Прегледни чланак 343.14:004.424.4
doi:10.5937/zrpfns49-8135

*Милана М. Писарић, асистент*
*Универзитет у Новом Саду*
*Правни факултет у Новом Саду*
mpisaric@pf.uns.ac.rs

# ПРЕТРЕСАЊЕ РАЧУНАРА РАДИ ПРОНАЛАСКА ЕЛЕКТРОНСКИХ ДОКАЗА[1]

***Сажетак:*** *Да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских мрежа и система, разумљиво је настојање држава да прилагоде, односно употпуне постојеће кривично законодавство сврсисходним одредбама. За стварање одговарајућег правног оквира за супротстављање високотехнолошком криминалу, осим што се у прописима кривичног материјалног права одређена понашања предвиђају као кривична дела против поверљивости, целовитости и доступности рачунарских података, рачунарских система и мрежа, неопходно је да прописи кривичног процесног права садрже овлашћења надлежних органа адекватна за откривање извора недозвољене радње, односно прикупљање података о учињеном кривичном делу и учиниоцу, који могу бити искоришћени као доказ у кривичном поступку, а водећи рачуна о специфичностима високотехнолошког криминала и окружења у оквиру кога се недозвољене активности предузимају. Сходно томе, одредбама кривичног процесног права би требало омогућити да се превазиђу одређени изазови у откривању и доказивању дела високотехнолошког криминала, а нарочит значај имају одредбе којима се уређује претресање рачунара ради проналаска електронских доказа.*

***Кључне речи:*** *високотехнолошки криминал, рачунари, претресање, електронски докази.*

## 1. Уводна разматрања

Поједина кривична дела извршена злоупотребом достигнућа информационе технологије донекле су слична, условно речено, традиционалним кривичним делима. Крађа, превара, вандализам, неовлашћен приступ при-

[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.

ватној сфери појединца, искоришћавање деце у порнографске сврхе и кршење ауторских права су проблеми који су постојали и пре појаве рачунара и Интернета. Стога *постојећи прописи* могу представљати *солидну основу* за откривање и хватање лица која су извршила кривична дела слична наведеним али у кибер простору. Оно што треба имати на уму је да проблеми у вези са откривањем кривичних дела и гоњењем учинилаца настају, не толико услед природе недозвољених активности, већ *због својстава информационих технологија* које су омогућиле њихово извршење на начин квантитативно и квалитативно другачији у односу на традиционална кривична дела. Могло би се рећи да поједине карактеристике савремених рачунарских система и мрежа представљају озбиљну препреку за обезбеђивање доказа потребних за оптужење и вођење кривичног поступка за дела високотехнолошког криминала[2]. Ови аспекти чине високотехнолошки криминал специфичним обликом криминала, па морају бити узети у обзир, како би се што потпуније разумеле и превазишле тешкоће у откривању и доказивању кривичних дела и суђењу учиниоцима истих. Имајући у виду наведено, а да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских мрежа и система, *разумљиво је настојање држава да прилагоде, односно употпуне постојеће кривично законодавство сврсисходним одредбама*[3]. За стварање одговарајућег правног оквира за супротстављање овој врсти криминала, осим што се у прописима кривичног материјалног права одређена понашања предвиђају као кривична дела против поверљивости, целовитости и доступности рачунарских података, рачунарских система и мрежа, неопходно је да прописи кривичног процесног права садрже овлашћења надлежних органа адекватна за откривање извора недозвољене радње, односно прикупљање података о учињеном кривичном делу и учиниоцу, који могу бити искоришћени као доказ у кривичном поступку, а водећи рачуна о специфичностима високотехнолошког криминала и окружења у оквиру ког се недозвољене активности предузимају.

## 2. Нормативни оквир за претресање рачунара

По сазнању да је учињено кривично дело злоупотребом информационих технологија, потребно је одговорити на следећа питања: Шта се десило? Каква је природа напада на рачунарски систем/мрежу? Да ли је уопште дошло до напада? На који начин је извршен напад на рачунарски си-

[2] B. Maier, „How Has the Law Attempted to Tackle the Borderless Nature of the Internet?“, *International Journal of Law and Information Technology* 2/2010, 153.

[3] Вид. М. Писарић, „Потребни нормативни одговор на проблеме откривања и доказивања дела високотехнолошког криминала“, Зборник радова Правног факултета у Новом Саду 1/2013, 291-309.

стем који је објект напада? Да ли је било више напада? Шта се тражи? Које безбедносне мере су биле активне у систему у моменту напада? Које лице је било у позицији да узрокује/омогући извршење напада? Одговор на сва ова питања могу дати одређени рачунарски подаци који су похрањени или се преносе у рачунарском систему и/или рачунарској мрежи, а који тиме могу имати значај доказа у кривичном поступку. Такви рачунарски подаци се могу означити као *електронски докази*[4].

Рачунарски подаци се могу пронаћи у рачунарској мрежи или у неком рачунарском систему у поседу осумњиченог лица, оштећеног лица или трећег лица(нпр. пружалаца комуникационих услуга), а осим тога, могу се пресрести у току преноса кроз рачунарску мрежу. Правила кривичне процедуре уређују под којим условима и на који начин органи поступка могу на законит начин доћи до релевантних рачунарских података и на који начин подаци постају доказ о извршеном кривичном делу. Да би се рачунарски подаци могли користити као доказ у кривичном поступку, потребно је утврдити да су прикупљени и обрађени у складу са законом (*услов законитости*), да није било намерне или случајне измене/губитка електронских записа, односно да су записи представљени као доказ пред судом ни мање ни више у односу на време када су били прикупљени (*услов аутентичности*) и да су подобни за утврђивање постојања и истинитости одређене чињенице у кривичном поступку (*услов релевантности*). Да би био задовољен услов законитости, радње и мере које служе прикупљању електронских доказа морају бити предузете у складу са законом који уређује кривичну процедуру, приликом чега морају бити поштована правила дигиталне форензике у циљу испуњења услова, аутентичности док се услов релевантности везује за околности конкретног случаја. Примена техника дигиталне форензике не подразумева просто копирање и прегледање ускладиштених рачунарских података. Резултати предузетих радњи не могу и неће увек бити доказ на суду – некада имају само значај оперативних сазнања који ће усмерити даљи ток поступања надлежних органа а могу се употребити као доказ само ако су прикупљени на начин у складу са одредбама кривичног процесног законодавства[5]. Иако је технички изводљиво много тога, само оно до чега са дошло под условима, на начин и у облику који прописује законодавство моћи ће да буде доказ у кривичном поступку.

