Прегледни чланак 343.14:004.6
doi:10.5937/zrpfns48-5898

Милана Писарић, асистент
Универзитет у Новом Саду
Правни факултет у Новом Саду

МЕРА ХИТНОГ ЧУВАЊА УСКЛАДИШТЕНИХ РАЧУНАРСКИХ ПОДАТАКА[1]

Сажетак: *Услед развоја и свеприсутности информационих технологија у свакодневном животу, повећан је и број криминалних активности које су учињене коришћењем рачунарских система и мрежа. Трагови учињених кривичних дела у вези са злоупотребама информационих технологија налазе се у облику електронских записа, односно рачунарских података који настају или као резултат радњи извршиоца или су аутоматски створени и ускладиштени у рачунарском систему/мрежи. Међутим, рачунарски подаци су веома подложни изменама, па је неопходно да се на одговарајући начин обезбеди њихова заштита. За стварање одговарајућег правног оквира за супротстављање овим изазовима, у прописима кривичног процесног права потребно је утврдити одговарајућа овлашћења надлежних органа у циљу прикупљања и обезбеђења рачунарских података о учињеном кривичном делу и учиниоцу који могу бити искоришћени као електронски доказ у кривичном поступку.*

Кључне речи: *рачунарски подаци, хитно чување, електронски докази.*

1. Уводна разматрања

Рачунарски подаци који се складиште, обрађују и преносе у рачунарским мрежама и системима, који би могли бити од значаја као електронски доказ у кривичном поступку, по природи су непостојани и подложни изменама, а како би се створио основ да се захтева заштита ових података до добијања овлашћења надлежних органа да приступе тим подацима у складу са законом, у процесно законодавство је потребно увести одређене мере

[1] Овај рад је настао као резултат научно-истраживачког рада на Пројекту „Теоријски и практични проблеми стварања и примене права (ЕУ и Србија)“ чији носилац је Правни факултет у Новом Саду.

и радње у циљу да се спречи губитак или измена тих рачунарских података[2]. Како је Република Србија потписала Конвенцију Савета Европе о високотехнолошком криминалу[3], која у члану 14. став 2. предвиђа обавезу држава потписница да у својим прописима предвиде одговарајућа процесна овлашћења надлежних органа потребна не само за откривање кривичних дела високотехнолшког криминала и гоњење учинилаца тих дела (у смислу одредаба чланова 2. до 11. Конвенције),него и других кривичних дела која су извршена путем рачунарског система као и за прикупљање доказа у електронском облику за сва кривична дела, полазну основу за разматрање могућег легислативног решења за хитну заштиту ускладиштених рачунарских података чине управо одговарајући чланови ове Конвенције[4].

2. Одредбе Конвенције о високотехнолошком криминалу које се односе на хитно чување рачунарских података

Члан 16. Конвенције предвиђа да је свака страна уговорница у обавези да усвоји законодавне и друге мере потребне да се њеним надлежним органима омогући да нареде или на други сличан начин обезбеде експедитивно чување одређених рачунарских података, укључујући податке о саобраћају остварених комуникација, који су ускладиштени у оквиру рачунарских система, нарочито у ситацијама када постоји опасност да су рачунарски подаци који би могли бити електронски доказ у конкретној кривичној ствари посебно осетљиви у смислу губитка или измена. Уколико је предвиђено да се обезбеђење података остварује издавањем наредби лицу ради чувања одређених ускладиштених рачунарских података који су у поседу или под контролом тог лица, потписница је дужна да усвоји потребне законодавне и друге мере како би се то лице обавезало да сачува и одржи интегритет рачунарског података за потребни временски период, а најдуже до деведесет дана (са могућношћу продужења тог периода за још деведест дана). Наиме, сврха прописивања обавезе чувања података за одређени временски период је да се омогући надлежним органима да у одговарајућој процедури захтевају и добију дозволу, односно одобрење да им се ти подаци учине доступним и да се упознају са њиховом садржином. При то-

[2] Више о електронским доказима, видети: Т. Лукић, „Дигитални докази“, *Зборник радова Правног факултета у Новом Саду* 2/2012,177-192*;* М. Писарић, „Електронски записи као доказ у кривичном поступку“, *Зборник радова Правног факултета у Новом Саду* 2/2009, 519-536.

[3] Закон о потврђивању Конвенције о високотехнолошком криминалу („Сл.гласник РС–Међународни уговори“, бр. 19/2009).

[4] Више о процесним овлашћењима надлежних органа, видети: М. Писарић, „Потребни нормативни одговор на проблеме откривања и доказивања дела високотехнолошког криминала“, *Зборник радова Правног факултета у Новом Саду* 1/2013, 291-307.

ме наредба се може издати сваком лицу које у поседу, односно под контролом има потребне рачунарске податке, дакле, било ком физичком и било ком правном лицу.

Осим што је потребно надлежним органима дати овлашћење да захтевају од лица да хитно и у најкраћем року обезбеди на одговарајући начин од губитка, односно измене потребне рачунарске податке и да их чува одређени временски период, да би такво поступање имало смисла и да се не би угрозили интереси истраживања конкретног кривичног случаја, држава потписница треба да усвоји и такве законодавне и друге мере које су потребне да би се лице могло обавезати да поступање по таквом налогу чува као поверљив податак одређени временски период који је предвиђен законом.

Члан 16. заправо се односи на привремену меру која треба да омогући надлежним државним органима да наређе тренутно чување података који се већ налазе ускладиштени у рачунарском систему, као својеврсно „замрзавање“ у неизмењеном облику. Ова мера се може односити како на податке о саобраћају, тако и на садржај остварене комуникације, и може обухватити податке у поседу пружалаца услуга електронских комуникација, али и било ког другог физичког или правног лица. Мера хитног чувања ускладиштених рачунарских података се односи на тачно одређене рачунарске податке који могу бити од користи за конкретан случај, односно употребљени као електронски доказ у кривичном поступку, а не на неодређене рачунарске податке. Интегритет потребних рачунарских података иначе може бити обезбеђен и предузимањем неких других радњи и мера, пре свега претреса рачунара и рачунарске мреже и одузимања података (на које се односи члан 19. Конвенције) или издавањем налога за предају података (на које се односи члан 18. Конвенције), али процедура за предузимање тих радњи често захтева више времена и сложенија је (захтева се оправдање за предузимање мере, одобрење суда, обавештавање осумњиченог и његова одговарајућа права) у односу на експедитивно чување података које има карактер хитне мере. Дакле, имлементација члана 16. Конвенције има за циљ да надлежни органи захтевају „замрзавање“ података и тиме њихово обезбеђење од губитка и/или измена за време које је потребно док се добије одобрење за предузимање радњи из чланова 18. и 19. Конвенције, односно одговарајућих радњи и мера којима се остварује увид у рачунарске податке у складу са прописима држава потписница.

