др *Звонимир ИВАНОВИЋ*
Криминалистичко-полицијска академија, Београд
проф. др *Божидар БАНОВИЋ*
Правни факултет, Универзитет у Крагујевцу

UDK 316.772::001.893::341.413
Прегледни научни рад
Примљено: 6.09.2011.

Анализа правне регулативе надзора над комуникацијама и пракса Европског суда за људска права*

Апстракт: *Мера надзора над комуникацијама је релативно нова у нашем законодавству, али појавом нових технологија применљивих на најразличитије облике комуникација јављају се многобројни проблеми. Наравно, ово није случај само у Србији, већ много шире. Слична проблематика јавља се и у Европској унији, а ми се као потписница европске Конвенције о људским правима (ЕКЉП) морамо руководити и праксом Европског суда за људска права у Стразбуру (ЕСЉП). Стандарди који се у европским земљама постављају у овој области у својој основи садрже правила установљена управо у пракси овог суда. Без обзира на све трендове и догађаје у овој области наш законодавац, у последње време, није у потпуности на нивоу европских. Аутори анализирају чињенице и околности везане за законско регулисање мере надзора и снимања телефонских и других облика комуникација, уз упоредно правну анализу праксе ЕСЉП, али и суда ЕУ у Луксембургу. У ову анализу уноси се и разматрање предлога нацрта новог Законика о кривичном поступку (ЗКП). Аутори анализом и приказом упоредно правне праксе покушавају и да дају предлоге de lege ferenda у Србији.*

Кључне речи*: тајни надзор комуникација, Суд за људска права у Стразбуру, људска права, прислушкивање, полиција.*

Увод

С обзиром на свакодневно сусретање са новим технологијама у савременом животу, може се спекулисати о *ропствовању* људске расе

* Рад је резултат реализовања научноистраживачког пројекта под називом Развој институционалних капацитета, стандарда и процедура за супротстављање организованом криминалу и тероризму у условима међународних интеграција, који финансира министарство надлежно за науку у Републици Србији (бр. 179045), а реализује Криминалистичко-полицијска академија у Београду (2011-2014). Руководилац пројекта је проф. др Саша Мијалковић.

високим технологијама. Нове облике технолошких решења која човеку помажу у свакодневном животу и активностима готово да више и не примећујемо, они истог тренутка када се појаве постају саставни део наше свакодневице. Ту већ више није битно да ли је у питању телефонски уређај или *таблет* рачунар са напредним комуникацијским карактеристикама − важно је да има мултифункционалност и да омогућава разне облике комуникације, који се не састоје само у разговору, већ и размени великих количина података између два или већег броја лица. Криминалне и криминалистичке аспекте злоупотребе, односно употребе комуникационих технологија, веома је тешко појмити уколико се не влада стручном материјом комуникација, чиме се издвајају и два основна правца сагледавања ове материје у криминалистици. Први се односи на могућности злоупотребе технолошких достигнућа у комуникационим технологијама у сврху извршења кривичних дела, које сваким даном све више расту и развијају се. Са друге стране, ова област представља најофанзивнији елемент савремене стратегије сузбијања криминалитета, посебно његових најсложенијих форми. С обзиром на тековине демократских друштава која су поставила границе у задирање јавне власти у прокламована права и слободе грађана, посебно у право на уживање приватности, значајно је размотрити постојеће стандарде у овој области.

Конвенција Савета Европе о високотехнолошком криминалу и надзор над комуникацијама

Као један од начина и метода супротстављања транснационалном организованом криминалу јавља се тајни надзор над комуникацијама. *Конвенција Савета Европе о високотехнолошком криминалу*[1] (ВТК) – ЦЕТС 185 предвиђа различите механизме за борбу против ВТК (Урошевић, Ивановић, 2010а:65). Један од механизама је мера пресретања садржаја података у комуникацији. Она предвиђа овлашћења надлежних органа да прикупљају или снимају, у реалном времену, податке из садржаја одређених комуникација пренетих преко рачунарског система, или да прикупљају или снимају податке из садржаја о одређеним комуникацијама које се преносе на територији државе (чија је јурисдикција) применом техничких средстава, која се налазе на тој територији (члан 21 ЦЕТС). У одређеним земљама мера има назив проспективни надзор[2], она подразумева претра-

[1] *Council of Europe Convention on Cybercrime*, CETS No. 185, *Закон о потврђивању Конвенције о високотехнолошком криминалу*, Службени гласник РС − Међународни уговори, бр. 19/2009.

[2] У емпиријском истраживању једног од аутора у оквиру докторске дисертације одбрањене на Правном факултету у Крагујевцу, испитаници (припадници полиције, судства, тужилаштва и експерти у облсти ВТК) су се у погледу овако назване мере одредили у следећим оквирима:

живање интернета у реалном времену и „ослушкивање“[3] саобраћаја, уколико је у питању комуникација интернетом, а уколико су у питању други начини преноса података постоје различита ограничења.

Мере садржане у ЦЕТС 185, по мишљењу међународне заједнице, представљају неопходан минимум стандарда за обезбеђење предуслова за успешно сузбијање ВТК, које би требало уградити у национална законодавна решења. Ипак, државама које су потписале и ратификовале ЦЕТС 185[4] остављена је могућност стављања резерве на примену мера које се односе на прикупљање података о саобраћају у реалном времену и пресретање података из садржаја. Сврха стављања резерве јесте да се странама уговорницама омогући да успостављање, спровођење и примену овлашћења из *Конвенције* усагласе са условима и ограничењима предвиђеним домаћим законодавством, што треба да омогући одговарајућу заштиту људских права и слобода, у складу са преузетим међународним обавезама.

Процедурална правила морала би се поштовати у погледу кривичних дела прописаних одредбама ЦЕТС 185, али и других кривичних дела извршених рачунаром, рачунарским системима и мрежама, као и код проналажења, изазивања, обезбеђења и прикупљања трагова у електронској форми везаних за оваква кривична дела[5].

Према ЦЕТС 185, надлежни органи гоњења имају овлашћења: да наређе или на сличан начин прибаве или остваре хитну заштиту одређених рачунарских података, укључујући и податке о саобраћају који су били похрањени посредством рачунарског система, у оним случајевима када постоји основана сумња да су ти подаци подложни изменама или губитку[6]; да наређе предају одређених рачунарских података одређе-

56,25% испитаника сматра га полицијском мером предвиђеном за одређена кривична дела у законодавству; у делфи верзији 33,33% испитаника одредило се за овај одговор; 12,5% испитаника сматра да он представља форму полицијске мере против свих кривичних дела и учинилаца. Посебна мера која се спроводи само на основу одлуке суда (наредба, налог) представља одговор 31,25% испитаника основне анкете али и 66,67% испитаника делфи верзије анкете.

3 У употреби је и термин „њушкање“ (енг. sniffing).

4 Закључно са 31. 7. 2011. године *Конвенцију* је ратификовало 30 држава чланица Савета Европе и САД као држава нечланица, а 13 држава чланица и 3 које нису чланице Савета Европе је потписало, али је још увек није ратификовало – види: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG − доступно на дан 31. 7. 2011.

5 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p. 19. доступан 14. 3. 2010.

6 Члан 16 *Конвенције* − Подаци о којима је реч су они који нису обрисани до тренутка достављања овакве наредбе. Овакво прибављање, по *Конвенцији*, може трајати најдуже до 90 дана. Међутим, није прописана обавеза интернет сервис провајдера (ИСП) да овакве податке доставе органима гоњења, већ их они прибављају самостално. Значајно је рећи да је ово овлашћење различито од овлашћења задржавања података. Природа комуникација и савремених облика саобраћаја приморава креаторе мера да раздвоје облике активности са подацима, како због провајдера ових услуга, тако и због корисника и самих органа гоњења. Но, *Конвенција* само оквирно регулише ове одредбе, а на државама чланицама је да пропишу сопствене процедуре и мере заштите свих учесника у комуникационом саобраћају.