*Претрес рачунара и других уређаја за електронску обраду и пренос података заузима централно место* међу радњама и мерама које надле-

[4] Вид. Т. Бугарски, "Дигитални докази", Зборник радова Правног факултета у Новом Саду 2/2012, 177-193.

[5] A. Wolfson, "Electronic fingerprints: doing away with conception of computer-generated records as hearsay", *Michigan Law review* l/2005, 156.

жни органи предузимају ради проналаска похрањених рачунарских података као трагова о извршеном кривичном делу против/посредством рачунарских система и мрежа а који могу бити доказ у кривичном поступку. Стога је у процесном законодавтсву *потребно да се одговарајућим одредбама створи основ за претрес уређаја који садрже електронске доказе за потребе конкретног кривичног поступка*. Претрес се односи на претрагу ради проналаска похрањених података у меморији рачунара и других уређаја, али не и података о саобраћају или садржају комуникација које се остварују посредством информационих технологија.

У настојању да се пронађу инспиришућа решења, анализирана су законодавства појединих држава, а *анализа је потврдила изузетан допринос Конвенције о високотехнолошком криминалу*[6], као свеобухватног оквира за прилагођавање кривичног процесног законодавства посебностима доказивања дела високотехнолошког криминала. Наиме, члан 19. Конвенције Конвенције о високотехнолошком криминалу садржи обавезу држава потписница да у својим законодавствима регулишу претрес и одузимање рачунара и других уређаја који могу садржати електронске доказе, регулишући следећа овлашћења надлежних органа:

1. Да врше претрес или сличан приступ:
   - рачунарском систему или делу рачунарског система и рачунарским подацима похрањеним у њима;
   - уређају за складиштење података у ком су похрањени рачунарски подаци.
2. Да иницијални претрес прошире, уколико приликом вршења претреса или другог сличног приступа рачунару постоји вероватноћа да се подаци који се траже налазе похрањени у другом рачунарском систему или делу система на територији државе а таквим подацима је могуће на законит начин приступити из рачунара или су том рачунару доступни[7];
3. Да одузму или на други начин обезбеде рачунарске податке којима се приступило током вршења претреса или сличног приступа, тако што:
   - одузму или на други начин обезбеде (ради очувања интегритета електронских доказа) рачунарски систем или део рачунарског система или уређај за складиштење података;

---

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

[7] При томе се начин на који се врши проширење претреса препушта државама. У пратећем извештају уз Конвенцију се као примери наводе: а) суд који је одобрио иницијални претрес конкретног рачунарског система проширује наредбу/одобрење и на други систем уколико процени да постоји довољан степен вероватноће у складу са прописима националног законодавства да се у повезаном рачунару налазе одређени подаци који се траже, или б) налог за претрес се извршава на обе локације истовремено на координисан и експедитиван начин. Вид. http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

- направе и задрже копију рачунарских података;
- одрже интегритет релевантних рачунарских података;
- привремено учине недоступним (нпр. применом технологије енкрипције) или обришу податке у рачунару ком је приступљено.

4. Да нареде лицу, које има сазнања о функционисању рачунарског система или мерама примењеним за заштиту похрањених података, да пружи потребна обавештења у циљу омогућавања вршења претреса рачунара.

С обзиром на неадекватност традиционалних истражних овлашћења и одсуство у већини земаља посебних процедуралних правила која би се примењивала у кибер простору, решења у Конвенцији су послужила као полазна основа за правно регулисање овлашћења надлежних органа неопходна за истрагу кривичних дела учињених у вези са рачунарским системима и мрежама.

## 3. Претресање рачунара у прописима појединих држава

У ***Италији*** су изменама Законика о кривичном поступку из 2008. године[8] унете одредбе које имају за циљ да омогуће вршење претреса рачунара[9]. Наиме, у члану 247. који одређује услове за предузимање радње претрес просторија, додат је став 1-*bis*. Уколико постоје разлози да се верује да се рачунарски подаци релевантни за конкретно кривично дело налазе у информационом или телекомуникационом систему, пре претраге тих система, предузимају се техничке мере ради заштите оригиналних података од измена или уништења. Уколико се током претреса пронађу подаци који могу имати значај доказа за кривичну истрагу, од држаоца рачунара се тражи предаја предавање, а уколико одбије да учини, суд може издати наредбу за привремено одузимање података. У вези са вршењем увиђаја, судска полиција је дужна да у односу на рачунарске податке и програме или рачунарске и телекомуникационе системе предузме техничке мере и обезбеди неопходне услове како би се осигурало њихово очување и предупредило мешање и онемогућавање приступа, те да, уз адекватну стручну подршку, спроведе дуплирање, односно прављење копија на лицу места тих уређаја, кроз процедуру која обезбеђује усклађеност са оригиналним примерком и његову непроменљивост (члан 354. став 2). Вредна помена је и одредба која се односи на чување заплењених предмета, која између осталог предвиђа да када су одузети електронски уређаји и рачунари, од оригинала уређаја и података похрањених у њима стварају се копије на од-

[8] Codice di Procedura Penale *(Testo coordinato ed aggiornato del D.P.R. 22 settembre 1988, n. 447),* http://www.altalex.com/index.php?idnot=36800.

[9] У оквиру наслова три: „средства за прикупљање доказа“ Треће књиге, друго поглавље уређује претрес просторија.

говарајућем медијуму у поступку који обезбеђује потпуну саобразност оригинала и копије (члан 259. став 2. и члан 260.став 2). У складу са чланом 352. став 1бис уколико је лице затечено у извршењу кривичног дела, пре него што приступи претраживању рачунарског/информационог система, судска полиција је овлашћена да предузме техничке мере у циљу обезбеђења оригиналних података и спречавања измена или уништења ако постоје разлози за бојазан да рачунарски подаци/програми релевантни за истрагу могу бити избрисани/уништени.

У ***Шпанији*** Закон о кривичном поступку[10] не садржи одредбе о претресу рачунара, па се сходно примењују одредбе о претресу просторија.

***Португалски*** Закон о компјутерском криминалу[11] у члану 15. регулише претрес ради претраге рачунарских података. Када је у току истраге потребно извршити претрес одређеног рачунара, да би се у њему пронашли одређени подаци, суд издаје наредбу коју криминалистичка полиција извршава у року до 30 дана, о чему саставља записник који прослеђује суду. Ипак, полиција може и без наредбе суда да изврши претрес рачунара у две ситуације : а) уколико пристанак да лице које је држалац рачунара или под чијом је рачунар контролом (а пристанак се документује у одговарајућој писаној форми), или б) у случају истраге тероризма или других кривичних дела са високим степеном насиља или организованости или уколико постоји непосредна опасност по живот или тело неког лица. У ове две ситуације је полиција дужна да о вршењу претреса без одлагања обавести суд који процењује неопходност ове радње и може је поништити, односно не одобрити. Уколико се током вршења претреса појави вероватноћа да су тражени подаци похрањени у другом рачунарском систему или делу система и да им се може законито преступити из иницијално претраживаног рачунара, претрес се може проширити и на тај други рачунар, уколико се за то прибави сагласност поменутих лица или наредба суда.