На одредбу члана 16. Конвенције надовезује се ***члан 17. Конвенције*** којим се додатно уређује експедитивно чување и делимично откривање података о саобраћају остварених комуникација. Према том члану, државе потписнице су дужне да у вези са подацима о оствареном саобраћају, који се по хитном поступку чувају (а применом мере на основу члана 16. Кон-

венција), усвоје законодавне и друге мере неопходне да се остваре два циља: а) да се обезбеди експедитивно чување података без обзира на то да ли је један или више пружалаца услуга електронских комуникација укључено у пренос комуникације, те б) да се надлежном органу открије довољно података о саобраћају остварених комуникација потребних за утврђивање идентитета свих пружалаца услуга, као и путање којом се комуникација остварује.

Предвиђање обавеза на основу члана 17. Конвенције је потребно из разлога што често у остварењу електронских комуникација учествује више од једног оператора, па је неопходно дати овлашћење надлежним органима да свима, за које се утврди да је коришћењем њихових услуга, односно мрежа остварена комуникација, издају наредбу за откривање довољно података о саобраћају на основу којих се тачно може утврдити извор и одредиште комуникације, а како би, потом, свима њима издали наредбу за хитно чување рачунарских података у складу са чланом 16. Конвенције.

3. Разлике у односу на задржавање података

У законодавству већине европских држава постоје прописи на основу којих су пружаоци услуга електронских комуникација дужни да одређене податке о саобраћају задржавају за прописани период времена и да те податке учине доступним надлежним органима ради откривања и доказивања тешких кривичних дела[5]. Задржавање података о саобраћају односи се на формална обележја а не на садржај електронских комуникација и обавезује само правна лица која су регистрована за пружање услуга у овој области[6].

Конвенција о високотехнолошком криминалу не познаје задржавање података у наведеном смислу и стога се не подразумева да је члан 16. имплементиран на одговарајући начин уколико у држави постоје само прописи који установљавају обавезу задржавања података, а не и овлашћење надлежних органа да захтевају чување одређених рачунарских података на експедитиван начин, јер задржавање података није исто што и њихово хитно чување у смислу одредаба Конвенције. Наиме, мера хитног чувања податка је у односу на задржавање података ужи појам, јер се ова мера односи на чува-

[5] Државе чланице Европске уније су биле дужне да такве прописе усвоје у складу са Директивом ЕУ 2006/24 о задржавању података (*Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF).

[6] Више о задржавању података видети: Т. Лукић, „Прислушкивање и задржавање телекомуникационих података“, *Правни живот* 9/2011, 837-853; Т. Бугарски, *Доказне радње у кривичном поступку*, друго измењено издање, Нови Сад 2014, стр. 50-56.

ње тачно одређених рачунарских података потребних у конкретној кривичној ствари који су у време подношења захтева за њихово чување већ ускладиштени у рачунарском систему, а не на чување неких неодређених података који би могли имати значаја за спречавање или откривање кривичних дела уопште, нити пак, на будуће чување података који ће тек настати почевши од момента издавања наредбе. Истовремено, мера хитног чувања податка је у односу на задржавање податка и шири појам, по томе што се не односи само на податке о претплатнику/кориснику услуга и податке о саобраћају, него обухвата и податке који се односе на садржај комуникације. Осим тога, мера обавезује не само пружаоце услуга него се издавањем наредбе може наредити било ком физичком или правном лицу које у поседу/ под контролом има потребне рачунарске податке да те податке и сачува. Такође, мера хитног чувања рачунарских података се може одредити у односу на било које кривично дело. Конвенција изричито у члану 14. ставу 2. предвиђа да је експедитивно чување података могуће захтевати не само у вези са кривичним делима у смислу Конвенције, него ради обезбеђења електронског доказа у кривичном поступку за сва кривична дела, невезано за њихову тежину, док је у Директиви о задржавању података заступљен принцип пропорционалности (приступ подацима о саобраћају остварених комуникација је могућ само у вези са истраживањем тешких кривичних дела).

4. Потребни нормативни елементи за правилну имплементацију одговарајућих одредаба Конвенције

Анализом прописа појединих држава потписница Конвенције, а узимајући у обзир одређене критеријуме, могуће је донети закључак о нивоу имплементације члана 16. и 17. Конвенције у њиховим законодавствима. При томе, могу се узети у обзир следећи критеријуми: да ли се експедитивно обезбеђење потребних рачунарских података остварује кроз меру хитног чувања ускладиштених рачунарских података или на други одговарајући начин, односно предузимањем неке друге радње и мере; да ли су надлежни органи овлашћени да издају наредбу било ком физичком или правном лицу које има у поседу/под контролом потребне рачунарске податке; да ли је меру могуће одредити у вези са било којим кривичним делом и у односу на било који рачунарски податак.

Што се тиче ***основа за предузимање мере*** хитног чувања ускладиштених рачунарских података, око половине држава потписница су у својим прописима предвиделе одредбе које се изричито односе на ову меру[7].

[7] Следеће државе потписнице су у својим законодавствима предвиделе специфична овлашћења у циљу имплемнтације члана 16. Конвенције: Албанија у члану 299/а Закона о

У осталим државама не постоје специфичне одредбе у смислу овлашћења надлежних органа да издају наредбу да се подаци хитно чувају, јер је законодавац вероватно пошао од тога да се сврха мере (а то је тренутно и експедитивно чување потребних рачунарских података) може остварити предузимањем постојећих радњи и мера, међутим, овакво опредељење законодавца не значи аутоматски да државе коју су поступиле на такав начин нису имплементирале члан 16. Конвенције. Наиме, наведени члан обавезује државу потписницу да у законодавству предвиди овлашћење које треба да омогући надлежним органима да нареде или на „*други сличан начин обезбеде*" експедитивно чување одређених рачунарских података. Управо таква формулација („на други сличан начин") даје основ за закључак да се у смислу Конвенције не тражи прописивање специфичних овлашћења за хитно чување подтака уколико се циљ може остварити нпр. вршењем претреса или привременог одузимања предмета или предузимањем других радњи које имају за циљ да се обезбеде електронски докази. Ипак, потребно је да је тај циљ могуће остварити:

1. у вези са било којим кривичним делом;
2. у односу на било које физичко или правно лице;
3. у погледу свих рачунарских података;
4. на експедитиван начин.

