецификацију система који треба да се претражи, а што изискује непосредан физички контакт с истим пре добијања такве наредбе. Проширење овлашћења на рачунаре и системе који су повезани с њима могуће је само уз претходно одобрење или дозволу суда, док се овлашћења полиције и тужилаштва прописују ставом 3 тог члана. Овлашћење садржи атрибут хитности, који је у непосредној колизији с обавезом за претходно одобравање, чиме се успорава примена овлашћења, те је, у том случају, могло бити уведено и накнадно одобравање такве мере. Али, с обзиром на могућности интернационализације проблема, можда ни овакво решење није лоше. Албански законодавац није предвидео прикупљање података у реалном времену (члан 20 ЦЕТС 185), већ је увео систем задржавања података, тако да члан 101 обавезује мрежне оператере и оператере јавне електронске комуникације да задржавају одређене податке (о идентитету претплатника, о опреми коју користе, као и о саобраћају комуникације) у периоду од две године. На то овлашћење се односе и чл. 191/а и 221 АЗКП. Пресретање података о садржају комуникације (члан 21 ЦЕТС 185) добило је своје отелотворење у члану 221 АЗКП, којим се може наредити пресретање телефонске и друге тајне комуникације (нпр., на тајном месту) техничким средствима. Лица која су у том случају објекат мере су или осумњичени или лице за које се сумња да одржава комуникацију с осумњиченим лицем. На одлуку суда о тој мери се може жалити тужилац, а основ за захтевање наредбе могу бити: а) умишљајно кривично дело за које је запрећена казна од најмање 7 година затвора и б) претње или увреде нанете или извршене уз помоћ телефонског система. Приказани услови су веома проблематични с обзиром на то да су у питању изразито дивергентни оквири и да

је запрећена казна, која је минимум у том случају, везана за изузетно тешка дела, док је увреда или претња обично везана за лакша кривична дела. Мера се одређује на основу наредбе суда а на образложен захтев тужиоца. Међутим, у хитним случајевима, тужилац може одредити меру уз могућност накнадног одобравања суда у року од 48 часова. Иначе, услови спровођења мере (методе и средства) одређују се наредбом, као и временско трајање мере[7].

## Хрватска[8]

Изменама КЗ Хрватске[9] из 2004. године унете су одредбе у вези с дечјом порнографијом, злоупотребом поверења, интегритетом и доступношћу рачунарских система, рачунарских података и програма, рачунарским фалсификовањем и рачунарским преварама. Дефиниције специфичних појмова одређених Конвенцијом су дате у члану 89 Кривичног законика Хрватске (КЗХ), а посебно у тач. 31 и 32, којима је укључен члан 1 ЦЕТС.

Неовлашћен приступ (члан 2 ЦЕТС) је уређен чланом 223(1) и, поред неовлашћеног приступа, прописује и приступ „упркос предузетим заштитним мерама", што представља шири оквир од ЦЕТС 185. Објекат кривичног дела је податак а не рачунарски систем или садржалац података, чиме се даје специфична заштита посебном и специфичном објекту.

Незаконито пресретање (члан 3 ЦЕТС 185) је прописано чланом 223(4), а у односу на Конвенцију има следеће разлике: одређење „путем техничких средстава" није унето у тај члан као што прописује ЦЕТС, нити се у њему инкриминише понашање лица које омогућава неовлашћеним лицима да приступе таквим подацима. Као објашњење обично се наводи да за пресретање таквих података није увек неопходно техничко средство, јер се подаци могу пресретати и визуелном или другом врстом опсервације. С тим циљем, неопходно је постојање елемента

[7] Најдуже може трајати 15 дана, али се може продужити за 20 дана, односно у случајевима тешких кривичних дела и до 40 дана.

[8] Хрватска је ЦЕТС потписала 2001. године, ратификовала 17.октобра 2002. године, а на правну снагу је ступила у Хрватској 1. септембра 2005. године. Додатни протокол ЦЕТС 189 је потписан 26. марта 2008. године, а ратификован је 4. јула исте године. На правну снагу је ступио 1. новембра 2008. године. Хрватска је потписала и ЦЕТС 201 25. октобра 2007. године, ратификовала је 29. септембра 2011. године, а на правну снагу је ступила 1. јануара 2012. године.

[9] НН 110/97, 27/98, 50/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08 и 57/11.