Члан 16. Закона предвиђа да уколико се током претреса пронађу рачунарски подаци који су потребни као доказ за утврђивање истине у кривичном поступку, криминалистичка полиција је овлашћена издатом наредбом за претрес да те податке одузме. Уколико се претрес врши без наредбе суда, подаци се могу пре добијања судске наредбе одузети само уколико то налажу разлози хитности или опасност од губитка података. Одузимање података у сваком случају мора одобрити суд у року од 72 часа иначе се не могу користити као доказ. Предвиђено је ограничење у погледу одузимања одређених категорија података. Наиме, ако током претреса ради претраге рачунарских података полиција нађе документе са личним или интимним

[10] http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20140725&vd=#preambulo.
[11] http://www.gddc.pt/codigos/code_criminal_procedure.html.

садржајем чије би сазнавање повредило приватност држаоца рачунара или трећег лица, ти документи се предају судији који доноси одлуку о употреби тих података ценећи околности конкретног случаја. Подаци који се односе на вршење правничких, медицинских или банкарских послова могу се користити само уз поштовање ограничења које предвиђа Закон о кривичном поступку а приликом претреса рачунара које користе новинари узимају се у обзир одговарајуће одредбе Закона о новинарству. Осим тога, овај члан упућује на Закон о кривичном поступку у погледу режима државне, службене и професионалне тајне. Потребни рачунарски подаци се одузимају на три начина (утврђује се начин који је у највећој мери одговарајући или пропорционалан на основу процене околности случаја): 1. Рачунарски систем са свом опремом, уређаји за складиштење података и уређаји за очитавање података се одузимају са лица места и транспортују у форензичку лабораторију; 2. Прави се копија само потребних рачунарских података на лицу места (праве се две копије од којих се једна предаје у судски депозит и оверава дигиталним потписом а друга се прослеђује на обраду у форензичку лабораторију); 3. Применом техничких средстава се обезбеђује интегритет података, без копирања или уклањања података из система; 4. Уклањају се рачунарски подаци или се онемогућава приступ њима у систему.

У вези са вршењем претреса ради претраге рачунарских података је и члан 14. Закона по ком суд може наредити лицу које је држалац рачунара или има контролу над њим да преда, односно омогући криминалистичкој полицији приступ потребним подацима (који се одређују у наредби). Уколико то лице одбије да поступи по наредби, против њега се може покренути кривични поступак за кривично дело ометања правде. Наредбом се могу обавезати и пружаоци телекомуникационих услуга да предају податке о кориснику услуга, и то: а. Податке о врсти комуникационе услуге, техничким условима и периоду коришћења услуга; б. Податке о идентитету корисника, адреси, броју телефона, плаћању услуге на основу уговора са корисником; в. Податке о опреми која је предата кориснику на основу уговора. Ипак, Закон предвиђа да се на предају података не може обавезати окривљени, као ни лица која нису дужна да сведоче у кривичном поступку услед постојања обавезе чувања државне, службене и професионалне тајне (што се односи на одређене професије).

У ***Француској*** у складу са чланом 97. Законика о кривичном поступку[12] судска полиција врши претрес стана окривљеног или другог лица за које се сумња да у поседу има рачунарске податке који могу послужити као доказ у кривичном поступку о чему саставља извештај. Пре одузимања

[12] http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154.

рачунарских података, врши се претрес рачунара на лицу места, уз поштовања права окривљеног и докумената који представљају професионалну тајну. Одузимају се само они рачунарски подаци који могу бити корисни за утврђивање истине у кривичном поступку, а на основу одобрења суда. Подаци се одузимају или тако што се уређај у ком су похрањени изузима са лица места и предаје у судски депозит или тако што се *in situ* прави копија потребних података. Копирање се врши у присуству држаоца просторије или лица које он одреди или два сведока. Лица која могу дати корисна обавештења о функционисању рачунарског система се задржавају на лицу места колико је потребно да се радња изврши, а уколико лице одбије да преда потребне рачунарске податке, судска полиција може казнити новчаном казном од 4500 еура (члан 98). Одлуком суда рачунарски подаци чије поседовање или употреба су незаконити или представљају опасност по општу безбедност могу се трајно обрисати из уређаја који нису предати у судски депозит. У складу са чланом 57-1, судска полиција је овлашћена да прошири претрес рачунара на други рачунарски систем у тој просторији или на другом месту, уколико се истом може приступити из иницијалног рачунара, те да приступи у њима похрањеним релевантним подацима и да их копира на одговарајући уређај.

***Немачки*** Закон о кривичном поступку[13] не садржи посебне одредбе о претресу рачунара, него се примењују опште одредбе о претресу просторија и покретних ствари садржане у Одељку VIII Закона[14]. Ипак, у члану 110. став 3, који се односи на прегледање документације (исправа) на лицу места, наведено је да се претрес електронског медија за похрањивање података у поседу лица које се претреса може проширити и на медије за похрањивање података који су од истог просторно удаљени, ако се њима може приступити са тог медија за похрањивање података, те ако постоји бојазан да ће у супротном доћи до губитка тражених података. Подаци који се том приликом пронађу, а могу бити од значаја за истрагу могу се одузети ради обезбеђења. Како су рачунарски подаци изједначени са исправама, потребно је указати на обавезу лица, које држи предмете који могу бити од значаја као доказ за кривични поступак, да их на захтев органа предочи и преда, а ако то не учини, предмети ће се привремено одузети на основу одлуке суда (у изузетним околностима то могу учинити и полиција и тужилаштво, али су о томе дужни да обавесте суд у року од 3 дана). Лице које одбија да преда предмете се може казнити прекршајном казном или мера-

[13] http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0430.

[14] Овај одељак се односи на регулисање одузимања предмета, надзор телекомуникација, компјутерско сравивање личних података, коришћење техничких средстава, коришћење прикривених истражитеља и претресање.