ним лицима у чијем поседу (државини) се исти налазе у одређеном рачунарском систему или одређеном медију за похрањивање података; да наређе интернет провајдерима предају података о корисницима услуга везаним за овакве услуге који су у поседу интернет провајдера или у његовој фактичкој власти[7]; да захтевају парцијално откривање података о саобраћају[8]; да прегледају (претресу) и заплене сваки рачунар или његов део, и рачунарске податке похрањене на њима, као и медиј за смештање (архивирање) рачунарских података уколико постоји основана сумња да се на њему налазе инкриминишући материјали[9]; као и да од провајдера електронских комуникација прикупљају податке који се односе, пре свега, на употребу интернета и кредитних картица, а на основу којих се може доћи до имена или ИП адресе потенцијалног учиниоца кривичног дела[10]. Када је реч о мерама предвиђеним *Конвенцијом* можемо навести следеће:

− Хитна заштита сачуваних рачунарских података[11] предвиђа могућност надлежних државних органа да наређе или на сличан начин остваре заштиту одређених рачунарских података (укључујући ту пода-

---

[7] Чл. 18 *Конвенције* − Подаци о којима је реч су сви они подаци (рачунарски, али и подаци у другој форми) у државини провајдера а који се односе на корисника услуга и коришћење услуга осим података о садржини комуникације. То су подаци на основу којих се може установити: тип комуникационе услуге који је коришћен, техничке мере предузете у том циљу, као и период коришћења услуге; идентитет преплатника, његова поштанска или географска адреса, телефонски или други приступни број; информације о рачуну и плаћањима услуге, који су доступни у зависности од уговора о пружању услуга; свака друга информација присутна на месту инсталације комуникационе опреме доступна на основу уговора о пружању услуга.

[8] Чл. 17 *Конвенције* − Ово овлашћење везује се за случај када је у упитању више различитих провајдера. Такође се односи и на пружање више различитих услуга које би се могле при комуникацији искористити – приступни провајдери, такозване бесплатне бежичне локалне мреже или бежичне бесплатне тачке за интернет, али и информације о рутерима.

[9] Чл. 19 *Конвенције* − Значајно је поменути и става 2 овог члана који указује на могућност претраге података у виртуелном окружењу, који се физички не налазе на територији државе под чијом јурисдикцијом се врши претресање. Наравно, овде се указује и на поштовање националног суверенитета. Став 3 наводи да ова овлашћења морају да омогуће: а) привремено одузимање или сличан облик обезбеђења рачунарског система, његовог дела или медијума за архивирање релевантних рачунарских података; б) да сачине и задрже копије оваквих рачунарских података; в) да очувају интегритет (целовитост) релевантних похрањених података, и г) да изазову читљивост недоступних података или изузму такве податке са рачунарског система којем је приступљено.

[10] Чл. 20. *Конвенције*, тач. б, предвиђа да је провајдер услуга дужан да у оквирима својих техничких могућности: 1) прикупи или похрани податке путем техничких средстава на територији државе; 2) да сарађује и пружи асистенцију релевантним органима у прикупљању или похрањивању података о саобраћају у реалном времену везаних за одређену комуникацију на сопственој територији пренету путем рачунарског система. Неопходно је и да одржи интегритет тих података, а препоручује се да у ту сврху користи и средства математичких алгоритама. У поређењу са садржинским пресретањем података, овај облик прикупљања рачунарских података је мање интрузиван, не омогућава директан приступ садржинским оквирима комуникације, већ само информацијама које су неопходне за спровођење криминалистичких мера и радњи.

[11] У Србији је ова мера била прописивана подзаконским актима и тек је, крајем јула 2010, *Законом о електронским комуникацијама*, чл. 128, покушано да се одговори на ове обавезе из *Конвенције*.

тке о саобраћају сачуване преко рачунарског система), посебно у случајевима када се верује да су такви подаци подложни губитку или измени; да се лице или установа на које се таква наредба односи обавеже да штити и сачува целовитост тих рачунарских података за неопходан временски период, а највише до 90 дана, као и да се обавеже да штити тајност таквих поступака (чл. 16 ЦЕТС 185). Практично, у питању су случајеви када постоји оперативна, форензичка или практична потреба за очувањем података како би се они могли даље адекватно користити. Лица задужена за задржавање оваквих података и уређаја морају чувати податке о њима као поверљиве[12].

− Хитна заштита и делимично откривање података о саобраћају у реалном времену предвиђа могућност хитне заштите података о саобраћају у односу на податке из претходне мере, без обзира да ли је у преносу поруке учествовао један или више давалаца услуга, као и могућност откривања количине података у саобраћају довољне за идентификацију давалаца услуга, и путање којом је саобраћај извршен (чл. 17).

− **Претраживање и заплена (привремено одузимање) сачуваних рачунарских података** предвиђа могућност надлежних органа да на својој територији претраже одређени рачунар[13], рачунарски систем, рачунарски програм[14] или његов део, и у њему сачуване рачунарске податке, медије за чување рачунарских података, или да, уколико су тражени подаци сачувани на неком другом рачунарском систему, а тим подацима се може приступити са почетног рачунарског система, прошире претрагу или на други сличан начин приступе том рачунарском систему (чл. 19). Предвиђена је и могућност да надлежни органи заплене или на сличан начин обезбеде рачунарски систем или његов део, као и медије за чување података, да направе и задрже копије тих рачунарских података, одрже целовитост битних рачунарских података и учине рачунарске податке недоступним, или их уклоне из рачунарског система ком је приступљено. Постоји могућност да се сваком лицу које познаје начин рада рачунарског система или мере примењене за заштиту података на том систему, нареди да, у разумној мери, пружи неопходне податке, како би се омогућило предузимање описаних мера. Према

[12] ИТУ у свом приручнику за ВТК легислативу, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf стр. 27, иде и даље предлажући да се у вези са међународном сарадњом у погледу ове радње не сме постављати услов двоструке кажњивости. У истом приручнику наводи се да је одбијање пружања међународне правне помоћи у овој области могуће само уколико се захтев односи на политичко кривично дело или је везан за такво дело, или уколико замољена држава сматра да се тиме задире у суверенитет, безбедност, јавну безбедност или друге државне интересе. Такође, неће се обезбедити доступност података уколико се њима угрожава поверљивост спровођење неке истраге државе на чијој територији су такви подаци, осим уколико та држава, након обавештења државе молиље, не одлучи супротно.

[13] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p. 23, последњи пут приступљено 8. 6. 2011.

[14] Ibid.

ИТУ-овом приручнику за израду ВТК легислативе, неопходно је размотрити и претраге у повезаним системима[15].

Наиме, уколико разматрамо претраге које се у виртуелном свету простиру и на територије других држава, неопходно је предвидети и могућност спровођења оваквих претрага од стране других држава и њихових органа гоњења. Услови за ово су да се предмет претраге јавља доступним са: рачунара, система, програма или његовог дела чији власник има приступ или могућност контроле, а за који постоји наредба за претресање (или сличан акт којим се омогућава претрага), па је зато неопходно дати легислативну могућност проширења претрага и кроз овакве могућности. У овом смислу посебно треба водити рачуна о тзв. *open source* (отвореним) изворима, који су свима доступни без обзира где се налазе (па би било парадоксално постављати питање њиховог приступа од стране власти једне државе), али и о јавно доступним похрањеним подацима, програмима, подацима о саобраћају комуникација и садржају истих, без обзира на чијој територији се налазе. Што се тиче привременог одузимања предмета, оно се односи на претходно помињане дигиталне податке и подразумева следеће[16]: заплену или слична средства за обезбеђење рачунара, рачунарског система или његовог дела, или медијума за похрањивање података; прављење и задржавање „имиџа“ (врсте идеалне електронске копије) помињаних података; очување интегритета ових података и обезбеђење документовања оваквог очувања интегритета путем примене средстава математичких алгоритама; изазивање прикривених или неприступачних података и њихово изузимање са рачунара (система).