Из наведеног следи да уколико у држави није изричито прописана као привремена мера могућност надлежног органа да нареди хитно чување ускладиштених рачунарских података, може се сматрати да је држава испунила обавезу из члана 16. Конвенције уколико се рачунарски подаци који могу бити употребљени као електронски докази могу обезбедити под наведеним условима и неком другом мером или радњом. Ипак, у тачки 160. Извештаја, који је Комитет министара Савета Европе усвојио уз Конвенцију, дата је препорука потписницама да размотре могућност изричитог прописивања овлашћења и процедура којим се лицу у поседу података наређује експедитивно чување података у смислу члана 16. Конвенције[8]. Дакле, иако се сврха може остварити применом неких других овлашћења

кривичном поступку; Бугарска у члану 159. Закона о кривичном поступку; Финска у поглављу 4. одељак 4б и ц Закона о радњама процесне принуде; Француска у члану 60-2. Закона о кривичном поступку; Мађарска у члану 158/А Закона о кривичном поступку; Италија у неколико одредаба Закона бр.92/2008; Летонија у члану 191. Закона о кривичном поступку; Молдавија у члану 7. Закона о спречавању и борби против високотехнолошког криминала; Холандија у члану 126. Закона о кривичном поступку; Норвешка у члану 215а Закона о кривичном поступку; Португалија у члану 12. Закона о високотехнолошком криминалу; Румунија у члану 54. Закона 161/2003; Словачка у члану 90. Закона о кривичном поступку; САД у наслову 18.одељак 2703(ф) Савезаног закона о кривичном поступку.

[8] http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

надлежних органа, сматра се да се хитно чување ускладиштених рачунарских података најефикасније може остварити прописивањем специфиних овлашћења надлежних органа.

У погледу ***врсте кривичних дела*** у односу на које се мера може одредити, битно је истаћи да Конвенција не предвиђа ограничење, у смислу да се односи на одређену категорију кривичних дела, нпр. само на тешка кривична дела или само кривична дела против безбедности, целовитости или доступности рачунарских података, већ је приликом имплементације потребно предвидети да се хитно чување података може обезбедити у вези са било којим кривичним делом (као уопште све процесне одредбе у смислу члан 14. став.2. Конвенције). Овај захтев је испуњен у већини држава потписница, уз постојање одређених допунских услова за одређивање мере у случају тешких кривичних дела. Међутим, за државе које се у имплементацији члана 16. ослањају само на прописе о задржавању података у смислу Директиве ЕУ у којој је заступљен принцип пропорционалности (приступ подацима о саобраћају остварених комуникација је могућ само у вези са истраживањем тешких кривичних дела), не би се могло констатовати да су на одговарајући начин испуниле обавезу предвиђену у члану 16. Конвенције.

Рачунарски подаци који се могу користити као електронски доказ могу бити у поседу како физичког, тако и правног лица, па је потребно да се експедитивно чување тих података од губитка/ оштећења може наредити према ***свим лицима***. Електронски записи за потребе кривичног поступка у највећем броју случајева су у поседу пружалаца услуга електронских комуникација, и у већини држава су предвиђена законска овлашћења, понекад допуњена аранжманима о сарадњи[9], који омогућавају надлежним органима да наређе провајдерима да сачувају податке или да приступе подацима у поседу пружалаца услуга. Док је обавеза задржавања података ограничена на пружаоце услуга, хитно очување података се може наредити и другим правним а тако и физичким лицима. Поједине државе стога нису испуниле обавезу предвиђену у члану 16. Конвенције јер издавање наредбе за извршење ове мере ограничено само на провајдере. Осим тога, у ве-

[9] У појединим државама постоје и споразуми о сарадњи надлежних државних органа са пружаоцима електронских комуникација. Тако примера ради, у Литванији у складу са споразумом највећи провајдер (*ProWeb)* омогућава надлежним државним органима приступ подацима о саобраћају остварених комуникација и о претплатницима на услуге које провајдер пружа. У Норвешкој домаћи провајдери имају отворене онлајн центар за пружање информација по захтеву полиције а и транснационалне компаније провајдери поступају по захтеву полиције под одређеним условима, док су са одређеним пружаоцима услуга електронских комуникација закључени споразуми о употреби специјалних филтера за приказе дечје порнографије у рачунарској мрежи.

ћини држава у складу са чланом 16. став 3. Конвенције је предвиђено да физичко или правно лице коме је издата наредба за очување података има дужност да предузимање такве мере чува као тајну. Тако у Норвешкој, појединац на кога се односе подаци који су очувани мора бити о предузимању мере обавештено најкасније до тренутка када надлежни органи стекну право приступа подацима, осим уколико суд не одлучи другачије.

У погледу ***врсте ускладиштених рачунарских података*** чије хитно чување се обезбеђује предметном мером, у већини држава потписница мера се односи на све податке (подаци о претплатнику, те подаци о саобраћају и садржају остварених комуникација), са изузетком Јерменије и Украјине у којима се мера може одредити само у погледу података о саобраћају остварених комуникација, док се у Немачкој штавише посебно регулише одузимање података о саобраћају а посебно о садржају остварених комуникација. Осим тога готово све потписнице (осим Јерменије, Немачке, Норвешке и САД) се такође у имплементацији члана 16. Конвенције ослањају на обавезу задржавања података, с тим што се обавеза односи само податке о саобраћају али не покрива податке о садржају комуникације на које се такође односи члан 16. Конвенције, па се за те државе не може сматрати да су у целости импленетирале овај члан.

Суштина члана 16. Конвенције је да се омогући ***експедитивно чување*** података које се заснива на потреби да се хитно предузму мере како би се обезбедили подаци у случају да постоји опасност да би исти у временском периоду, у оквиру ког се реализују формалне процедуре за добијање приступа подацима, могли бити измењени или уништени или постати недоступни. Мера хитног очувања података наређена пружаоцу услуга или другом физичком или правном лицу које има приступ подацима је мера привременог карактера која би требало да буде наређена без одлагања и тиме да омогући да се подаци не изгубе, односно не измене за време које је потребно да се од суда добије одобрење за приступ и одузимање података. У државама у којима постоје посебне законске одредбе, захтев да постоји могућност за предузимање ове хитне мере је испоштован, јер у тим системима јавни тужилац (у већини земаља) или полиција (у појединим земљама) или било који државни орган (што је случај у САД), може наредити да се хитно сачувају ускладиштени рачунарски подаци у вези са истраживањем било ког кривичног дела. Међутим, то не значи да у државама у којима не постоје посебне одредбе којима би се регулисала ова хитна мера није испоштована обавеза из члана 16. Конвенције. Наиме, у државама у којима се друге радње и мере користе, процедура се обично своди на претходно добијање судког одобрења за предузимање претреса рачунарског система (за шта је потребно некад 24 часа а некада и неколико дана), па је

зато потребно услове за предузимање тих других радњи у циљу очувања података не поставити сувише рестриктивно. Тако би, примера ради, у државама у којима се обезбеђење електронских доказа остварује предузимањем претреса рачунара, требало предвидети да у изузетно хитним случајевима, пре добијања судског одобрења за приступ подацима, чување тих података може наредити и јавни тужиац, па и полиција.