ма које се примењују према лицима која одбијају да сведоче. Наиме према лицима судија за претходни поступак може одредити обавезу сношења трошкова насталих због таквог одбијања, новчану казну, а ако је не плати, и затвор (може се казнити затвором како би пристао да сведочи, а затвор не сме трајати дуже од времена трајања поступка, нити дуже од шест месеци) уз напомену да кад се искористе све ове мере, новчане казне се не могу поново одредити у истом поступку. Обавеза предавања предмета не односи се на лица који имају право да не сведоче (вид. члан 52[15] и 53[16]). Од појединих категорија лица није дозвољено ни одузимање предмета докле год се користе правом да не сведоче (вид. члан 97. став 4), односно одређених врста предмета[17], али је и у овим случајевима одузимање дозвољено ако је исто, уважавајући основна права из члана 5.става 1. реченице 2. Устава, сразмерно значају предмета и разјашњавању чињеничног стања или се место боравка учиниоца не може на други начин утврдити или би утврђивање било отежано. У погледу заштите података који се сравњују, важне су одредбе које одређују третман података. Наиме, ако су подаци прослеђени на носиоцима података, исти се морају вратити одмах након

[15] У складу са чланом 52. право да одбије сведочење има: 1. лице са којом је окривљени верен, односно са којим је размењо обећање да ступи у животну заједницу; 2. брачни друг окривљеног, чак и након престанка брака; 2а. ванбрачни друг окривљеног, чак и након престанка ванбрачне заједнице; 3. сродник осумњиченог по крви у правој линији до било којег степена, у побочној линији до трећег степена, а по тазбини до другог степена.

[16] Право да одбију сведочење имају и следећа лица: 1. верски службеник о ономе што му је поверено или је сазнао у својству исповедника; 2. бранилац о ономе што му је поверено или је сазнао у обављању свог занимања; 3. адвокати, адвокати за патенте, нотари, независни ревизори, овлашћене рачуновође, порезни саветници и пуномоћници, лекари, стоматолози, психотерапеути, дечији психотерапеути, фармацеути и бабице о чињеницама које су им поверене или су сазнали у обављању свог занимања; чланови адвокатске коморе имају исти ранг као адвокати; 3а. чланови или овлашћени представници лиценцираног саветовалишта, у складу Законом о конфликту трудноће, о ономе што им је поверено или су сазнали у обављању свог занимања; 3б. саветници за питања зависности од наркотика у саветовалишту које је лиценцирано или основано од стране државног органа или правног лица, установе или фондације, о ономе што им је поверено или су сазнали у обављању свог занимања; 4. чланови Парламента, Савезне скупштине, Европског парламента или покрајинског парламента о лицима које су им у својству чланова тих органа повериле чињенице или којима су оне поверили чињенице, као и о самим тим чињеницама; 5. лица које професионално учествују или су учествовали у припреми, изради или ширењу штампаних материјала, у радио и ТВ емисијама, филмским извештајима или информативним или комуникацијским службама које служе информисању или стварању мњења.

[17] Није дозвољено одузимање носилаца аудио и видео снимака и носилаца података, слика и других илустрација која држе лица које професионално учествују или су учествовали у припреми, изради или ширењу штампаних материјала, у радио и ТВ емисијама, филмским извјештајима или информативним или комуникацијским службама које служе информисању или стварању мњења

окончања сравњивање, а лични подаци који су пренесени на друге носиоце података, морају се одмах избрисати чим престане потреба за њиховим коришћењем у кривичном поступку. Осим тога, након завршетка мере обавештавају се државни органи који су надлежни за надзор над поштовањем прописа о заштити података.

***Холандски*** Закон о кривичном поступку[18] уређује претрес рачунара међу одредбама којима се регулише претрес просторија и претрес других предмета. Разликује се ситуација у којој рачунару приступа истражни судија од ситуације у којој то чини јавни тужилац, што је предмет одређених ограничења. У случају постојања сумње да је извршено тешко кривично дело, тужилац може ући у било коју просторију (осим места становања) без сагласности држаоца просторије. У хитним случајевима јавни тужилац може за то да овласти и свог заменика, а у осталим случајевима је то могуће само на основу одобрења истражног судије, на писани и образложени предлог тужиоца. Члан 125и регулише претрес просторија у циљу обезбеђења рачунарских података који су похрањени на уређају који се налази у тој просторији, тако што се полиција овлашћује да предузме мере ради спречавања губитка, оштећења или измене података који се имају одузети, а до доласка истражног судије (или јавног тужиоца) који су овлашћени да врше претрес просторије. Закон прописује да се покретне ствари могу одузети уколико су потребне за кривични поступак, а што се тиче одузимања рачунара и других електронских уређаја који садрже електронске доказе, исти се могу одузети, али овлашћење за одузимање не садржи овлашћење прегледања и коришћења рачунара или копирања података, него се одузимање врши у циљу одношења у лабораторију ради прегледа од стране форензичара. Да би се могао прегледати рачунар ради уочавања присуства података потребних за кривични поступак, најпре је потребно обезбедити приступ месту на ком се рачунарски систем налази, а закон одређује ко, у којим случајевима и по ком основу је овлашћен да приступи систему. Члан 125ј предвиђа могућност да се приликом претреса рачунара приступи са њим повезаним рачунаром који се налази на другој локацији ради проналаска доказа који су „оправдано потребни“ за утврђивање истине, а уколико се такви докази пронађу, они се обезбеђују, односно копирају. На основу одредбе члана 125к може се обавезати лице за које се претпоставља да има сазнања о примењеним сигурносним мерама у рачунарском систему да пружи обавештења о томе, односно у случају енкрипције да омогући приступ подацима. Међутим, изричито је наведено да се овако нешто не може наредити окривљеном нити лицу које је у складу са Законом ослобођено дужности сведочења (у погледу дужности чувања професионалне тај-

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

не). Исто тако, у члану 125л је наведено да се не могу одузети рачунарски подаци које су у рачунар унела лица (или у њихово име) са дужношћу чувања професионалне тајне (државни службеници, јавни бележници, медицинско особље), осим ако не буду ослобођени те дужности. Такође је релевантан члан 125о који предвиђа да се приликом претреса уређаја за аутоматску обраду, преношење и складиштење података пронађу подаци који указују на извршење кривичног дела, јавни тужилац, однос истражни судија (у фази претходног саслушања) може одлучити да се такви подаци учине недоступним док је то потребно да се спречи довршење или покушај другог кривичног дела, при чему чињење недоступним подразумева: предузимање мера ради спречавања корисника аутоматског уређаја или трећег лица да сазна за постојање таквих података, односно да се онемогући њихово коришћење, као у уклањање тих података из уређаја (уз претходно обезбеђење података за потребе кривичног поступка). Осим тога, предвиђено је да се, уколико је претрес резултирао копирањем података, о томе обавештавају што је пре могуће (обавештавање се може одложити на основу одлуке истражног судије уколико би оно угрозило кривични поступак) у писаном облику следећа лица: окривљени, контролор података, држалац просторије у којој је вршен претрес. Закон садржи и одредбу којом се, ради заштите приватности лица која су погођена овом мером, прикупљени подаци уништавају, чим се утврди да прикупљени подаци до којих се дошло претресом рачунара нису више потребни за кривичну истрагу, осим уколико јавни тужилац не процени да би били корисни за истрагу у другом предмету (члан 125н).