Једна од вероватно најдалекосежнијих одредби тиче се тзв. „пресретања података“[17] − фактички прислушкивања електронских комуникација, првенствено оних везаних за интернет (чл. 21 ЦЕТС 185). Интересантно је размотрити разлоге које су при увођењу ове мере навели аутори *Конвенције*: према њима, у одређеним случајевима није могуће, или чак није довољно само прикупити податке о оствареном саобраћају[18], већ је неопходно прикупити доказе који ће довести до процесуирања и осигурати осуђујућу пресуду за извршиоца. Ово је нарочито актуелно у случајевима када је извршилац познат и када је позната особа са којом комуницира, те средства те комуникације, а предмет и садржина ове комуникације су инкриминишући. До ове мере ће доћи

[15] Ibid.

[16] Ibid.

[17] Термин је усвојен из: Николић и др., 2010:48, у циљу одржавања униформности, мада је можда боље користити термин пресретање комуникација или процеса преноса података.

[18] Ово је интересантна терминолошка одредница и прављење дистинкције с обзиром да се према ставу праксе ови елементи комуникација разликују, па и услови за полицијско и тужилачко поступање у погледу садржине и форме комуникација.

онда када је за доказивање кривичног дела неопходно имати материјал сакупљен у, како се наводи у ЦЕТС 185, „реалном времену“, односно у тренутку када се комуникација одиграва[19]. Веома је значајно од ове мере разликовати меру предвиђену чл. 20, која подразумева прикупљање у реалном времену рачунарских података о комуникационом саобраћају. Прикупљање података о комуникационом саобраћају у реалном времену предвиђа овлашћења надлежних органа да прикупљају или снимају у реалном времену податке о саобраћају одређених комуникација пренетих преко рачунарског система или да прикупљају или снимају податке о саобраћају повезане са одређеним комуникацијама које се преносе на територији једне државе применом техничких средстава која се налазе на тој територији (чл. 20 *Конвенције*).[20] Интересантно је поменути и да се даје могућност да се у овом смислу користе и провајдери услуга – да се путем налога они принуде (или од њих захтева) да предузму овакве радње.[21]

Ова област интервенције државних органа је и најосетљивија јер се практично задире (повређује се) у право на приватност и право на преписку, односно слободу изражавања (првенствено чл. 8 и 10 *Европске конвенције о људским правима и основним слободама* – ЕКЉП), док сама *Конвенција* ЦЕТС 185 не садржи одговарајућа ограничења и гаранције да таква права неће бити злоупотребљена (осим генералног ограничења да се при извршењу свих мера морају поштовати међународни стандарди људских права постигнути кроз поменуте међународне документе). Наравно, у питању су фундаментална права, а уз то неопходно је поштовати и одредбе *Конвенције Савета Европе* бр. 108 о заштити права појединца у вези са аутоматском обрадом личних података.[22]

Члан 21 ЦЕТС 185, који регулише пресретање података, наводи да ће се ова мера предузети за „озбиљна дела“ (више о овом термину и тумачењу појма у: Мијалковић, С., Манојловић, Д., 2008:154,156), па је

---

[19] Насупрот томе стоји мера заплене постојећих доказа који су раније снимљени на рачунару или другом медијуму за чување и пренос података, коју *Конвенција* такође предвиђа у чл. 19. У односу на ову меру имамо најразличитија тумачења и практичне примере у земљама потписницима *Конвенције*, у вези са начином складиштења тих података и трансфера тако складиштених информација.

[20] У ЕУ *Директива о приватности и електронским комуникацијама* (*Directive 2002-22-EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services,* Official Journal of the European Communities, L108/51-77, од 24. 4. 2002) дефинише да се подаци о телекомуникационом саобраћају корисника, који се обрађују и похрањују од стране пружалаца јавних мрежа или услуга, морају обрисати или учинити анонимним након што више нису неопходни за сврхе преноса комуникација, а то се односи и на податке о локацији корисника. Наравно, једини изузетак употребе оваквих података је у случају полицијске истраге, када је легитиман.

[21] Посебно када говоримо о међународној правној помоћи, треба поменути да по основу реципроцитета може бити постављена обавеза органа на пружање овакве асистенције.

[22] *Конвенција* је доступна на адреси: http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm последњи пут приступљено 31. 1. 2010.

остављено државама да пропишу круг дела на која би се она применила. Оваква формулација је практична, али носи и могућност злоупотребе. Шта више, став 3 поменутог члана одређује да државе морају прописати услове под којима ће провајдери, који нужно морају учествовати у сакупљању ових информација, поступати у вези са околношћу да се одређени корисник надзире или његова комуникација прати и снима (у смислу постојања права да о он томе, евентуално, у одређеном моменту буде обавештен), као и то да ће садржину на тај начин прикупљених података морати да чувају као тајну. У односу на приказане мере из чл. 20 и 21 ЦЕТС 185 постоји и мера издавање наредбе која предвиђа могућност надлежних државних органа да наређе лицу на својој територији да преда одређене рачунарске податке које поседује или контролише, а сачувани су у рачунарском систему или на медију за чување рачунарских података, као и даваоцу услуга који пружа услуге на територији стране уговорнице да преда податке о претплатнику који се односе на услуге које тај давалац услуга поседује или контролише (члан 18).

Према *Приручнику за обуку судија Савета Европе*[23]*,* пресретање процеса преноса података не даје могућност анализе садржаја размењених у оваквој комуникацији уколико је комуникација била заштићена неким уређајем или процесом шифровања.[24] Оваква технологија може се користити не само у оквирима размене података или датотека – *file exchange*, већ и у случајевима ВоИП комуникација (*Voice over IP*), посебно у светлу актуелних догађања на тржишту социјалних мрежа (у виду сарадње Фејсбука и Скајпа, Гугл+ и Гугл тока и сл.).[25]

У сваком случају неопходно је разликовати описано пресретање комуникација (остваривање увида у садржај), од задржавања података о комуникацији (формални аспекти комуникационог саобраћаја) и прикупљања рачунарских података у реалном времену. Ова подела има и своју практичну страну. *Конвенција* не предвиђа аутоматско прикупљање и снимање података (рачунарских и комуникационих) од стране провајдера. Најпре зато што би овакво обавезивање изискивало значајна новчана средства и ангажовање великог броја људи од стране провајдера, а корист не би пропорционална оваквим ангажовањима. *Конвенција* предвиђа само циљано сакупљање података, након прибављања адекватног, законом прописаног акта надлежног органа (судског или

[23] *Приручник за обуку судија у супростављању кибер криминалу* доступан на интернет страници: http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_en.pdf доступан дана 26. 1. 2010.

[24] О другачијем схватању видети у: Урошевић, В., Ивановић, З., 2010а:64-71).

[25] Више о проблему заштићених комуникација и њиховом пресретању на интернет страници: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf доступан 29. 1. 2010, а о злоупотребама погледати (Урошевић, В., 2009).

другог органа који омогућава независну оцену) који спроводи поступак (чл. 15 ЦЕТС 185)[26]. Разлози за овакво решење везују се за процес настанка *Конвенције*[27], али и за околности које прате судску праксу Европског суда за људска права (ЕСЉП)[28], посебно у вези са одлукама о чл. 8 ЕКЉП[29]. У овом смислу многа законодавства, а посебно је то актуелно у оквирима ЕУ, кроз проблематику директиве о задржавању података (*Data retention Directive* 2006/24/ЕС)[30] уводе обавезу задржавања података о комуникационом саобраћају за привредна друштва која пружају комуникационе услуге. У Србији се ова мера одређује као надзор и снимање телефонских и других комуникација и предвиђена је чл. 504е *Законика о кривичном поступку* (ЗКП)[31] (упоредити са Тањевић, Н., 2009:156).

Проблеми традиционалног законског оквира надзора над комуникацијама

Питање које је последњих година врло актуелно јесте − како „слушати“ комуникације а не угрозити право на приватност појединца (Комлен Николић, Л., и др. 2010:135-140; упоредити и са: *Приручник за тренинг тужилаца и судија у области високотехнолошког криминала*, 2009:77-82.)[32]. За разлику од истраге поводом других кривичних дела, код којих нпр. прислушкивање телефона долази као мера којој претходе неке друге истражне радње које би идентификовале да је неко лице умешано у противправно деловање, код високотехнолошког криминала понекад се не може утврдити јасна граница када постоји сумња, односно када је тражење појединих приватних података о личности дозвољено, и уопште релевантно за истрагу. Овај проблем се не јавља услед постојања тенденције полицијских и других органа да своја овлашћења тумаче широко. Напротив, сама природа високотехнолошког криминала је таква да је он „скривен“ и да је потребно значајно знање и искуство да би се уопште перципирао. Такође, оваква криминална средина већ, сама по себи, изискује примену мера и у иницијлном моменту расветљавања оваквих кривичних дела.