„није намењено за његову употребу" као разлика у односу на нејавну. Једино што би се могло додати тој одредби јесте да треба размотрити могућност увођења елемента виности у поступак лица које одређеним лицима која нису овлашћена на такав приступ „умишљајно" омогућава приступ таквим подацима. Неовлашћено поступање са подацима (члан 4 ЦЕТС 185) прописано је чланом 223(3). Разлика у односу на основни текст Конвенције је у уношењу израза „или други начин" чињење туђих рачунарских података неупотребљивим или недоступним.

Неовлашћен приступ заштићеном рачунару и рачунарској мрежи (члан 5 ЦЕТС 185) изгледа да није у потпуности примењен у Хрватској, а профил државе објављен на сајту Савета Европе указује, у том смислу, на члан 223(3) КЗХ који ипак не одражава суштину тог облика приступа. Вероватно се сматра да је описана одредба увођењем „другог начина" довољно широка да може обухватити и члан 5 ЦЕТС 185. Члан 223(5) прописује тежи облик у случају када су објекат напада рачунарски систем, рачунарски податак или програм владине агенције (тела државне власти), јавне установе или трговачког друштва од посебног јавног интереса, као и у случају проузроковања знатне штете. Злоупотреба уређаја (из члана 6 ЦЕТС 185) је прописана чланом 223(5), а следећим ставом је прописано и одузимање таквих средстава (члан 223(6)). Посебно питање се тиче подобности за одузимање уређаја у питању, а у вези с чланом 19 ЦЕТС 185. Рачунарско фалсификовање (члан 7 ЦЕТС) је прописано чланом 223а(1), а тај члан предвиђа као кажњиво и стварање лажних електронских докумената као и употребу таквих докумената. Тежи облик је исти као код члана 223(5) у погледу субјеката који су објекат напада, док се ставови 3 и 4 понављају и, као у случају 223(5) и (6), покушај је и овде кажњив.

Рачунарска превара (члан 8 ЦЕТС 185) је уграђена у члан 224а – став 1 описује елементе класичног дела преваре, став 2 одређује привилеговани облик када је дело учињено с намером да се неко само оштети, док став 3 инкриминише неовлашћено израђивање, набављање, продају, поседовање или чињење доступним направа, средстава рачунарских података или програма створених или прилагођених за вршење тих дела. Наравно, инкриминише се и покушај тог дела (став 5). Дела у вези с дечјом порнографијом (према члану 9 ЦЕТС) су у потпуности уграђена у члан197а КЗХ. Као пасивни субјекти тог дела се јављају и деца и малолетна лица, а инкриминација се односи на производњу, нуђење, дистрибуцију, прибављање за себе или другога, уз помоћ рачунарског система или мреже, или поседовање у рачунарском систему или на медијима за похрану рачунарских података порнографских садржаја, који при-

казују децу или малолетнике у сексуалном експлицитном понашању или су усредсређени на њихове полне органе. Та дефиниција представља ширу дефиницију од оне дате Конвенцијом, која не предлаже „приказе усредсређене на... полне органе", што је, дакле, ширег домашаја у односу на Конвенцију. С друге стране, неинкриминисање противправности подразумева могућност да се и фотографије или видео записи настали у медицинске сврхе окарактеришу на тај начин и да чине кривично дело, што представља значајан недостатак. Као тежи облик, у ставу 2 је инкриминисано чињење доступним деци таквих садржаја (слика, аудиовизуелних садржаја или других предмета порнографског садржаја). Прописано је и одузимање предмета извршења тог дела у ставу 3. Дела која се односе на пиратерију и злоупотребу права интелектуалне својине (из члана 10 ЦЕТС 185) су уграђена у чл. 230 (Недозвољена упораба ауторског дјела или изведбе умјетника извођача) и 231 КЗХ[10] (Повреда права производитеља звучне или сликовне снимке и права у свези с радиодифузијским емисијама).

Закон о казненом поступку Хрватске – ЗКПХ[11] примењује експедитивно очување похрањених рачунарских података (из члана 16 ЦЕТС) у члан 257, ст. 1 и 2 (који уређује претрес покретних ствари и банковног сефа, али и рачунара и с њим повезаних уређаја, који служе прикупљању, похрањивању и преносу података телефонским, рачунарским и другим комуникацијама, као и носилаца података). Став 2 даје овлашћење суду да предузме претресање, након чега се хитно предузимају мере за очување (у смислу превенције губитка или измена тачно одређених) података. Непоступање у складу с тим обликом налога повлачи могућност кажњавања на захтев ЈТ (државног одвјетника) од стране суда. Разлике у односу на ЦЕТС (члан16) могу се одредити у следећем: та мера је у ЗКПХ везана за меру претресања и изискује постојање наредбе, док се у ЦЕТС она не везује за тај институт и могуће ју је спровести и без наредбе суда; такође, у ЗКПХ се не говори о основу када ће се применити та мера, док ЦЕТС говори о „случајевима када постоје основи сумње да су рачунарски подаци посебно подложни губитку или модификацијама", што у случају ЗКПХ претпоставља примену у било којем случају, па чак и када нема никакве сумње за тим, што даје велику ширину у дискреционој оцени суду и тужилаштву[12]. Такође, изостали су рокови у којима би се ти подаци очували, као и елементи који се односе на дужност о по-