5. Имплементација одговарајућих одредаба Конвенције у законодавству појединих држава

У ***Италији*** су изменама Законика о кривичном поступку из 2008. године[10] у процесном законодавству измењене или унете одредбе које имају за циљ да омогуће предузимање хитних мера за обезбеђење електронских доказа. Тако, на основу члана 244. ЗКП-а, који се односи на преглед рачунарског система, судска полиција може наредити предузимање свих потребних техничких мера у циљу експедитивног чувања података од измене или губитка, а на основу члана 254бис, који се непосредно односи на издавање наредбе за хитно чување података, судска полиција може и пружаоцима телекомуникационих услуга наредити да сачувају у неизмењеном облику податке о саобраћају остварених комуникација за потребе конкретног случаја до добијања одобрења од стране суда за одузимање тих података. За предузимање ових мера, по правилу је потребно одобрење суда, али ако то налажу разлози изузетне хитности или у случају *in flagranti*, судска полиција може по наредби јавног тужиоца захтевати од било ког физичког или правног лица „замрзавање у неизмењеном облику“ свих врста рачунарских података. Осим тога, полицији је дато и овлашћење на основу Закона о заштити података[11]. Наиме, на основу члана 132. Закона телекомуникациони оператери и други пружаоци услуга електронских комуникација дужни су да чувају податке о саобраћају остварених комуникација за период до 30 месеци за потребе кривичног поступка, па уколико су ти подаци потребни у предистражном поступку за откривање или спречавање конкретног кривичног дела, полиција може захтевати од провајдера да их обезбеде. Мера може трајати најдуже деведесет дана а из оправданих разлога се њено трајање може продужити до максимално шест месеци. Наиме, у оквиру истражних активности судска полиција и финансијска полиција могу тражити од јавног тужиоца да изда наредбу провајдерима за пружање рачунарских података потребних за откривање кривичног дела и

[10] http://www.altalex.com/index.php?idnot=41643.

[11] *Codice in materia di protezione dei dati personali. (GU n.174 del 29-7-2003 - Suppl. Ordinario n. 123),* http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta =2003-07-29&atto.codiceRedazionale=003G0218&currentPage=1.

учиниоца. Након што утврди да су испуњени законски услови, јавни тужилац издаје наредбу на основу члана 256.ЗКП коју одобрава суд. Судска полиција потом обавештава пружаоца Интернет или других јавно доступних телекомуникационих услуга који поступајући по наредби предају полицији претходно сачуване податке а које полиција доставља надлежном суду.

У ***Шпанији*** процесно законодавство не садржи одредбе о чувању рачунарских података на експедитиван начин. У складу са прописима ЕУ о задржавању података постоји обавеза за све пружаоце електронских услуга да задржавају рачунарске податке о саобраћају остварених комуникација и податке о кориснику услуга, а уз судско одобрење надлежни органи могу добити приступ задржаним подацима. Међутим, подаци се могу добити само ако су у вези са кривичним делима која су учињена употребом рачунарских система. Дакле, Шпанија није имплементирала одредбу члана 16. Конвенције на одговорајући начин, због тога што се односи само на податке о саобраћају остварених комуникација а не на њихов садржај, што се подаци могу тражити само од пружалаца услуга а не било ког физичког или правног лица и то не у вези са свим кривичним делима. Такође, Шпанија није имплементирала ни одредбу члана 17. Конвенције јер не постоје специфичне одредбе у погледу експедитивног чувања и делимичног откривања података о саобраћају комуникација у процесном законодавству а прописивањем обавеза пружалаца услуга елеконтрских комуникација да задржавају податке о саобраћају и о кориснику услуге не омогућава надлежним органима откривања и доказивања кривичних дела да траже и добију приступ потребним рачунарским подацима у вези са свим, већ само у погледу тешких кривичних дела.

На основу члана 12. Закона о компјутерском криминалу[12] ***у Португалији*** суд може издати наредбу за хитно чување одређених рачунарских података (укључујући и податке о саобраћају комуникација) потребних за кривични поступак, уколико постоји опасност да би они могли бити измењени, изгубљени или недоступни. У изузетним ситуацијама, наредбу може издати и полиција, али је дужна да у најкраћем року о томе обавести суд. Наредба обавезно садржи опис података (врсту) које треба сачувати, порекло и одредиште тих података уколико су познати (у погледу података о саобраћају комуникација) и временски период за који је податке потребно сачувати. Законодавац прописује да се може тражити чување података у трајању од највише три месеца, али истовремено предвиђа могућност обнављања, тј.продужења трајања мере, па иста може трајати до годину дана од издавања наредбе. Након издавања наредбе, физичко или правно лице које има приступ или контролу над потребним подацима је дужно да од-

[12] http://www.wipo.int/wipolex/en/text.jsp?file_id=181616.

мах сачува захтеване податке и да их обезбеди од измене/уништења док надлежним органима од стране суда не буде одобрен приступ сачуваним подацима (али само у оквиру временског периода који је одређен наредбом). Осим тога, у члану 13. Закона предвиђена је обавеза за пружаоце услуга електронских комуникација да полицији открију податке на основу којих се може утврдити идентитет других провајдера чије услуге су коришћене у оствареној комуникацији.

У ***француском Законику о кривичном поступку***[13] не постоји специфична одредба о хитном чувању рачунарских података али се у оквиру овлашћења судске полиције да по наредби јавног тужиоца изврши претрес рачунара и нареди предавање рачунарских података, може захтевати од лица које у поседу има потребне податке, не само да на експедитиван начин сачува те податке о саобраћају остварене комуникације, него и да делимично полицији открију одређене податке (члан 56. ЗКП). На основу члана 60-2 ЗКП сва правна лица су дужна да полицији открију све ускладиштене рачунарске податке потребне за истраживање конкретног случаја. Осим тога, судска полиција може, по налогу јавног тужиоца а по претходном одобрењу судије за људска права, да захтева од пружалаца електронских комуникација да предузму све потребне техничке мере да се садржај рачунарских података чува и то за период од најдуже годину дана. Лице које без оправданог разлога одбије да поступи по наредби може се казнити новчаном казном у износу од 3750 еура.