---

[26] У питању је широка формулација коју, како ћемо видети касније, покушава да искористи и наш законодавац.

[27] Није постојао шири консензус да би се ово питање уредило на начин који омогућава другачије решење. Више у: *Convention on Cybercrime – Explanatory Report*, http://conventions.coe.int/treaty/en/reports/html/185.htm p. 25, последњи пут приступљено 31. 3. 2011.

[28] На ово се *Конвенција* позива у чл. 15, ст. 1.

[29] Члан којим се третира право на поштовање приватног и породичног живота.

[30] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF последњи пут приступљено 11. 7. 2011.

[31] Али је предвиђена и *Законом о електронским комуникацијама*, чл. 127.

[32] У питању је право које произлази из чл. 8 *Европске конвенције о људским правима*.

Надзор и снимање телефонских и других комуникација (телекомуникационих линија) и праћење и снимање активности (прислушкивање) рачунарских система и њихових корисника може помоћи у истрази, нарочито у случајевима када овакви системи само емитују податке, без њиховог записивања, тамо где подаци једва да прелазе граничне оквире, и у оним случајевима када је неопходан константан надзор над телекомуникацијама лица. Оваква специјална истражна мера и радња[33] са једне стране је изузетно ефикасна у смислу доказивања кривичног дела (јер се лице појављује као директан актер кривичног дела или се самоинкриминише), као и за утврђивање организационе структуре и веза у организованој криминалној групи, док са друге стране ова радња представља веома офанзивно, значајно и директно задирање у сферу приватних права и слобода лица чије се комуникације надзиру[34].

Атрибути који су претходно наведени најпре произлазе из тајности и прикривености спровођења ових специјалних мера и радњи. У већини земаља код ових облика специјалних мера и радњи постављају се много ригорознији услови него што је то случај са другим облицима

[33] У суштини, у питању је више радњи и веома је значајно издиференцирати активности о којима је реч. Наиме, надзор и снимање телефонских и других комуникација мора се разликовати најпре у области ВТК. Када говоримо о тајном прислушкивању и снимању, оно не обухвата меру аутоматског рачунарског претраживања личних и других са њима повезаних података (при чему *Конвенција* о ВТК не предвиђа ову меру) из члана 504љ, већ меру из чл. 504е ЗКП. Свака аутоматска рачунарска обрада података о комуникацијама дефинитивно је обрада која обухвата одређене личне или са њима повезане податке. Овакве околности омогућавају најразличитији софтверски пакети а савремени трендови иду ка обједињавању свих могућности дајући мултифункционалност програмима и чинећи их примамљивим за кориснике. Најлакше је то схватити кроз пример примене софтверског пакета И2 Analyst notebook или Encase форензичке алатке на остварeним комуникацијама на подацима о саобраћају комуникација, а не на садржини истих (Више о томе у: Ранђеловић, Д., 2009:270). Неки аутори говоре и о „метерингу“ (eng. *metering, meter check printer* – евидентирање телефонских бројева са којих се позива и бројева који се позивају, време позивања и трајања позива, али не и евидентирање садржаја разговора) у овим случајевима. Теоретски је могућа и ситуација у којој се може применити аутоматска рачунарска обрада података и приликом пресретања комуникација у реалном времену, али је у овом тренутку она неизводљива за техничке могућности у Србији. (Више о *data mining-у* у: Маринковић и др., 2009:70). Из тог разлога неопходно је разликовати ове мере али и разумети њихов однос и могуће разлике са другим мерама. Задржавање података о комуникационом саобраћају има карактеристике аутоматског рачунарског претраживања, али је ова мера наметнута оператерима с обзиром да они у сваком случају остварују анализу ових елемената комуникационог саобраћаја. Подаци о времену и дужини обављеног разговора, позицији израчунатој на основу базних станица, идентификацији држалаца ГСМ картица, али и ИП адреса, МАЦ адреса и других идентификујућих елемената већ представљају резултате аутоматске рачунарске обраде података у области деловања телекомуникационог оператера.

[34] Такође, имамо земље у којима су неке фазе радњи које су овде разматране подељене на различите специјалне истражне мере и радње (СИМ). То можда представља једно од логичних решења с обзиром на количину података и материјала који се могу прибавити применом само једне мере, а на тај начин се могу конкретније заштитити слободе и права грађана. Основ разликовања момената примене различитих радњи је природа комуникација, па се под надзором над комуникацијама подразумева активност која покрива све информације које излазе из рачунара и усмерене су на друго лице, али не и оне које се стварају и саобраћају само унутар рачунара, не и изван њега или унутар одређеног рачунарског система.

задирања у људска права и слободе, на пример код радње претресања станова и других просторија. Управо због тога неопходно је да државни органи у потпуности поштују принцип законитости, односно *да предузимају само оне мере које су изричито предвиђене законским одредбама*, уколико су друге блаже мере којима би се могао остварити циљ према начелу супсидијарности исцрпљене и за које је претходно прибављена наредба надлежног органа (Мијалковић и др., 2009:156). Питање да ли се традиционална овлашћења телефонског прислушкивања могу проширити и на друге облике телекомуникација веома је осетљиво питање и у компаративном праву. Решења иду у распону од оних која не праве посебно питање код рачунара као облика или средства комуникације чија се активност може надзирати и снимати, наводећи „надзор телекомуникационог саобраћаја укључујући и снимање садржаја истог", до оних који сматрају да се мора разликовати и дозволити само надзор над конверзацијом или комуникацијом или „надзор и снимање телекомуникационог саобраћаја на носиоцима звука" (Мијалковић и др., 2009:156).

Теоретичари проблематизују и питање начина остваривања телекомуникационог саобраћаја, па уводе и околности техничко-технолошких основа комуникације, где се разликују нпр. комуникације остварене преко ВоИП технологије и електронском поштом (у САД се разликују услови за добијање наредбе за надзор и снимање комуникација које се остварују у датом моменту између учесника у комуникацији, од оних код којих долази до складиштења садржаја комуникације). Оваква ограничења веома су проблематична када посматрамо питање аналогне примене принудних мера у јурисдикционим подручјима других држава[35].

Постоје аутори који указују на различите сегменте у оквиру ове мере и радње препознајући надзор (нарочито одређених карактеристика комуникације, телефонских листинга и у мобилним и фиксним телефонијама, ИМЕИ и ИМСИ бројева и претрага коришћења ових бројева у различитим мрежама и сл.) као могући посебан облик ове комплексне радње (Милидраговић, 2010:217-227). Овакву поделу приказује и *Конвенција о ВТК*, кроз форму и садржину комуникација.

[35] Нису само традиционални оквири они који овде представљају проблем. Карактеристичан пример је Немачка, у којој се у погледу доношења *Закона о прислушкивању електронских комуникација* подигла велика прашина 2009. и 2010. године, а у сукобу су били влада и председник, и група од 34.000 грађана. Наиме закон је донет, председник је одбио да га потпише, а грађани су поднели тужбу Немачком уставном суду (иницијативу за оцену уставности и законитости). Закон је на крају повучен. Више о томе на: http://www.netzpolitik. org/2009/ticker-muendliche-anhoerung-zur-vorratsdatenspeicherung/ доступан 29. 3. 2010. Посебно треба обратити пажњу на бугарски закон из јануара 2010. који даје широка овлашћења полицији, а што је такође изазвало протесте незадовољних грађана. Више о томе на: http://www.sofiaecho.com/2009/12/18/831890_the-eyes-have-it доступан 29. 3. 2010.

Као крајња консеквенца ове поделе јавља се третирање одређених радњи (у оквиру надзора), којима би се могла обухватити комуникација другим средствима, као оперативно-тактичких а не као истражних радњи, чиме би и доказна вредност ових радњи изостала.