У ***Финској*** је претрес рачунарских уређаја регулисан у оквиру поглавља 8. Закона о мерама процесне принуде[19] (тачније члановима 20-23) као претрага података који су похрањени у рачунару, другом техничком средству или информационом систему у време предузимања радње. Да би се претрага података извршила потребно је да буду испуњена два материјална услова: 1. да постоји разлог за сумњу да је извршено кривично дело за које је могуће изрећи казну затвора од најмање 6 месеци; 2. да се може претпоставити да претрага може довести до проналажења докумената или података који се имају одузети за потребе кривичног поступка. Уколико су испуњени ови услови, орган који је овлашћен да нареди лишење слободе (на основу члана 9. Закона), овлашћен је и да изда наредбу за претрагу података похрањених у уређају. Одлука којом се одобрава вршење претреса просторија може да обухвата и претрагу техничких уређаја и информационих система за које се претпоставља да су у просторији. У том случају се примењују све одредбе Закона које важе за претрес стана (одређене проце-

[19] http://www.finlex.fi/fi/laki/kaannokset/2011/en20110806.pdf.

дуре и присуство одређених лица у смислу чланова 5-13 и 19. Закона). Претрага уређаја се може извршити и да би се уређај вратио власнику, уколико постоји сумња да је одузет од тог лица у вези са извршењем кривичног дела. Претрага података се, по правилу, врши на лицу места, а уколико је није могуће извршити на лицу места, полиција може одузети уређај. Лице које поседује или обрађује информациони систем је дужно да на захтев органа поступка пружи информације потребне за спровођење претраге података садржаних у уређају (о чему се лицу може на његов захтев издати потврда). Овакава обавеза се не може наметнути окривљеном нити лицима која у складу са законом имају право, односно обавезу да одбију сведочење (у складу са поглављем 7, чланом 3, ставовима 1. и 2).

У Закону о кривичном поступку ***Летоније*** је у члану који регулише вршење увиђаја (члан 160) наведено да уколико се током вршења увиђаја појави потреба да се изврши претрес просторије или предмета, то је могуће само у складу са одредбом која регулише вршење претреса, за шта је потребно одобрење истражног судије. Истражни судија наређује претрес система за аутоматску обраду података (или дела система) уколико постоји вероватноћа да се у систему налазе електронски докази (а то су у смислу члана 136. информације о одређеним чињеницама у електронском облику која је обрађена, похрањена или се преноси у уређајима или системима за аутоматску обраду података). Изричито је предвиђено да се преглед система за аутоматску обраду података не врши на лицу места, него да се систем (или његов део) одузима, на начин да се не измени интегритет података које садржи (члан 160. став 6). У складу са чланом 219. претрес рачунара се врши ради проналажења похрањених рачунарских података и остваривања приступа тим подацима, а могуће је одредити и уклањање одређених података без знања лица које је власник или држалац система, као и прављење копија података и система у целини. Уколико постоји потреба за приступ подацима којима је могуће приступити преко система који је предмет претреса, полиција је овлашћена да то учини и без нове одлуке истражног судије. Полиција може наредити лицу које је власник или држалац електронског информационог система (а то је и физичко и правно лице које обрађује, складишти или преноси податке у електронском информационом систему, укључујући и пружаоца услуга електронских комуникација) да предузме све неопходне радње да се очува потпуност одређених рачунарских података за потребе кривичног поступка, као и недоступност тих података другим лицима, и то за период до 30 дана, који се може продужити за још толико на основу одлуке истражног судије. Такође, полиција може наредити лицу које надгледа функционисање рачунарског система или обавља задатке у вези са обрадом, складиштењем или преносом пода-

така у систему да пружи информације потребне за предузимање претреса, као и да предузме неопходне техничке мере да се осигура интегритет рачунарских података, а нарочито да се учине недоступним трећим лицима. Осим тога, та лица се обавезују на дужност да као тајну чувају чињеницу да се предузима претрес, као и на последице непоступања по истој.

Међу посебним доказним радњама Законик у члану 215. предвиђа и контролу података који су похрањени у системима за аутоматску обраду података (тачка 3). Ова посебна доказна радња може одредити у погледу лакших, тешких и нарочито тешких кривичних дела[20], ради прикупљања само оних информација потребних за доказивање чињеница у кривичном поступку за конкретно кривично дело или за доказивање другог кривичног дела за спречавање непосредне и значајне претње по јавну безбедност (члан 211). Кривична дела поводом којих се може одредити ова радња су сва за која је могуће одредити казну затвора од најмање три месеца, тако да Закон ову радњу третира као посебну не с обзиром на тежину кривичног дела, већ зато што су прикривене, односно врше се без обавештавања лица на које се односе.

У процесном законодавтсву ***Норвешке*** се на претрес рачунара примењују генералне одредбе о претресу просторија[21] а само једна одредба се изричито односи на претрес уређаја и система за аутоматску обраду података (члан 199а) којом је предвиђено да су сва лица која имају контролу над системом дужна да пруже обавештења неопходна за приступ подацима похрањеним у њима, јер се у супротном против њих може покренути поступак за кривично дело ометања правде.

У ***Великој Британији*** у складу са другим одељком Закона о полицији и кривичнопроцесним доказним радњама[22] полиција може тражити од суда доношење наредбе за претрес уколико постоје вероватноћа одређеног степена (оправдани разлози за веровање: *reasonable grounds for believing*) да је извршено кривично дело за које се може подићи оптужница (*indicta-*

[20] Кривични закон одређује категорије кривичних дела, тако што су мање озбиљна она кривична дела за које је могуће изрећи казну затвора од 3 месеца до 3 године, тешка су она кривична дела за које је могуће изрећи казну затвора од 3 до 8 година, а нарочито тешка су кривичних дела за које је могуће изрећи казну затвора од најмање 8 година или доживотну казну. Вид. члан 7. КЗ: http://www.knab.gov.lv/uploads/eng/the_criminal_law2014.pdf.

[21] Вид. чланове 190-202. http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

[22] *Police and Criminal Evidence Act 1984*, http://www.legislation.gov.uk/ukpga/1984/60. На основу овог Закона донет је Правилник о претресу просторија и одузимању предмета (*Code of practice for searches of premises by police officers and the seizure of property found by police officers on persons or premises*) којим се прецизирају релевантне одредбе Закона, али се ниједна изричито не односи на претрес рачунара. Вид. https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/117591/pace-code-b-2011.pdf.