[10] Упоредити са: Веић, П., Глушчић, С. (2004): *Основе Казненог права*, Министарство унутарњих послова Републике Хрватске, Загреб.
[11] НН 152/08, 76/09, 80/11 и 121/11.
[12] Више о томе видети у: Карас, Жељко (2006): *Незаконити докази*, Ласерплус, Загреб.

верљивости у погледу поступања с тим подацима. Члан17 ЦЕТС 185, у вези с хитним очувањем и делимичним чињењем доступним података о саобраћају, није инкорпориран с обзиром на то да је Хрватска усвојила систем о задржавању података до једне године. Члан18 ЦЕТС предвиђа наредбу за прибављање података, док је она у ЗКПХ примењена као саставни елемент овлашћења за претресање. Члан 261 ЗКПХ уређује обавезе лица која су у државини ствари и предмета подложних претресању и прописује да предмет може бити привремено одузет уколико је то одређено законом или неопходно за утврђивање чињеница. Обавезе описаних лица подразумевају дужност предаје таквих предмета на наредбу (захтев) овлашћених лица, а непоступање према том захтеву или наредби представља кривично дело. Наравно, та инкриминација се не односи на окривљеног и особе одређене чланом 285 ЗКПХ[13]. Чланом 263 се омогућава примена члана 261 у рачунарском окружењу на податке похрањене у рачунарском систему, као и на податке о кориснику у државини провајдера. Члан 262 набраја који се објекти и документи не могу (ни у електронском ни у физичком облику) привремено одузети.[14]

[13] (1) Ослобођени су обавезе сведочења: 1) особа с којом је окривљени у браку или ванбрачној заједници; 2) рођаци окривљеног у правој линији, рођаци у побочној лози до трећега степена закључно, те сродници по тазбини до другог степена закључно; 3) усвојеник и усвојилац окривљеног; 4) јавни бележници и порески саветници у оквиру законске обвезе чувања тајне; 5) адвокати, лекари, зубари, психолози и социјални радници о ономе што су у обављању свог занимања сазнали од окривљеног и 6) новинари и уредници у средствима јавног информисања о изворима обавештења и података за које су сазнали у обављању свога занимања и који су употребљени приликом уређивања средстава јавног информисања, осим у поступку због кривичних дела против части и угледа учињених коришћењем средстава јавног саопштавања и у случају прописаном посебним законом. 4) Малолетник који с обзиром на старост и душевну развијеност није способан схватити значење права да не мора свједочити не може се испитати као сведок, али се сазнања добијена од њега путем стручних особа, рођака или других особа које су с њим биле у контакту могу користити као доказ.

[14] Привременом одузимању не подлежу: 1) списи и друге исправе државних тела чије би објављивање повредило обавезу тајности док надлежно тело не одлучи другачије; 2) писана саопштења окривљеног браниоцу, осим ако окривљени не захтева другачије; 3) снимке и приватни дневник пронађени код особа из члана 285, става 1, тач. 1–3 ЗКП, које су те особе снимиле или написале, а садрже снимке или записе о чињеницама о којима су те особе ослобођене дужности свједочења; 4) записи, изводи из регистара и сличне исправе које се налазе код особа из члана 285, става 1, тачке 4 ЗКП, састављени о чињеницама које су у обављању свога занимања те особе сазнале од окривљеног и 5) записи о чињеницама које су саставили новинари и уредници у средствима јавног информисања о изворима обавештења и подацима за које су сазнали у обављању свог занимања и који су употребљени приликом уређивања средстава јавног информисања, а који се налазе у њиховом поседу или у уредништву у којем су запослени.