Иако ***у Немачкој*** не постоје специфичне одредбе које се односе на хитно чување ускладиштених рачунарских података, чланови 16. и 17. Конвенције су имплементирани на одговарајући начин је немачки Законик о кривичном поступку[14] садржи одредбе чијом применом се омогућава да се „на други сличан начин“ у смислу формулације из Конвенције обезбеде потребни подаци. Конвенција је имплементирана кроз одредбе ЗКП-а које се односе на обезбеђење и одузимање предмета уопште, као и одредбу члана 100г ЗКП који даје основ за хитно чување података о саобраћају у складу са принципом сразмерности.

Лице које у поседу има предмете (и рачунарске податке) који су од значаја за кривични поступак, између осталог и рачунарске податке, дужно је да их преда полицији (члан 94.ЗКП). За одузимање предмета (и рачунарских података) потребна је, по правилу, наредба суда[15]. Поред тога,

[13] http://www.legifrance.gouv.fr/Traductions/Liste-des-traductions-Legifrance.

[14] *Strafprozessordnung*, http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0430.

[15] Судску наредбу је у пракси могуће добити на експедитиван начин јер су организовани тзв. позивни центри у којима се судије ротирају па се наредба издаје у кратком

законодавац предвиђа да у изузетним ситуацијама када није могуће добити одобрење суда у довољно кратком временском периоду, наредба јавног тужиоца или полиције може бити довољна за одузимање предмета. У погледу рачунарских података, изузетна ситуација би се односила на постојање опасности од њиховог губитка/измене. Наиме, уколико јавни тужилац или полиција процени да постоји опасност да би подаци важни за поступак могли бити измењени или уништени, овлашћени су и дужни да услед таквих разлога хитности поступе и нареде одузимање података ради њиховог обезбеђења. Законик не предвиђа никакава ограничења у погледу лица према којима се наредба може издати нити у погледу којих кривичних дела се подаци могу чувати и одузети. Из свега наведеног, може се закључити да Немачка јесте имплементирала одредбе члана 16. Конвенције обезбеђујући алтернативни начин за експедитивно обезбеђење рачунарских података.

Што се, пак, тиче података о саобраћају у поседу пружалаца услуга електронских комуникација, примењује се члан 100г ЗКП, при чему се примењује принцип сразмерности и предвиђена су поједина ограничења у погледу приступа тим подацима. Наиме, ако постоји основ сумње да је лице (извршилац, саизвршилац, подстрекач или помагач) извршило кривично дело од изузетног значаја у конкретном случају, а нарочито ако се ради о кривичним делима која су наведена у члану 100а (у погледу који се може одредити посебна доказна радња пресретања комуникација) или покушало извршење таквог дела, у случају да је покушај кажњив, или је извршило било које кривично дело употребом рачунарског система[16], подаци о саобраћају (и то само они у складу са чланом 96. и 113а Закона о телекомуникацијама) могу се захтевати од провајдера и без знања и сагласности корисника услуга[17]. Осим што постоје ограничења у погледу кривичних дела за која се мера може наредити, Законик предвиђа и да се у складу са принципом сразмерности, потребни подаци могу овако прикупити само ако се

временском периоду. Исто тако, дежурства су организована и у јавном тужилаштву и полицији, па систем ефикасно функционише.

[16] Ова одредба се, дакле, може применити у свим случајевима када је је кривично дело почињено употребом телекомуникационих средстава, без обзира на то да ли се ради о тешком кривичном делу или делу малог значаја, нпр. када су електронска пошта, телефонски позиви или интерент употребљени за извшење кривичног дела, нпр. за онлајн превару.

[17] У Немачкој није могуће затражити задржавање података о саобраћају од провајдера уколико не постоји одређен степен сумње да је учињено одређено кривично дело од када је Уставни суд 2010. године прогласио закон који имплементира Директиву ЕУ о задржавању података неуставним. Ипак, провајдери и даље задржавају податке на основу члана 96. Закона о телекоминикацијама, и ти подаци се могу затражити у складу са поменутом одредбом ЗКП-а.

резултати нису могли остварити на другачији начин и ако су трошкови прикупљања сразмерни за значајем конкретног случаја. За предузимање ове мере, по правилу, је потребна наредба суда, а када то налажу разлози изузетне хитности, довољно је и одобрење јавног тужиоца.

Осим наведеног, полиција може упутити захтев за утврђивање идентитета корисника динамичке ИП адресе (у виду тзв. захтева за откривање података о претплатнику услуге), што је нарочито корисно у пракси. Наиме, на основу члана 163. ЗКП полиција је овлашћена да од свих физичких и правних лица захтева откривање свих података потребних за утврђивање идентитета учиниоца кривичног дела, а у вези са чланом 113 (1) Закона о телекомуникацијама овлашћена је да од провајдера телекомуникационих услуга захтева откривање података о кориснику (име и презиме корисника, број телефона и друге податке који се односе на конекцију са пружаоцем услуга). За упућивање оваквог захтева није потребно судско одобрење (само накнадно обавештавање јавног тужиоца) а овлашћење није ограничено на одређена кривична дела. Једини услов за прикупљање података о претплатнику је да је то неопходно за процесуирање учиниоца кривичног дела које се гони по службеној дужности.

У недостатку специфичних одредаба које се односе на експедитино чување и делимично откривање података о саобраћају комуникација, користи се иста процедура као код хитног очувања података уопште. Ипак, постоје одређена ограничења с обзиром на то да се чување и откривање података о саобраћају може захтевати само у погледу тешких кривичних дела или која су учињена употребом рачунарских система, па је тиме члан 17. Конвенције само делимично имплементиран у немачко законодавство.

У ***холандском*** Закону о кривичном поступку[18] постоји одреба која регулише меру хитног очувања података. Наиме, на основу члана 125к ЗКП јавни тужилац упућује захтев било ком физичком или правном лицу у чијем поседу/ под чијом контролом су рачунарски подаци подложни губитку/измени а који су релевантни за процесуирање учинилаца одређеног кривичног дела, да их сачува у неизмењеном облику, а на основу члана 125м уколико се подаци односе на електронску комуникацију, пружалац услуга је дужан да пружи довољно података потребних за утврђивање идентита других провајдера чије мреже или услуге су коришћене у релевантној комуникацији. Захев се може упутити у писаном облику или усмено (али тада мора у року од три дана бити састављена у писаном облику наредба са потписом јавног тужиоца) и мора да садржи следеће елементе: тачно одређење података које је потребно сачувати, образложење, времен-

[18] *Wetboek van Strafvordering*, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html.