Питање одобравања оваквих радњи значајно је са аспекта задирања у приватност лица чија се комуникација надзире, па је могуће да такав случај изискује наредбу истражног судије (Голић, Цудовић, 2010:243). Ово у сваком случају зависи од тумачења појма комуникација и онога шта он све обухвата.

Комуникацију можемо посматрати и као скуп два елемента – садржине и форме, па уколико се пресретање односи на садржину – подразумевала би се наредба истражног судије и третман акта као истражне радње, а уколико је у питању форма[36] – имала би третман радње мањег значаја у задирању у људска права и слободе за шта је могући основ и одобрење ЈТ[37]. Овакав став одговара досадашњој пракси и законом прописаним оквирима.

Поједине одлуке ЕСЉП прихваћене су као референтне у овој проблематици. Конкретно, ради се о пресудама Малоне против Уједињеног Краљевства[38] (где је утврђено да прикупљање информација о позиваним телефонским бројевима, времену и дужини позива потпада под појам комуникација)[39], и Копланд против Уједињеног Краљевства[40] (у којој је прецизирано да појам приватности и преписке обухвата не само телефонске комуникације, него и електронску пошту и употребу

[36] Форма о којој је реч први пут је у нашој пракси регулисана писаним актом – *Законом о електронским комуникацијама*, члан 129. Обавеза оператора из члана 128, став 1 овог закона односи се на податке потребне за:
– праћење и утврђивање извора комуникације;
– утврђивање одредишта комуникације;
– утврђивање почетка, трајања и завршетка комуникације;
– утврђивање врсте комуникације;
– идентификацију терминалне опреме корисника, и
– утврђивање локације мобилне терминалне опреме корисника.
Обавеза задржавања података обухвата и податке о успостављеним позивима на које није одговорено, али не обухвата податке о позивима чије успостављање није успело.

[37] Ово и јесте случај нпр. са предлогом нацрта новог ЗКП и чл. 286, ст. 3, текст доступан на http://www.mpravde.gov.rs/cr/articles/zakonodavna-aktivnost/ последњи пут приступљено 21. 7. 2011.

[38] Malone v. United Kingdom (Application no. 8691/79), пресуда од 2. августа 1984, ст. 83-84.

[39] У питању је релативно стар случај код којег је постављено питање основаности и природе надзора над формом комуникација, а у питању су били „листинзи" обављених разговора, моменат њиховог остваривања са одређених бројева, дужина трајања, фактички и локације позива. Ови листинзи су прављени штампачима у оквиру телефонске компаније, без наредбе суда. Одлуком је установљена пракса по којој се форма комуникације изједначава са садржином, по правној заштити, па је и за ове облике или карактеристике комуникације неопходно постојање наредбе суда. Посебно интересантно би било тумачење које се из овог случаја може извести према карактеристикама интернет комуникација, података о оствареним комуникацијама у најширем смислу, као и триангулација информација о оствареним комуникацијама кроз елементе форме, уз укрштање са ГПС подацима.

[40] Copland v. United Kingdom (Application no. 62617/00), пресуда од 3. априла 2007, ст. 43.

интернета)[41], али и о пресуди Круслин против Француске[42] (која је од значаја за превентивну или постфестум надзорну улогу суда у случајевима надзора и снимања комуникација), и Коп против Швајцарске[43] (у вези са идентификацијом одређене особе која комуницира са одређеног корисничког броја, али и чувањем података о комуникацији и надзору над комуникацијама). Описане одлуке дају стандарде по којима је:

- изједначена форма комуникације са њеном садржином у погледу задирања „јавне власти“ у приватност комуникације, у вези са чл. 8 ЕКЉП. Овај стандард је примењив и на интернет комуникације, а у савременим условима постоји више потребе за овим у односу на друге видове комуникације. Интернет пружа много више могућности за задирање у приватност комуникација коришћењем свих карактеристика комуникације, како од провајдера услуга, тако и са рачунара и сервера које корисник користи;
- изједначена електронска пошта са другим облицима комуникације у погледу правне заштите, али и статуса; такође и употреба ове поште у оквирима пословних комуникационих канала. Постављањем ових стандарда очекује се од држава да успоставе стандарде за издавање наредби у овој области које би покривале и електронску пошту и које би спадале у појам комуникација, а такође би обухватале и приватно коришћење пословне комуникације. Према овим стандардима чл. 8 обухвата и пословну комуникацију коришћену у приватне сврхе;
- уводе се основи за превентивну и постфестум судску контролу надзора и снимања комуникација;
- постављени су стандарди о дужини трајања и похрањивању архиве података о надзору комуникација.

Према ЗКП-у, одредбе које прописују (услове под којима је могуће наредити) надзор и снимање телефонских и других разговора или комуникација другим техничким средствима (рачунарске мреже), и оптичка снимања лица за која постоје основи сумње да су сама или са другим извршила или изузетно припремају поједина кривична дела[44]

[41] У овом случају изједначена је комуникација која се остварује путем интернет електронске поште са другим облицима комуникације, где је установљена пракса по којој је неопходно да буде испуњен сет одређених услова како би се остварио надзор над комуникацијама ове врсте. Такође се изједначава постојање приватности у оквирима пословне комуникације са приватном, где се у суштини проширује домет права на приватност комуникација и на пословне комуникације. У питању је широко схваћен појам „јавне власти“ и ограничење њеног задирања у приватне облике комуникације лица.

[42] Kruslin v. France (Application no. 11801/85), пресуда од 24. априла 1990.

[43] Kopp v. Switzerland (13/1997/797/1000), пресуда од 25. марта 1998.

[44] У питању су лица за које постоје основи сумње да су учинила кривично дело из члана 504а овог законика, ако се на други начин не могу прикупити докази за кривично гоњење, или би њихово прикупљање било знатно отежано. Мере из става 1 овог члана изузетно се могу одредити и ако постоје основи сумње да се припрема неко од кривичних дела из члана 504а, а

није могуће применити за кривична дела ВТК, с обзиром да таксативно наведеним кривичним делима на која се ове мера односи (глава XXIXa ЗКП под насловом Посебне одредбе о поступку за кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела[45]) нису обухваћене и инкриминације из области ВТК. И остале специјалне истражне методе, као што су пружање симулованих правних услуга, ангажовање прикривених иследника, контролисана испорука, остала су ван домашаја примене од стране органа за борбу против високотехнолошког криминала, имајући у виду да су, према законским одредбама, примењиве само за кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела, а дела БТК нису обухваћена овим каталогом[46].

околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати, или би то изазвало несразмерне тешкоће или велику опасност.

[45] Оне садрже поједина посебна правила поступка за кривична дела организованог криминала, корупције и друга изузетно тешка кривична дела. У кривична дела корупције из става 1 овог члана, и ако нису резултат деловања организоване криминалне групе, спадају кривична дела: злоупотреба службеног положаја (чл. 359 *Кривичног законика*), противзаконито посредовање (чл. 366 КЗ), примање мита (чл. 367 КЗ) и давање мита (чл. 368 КЗ). У друга изузетно тешка кривична дела из овог члана, и ако нису резултат деловања организоване криминалне групе, спадају кривична дела: убиство (чл. 113 КЗ), тешко убиство (чл. 114 КЗ), отмица (чл. 134 КЗ), разбојништво (чл. 206, ст. 2 и 3 КЗ), изнуда (чл. 214, ст. 3 и 4 КЗ), фалсификовање новца (чл. 223, ст. 1 до 3 КЗ), прање новца (чл. 231, ст. 1 и 2 КЗ), неовлашћена производња, држање и стављање у промет опојних дрога (чл. 246, ст. 1 и 2 КЗ), кривична дела против уставног уређења и безбедности Републике Србије (чл. 305 до 321 КЗ), недозвољено држање оружја и експлозивних материја (чл. 348, ст. 3 КЗ), недозвољен прелаз државне границе и кријумчарење људи (чл. 350, ст. 2 и 3 КЗ), трговина људима (чл. 388 КЗ), трговина децом ради усвојења (чл. 389 КЗ), међународни тероризам (чл. 391 КЗ), узимање талаца (чл. 392 КЗ) и финансирање тероризма (чл. 393 КЗ). Одредбе ове главе које се односе на кривична дела из става 3 овог члана примењују се и у поступку за кривична дела из чл. 370 до 386 КЗ, као и у поступку за тешка кршења међународног хуманитарног права извршена на територији бивше Југославије од 1. јануара 1991. године, која су наведена у статуту Међународног кривичног суда за бившу Југославију. Одредбе ове главе које се односе на кривична дела из става 3 овог члана примењују се и у поступку за кривична дела из чл. 322, ст. 3, чл. 323, ст. 3, чл. 335, чл. 336, ст. 1, 2 и 4 и чл. 337 и 339 КЗ, ако су извршена у вези са кривичним делима из става 3 овог члана, као и у поступку за кривично дело из члана 333 КЗ, ако је извршено у вези са кривичним делима из ст. 3 и 7 овог члана.