(2) Забрана привременог одузимања предмета, исправа и техничких снимки из става 1, тач. 2–5 овог члана не примјењује се: 1) у погледу браниоца или особе ослобођене оба-

Законик даје овлашћење ЈТ да нареди откривање одређених података и истом наредбом може одредити и рок у којем се подаци морају предати, а одбијање предаје може бити подложно санкцији[15]. Члан 263, став 3 обавезује на поштовање прописа о одређеним професионалним и другим тајнама приликом снимања података о којима је реч, док се ставом 4 обезбеђује могућност заштите и чувања (на предлог ЈТ, наредбом истражног судије) свих описаних рачунарских података све док је то потребно за истрагу а најдуже 6 месеци, након чега се враћају, осим у законом предвиђеним случајевима[16]. На ту меру држалац се може жалити у року од 24 часа, с тим да жалба не одлаже извршење решења. У таквим случајевима је практично употребљивија могућност прављења копија података, па уколико жалба успе, онда је нормално уништити копије а након тога обавестити лице које има правни интерес о брисању и околностима у питању. Када је реч о претресању и привременом одузимању података (члан 19 ЦЕТС 185), они су у ЗКПХ садржани у члану 257. На захтев органа који предузима претресање, особа која се користи рачунаром или има приступ рачунару или другом уређају или носиоцу података и пружалац телекомуникационих услуга су дужни да омогуће приступ рачунару, уређају или носиоцу података и дају потребна обаве-

---

везе сведочења према члану 285, ставу 1 ЗКП ако постоји вероватноћа да су окривљеном помогли у чињењу кривичног дела, пружили му помоћ након извршења кривичног дела или поступали као прикривачи; 2) у погледу новинара и уредника у средствима јавног информисања ако постоји вероватноћа да су окривљеном помогли у чињењу кривичног дела, пружили му помоћ након извршења кривичног дела или поступали као прикривачи кривичног дела, те за казнена дела из чл. 305 и 305а Казненог закона и 3) ако је реч о предметима који се имају одузети према закону.

(4) Забрана привременог одузимања предмета, исправа и снимака из става 1, тач. 2–5 овог члана, не примењује се у предметима ктивичних дела почињених на штету деце и малолетника из члана 117 Закона о судовима за младеж.

(5) Државни одвјетник, истражитељ или полиција могу одузети предмете према ст. 1, 2 и 3 овог члана и када спроводе увиђај кривичних дела или када истражитељ или полиција извршавају налог суда.

(7) Предмет одузет супротно одредбама става 1 овог члана не може се употребити као доказ у поступку.

[15] Члан 259 – За неизвршавање захтева судија истраге, на образложени предлог државног одвјетника, казниће ту особу новчаном казном у износу до 50.000,00 куна, а ако и након тога не поступи према захтеву, може се казнити затвором до извршења захтева, а најдуже месец дана. Окривљени се не може казнити.

[16] 1) Ако нису укључени у извршење следећих кривичних дела из кривичног закона: повреду тајности, целовитости и доступности рачунарских података, програма или система (члан 223), рачунарско кривотворење (члан 223а) и рачунарске преваре (члан 224а); 2) ако нису укључени у почињење другог кривичног дела за које се гони по службеној дужности, почињеног помоћу рачуналног система и 3) ако не служе као доказ за кривично дело за које се води поступак.

штења за несметану употребу и остваривање циљева претраге. Наведено се не односи на окривљеног. Овде је значајно напоменути да је описан приступ веома сличан класичном приступу у погледу привременог одузимања предмета, али је у новој светлости и у специфичним околностима такво привремено одузимање проблематично[17]. Дилеме попут од кога се одузима, да ли је у питању дефинитивно одузимање, као и да ли се физичким одузимањем уређаја у питању условљавају нови проблеми (сервер више не функционише а није га користио само осумњичени, већ и друга лица, тако да су и она погођена том мером) повлаче за собом низ значајних питања[18]. Члан 19 прописује да је могуће одузимати и носиоце података, али да је примереније стварање копија, првенствено због тога што су такви подаци већ у етру и што су доступни и другим лицима, тако да се њиховим одузимањем ускраћују лица која тиме ни би требало да буду погођена[19]. Из истог разлога ЦЕТС прописује задржавање и остваривање приступа на неки други начин, јер би брисање тих података из датог система могло произвести нестабилност система и изазвати диспропроционо дејство, посебно уколико се надзор и претресање могу спровести прављењем веродостојних копија и без њиховог брисања. Посебно би се морала обратити пажња на случајеве енкрипционе заштите тих података, те у таквом случају прописати посебне мере обезбеђења и поступања с подацима. Претресање повезаних система је уопштено дозвољено с обзиром на то да је у овом члану наведено, али је неопходно поменути да је за тако нешто потребна судска контрола, нарочито након спроведеног претресања. Но, овде је проблем у случајевима када се наредба односи само на дати рачунар, па је за активне конекције потпуно илузорно захтевање нове наредбе, која би тим путем обухватила и новонасталу ситуацију, јер би се иста могла подвести под првобитну. Све то под условом да је могуће приступити том другом систему из просторија где се налази предмет претресања и да се такав приступ може легално остварити, као и у случајевима када постоје основи сумње да тражени подаци могу бити избрисани или измењени и фалсификовани. Прикупљање података о саобраћају комуникација у реалном времену (члан 20 ЦЕТС 185) и пресретање података о садржају

[17] Погледати у: Крапац, Давор (2002): *Закон о казненом поступку и други извори хрватског поступовног права*, Народне новине, Загреб, као и у: Крапац, Давор (2007): *Казнено процесно право: институције*, Народне новине, Загреб.