ски период за који се захтева чување података, те да ли се захтев односи и на податке потребне за откривање идентитета других провајдера чије услуге или мреже су коришћене у релевантној комуникацији. Јавни тужилац о упућеном захтеву у сваком случају сачињава службени извештај. Међутим, како ова процедура могућа само у погледу кривичних дела за које је могуће одредити притвор у претходном поступку (наведене у члану 67. ЗКП), може се уочити да холандски ЗКП није у потпуности у сагласности са обавезама из члана 16. и 17. Конвенције.

У ***Финској*** је у члану 24. Закона о мерама процесне принуде[19], а у вези са претресом рачунарских уређаја (чланови 20-23), изричито регулисано хитно чување података. Када постоји опасност да ће се рачунарски податак од значаја за истрагу конкретног кривичног дела изгубити или изменити пре добијања одобрења за претрес рачунарског уређаја, орган који је овлашћен да нареди лишење слободе (на основу члана 9. Закона), овлашћен је и да изда наредбу у писаном облику да се потребни подаци сачувају неизмењени. Мера се може наредити према било ком физичком или правном лицу који има у поседу или под контролом потребне рачунарске податке (осим према осумњиченом), и то у погледу свих типова података који су ускладиштени у систему, па и на податке у поруцу која се преноси у информационом систему (а садржи податке о извору, одредишту, путањи и величини поруке као и времену, трајању, природи и другим околностима које се односе на пренос поруке). Осим тога, мера се може односити и на податке за које се претпоставља да ће бити упућен рачунарском уређају, односно пренет кроз информациони систем у временском периоду од месец дана од момента издавања наредбе. Надлежни орган није овлашћен да се упозна са садржином података до добијање наредбе за претрес рачунарског уређаја. Уколико је више пружалаца услуга укључено у комуникацију, надлежни орган је овлашћен да захтева податке потребне за идентификацију свих провајдера. Наредба се у складу са чланом 25. Закона може издати на максимално три месеца, а ако интереси истраге то захтевају, трајање мере се може продужити за још три месеца. Лице према коме је наредба издата дужно је да поступање по наредби чува као тајну, у супротном се може против њега покренути поступак за кривично дело одавање тајне (предвиђена новчана казна или казна затвора до годину дана). Из наведеног се може закључити да је Финска у потпуности испунила обавезу из члана 16. и 17. Конвенције.

Законик о кривичном поступку ***Летоније***[20] уређује и питање експедитивног чувања рачунарских података (члан 191. ЗКП) и питање парцијал-

[19] *Pakkokeinolaki 806/2011*, http://www.finlex.fi/fi/laki/kaannokset/2011/en20110806.pdf.
[20] http://legislationline.org/documents/section/criminal-codes.

ног откривања података о саобраћају остварених комуникација (члан 192. ЗКП). Истражитељ из посебне јединице полиције за борбу против компјутерског криминала и заштиту интелектуалне својине упућује захтев истражном судији за издавање наредбе. По издавању наредбе истражитељ захтева од лица (било ког физичког или правног лица, укључујући и пружаоце услуга електронске комуникације), које има у поседу или врши контролу над рачунарским системом у ком су ускладиштени потребни подаци да потребне податке сачува у неизмењеном облику за период до тридесет дана (а тај период може бити продужен по одобрењу истражног судије за још тридесет дана). Наредба се односи на чување било које врсте рачунарских података који су релевантни за истрагу, а предвиђена је и одговорност лица према коме је издата наредба уколико обелодани информације које се односе на вођење истраге. Иако у ЗКП Летоније постоји и изричита одредба о експедитином чувању и делимичном откривању података о саобраћају комуникације (члан 192.ЗКП) у погледу чега је потребна или наредба истражног судије или пристанак лица које има у поседу те податке, ова одредба нема практични значај јер према прописима о задржавању података провајдери чувају све рачунарске податке и доступни су полицији у погледу свих кривичних дела и то без одлуке суда.

Одредба која регулише хитно обезбеђивање рачунарских података у ***Норвешкој*** садржана је у члану 215а Законика о кривичном поступку[21] и примењује се на све врсте рачунарских података и у погледу свих кривичних дела. Надлежни јавни тужилац може издати наредбу да се обезбеде ускладиштени рачунарски подаци који могу имати значај електронског доказа, укључујући и податке о оствареним електронским комуникацијама који су у поседу пружаоца услуга приступа мрежи или других услуга електронских комуникација, и то за период до деведесет дана. Наредба се преко полиције упућује (електронском поштом или факсом, уз претходно обављени телефонски разговор) компанији којој се налаже да сачува релевантне податке, а компанија пружалац услуге је дужна да након поступања по налогу потврди (електронском поштом или факсом) да је сачувала тражене рачунарске податке и то за одређени временски период. Осумњичено лице се обавештава о предузетој мери одмах након што су подаци обезбеђени. Међутим, како у Норвешкој не постоје обавезе задржавања података, проблем је што захтев за хитно очување података често стигне до компаније прекасно, тј.када подаци више нису доступни.

У ***Великој Британији*** не постоје специфичне одредбе о мери хитног чувања података али постоји низ овлашћења надлежних органа чијом при-

[21] *Lov om rettergangsmaten i straffesaker (Straffeprosessloven) 53/2006,* http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

меном се може остварити експедитивно обезбеђење рачунарских података. Пре свега, ради се о одредбама члана 102. Закона о борби против тероризма, криминала и безбедности из 2001.године[22], затим одговарајућих чланова Закона о уређењу истражних овлашћења из 2000.године[23] и Закона о полицијским и кривичнопроцесним доказним радањама из 1984.године[24]. У складу са Законом о полицијским и кривичнопроцесним доказним радњама, полиција може тражити од суда одобрење да им се обезбеди приступ потребним рачунарским подацима као и њихова предаја. У складу са Законом о уређењу истражних овлашћења добијање одобрења за улазак у просторије обухвата и могућност да се лицу у чијем поседу или под чијом контролом су потребни подаци нареди да исте сачува и преда полицији. Осим тога, претрес рачунарских уређаја и експедитивно очување рачунарских података могуће је предузети у ситуацијама када то налажу разлози изузетне хитности и без претходног одобрења суда, као и у случају података који су задржани у складу са прописима који имплементирају регулативу ЕУ о задржавању података.