[46] Према изменама *Закона о организацији и надлежностима државних органа у борби против високотехнолошког криминала* (ЗОНДОБВТК), у чл. 3 екстензивним тумачењем се може доћи до појединих дела која би спадала у надлежност у оквиру примене ових мера: у тач. 2 − кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2.000 или настала материјална штета прелази 1.000.000 динара; као и у тач. 3 − кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чл. 2, ст. 1 овог закона. А чл. 2 гласи: „Високотехнички криминал у смислу овог закона представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику“.

Закон о електронским комуникацијама предвиђа тајност електронских комуникација, па чл. 126 и наводи: пресретање електронских комуникација којима се открива садржај комуникације није допуштено без пристанка корисника, осим на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Оператор је дужан да омогући законито пресретање електронских комуникација.

Надлежни државни орган који спроводи послове законитог пресретања дужан је да води евиденцију о пресретнутим електронским комуникацијама, која нарочито садржи одређење акта који представља правни основ за вршење пресретања, датум и време вршења пресретања, као и да ову евиденцију чува као тајну, у складу са законом којим се уређује тајност података.

Оператор је дужан да, ради остваривања ове обавезе, о свом трошку обезбеди неопходне техничке и организационе услове (уређаје и програмску подршку).

Предлог нацрта ЗКП-а, чланом 161 предвиђа посебне доказне радње. као и услове за одређивање. Посебне доказне радње могу се одредити према лицу за које постоје основи сумње да је учинило кривично дело из члана 162[47], а на други начин се не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Оне се, изузетно, могу одредити и према лицу за које постоје основи сумње да припрема неко од ових кривичних дела, а околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати, или би то изазвало несразмерне тешкоће или велику опасност.

[47] Кривична дела у односу на која се примењују посебне доказне радње. Под условима из члана 161 овог законика посебне доказне радње се могу одредити за следећа кривична дела:
− за која је посебним законом одређено да поступа Тужилаштво за организовани криминал или Тужилаштво за ратне злочине;
− тешко убиство (чл. 114 *Кривичног законика*), отмица (чл. 134 КЗ), приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију (чл. 185, ст. 2 и 3 КЗ), изнуда (чл. 214, ст 4 КЗ), фалсификовање новца (чл. 223, ст. 1 до 3 КЗ), прање новца (чл. 231, ст. 1 до 4 КЗ), неовлашћена производња и стављање у промет опојних дрога (чл. 246, ст. 1 до 3 КЗ), угрожавање независности (чл. 305 КЗ), угрожавање територијалне целине (чл. 307 КЗ), напад на уставно уређење (чл. 308 КЗ), позивање на насилну промену уставног уређења (чл. 309 КЗ), оружана побуна (чл. 311 КЗ), диверзија (чл. 313 КЗ), саботажа (чл. 314 КЗ), шпијунажа (чл. 315 КЗ), одавање државне тајне (чл. 316 КЗ), изазивање националне, расне и верске мржње и нетрпељивости (чл. 317 КЗ), повреда територијалног суверенитета (чл. 318 КЗ), удруживање ради противуставне делатности (чл. 319 КЗ), припремање дела против уставног уређења и безбедности Србије (чл. 320 КЗ), тешка дела против уставног уређења и безбедности Србије (чл. 321 КЗ), недозвољена производња, држање, ношење и промет оружја и експлозивних материја (чл. 348, ст. 3 КЗ), недозвољени прелаз државне границе и кријумчарење људи (чл. 350, ст. 2 и 3 КЗ), злоупотреба службеног положаја (чл. 359 КЗ), трговина утицајем (чл. 366 КЗ), примање мита (чл. 367 КЗ), давање мита (чл. 368 КЗ), трговина људима (чл. 388 КЗ) и узимање талаца (чл. 392 КЗ);
− спречавање и ометања доказивања (чл. 336, ст. 1 КЗ) ако је учињено у вези са кривичним делом из тач. 1 и 2 става 1 овог члана.

Под овим условима посебна доказна радња тајног надзора комуникације се може одредити и за следећа кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права (чл. 199 *Кривичног законика*), оштећење рачунарских података и програма (чл. 298, ст. 3. КЗ), рачунарска саботажа (чл. 299 КЗ), рачунарска превара (чл. 301, ст. 3 КЗ) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (чл. 302 КЗ).

Тајни надзор комуникације, предвиђен чл. 166, може бити одређен од стране суда (на образложен предлог ЈТ) уколико су испуњени ови услови и обухватиће надзор и снимање комуникације која се обавља путем телефона или других техничких средстава, или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки.

У овако дефинисаном системском простору за надзор комуникација, чак ни у последњем законском предлогу није обухваћен нумерационо сваки облик комуникације, већ се изискује за сваки њен облик посебно тумачење. Већ помињани, али и неки нови облици комуникационих карактеристика, на пример, МАЦ адресе уређаја који се користе, ИП адресе, прокси серверске маске, претраживачка историја одређеног корисника, историја крстарења интернетом, историја коришћења претраживачких сервиса (google, yahoo, krstarica), коришћење различитих социјалних мрежа и „клауд компјутинг“ могућности које оне пружају (комуникација и четовање у оквиру клауд окружења, похрањивање података у оквиру истих и сл.) тешко се могу обухватити оваквим решењима без опширнијих образлагања и објашњења.

Међутим, уколико је неопходно да се овакве одредбе унесу у законски текст, онда је потребно предвидети различите нивое услова у погледу прибављања наредби за издавање различитих комуникационих карактеристика, нпр. листинга мобилних телефона, или за прибављање евиденција у вези са информационо-комуникационим технологијама (ИКТ), од ИП и МАЦ адреса уређаја до мејлова и римејлера коришћених у комуникацији. У сваком случају, неопходно је да овакве наредбе доноси суд, али се у испуњавању услова за њих могу прописати различите одредбе. Могуће је предвидети и различите нивое судова за издавање различитих наредби, што такође може бити основ за њихово лакше прибављање. Такође, могуће је предвидети оне мере прописане *Конвенцијом* (у облику и са домашајем које она предвиђа) и на тај начин решити овај проблем.

Пракса Европског суда за људска права и најважнији стандарди у овој области

Према пракси ЕСЉП неопходно је да постоје одређени услови везани за имплементацију одреби о тајном надзору над комуникацијама.

Првенствено постављен стандард везан за чл. 8[48] ЕКЉП у пракси је у погледу одредби за тајни надзор комуникација одређен кроз принцип законитости „у складу са законом“, при чему се, с обзиром да су потписнице *Конвенције* и земље прецендентног права, узима у обзир најшире могуће тумачење појма закона. У овом смислу треба консултовати одлуку Круслин против Француске, од 24. априла 1990, према којој ЕСЉП узима у обзир да су судови држава чланица ти који су најкомпетентнији да тумаче норме националног законодавства, па је могуће да постоје („законски“) основи постојећи и у судској пракси (иако она не представља изворе права), или поступању органа гоњења, али се поставља питање квалитета тог основа. Дакле, чак и да није прописано законом и да је судска (и оперативна) пракса постојећа, могуће је и њу, условно речено, узети за правила поступања, посебно уколико је тако посматрају и судови. Ово представља још један стандард који се мора узети у обзир приликом тумачења случајева надзора комуникација. Могуће је да ће суд, у датом случају, утврдити да постоје неквалитетно постављене законске норме којима се неадекватно и несразмерно даје могућност „јавним властима“ да задиру у приватност грађана. Овакав је случај, на пример, са широким постављањем основа за надзор комуникације, не прописујући посебно различите мере које обухватају посебне елементе комуникационог корпуса, као што то ЦЕТС 185 одређује.