[18] Упоредити са: Павишић, Берислав (2005): *Коментар Закона о казненом поступку*, Жагар, Ријека, и са: Павишић, Берислав (2006): *Казнено право Вијећа Европе*, Голден маркетинг-Техничка књига, Загреб.

[19] Као нови проблем овде се може јавити и околност да се потребни подаци налазе у кеш или у РАМ меморији рачунара.

комуникација (члан 21 ЦЕТС) добили су своје отелотворење у члану 332 ЗКПХ и то[20] само према учиниоцу или саучеснику у кривичном делу из члана 334 (тешка кривична дела, укључујући и дела дефинисана у ЦЕТС 185 у чл. 223, 223а и 224а ЗКПХ). Изузетно, када околности налажу да се с извршењем радњи започне одмах, налог из става 1 пре почетка истраге, на време од 24 часа, може издати ЈТ са ознаком времена издавања и образложењем и мора га, у року од осам сати од издавања, доставити истражном судији. Истражни судија одмах одлучује решењем о законитости налога. Ако судија одобри налог, ЈТ ће поступити према ставу 1. Уколико судија истраге одбије налог, ЈТ може у року од осам сати поднети жалбу. О жалби одлучује ванрасправно веће у року од 12 сати. Према члану 335, ставу 2 ЗКПХ, Оперативно-технички центар за надзор телекомуникација, који обавља техничку координацију с провајдером телекомуникацијских услуга у Републици Хрватској, као и оператери телекомуникационих услуга, дужни су да обезбеде полицији потребну техничку помоћ. За поступање противно тој обавези, истражни судија, на образложени предлог ЈТ, казниће пружаоца телекомуникационе услуге новчаном казном до 1.000.000,00 куна, а одговорно лице у Оперативно-техничком центру за надзор телекомуникација и провајдера телекомуникационих услуга у Републици Хрватској новчаном казном у износу до 50.000,00 куна. Уколико и након тога не изврши решење, одговорно лице се може казнити затвором до извршења, али најдуже месец дана. О жалби против решења којим је изречена новчана казна или је одређен затвор одлучује веће. Жалба против решења о новчаној казни и затвору не задржава извршење решења. ЦЕТС 185 прописује за оба члана обавезу поштовања приватности, док се у ЗКПХ та обавеза не разматра, већ је другим системским и гранским прописима остављено да ту обавезу наметну провајдерима и операторима.

## Турска[21]

Члан 1 ЦЕТС, у вези с дефинисањем појединих појмова из ЦЕТС у турском законодавству, није прописан Кривичним закоником (КЗТ), већ се поједини појмови могу наћи у Закону број 5651 од 5. маја 2007.

[20] Прва мера према ставу 1, тачки 2, а друга према ставу 1, тачки 1.

[21] Турска је потписала ЦЕТС 185 10. октобра 2011. године, а ЦЕТС 201 25. октобра 2007. године. Ниједну од наведених конвенција није ратификована до овог тренутка, док Додатни протокол ЦЕТС 189 није ни потписала. Поред наведеног, Кривични законик Турске (КЗТ) ипак садржи одређене одредбе које могу бити примењене у случајевима ВТК.