У ***САД-у*** је се експедитивно чување рачунарских података могуће одредити на основу члана 2703(ф) Савезног кривичног закона[25]. Ова мера је од круцијалног значаја и често се користи у истрагама у САД јер омогућава истражитељима и тужиоцу да се не изгубе битни подаци од пружалаца услуга електронских комуникација док не буду обавезани да исте открију, односно учине доступним надлежним органима. Наиме, хитно чување података је први корак у правном механизму који се окончава налогом издатог од стране судских органа. Дакле, сама мера не омогућава полицији и тужилаштву да се упознају са садржајем података него се тиме обезбеђује да се сачувају ускладиштени подаци. Ова мера је изузетно важан инструмент у том погледу, јер у САД не постоје прописи о задржавању података па провајдери према компанијској политици имају слободу да избришу или сачувају податке о кориснику и његовим активностима, па би у случају да не постоји захтев за хитно чување података, истражитељи изгубили приступ великом броју података.

Када се у току истраге утврди да физичко или правно лице има приступ или под контролом рачунарске податке који су релевантни за даљи ток поступка, истражитељ или тужилац упућује држаоцу података наредбу

---

[22] *Anti-Terrorism, Crime & Security Act (ATCS) 2001*, http://www.legislation.gov.uk/ ukpga/2001/24/contents.

[23] *Regulation of Investigatory Powers Act (RIPA) 2000*, http://www.legislation.gov.uk/ ukpga/2000/23/contents.

[24] *Police and Criminal Evidence Act (PACE) 1984*, http://www.legislation.gov.uk/ ukpga/1984/60/contents.

[25] *The U.S. Federal Criminal Code*, http://www.law.cornell.edu/uscode/text/18/2703.

да предузме све потребне радње како би се сачували у неизмењеном облику тачно одређени подаци. Занимљиво је да за издавање наредбе за очување података није овлашћен само суд или јавно тужилаштво, већ представник сваког државног органа. Мера се може односити на било коју врсту рачунарских података а у вези са било којим кривичним делом. Наредба се може упутити поштом, факсом или електронском поштом, а велике компаније пружаоци телекомуникационих услуга имају онлајн формуларе за примање ових захтева. Од пружалаца услуга електронских комуникација државни органи могу захтевати хитно чување (а по одобрењу суда и предају) следећих података: име и презиме и адресу корисника услуга; податке о остварeним комуникација, са временом трајања тих комуникација; врсту и време коришћења појединих услуга; телефонски број или други идентификациони број корисника, као и привремено додељену ИП адресу (динамичке ИП адресе); средства плаћања услуге. Лице коме је захтев за чувањем података упућен, дужно је да по њему поступи и да податке који могу имати значај доказа у кривичном поступку чува обезбеђене док суд надлежним органима не одобри приступ садржају тих података, и то за времески период одређен у наредби (најдуже до деведесет дана, с тим што се овај период може наредбом додатно продужити за још деведесет дана).

Мера хитног чувања података се у САД сматра корисном и често се користи у пракси (издаје се неколико хиљада наредби годишње[26]). Међутим, истражитељи не добијају издавањем наредбе никакве податке о налогу, укључујући и податак да ли налог постоји, јер провајдере у откривању оваквих података спречавају прописи о поверљивости података о корисницима, а што ће бити могуће тек по добијању судког налога. Још један проблем произилази из односа поверљивости према кориснику, јер постоји дужност провајдера да корисника налога обавесте о издавању наредбе за чување података и поступању по тој наредби, а ово може трајно да нанесе штету истрази.

У ***Србији*** у погледу обезбеђења ускладиштених рачунарских података који могу имати значај електронског доказа, Законик о кривичном поступку[27] у члану 152. став 3. предвиђа да се претресање уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи, предузима на основу наредбе суда и, по потреби, уз помоћ стручног лица. У члану 152. став 2. предвиђено је да се претресање стана и других просторија или лица предузима на основу наредбе суда, *али и да се*

[26] Privacy: An Overview of the Electronic Communications Privacy Act, https://www.fas.org/sgp/crs/misc/R41733.pdf.

[27] Законик о кривичном поступку, „Службени гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013 и 45/2013.

изузетно може предузети без наредбе (у складу са члановима 158-160.ЗКП). Могућност *претресања уређаја* за аутоматску обраду података и *опреме* на којој се чувају или се могу чувати електронски записи *без наредбе није изричито уређено, нити је предвиђена сходна примена правила* о претресању стана и други просторија без наредбе. Како то значи да је за претресање ових уређаја и опреме у сваком случају потребна наредба суда, а што је у складу са Уставом зајемченом неповредивошћу тајности писама и других средстава комуникације, произилази *да не постоји начин за обезбеђење рачунарских података* ускладиштених у тим уређајима, односно опреми на *експедитиван начин* у смислу члана 16. Конвенције.

Што се тиче имплементације члана 17. Конвенције, у члану 286. став 3. ЗКП (у вези са дужношћу полиције да уколико постоје основи сумње да је извршено кривично дело за које се гони по службеној дужности предузме потребне мере да се пронађе учинилац кривичног дела, да се учинилац или саучесник не сакрије или не побегне, да се открију и обезбеде трагови кривичног дела и предмети који могу послужити као доказ, као и да прикупи сва обавештења која би могла бити од користи за успешно вођење кривичног поступка) прописано је овлашћење полиције да по налогу јавног тужиоца прибави евиденцију остварене телефонске комуникације, коришћених базних станица или извршити лоцирање места са којег се обавља комуникација. Међутим, ово овлашћење дато у циљу остварења наведених дужности односи се само на прибављање појединих података о саобраћају у погледу телефонске комуникације, не и осталих видова електронске комуникације, па се не може сматрати да члан 17. Конвенције имплементиран на одговарајући начин. Истовремено, поставља се и питање усклађености овог решења са Уставом, јер је решењем по ком јавни тужилац налаже прибављање евиденције остварене комуникације или лоцирање места са ког се врши комуникација у супротности са гарантованом неповредивошћу тајности писама и других средстава комуникације на основу које би само суд могао наредити предузимање ових радњи.

Осим поменутих одредаба Законика о кривичном поступку, за предметну проблематику релевантан је и Закон о електронским комуникацијама[28]. У члану 128. Закона установљена је обавеза пружалаца услуга електронских комуникација да задрже одређене податке о саобраћају[29] за по-

[28] Закон о електронским комуникацијама, „Службени гласник РС“, бр. 44/2010 и 60/2013 – одлука УС.