*ble offence*), да се у одређеној просторији могу пронаћи предмети од значаја за истрагу кривичног дела који могу бити релевантни докази, а на које се не односе законске привилегије или се не примењују посебне процедуре (члан 15). Уколико су испуњени наведени услови, суд овлашћује полицију да уђе у одређене просторије, изврши претрес и одузме одређене предмете (члан 16). Могу се одузети предмети у вези са наведеним или било којим другим кривичним делом, као и предмети за које постоји опасност да буди измењени, изгубљени или уништени (члан 19.став 3). Следећи став се односи на проширење овлашћења на одузимање компјутеризованих информација. Наиме, изричито је наведено да лице овлашћено да изврши претрес просторије има право и да захтева да се информације сачуване у електронском облику, а које су садржане у рачунару и којима се може приступити из просторије обухваћене наредбом за претрес, предају у видљивом и опипљивом облику подобном да се изузме са лица места или у облику из ког се може провести у видљиву и читљиву форму, уколико постоји оправдан разлог да се верује да представљају доказ за кривично дело поводом ког се врши претрес или било ког другог кривичног дела или су настали извршењем било ког кривичног дела (члан 19. став 4). Предмети се одузимају ради форензичке обраде за потребе коришћења у поступку пред судом (члан 22. став 3).

Трећи део Закона о уређењу истражних овлашћења[23] посвећен је поступању са рачунарским подацима заштићеним енкрипцијом, а који су прикупљени или у вези са претресом рачунара или у вези са пресретањем комуникација које се остварују преко пружалаца услуга електронских комуникација. Уколико постоји вероватноћа (у виду оправданих разлога за веровање) да лице поседује кључ за енкрипцију који омогућава приступ заштићеним рачунарским подацима, полиција може захтевати да открије те податке, уколико је то потребно и неопходно за остваривање одређених циљева (између осталог, и ради откривања и спречавања кривичних дела) а ти подаци се не могу прикупити ни на који други начин. Лицу које одбије да поступи по захтеву, може бити одређен затвор у трајању до 2 године[24].

У ***САД*** судија прегледа документацију коју преко тужилаштва доставља полиција у виду предлога за издавање налога за претрес, те процењује да ли постоји вероватноћа (*probable cause*) да се у одређеном рачунару који се налази на одређеном месту могу пронаћи одређени дигитални докази. Уколико судија процени да су испуњени сви потребни формални и материјални услови (довољан степен одређености и вероватноћа), издаје налог

[23] http://www.legislation.gov.uk/ukpga/2000/23/contents
[24] Вид. чланове 49-56.

за претрес рачунара ради прикупљања података похрањених у електронском облику (*Warrant Seeking Electronically Stored Information*[25]). Налог овлашћује надлежни орган да одузме уређај или да одузме или копира податке похрањене у електронском облику, а осим тога, уколико није другачије одређено, налог садржи и овлашћење за накнадни преглед одузетог уређаја. У погледу издавања налога за претрес рачунара, међутим, осим поменутих услова, поједини судови траже од тужилаштва испуњење додатних услова пре издавања налога за претрес рачунара[26], и то да се сагласи, између осталог, да се одриче од могућности позивања на тзв. *plain view doctrine*[27] као и да претрес рачунара не обављају иста лица која врше претрес простора (односно, да полицијски истражитељи који добију овлашћење да изврше претрес простора неће имати никакву улогу у претресу рачунара који су идентификовани у налогу за претрес, него ће те задатке обавити независна трећа страна или стручњак дигиталне форензике (који је у систему кривичног правосуђа)[28]. Примену ових ограничења судови прав-

[25] Претрес је регулисан правилом бр. 41. Федералних правила о кривичној процедури, а правилом бр. 41(е)(2)(В) предвиђено је издавање налога ради проналаска електронских доказа, вид. *Federal Rules of Criminal Procedure*, http://www.law.cornell.edu/rules/frcrmp.

[26] Судови се позивају на додатне рестриктивне услове (тзв. *CDT* II услови) који су установљени 2009.године у прецеденту *United States v. Comprehensive Drug Testing, Inc.,* 579 F.3d 989 9th Cir. (2009). Више о томе вид. J. Saylor, „Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches“*, Fordham Law Review* 6/ 2011, 2839-2845.

[27] Четврти амандман на Устав САД штити грађане од претреса простора у ком имају разумно очекивање приватности, осим уколико су надлежни органи за то овлашћени налогом који је издао судија. Ипак постоји неколико изузетка од тог правила, односно неколико могућности да се претрес изврши и без таквог налога, а један од тих изузетака је и „*plain view doctrine*“ (установљена у прецеденту *Horton v. California,* 496 US 128 (1990). По овој доктрини, органу није потребан налог да прибави доказ уколико 1) се налази у законитој позицији да нешто посматра, односно уочи (нпр. има налог за претрес рачунара); 2) има законито право да приступи одређеном предмету који је у “*plain view*” (односно налази се пред њим, нпр. да отвори одређену датотеку током вршења претреса рачунара); 3) а инкриминишућа природа тог доказа је неминовно уочљива одмах (“*immediately apparent*”) (нпр. датотека коју отвори садржи графички приказ злостављања детета). Уколико су испуњени ови услови, орган може и без налога да одузме предмете,односно доказе који нису били одређени у налогу јер га је управо првобитно издати налог (иако није предвидео могућност проналаска тог доказа) довео у закониту позицију да посматра и уочи доказе на законит начин.

[28] Што се тиче услова да претрес рачунара могу да врше од стране суда одређени стручњаци, и то: или независна трећа страна (по основу Закона о похрањеним подацима о комуникацијама (*Stored Communications Act*), пружаоци услуга електронских комуникација и услуга удаљеног рачунарства извршавају налоге за претрес) или специјализована лица у оквиру органа (која се при том обавезују да информације до којих су дошли претресом а које се не односе на кривична дела поводом којих је налог за претрес издат не откривају полицији, односно тужилаштву), а да се тужилац и истражитељ (који имају сазнања о кон-

дају чињеницом да се претрес рачунарског система који садржи енормне количине података извршава применом метода и техника које су у далеко већој мери интрузивне од оних које се примењују током претреса у физичком свету, па је потребно додатно обезбедити заштиту права приватности корисника рачунара[29]. Уколико приликом претреса наиђе на датотеку која је иманентан доказ за друго кривично дело, позивањем на *plain view* изузетак полиција би могла да оправда прибављање доказа иако за њега није имала налог за претрес, односно да пронађену датотеку искористи као *probable cause*, односно неопходни формални услов за издавање другог налога за претрес ради проналаска додатних доказа о другом кривичном делу. Међутим, условљавањем издавања налога за претрес непозивањем на поменуту доктрину суд штити слободу корисника рачунара од неоснованог претреса (укида се изузетак од важења 4. Амандмана). Иако поједини аутори сматрају да је такво поступање суда не само прихватљиво, него је то и њихова обавеза ради заштите приватности корисника рачунара[30], не по-