године који говори о уређивању интернет публикација, као, на пример, подаци (у вези с чланом 2 ЦЕТС у смислу незаконитог и неовлашћеног приступа)[22] и појам приступа преко провајдера тим подацима, а такође и у вези с приступом садржају комуникација. Члан 2 ЦЕТС о неовлашћеном приступу је разматран у члану 243 КЗТ, који у ставу 1 инкриминише незаконит приступ у целости или у делу система за обраду података или незаконито „успостављање" и „одржавање" таквог система. Тежи облик је предвиђен у ставу 3, а подразумева брисање или мењање неких података у систему електронске обраде података. Члан 3 ЦЕТС 185, у вези с незаконитим пресретањем, у турском законодавству није посебно дефинисан облик, већ се посредним тумачењем може доћи до члана 243 КЗТ. У питању су изрази дати под наводницама у претходним реченицама – успостављање и одржавање, где израз „одржава" може обухватити незаконито поступање након остваренog незаконитог приступа. Ипак, на тај начин се значење члана 3 ЦЕТС доводи у питање у том смислу, јер не захтева претходећи незаконит приступ рачунарском систему, већ инкриминише надзор и опсервацију података и трансфер података док их обрађује систем аутоматске обраде података (АОП) уз помоћ техничких средстава (укључујући и посебан софтвер). Другим речима, члан 2 ЦЕТС подразумева приступ „на предња врата", док је члан 3 усмерен ка другим типовима метода. Члан 4 ЦЕТС о неовлашћеном поступању с подацима је примењен у члану 244, ставу 2 КЗТ, а односи се на брисање, измену и сличне начине поступања с подацима или трансмисију (пренос) постојећих података на неко друго место. Подразумева се да су у питању рачунарски подаци, а не подаци у смислу члана 2 ЦЕТС, помињани у Закону број 5651, који обухватају веома широк круг појмова. Значајно је напоменути да се у том члану (244) не помињу противправност ни неовлашћеност, па се може десити да то дело учини и лице које је овлашћено да поступа с подацима, односно лице које је било овлашћено а поступало у заблуди, обмани или с евентуалним умишљајем. Члан 5 ЦЕТС, који се односи на неовлашћен приступ заштићеном рачунару и рачунарској мрежи, прописан је у члану 244, ставу 1 КЗТ, где је објекат заштите превенција функционисања (и чињења неупотребљивим) система за обраду података без овлашћења (или неовлашћено) у вези с уносом, изменом или прикривањем рачунарских података. Начин извршења се првенствено везује за физичке нападе (насиље, ватра – паљевина), али и за друге, нефизичке нападе. Трећи облик тог дела је прописан за случај да су објекат напада системи од специјалног јавног или

[22] http://www.osce.org/fom/41091 последњи пут приступљено 9.5.2012. године.

државног интереса, као, на пример, јавне институције или банке (члан 244, став 3). У ту сврху се користе изрази „спречавање функционисања" и „чињење неупотребљивим", који су свеобухватнији од оног прописаног у ЦЕТС, дефинисаног као „озбиљно мењање". Поступање с незаконито прибављеним користима на тај начин, као и оним прибављеним вршењем рачунарских превара, уређени су истим законом (члан 244, став 4). Члан 7 – у вези с рачунарским фалсификовањем, није у потпуности примењен. Могло би се спекулисати о члану 245 КЗТ у вези са злоупотребом платних картица, док профил земље[23] указује на члан 244, став 2, који инкриминише раније описане радње у смислу стварања нових рачунарских података или датотека, или фалсификовања других електронских докумената. Ипак, то кривично дело не обухвата типичне елементе кривичних дела фалсификовања. Према описаном, закључак би имао прецизнији домет од профила државе у Савету Европе (СЕ). Рачунарска превара (члан 8 ЦЕТС) је прописана чланом 158 у оквиру класичног кривичног дела преваре и чланом 243, ставом 2 КЗТ у смислу специјалног облика дела. У другом случају није јасно да ли је покривен случај преваре техничким средствима или електронским сервисима, па је неопходно у некој блиској будућности проширити домашај инкриминишући и те елементе. Дела везана за дечју порнографију (члан 9 ЦЕТС) могу се посматрати у концепту ширих објеката заштите кривичног законодавства Турске у области опсцености. Члан 226 КЗТ се односи на излагање деце (Закон број 5237, члан 6, тачка б дефинише дете као особу млађу од 18 година) опсценом материјалу (приказивање материјала или читање текстова)[24]. Посебан облик (став 3) се односи на злоупотребу деце за продукцију опсценог писаног или аудиовизуелног материјала. Такође, истим ставом се инкриминишу и продаја, транспорт, похрањивање, извоз или нуђење на коришћење. Изузеци се односе (став 8) на научна, уметничка или литерарна дела, под условом да иста нису доступна деци. Члан 103, став 1 Закона број 5237 инкриминише примену силе или претње у стварању опсцених материјала. Члан 228 КЗТ потпуно инкриминише све елементе члана 9 ЦЕТС, али је у ставу 3 технолошки потпуно неутралан. Такође, опсценост није дефинисана, нити се дефинише дечја порнографија[25], што представља очигледан недостатак КЗТ. У турском законодавству кривична дела везана за злоупотребу ауторских и сродних права (члан 10 ЦЕТС) су уређена кроз више аката. Закон број

[23] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Turkey_2011_January.pdf, последњи пут приступљено 9. 5. 2012. године.
[24] http://www.osce.org/fom/41091 последњи пут приступљено 9.5.2012. године.
[25] У смислу тачака б и ц члана 9, става 2 ЦЕТС.