Такође, од круцијалног је значаја и да мере тајног надзора за грађане могу бити довољно „доступне и предвидиве“, формулисане у довољно значајном степену прецизности[49] како би грађани могли прилагодити своје понашање постојању оваквих мера које прете њиховој приватности. Овде је, поред Малоун, од значаја и одлука Аман против Швајцарске[50]. Кључни принцип је ексклузивна компетентност закона у ограничењу слобода, а оваква ограничења морају имати легитимне циљеве,

[48] Право на поштовање приватног и породичног живота: 1. Свако има право на поштовање свог приватног и породичног живота, дома и преписке; 2. Јавне власти неће се мешати у вршење овог права сем ако то није у складу са законом и неопходно у демократском друштву у интересу националне безбедности, јавне безбедности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, или ради заштите права и слобода других.

[49] У светлу кандидатуре за ЕУ, можда је значајно консултовати и одлуке Европског суда правде у Луксембургу. Тако се у одлуци *Österreichischer Rundfunk* (*the European Court of Justice Application* No. 35841/02, одлука од 7. децембра 2006, C-195/06; 2007/C 315/24) наводи да „свако ограничавање права на приватност мора бити формулисано са довољно прецизности како би се грађанима омогућило да своје понашање прилагоде оваквим нормама и захтевима предвидљивости“. За ову материју од значаја је и одлука S. and Marper v. United Kingdom, (*Applications* no. 30562/04 и 30566/04), од 4. децембра 2008.

[50] Amman v. Switzerland, пресуда од 16. фебруара 2000. У овом другом случају постављено је питање коришћења али и чувања података о надзору комуникација након дугог временског периода у различитим правним окружењима, када је више закона који се односе на материју измењено.

или да стреме једном од легитимних циљева одређених *Конвенцијом*, како је то у пресуди Аман против Швајцарске.

Основни услов за ограничење слобода и права, у смислу искључивања заштите предвиђене чл. 8 ЕКЉП, јесте да је то „неопходно као ограничење слобода и права у демократском друштву", као и да се то чини у сврху: заштите живота и здравља људи; заштите националне и јавне безбедности; заштите права других лица; спречавања немира и криминала; заштите економске снаге и безбедности земље. При том је од значаја и квалитет овлашћења предвиђених законом за државне органе у овом смсилу (овде је од значаја одлука Круслин против Француске). У сваком случају неопходно је да оваква мера буде предвиђена у складу са начелом *minus malum permittitur ut evitetur maius* (да се начини мање зло од зла које прети). Тумачење права на поштовање приватног и породичног живота мора бити схваћено најшире могуће, па се у ове оквире може унети и проширење на комуникације на послу (пресуда Њемец против Немачке[51]). За то је неопходно да случајеви буду релевантни и да за примену мере буду пружени адекватни разлози, праћени релевантном документацијом.

Посебно је интересантан стандард пружен у случају К. У. против Финске[52]. У овом случају је малолетник К. У. био шиканиран и узнемираван од стране непознатог извршиоца путем интернета. Ово је учињено на тај начин што је на једном сајту постављен његов број телефона са позивом да му се јаве особе које би га водиле и усмеравале у животу. Посебан вид шиканирања у овом случају представљало је и његово декларисање као младог геја коме је овакво усмеравање и вођење потребно од других, искусних, слично сексуално оријентисаних особа. У законодавству Финске није био предвиђен правни основ за откривање података о лицу које је поставило ове информације на дати сајт, па их полиција није могла прибавити. Оштећени К. У. је покренуо поступак пред ЕСЉП, па је судском одлуком утврђено кршење чл. 8 ЕКЉП и указано на околност да су полиција и други државни органи у обавези да поступају по извршењу кривичног дела и да су дужни да предузму све што је у њиховој моћи да би се дело расветлило. Такође, значајно је, у зависности од околности случаја и аспеката правног добра (односно аспекта приватности) које је угрожено, до које мере ће постојати могућност задирања државе у слободе и права[53]. Такође је веома значајно да и законски оквири омогуће расветљавање кривичних дела, а да не спречавају државне органе у поступању при расветљавању, нарочито у

[51] Niemietz v. Germany, (*Application* no. 13710/88), пресуда од 16. децембра 1992.

[52] Case of K. U. v. Finland (*Application* no. 2872/02), одлука од 2. децембра 2008.

[53] У том смислу интересантно је консултовати и одлуке August v. United Kingdom (dec.), no. 36505/02, одлука од 21. јануара 2003, као и M. C. v. Bulgaria, no. 39272/98, § 150, одлука од 4. децембра 2003.

случају жртава малолетних лица. При томе, неопходно је консултовати и околности осавремењивања стандарда у области ИКТ, о чему нарочито треба водити рачуна код ограничавања овлашћења органа, када су у питању мере предвиђене *Конвенцијом*[54]. Суд се у датом случају поставио као орган који констатује да је у случајевима извршења кривичног дела, посебно тамо где је жртва малолетник, неопходно да се органи гоњења понашају и поступају у складу са обезбеђивањем адекватне мешавине очувања права и слобода грађана, а да, са друге, ефикасно спроводе истраге.

Закључак

На основу приказаног може се закључити да наше законодавство пред проблемом регулисања тајног надзора комуникација, није у потпуности одговорило постављеним стандардима у овој области. Међутим, веома је индикативно да и земље Европске уније такође нису кадре да у потпуности одговоре оваквом изазову, посебно у имплементацији *Директиве о задржавању података*, услед реакција јавности, али и уставних судова земаља чланица. Наиме, уставни судови су утврдили повреде одредаба устава у случајевима покушаја примене закона који су имплементирали решења ове *Директиве* (Бугарска 2008, Немачка 2010, Чешка 2010, Пољска 2011, Мађарска 2011). Шта то законодавци правних система ових држава знају боље од нашег?

Проблеми третирања комуникација, у најопштијем смислу, могу довести до најразличитијих практичних препрека. Значајно је препознати могуће импликације описаних мера предвиђених *Конвенцијом*, и њихове облике имплементације у нашем законодавству. Према приказаном ипак можемо закључити да у нашем законодавству нису потпуно адекватно издиференциране све мере предвиђене *Конвенцијом*, а такође нису адекватно постављени ни услови за примену оних које су предвиђене. Покушало је са делимичним разликовањем услова за предузимање одређених мера и њихове проблемске структуре, кроз делимичну анализу комуникационе систематике. Дат је и приказ различитих схватања о конструкцији и схватању појма комуникација, са акцентом на околности које поједине земље препознају као значајне у имплементацији у кривичном поступку.

Посебно је интересантно укључити и анализу праксе ЕСЉП у овој области која се односи на примену чл. 8 ЕКЉП, а која успоставља стандарде у овој области, како у поступању органа гоњења и суда, тако и законодавца и актуелних, али и могућих будућих законских решења у

[54] За ове стандарде погледати: Christine Goodwin v. United Kingdom [GC], no. 28957/95, § 74, одлука од 11. јула. 2002.

овој области. Управо на овој равни покушали смо да, поред приказа актуелних чињеница и карактеристика мера и стандарда у њиховој примени, дамо и могуће алтернативе, уз критике постојећих решења.

Дакле, неопходно је издиференцирати мере предвиђене *Конвенцијом о ВТК*, предвидети наредбе о остваривању хитне заштите (или обезбеђења) одређених рачунарских података и наредбе о предаји тих података лицима која их имају у државини. Ова мера мора бити ограниченог трајања с обзиром на тешкоће које се везују за њену примену, па се може одредити краћи рок од оног предвиђеног у прописима ЕУ (180 дана). Код нас тај рок може бити, како је већ предвиђено, *Конвенцијом* – 90 дана. Ова врста мере мора имати посебан статус, с обзиром на личне податке и податке о комуникацијама који се овим путем откривају, а могуће је предвидети и различите нивое услова у случајевима „тешких кривичних дела" у односу на друга дела.