---

кретном случају) у потпуности искључују из вршења претреса рачунара (чак ни у виду надгледања или давања смерница), то се доводи у питање ефективност и ефикасност претреса, јер је неминовно да такво решење проузрокује повећање трошкова, временско одуговлачење, шири обухват претреса него што је неопходно, односно предвиђање битних доказа за конкретан случај. Ипак, смисао оваквог ограничења је да се створи брана превеликом дискреционом овлашћењу државних органа поверавањем извршења радње претреса непристрасном и незаинтересованом лицу. Вид. B. Simpson, "Preemptive suppression" – judges claim the right to find digital evidence inadmissible before it is even discovered", *Journal of Digital Forensics, Journal of Digital Forensics, Security and Law* 4/2012, 34.

[29] Позивањем на ову доктрину би полиција могла, након што буде овлашћена издавањем налога за претрес рачунара, сваки доказ који пронађе у рачунару (јер је у законитој позицији да уочи податке *in plain view*) да користи против одређеног лица (вид. R. Chang, „Why the plain view doctrine should not apply to digital evidence", *Suffolk journal of trial and appellate advocacy* 1/2007, 43). Постоји озбиљан ризик да се сваки налог за претрес ради проналаска електронских информација може претворити у незаконити општи налог (који је у супротности са захтевима 4. Амандмана) злоупотребом овлашћења у налогу да претресу рачунар ради проналаска одређеног доказа да је одређено лице извршило одређено кривично дело како би пронашли доказ о извршењу било ког кривичног дела. (више томе вид. R. Moore., "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice* 1/2004, 55-73; O.Kerr, „Searches and Seizures in Digital World", *Harvard Law Review* 2/2005, 531-585). Тиме што суд условљава издавање налога за претрес саглашавањем тужилаштва да се не позивају на ову доктрину значи да поједини докази који се не односе на дело поводом ког је издат налог за претрес не могу користити (иако законито прибављен). Вид. B. Simpson, "Preemptive suppression" – judges claim the right to find digital evidence inadmissible before it is even discovered", *Journal of Digital Forensics, Security and Law* 4/2012 , 25.

[30] *О потреби да се полицији на овај начин онемогући коришћење широких дискреционих овлашћења, више вид. P. Ohm, „*Massive Hard Drives, General Warrants, and the Power of Magistrate Judges", Virginia Law Review *1/2011, 97-130; J.Stinsman, „Computers and Searches, Rethinking the Applicability of the Plain View Doctrine",* Temple Law Review *4/2011, 1097-*

стоји ниједан правни основ да суд у сваком конкретном случају приликом одобравања претраге рачунара унапред оглашава доказе до којих се дошло поменутом доктрином недозвољеним, јер постоји механизам контроле појединачних доказа[31] (правило о издвајању незаконитих доказа, тзв. *exclusionary rule*[32]) применом ког би незаконито поступање полиције било санкционисано немогућношћу употребе доказа до ког се дошло на тај начин, односно противно налогу[33].

***Хрватски*** Закон о кривичном поступку прописују да се претрес предузима ако је вероватно да ће се пронаћи трагови и предмети потребни за кривични поступак[34], на основу налога судије истраге (који решава о захтеву одмах, а најкасније у року од четири сата од пријема захтева) а који се извршава се у року од три дана од дана издавања (након протека рока, претрес се више не може извршити на основу тог налога). Осим тога, јавни тужилац или полиција приликом вршења увиђаја лица места за кривично дело које се гони по службеној дужности може спровести претрес одмах, а најкасније осам сати након што је кривично дело откривено, уколико је то преко потребно ради отклањања опасности по живот и здравље људи или имовину већег опсега или ради осигурања трагова и доказа који су у непосредној вези с кривичним делом због којег се обавља увиђај (осим ако се ради о претрази дома). У члану 257. којим се уређује претрес покретне ствари, посебно је наведено да ова радња обухвата и претрес рачунара и с њим повезаних

---

*1120; M. Dodovich, „*The Plain View Doctrine Strikes Out In Digital File Searches", A Journal of Law and Policy for the Information Society *6/2011, 659- 691.*

[31] B. Simpson, *op.cit*, 31.

[32] Правило установљено (у прецеденту *Weeks v. US*, 232 US 383 (1918) да би се онемогућило да тужилаштво заснива оптужбу на доказима који су прибављени противно закону, односно кршењем Уставом загарантованих права.

[33] Поједини аутори сматрају да би једино следећа ограничења у налогу за претрес, а која се тичу начина извршавања радње, била оправдана: 1) ограничење у погледу хардвера који се претреса; 2) ограничења временског трајања претреса; 3) ограничења у погледу фаза извршења претреса како би се ограничио приступ доказима који нису обухваћени налогом; 4) ограничења у погледу момента враћања хардвера кориснику. Уколико се приликом претреса рачунара не би поштовала ова ограничења предвиђена налогом, такви докази би били незаконити и по правилу о издвајању недозвољених доказа, не би се могли користити у поступку (вид. O. Kerr, „Ex Ante Regulation of Computer Search and Seizure", *Virginia Law Review* 6/2010, 1241-1293). Значајна су и следећа ограничења: 1) налог би требало да одреди одговарајући метод којим се врши претрес спрам околности случаја; 2) *plain view doctrine* је могуће применити само у погледу доказа који су у везу са доказима поводом којих је налог за претрес издат; 3) налог треба да одреди начин извршавања којим се откривају само они докази поводом којих се налог и издаје; 4) налог одређује које лице извршава претрес (J Saylor., „Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches", *Fordham Law Review* 6/ 2011, 2854-2857).

[34] http://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku, вид. чланове 240-250.