5846/1951 (мењан и допуњаван 2006) дефинише све елементе везане за злоупотребе ауторских и сродних права, наводећи као кључни елемент и заштитни објекат литерарне и научне радове. У КЗТ су у питању три дела: члан 71 – Злоупотреба моралних или примарних права, члан 72 – Злоупотреба економских или секундарних права и члан 73 – Остала кривична дела те области и тежи облици, који су предвиђени чланом 74 (када су субјекти извршења кривичних дела физичка лица као представници правних лица, односно одговорна лица у правним лицима и под прокуром, тј. професионални менаџери) и чланом 75 (прецизирајућа правила у процедуралном смислу, као и дефинисање правила поступања с рецидивистима).

У погледу процесног дела, чл. 16, 17 и 18 ЦЕТС нису примењиви у законодавству Турске, осим у појединим прописима и то делимично. Претресање и привремено одузимање похрањених рачунарских података (члан 19 ЦЕТС) је уграђено у члан 134 Законика о кривичном поступку Турске (ЗКПТ). Тај члан овлашћује ЈТ да од истражног судије, на основу образложеног предлога, добије наредбу за претресање рачунарског система, рачунарског програма и логова осумњиченог. Став 2 прописује привремено одузимање уређаја и опреме, која се након декодирања и копирања одмах и без одлагања мора вратити особама којима је одузета. Став 3 прописује да када се привремено одузима рачунар или претресају датотеке, неопходно је да се направи потпуна копија система података (*бацкуп*). Уколико осумњичени или његов заступник то захтевају, копија тог *бацкуп*-а мора им се предати. Смисао таквих уских дефиниција је највероватније био тај да се очува ланац доказивања пошто ће се те претраге, по правилу, остваривати (вршити) у форензичким лабораторијама. Према турском законодавству, привремено одузимање предмета носилаца таквих података није неопходност, већ ће у свим случајевима када је могуће копирање целокупног система података заменити ту меру. Папирну копију (тзв. *хард цопу*) података који су копирани мора потписати надлежно лице. Чињеница је да већина норми које садржи члан 134 ЗКПТ одговара духу онога што је прописано чланом 19 ЦЕТС (у вези с претресањем и привременим одузимањем података). Законом није одређен предмет претреса рачунара у смислу шта се тражи, односно шта је предмет који се тражи. Такође, законом није одређено да предмет буде обавезни садржински елемент наредбе, али је јасно да предмет претресања рачунарског система подразумева претрагу његових компоненти, програма и садржине података. Ни логовање није много другачије када је у питању шта се претражује, али, наравно, кључни елемент у претрази „логова коришћених од стране осум-

њиченог" изгледа као веома уско дефинисана претрага. Из приказаног није потпуно јасно у каквом су односу наредба за претресање просторија и наредба за претресање рачунара (система). У погледу примене члана 20 ЦЕТС о прикупљању података о комуникационом саобраћају у реалном времену значајно је да је у Турској на снази систем задржавања података, дефинисан европском Директивом 2006/24/ЕЦ,[26] тако да због тога није неопходна примена чл. 6 и 20 ЦЕТС. Члан 6, став 1, тач. б и ц Закона број 5651/2007 обавезује интернет провајдере да чувају податке о саобраћају у периоду од 6 месеци до 2 године. Пресретања садржаја података из комуникације (члан 21 ЦЕТС) покрива члан 135 ЗКПТ. За време истраге или у току поступка, уколико постоји основана сумња да је извршено кривично дело и да не постоје други начини да се прибаве докази, суд или, у одређеним хитним случајевима, ЈТ може наредити да се идентификују, пресретну, сниме и процене подаци о сигналу осумњиченог (или оптуженог у случају подигнуте оптужнице, односно суђења) посредством телекомуникација. Која су дела у питању? Она су набројана у ставу 6, али међу њима нема дела високотехнолошког криминала. Пресретање комуникација остварених уз помоћ мобилних телефона омогућава и геолоцирање осумњиченог, с циљем његовог лишења слободе. Али, у том смислу, ту меру није могуће користити према лицима која су искључена од сведочења.