[29] Подаци се задржавају и чувају у изворном облику или као подаци обрађени током обављања делатности електронских комуникација и то тако да им се без одлагања може приступити, односно да се без одлагања могу доставити. Задржавају се и чувају подаци потребни за:1) праћење и утврђивање извора комуникације; 2) утврђивање одредишта комуникације; 3) утврђивање почетка, трајања и завршетка комуникације; 4) утврђивање

требе спровођења истраге, откривања кривичних дела и вођења кривичног поступка, као и за потребе заштите националне и јавне безбедности Републике Србије и да их чувају 12 месеци од дана обављене комуникације. Важно питање у вези са наведеним овлашћењима је право надлежних органа да приступе подацима о комуникацијама, како подацима о саобраћају тако и подацима који се односе на садржај комуникације, имајући у виду неповредивост тајности комуникација. У погледу остваривања приступа задржаним подацима, а за потребе кривичног поступка, Уставни суд Републике Србије је прогласио неуставном одредбу члана 128. став 5. Закона у делу којим је била установљена обавеза оператора да задржане податке, без обзира што се њима не открива садржај комуникације, учине доступним на захтев надлежног органа, а без претходно прибављене одлуке суда, јер се таквом одредбом нарушава неповредивост права на тајност комуницирања корисника електронских комуникација[30]. Наиме, Суд је утврдио да је једино суд надлежан да, ако је то неопходно ради вођења кривичног поступка, на одређено време и на начин предвиђен законом, одреди (дозволи) одступање од Уставом зајемчене неповредивости тајности писама и других средстава комуницирања, а не да се то право одређује у складу са законом[31].

6. Закључак

У складу са Уставом Републике Србије рачунарским подацима који се односе на електронске комуникације може се приступити, дакле, само на основу одлуке суда на начин предвиђен законом, па Законик о кривичном поступку предвиђа *да се радња претреса* уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи може предузети *само на основу наредбе суда*.

Иако се у смислу Конвенције о високотехнолошком криминалу не тражи прописивање специфичних овлашћења за хитно чување података (уколико се циљ ове мере може остварити предузимањем других радњи којима се могу обезбедити електронски докази, а у вези са било којим кривичним делом, у односу на било које физичко или правно лице, у погледу

врсте комуникације; 5) идентификацију терминалне опреме корисника; 6) утврђивање локације мобилне терминалне опреме корисника, као и подаци о успостављеним позивима који нису одговорени (али не подаци о позивима чије успостављање није успело). Изричито је предвиђено да је забрањено задржавање података који се односе на садржај комуникације.

[30] Одлука Уставног суда, ИУз број 1245/2010 од 13. јуна 2013. године, објављена у "Сл. гласнику РС", бр. 60/2013 од 10. јула 2013. године.

[31] Више о одлуци видети: Т. Бугарски, *Доказне радње у кривичном поступку*, друго измењено издање, Нови Сад 2014, стр. 53-54.

свих рачунарских података и на експедитиван начин), *једино адекватно решење*, које би представљало потпуну имплементацију одредаба чланова 16. и 17. Конвенције, јесте *уношење у Законик одредаба којима би се на изричит начин регулисала мера хитног чувања рачунарских података*, *како би се ускладиштени рачунарски подаци од значаја за кривични поступак на експедитиван начин* обезбедили од губитка/измене до окончања формалне процедуре у којој би надлежни органи стекли право приступа тим подацима, односно *до издавања од стране суда наредбе* за претрес уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи. Како се обезбеђење података применом ове мере односи само на издавање наредбе да се подаци чувају и задрже, а не подразумева се остварење приступа садржају тих података, меру би могао наредити и јавни тужилац.

Приликом регулисања ове мере требало би као могући узор узети једно од приказаних решења у прописима држава потписница Конвенције (или комбинацију решења) које су на одговарајући начин имплементирале одредбе Конвенције.

Дакле, у вези са претресом уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи (члан 152. став 3. Законика), потребно је, ради имплементације члана 16. Конвенције, унети следеће одредбе као нови члан под називом „Мера хитног чувања ускладиштених рачунарских података“:

Када постоји опасност да ће се рачунарски подаци ускладиштени у рачунарском систему, који могу бити од значаја за кривични поступак, изгубити или измењени до издавања наредбе за претрес уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи, полиција може упутити захтев јавном тужиоцу за издавање наредбе да се ти подаци сачувају у неизмењеном облику за рок до тридесет дана. Рок може бити продужен по одобрењу јавног тужиоца за још тридесет дана.

Мера хитно чување ускладиштених рачунарских података може се наредити према било ком физичком или правном лицу који има у поседу или врши контролу над рачунарским системом у ком су ускладиштени потребни подаци, и то у погледу свих врста података који су ускладиштени у систему.

Уколико је више пружалаца услуга електронске комуникације укључено у електронску комуникацију, надлежни орган је овлашћен да захтева податке потребне за идентификацију свих пружалаца услуга.

Наредба садржи следеће елементе: лице према коме се наредба издаје, тачно одређење података које је потребно сачувати, образложење, временски период за који се захтева чување података, да ли се захтев од-

носи и на податке потребне за откривање идентитета других пружалаца чије услуге или мреже су коришћене у релевантној комуникацији.

Лице према коме је наредба издата дужно је да поступање по наредби чува као тајну.

Полиција није овлашћена да се упозна са садржином података до издавања наредбе суда за претрес уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи.

У погледу имплементације члана 17. Конвенције, потребно је унети и следећу одредбу или као став у члану којим би се регулисала „Мера хитног чувања ускладиштених података“ или као нови члан под називом „Хитно чување и делимично откривање података о саобраћају комуникација“:

Ради обезбеђења хитног чувања података о саобраћају конкретне електронске комуникације која се остварује коришћењем услуга више пружалаца услуга електронске комуникације, пружалац услуга ком је издата наредба из члана... (којим би се регулисала „Мера хитног чувања ускладиштених података“) *дужан је да надлежном органу пружи довољно података потребних за утврђивање идентитета свих пружалаца коришћењем чијих услуга је комуникација остварена.*

Milana Pisarić, Assistant
University of Novi Sad
Faculty of Law Novi Sad

Expedited Preservation of Stored Computer Data

Abstract: *Due to the development and ubiquity of information technology in everyday life, the number of criminal activities committed using computer systems and networks has also increased. Traces of the crimes committed in connection with the misuse of information technologies are in the form of electronic records - computer data that occur as a result of the actions of the perpetrator or as automatically created and stored in a computer system / network. However, these computer data are subject to change , so it is necessary to adequately ensure their protection. To create an appropriate legal framework to counter these challenges , the rules of criminal procedure law have to determine the appropriate powers of the competent authorities for the purpose of collecting and providing computer data on the committed criminal offense and the offender can be used as electronic evidence in criminal proceedings.*

Key words: *computer data, expedited preservation of stored computer data, electronic evidence.*