Када су у питању наредбе о парцијалним формалним елементима комуникације, од непроцењивог је значаја третирати ову меру као елемент комуникације и предвидети је као радњу коју наређује суд, уз испуњење формалних елемената за њену примену. Ово директно произлази из приказаних стандарда ЕСЉП.

Такође, потребно је предвидети посебне услове за примену мере претресања рачунара и рачунарских система и мрежа, и са тим везане могућности заплене података са њих и са њима повезаним уређајима. С обзиром да је ова мера предвиђена *Конвенцијом*, значајно ју је предвидети као посебан облик претресања. Предвиђеност *Конвенцијом* није једини разлог, већ се може појавити и проблем одузимања неког важнијег сервера у држави. Тада је много економичније и целисходније урадити клон хард диска уређаја који би требало одузети, него одузети цео уређај. У таквим случајевима подаци се налазе само на хард диску овог сервера а не у RAM меморији или матичној плочи и евентуално кабловима уређаја. Могуће је предвидети и мере које препостављају претраге у повезаним системима.

У вези са мером пресретања комуникација у реалном времену, или тајним надзором (термин из предлога нацрта ЗКП), поред приказане проблематике и стандарда које би законодавац морао предвидети интересантно би било обухватити и могућност дешифровања енкодираних комуникација. У овом случају, према правилима струке, морали би се употребити и уређаји или софтверски пакети способни да открију и отклоне начин и метод шифровања комуникација.

Литература:

1. *Директива о приватности и електронским комуникацијама*, (2002). „*Directive 2002-22-EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services*“, Official Journal of the European Communities, L108/51-77, од 24. 4. 2002.
2. Bošković, A. (2003). *Radnje policije u pretkrivičnom postupku po zahtevu i naredbi drugih subjekata,* NBP: Nauka – Bezbednost – Policija, год. 8, бр. 2, стр. 145-156.
3. Голић, Д., Цудовић, М., (2010). *Упоредноправни приказ примене мере надзора и снимања комуникација*, Безбедност, год. 52, бр. 3, стр. 242-250.
4. Marinković, D., Branković, A., Milojković, B., (2009). *Computer data search and comparison – General reviews and application in crime investigation.* NBP – Žurnal za kriminalistiku i pravo, vol. XIV, бр. 1, стр. 63-78.
5. Маринковић, Д., Ђурђевић, З., (2010). *Рачунарско претраживање и упоређивање података у откривању и доказивању кривичних дела*, Ревија за криминологију и кривично право, вол. 48, бр. 3, стр. 245-264.
6. Мијалковић, С., Манојловић, Д., (2008). *Прибављање листинга телефонског претплатничког броја грађанина – контроверзе у раду националних система безбедности*, Страни правни живот, год. 52. бр. 2, стр. 150-168.
7. Милидраговић, Д., (2010). *Правни основ надзора комуникација путем телефонског листинга,* Право и форензика у криминалистици (зборник радова), Крагујевац, стр. 217-227.
8. Милошевић, М.; Бошковић, А. (2003) *Приручник за кривично процесно право*, Београд : Полицијска академија,
9. Николић Комлен, Л. et al. (2010). *Сузбијање вискотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца, АЕЦИД, Београд.
10. *Приручник за тренинг тужилаца и судија у области високотехнолошког криминала*, (2009). Удружење јавних тужилаца и заменика јавних тужилаца Србије, АТЦ, Београд.
11. Ранђеловић, Д., Делија, Д., Поповић, Б., (2009). *EnCase Форензички алат*, Безбедност, год. 51, бр. 1-2, стр. 286-313.
12. Тањевић, Н., (2009). *Компјутерски криминал – правна заштита на националном нивоу*, Безбедност, год. 51, бр. 1-2, стр. 152-167.
13. Урошевић, В., (2009). *Злоупотреба платних картица и рачунарске преваре*, Правни информатор, год. XII, бр. 9, Београд.

14. Урошевић, В., Ивановић, З., (2010а). *Злоћудни програми – malware*, ФОРУМ БИСЕЦ 2010, Конференција о безбедности информација, Београд: Метрополитан универзитет, ФИТ, стр. 64-71.
15. Урошевић, В., Ивановић, З., (2010б). *Фокуси у сарадњи криминалистичких полиција са аспекта Националног централног бироа ИНТЕРПОЛ-а Београд*, Безбедност, год. 52, бр. 1, стр. 62-73.
16. Amman v. Switzerland, пресуда од 16. фебруара 2000.
17. August v. United Kingdom (dec.), no. 36505/02, одлука од 21. јануара 2003.
18. Copland v. United Kingdom (*Application no. 62617/00*), пресуда од 3. априла 2007.
19. Christine Goodwin v. United Kingdom [GC], no. 28957/95, § 74, одлука од 11. јула 2002.
20. K. U. v. Finland, (*Application no. 2872/02*), одлука од 2. децембра 2008.
21. M. C. v. Bulgaria, no. 39272/98, § 150, одлука од 4. децембра 2003.
22. Malone v. United Kingdom **(***Application No. 8691/79)*, пресуда од 2. августа 1984.
23. Kruslin v. France, (*Application no. 11801/85*), пресуда од 24. априла 1990.
24. Kopp v. Switzerland, *13/1997/797/1000*, пресуда од 25. марта 1998.
25. Niemietz v. Germany, (*Application No: 13710/88*), пресуда од 16. децембра 1992.
26. Osterreichischer rundfunk, (*the European Court of Justice Application No. 35841/02*), одлука од 7. децембра 2006, C-195/06; 2007/C 315/24;
27. S. and Marper v. United Kingdom (*Application no. 30562/04 и 30566/04*), одлука од 4. децембра 2008.
28. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.19. доступан 14. 3. 2010.
29. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p. 23, последњи пут приступљено 8. 6. 2011.
30. http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm последњи пут приступљено 31. 1. 2010.
31. *Приручник за обуку судија у супростављању кибер криминалу* доступан на интернет страници: http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_ en.pdf дана 26. 1. 2010.
32. www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf доступан 29. 1. 2010.
33. *Convention on Cybercrime – Explanatory Report*, http://conventions.coe.int/treaty/en/reports/html/185.htm
34. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF последњи пут приступљено 11. 7. 2011.

35. http://www.netzpolitik.org/2009/ticker-muendliche-anhoerung-zur-vorratsdatenspeicherung/ доступан 29. 3. 2010.
36. http://www.sofiaecho.com/2009/12/18/831890_the-eyes-have-it доступан 29. октобра 2010.
37. http://www.mpravde.gov.rs/cr/articles/zakonodavna-aktivnost/ последњи пут приступљено 21. 7. 2011.

Analysis of Legislative Norms Regarding Communication Surveillance and of the Praxis of European Court Of Human Rights

***Abstract**: Communication surveillance is a relatively new measure in the Serbian legal system and with the development of new technologies applicable to various types of communication, new problems are emerging very fast. Of course this is not the case exclusively in Serbia, but much further. Similar problems emerge in the EU, and Serbia as a signatory of the European Convention on Human Rights, has to oblige with the case law of the European Court of Human Rights in Strassbourg (ECHR). Standards made in this area in the laws of the EU countries are derived from the rules made by case law of ECHR. Regardless of the depicted trends and occurences in this sphere, Serbian legislation has not been lately following the lead of European legislators. Authors are analyzing facts and circumstances in connection to legal defining and proscribing of the measure of communication surveillance, giving a parallel comparative legal analysis of ECHR and Luxemburg Court of EU. The analysis also includes considerations reagrding some articles from the draft Act on Criminal Procedure in Serbia pertaining to communication surveillance. The purpose of the analysis is to suggest certain regulations de lege ferenda in Serbia.*

***Key words**: secret communication surveillance, European Court of Human Rights, human rights, wiretaping, police.*