## Закључак

Циљ приказаног упоредноправног прегледа је анализа описаних система, уз могућност прихватања и укључивања датих успешних и добрих решења. У том смислу, занимљиво је размотрити следеће. Могуће је спровести инкриминисање тежег облика неовлашћеног приступања рачунарском систему када су у питању посебни рачунарски системи. Било би веома корисно прописати рачунарску превару у тежем облику када је дело извршено на организован начин, више од једном или када је нанета штета већих размера или је делом оштећено више лица, по угледу на АКЗ. Такође, процесно законодавство Албаније може бити од значаја у погледу мере хитног очувања похрањених рачунарских података, тј. да се као услов за примену одреде основи сумње да подаци могу бити изгубљени, оштећени или измењени. Неопходно је дефинисати у

[26] http://en.wikipedia.org/wiki/Data_Retention_Directive и http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF последњи пут приступљено 30. 5. 2012. године.

нашем процесном законодавству нове мере претраге и привременог одузимања похрањених података, али потпуније и уз могућност њиховог истовременог предузимања – инспирисано примером из АЗКП. У том смислу би било веома упутно и потпуније дефинисати „на сличан начин остваривање приступа". Посебно је занимљиво дефинисање проширења претраге изван граница државе, уз претходно судско одобрење или евентуално накнадно правно оснажење. Наравно, ту је и пресретање података о садржају комуникације одређено од стране ЈТ, уз могућност његове валидације судском одлуком у року од 48 часова. За наше законодавство је веома занимљиво размотрити решење претресања покретних ствари и банковног сефа, али и рачунара и с њим повезаних уређаја који служе прикупљању, похрањивању и преносу података телефонским, рачунарским и другим комуникацијама и носилаца података, као и немогућност привременог одузимања појединих предмета[27]. Још једно значајно решење је и могућност кажњавања провајдера телекомуникационих услуга и одговорних у њима због непоступање у складу с обавезом да пруже техничку помоћ полицији. По угледу на процесно законодавство Турске, значајно је размотрити и усвајање система европске Директиве у погледу задржавања података и уношења одредаба ЗКПТ, које прописују да геолоцирање као меру није могуће користити према лицима која су изузета од сведочења у односу на осумњичено лице из ЗКПТ.

## Литература:

1. Ivanović, Zvonimir; Banović, Božidar (2011): Analiza pravne regulative nadzora nad komunikacijama i praksa Evropskog suda za ljudska prava, *Bezbednost*, (1), 93–116.
2. Karas, Željko (2006): *Nezakoniti dokazi*, Laserplus, Zagreb.
3. Krapac, Davor i dr. (2001): *Kazneno procesno pravo: lista primjera*, Službeni list, Zagreb.
4. Krapac, Davor (2002): *Zakon o kaznenom postupku i drugi izvori hrvatskog postupovnog prava*, Narodne novine, Zagreb.
5. Krapac, Davor (2007): *Kazneno procesno pravo: institucije*, Narodne novine, Zagreb.
6. Pavišić, Berislav (2005): Komentar Zakona o kaznenom postupku, Žagar, Rijeka.

[27] Упоредити са: Ивановић, Звонимир; Бановић, Божидар (2011): Анализа правне регулативе надзора над комуникацијама и пракса Европског суда за људска права, *Безбедност*, (1), 93–116.

7. Pavišić, Berislav (2006): *Kazneno pravo Vijeća Europe*, Golden marketing i Tehnička knjiga, Zagreb.
8. Vasić, Aleksandra (2011): Liability of internet service providers based on the American law and the law of the EU, *NBP*, (3), 99–109.
9. Veić, Petar; Gluščić, Stjepan (2004): *Osnove Kaznenog prava*, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb.

## Интернет извори:

1. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Albania%20_15%20May%2007_En.pdf
2. http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp
3. http://www.osce.org/fom/41091
4. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Turkey_2011_January.pdf
5. http://en.wikipedia.org/wiki/Data_Retention_Directive

## Comparative Law Analysis of Measures Against Cybercrime

***Summary:*** Comparative legal analysis of certain legal concepts of three Southeast European countries is given in the text that lies before you. The analysis refers to certain substantive and procedural criminal law area, with sub-specialization in high-tech crime issues. This analysis is to compare the legaly technical solutions in those three different cultural, social and religious social systems and the implementation under these conditions of some specific institutes of the Council of Europe Convention on Cybercrime. This analysis includes a number of specific national legislation and the focus of the exercise of criminal and criminal procedural legislation of the subjects of analysis. Of particular importance is the analysis carried out with proposals for the implementation of practical solutions and law - application of certain forms of technical institutes and the measures provided for in this Convention and their simplicity and pragmatism can be of great use to our legal system.

***Key words:*** Cybercrime, Cybercrime Convention, Council of Europe, Countermeasures against Cybercrime, Analysis of Legislative Actions and Measures against Cybercrime