уређаја, других уређаја који служе прикупљању, похрањивању и преносу података, телефонским, рачунарским и другим комуникацијама и носилаца података. Лице које користи рачунар или има приступ рачунару или другом уређају или носиоцу података, те пружалац услуга електронских комуникација, дужно је да органу који спроводи претрес омогући приступ рачунару, уређају или носиоцу података и да пружи потребна обавештења за несметану употребу и остварење циљева претреса. Осим тога, лица су дужна по налогу органа који предузима радњу да предузму мере којима се спречава уништење или мењање података, а које радње орган може наложити и стручном помоћнику. Лице које користи рачунар или има приступ рачунару или другом уређају, као и пружалац телекомуникацијских услуга, а који не поступе у складу са поменутим обавезама, судија истраге може на предлог јавног тужиоца казнити (новчаном казном у износу до 50.000,00 куна, а ако и након тога не поступи по захтеву, лице се може се казнити затвором до извршења захтева, а најдуже месец дана), али се одредба о кажњавању не односи на окривљеног. У вези са претресом рачунара је радња привременог одузимања предмета. Привремено се одузимају предмети који се одузимају према кривичном закону или који могу послужити при утврђивању чињеница у поступку. Сва лица која држе такве предмете, дужна су да их предају на захтев јавног тужиоца или полиције, који држаоце предмета упозоравају на последице које произлазе из одбијања поступања по захтеву. Чланом 263. предвиђена је сходна примена општих правила о одузимању предмета и на податке похрањене у рачунарима и с њим повезаним уређајима, те уређајима који служе прикупљању и преносу података, носиоце података и на претплатничке информације којима располаже пружалац услуга. Подаци се на писани захтев јавног тужиоца у ком се одређује рок у ком се подаци предају, и у целовитом, изворном, читљивом и разумљивом облику. У случају одбијања предаје, судија истраге лица (осим окривљеног и лица које су ослобођене дужности сведочења) која одбију да предају предмете (а за то не постоје оправдани разлози), може на образложени предлог јавног тужиоца казнити (новчаном казном у износу до 50.000,00 куна, а ако и након тога не поступи по захтеву, лице се може се казнити затвором до извршења захтева, а најдуже месец дана). Подаци се снимају у реалном времену, а при прибављању, снимању, заштити и чувању података посебно се води рачуна о прописима који се односе на чување тајности одређених података. Према околностима, подаци који се не односе на кривично дело због ког се поступа, а потребни су лицу према којој се спроводи радња, могу се снимити на одговарајуће средство и вратити том лицу и пре окончања поступка. На предлог јавног тужиоца судија истраге може решењем одредити заштиту и чување свих рачунарских података, док је то потребно, а најдуже шест месеци, а на-

кон тога се враћају, осим ако су укључени у извршење кривичних дела против рачунарских система, програма и података или другог кривичног дела за које се гони по службеној дужности а учињено је помоћу рачунарског система.

## 4. Претрес рачунара у Законику о кривичном поступку

***Српски*** Законик о кривичном поступку[35] садржи неколико одредаба које би могле бити релевантне за остваривања приступа и увида у садржај похрањених рачунарских података. Међутим, могу се уочити недоследности у регулисању могућности предузимања увиђаја на стварима и претресања предмета. Наиме, када је за утврђивање или разјашњење неке чињенице у поступку потребно непосредно опажање органа поступка, може се предузети увиђај на стварима, приликом чега орган поступка по правилу тражи помоћ стручног лица форензичке струке, које, по потреби, предузима и проналази, обезбеђује или описује трагове, врши потребна мерења и снимања, сачињава скице или прикупља друге податке (члан 133). Претресање стана и других просторија или лица може се предузети ако је вероватно да ће се претресањем пронаћи окривљени, трагови кривичног дела или предмети важни за поступак, а у члану 152. став 3. предвиђено је да предмет претресања могу бити и уређаји за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи. У члану 152. став 2. предвиђено је да се претресање стана и других просторија или лица, по правилу, предузима на основу наредбе суда, али и да се изузетно може предузети без наредбе (у складу са члановима 158-160). Међутим, како *претресање уређаја* за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи *без наредбе није изричито уређено (чак шта више изричито је предвиђено да се предузима на основу наредбе суда), нити је предвиђена сходна примена правила* о претресању стана и других просторија без наредбе, простим језичким тумачењем се долази до закључка да је за претресање ових уређаја и опреме у сваком случају потребна судска наредба. Уколико би се приликом увиђаја места пронашли рачунари у којима могу бити похрањени електронски докази, орган поступка би, дакле, био овлашћен само да предузме мере обезбеђења, односно да уз помоћ стручног лица *предузима и проналази, обезбеђује или описује трагове,* не и да оствари приступ у смислу претресања рачунара, док не добије наредбу суда. Ове одредбе су неусклађене, јер се обезбеђивање трагова које стручно лице треба да изврши не може да се

[35] Законик о кривичном поступку, „Службени гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014.

предузме без остваривања приступа рачунару и прегледа. Зато би било корисно предвидети могућност да орган поступка може само у изузетним околностима, предузети претрес и без наредбе, уз обавезну помоћ стручног лица, а установити обавезно обезбеђивање трагова приликом вршења увиђаја на начин да се поштују права окривљеног и других лица.

Приликом предузимања увиђаја сва лица су дужна да органу поступка омогуће приступ стварима и пруже потребна обавештења. Слично томе, приликом претресања држалац уређаја и опреме или присутно лице се обавезује да омогући приступ и пружи обавештења потребна за њихову употребу, међутим, изричито је прописано да се то не односи на окривљеног, лица искључена (члан 93) и ослобођена (члана 94. став 1) од дужности сведочења, као ни на лица за која је вероватно да би тиме изложило себе или блиско лице (из члана 95. став 2) тешкој срамоти, знатној материјалној штети или кривичном гоњењу. Из овога би се могао извести закључак да је окривљени дужан да као и сва друга лица приликом предузимања увиђаја сарађује у наведеном смислу, што је супротности са привилегијом од самооптуживања, па је потребно ову одредбу изменити и при томе је усагласити са чланом 157. ставом 3.

Уколико се током увиђаја или претреса стана и других просторија пронађу предмети који могу имати значај доказа, под условима из члана 147, могу се привремено одузети, и то предмети који се по Кривичном законику морају одузети или који могу послужити као доказ у кривичном поступку привремено одузети (по потреби, уз претходни преглед предмета у присуству стручног лица). Лица која држе те предмете дужна су да органу поступка омогуће приступ предметима, пруже обавештења потребна за њихову употребу и да их на захтев органа предају (осим окривљеног и лица која су искључена од дужности сведочења), а уколико то не учине, јавни тужилац или суд може их казнити новчано до 150.000 динара, а ако и после тога одбије да испуни своју дужност, може га још једном казнити истом казном. У предмете који се привремено могу одузети спадају и уређаји за аутоматску обраду података и уређаји и опрема на којој се чувају или се могу чувати електронски записи. Иако Законик није предвидео сходну примену ових правила и на рачунарске податке, обавеза би се могла односити и на предавање рачунарских података јер се они у смислу члана 2. става 26. сматрају исправом уколико су подобни или одређени да служе као доказ чињенице која се утврђује у поступку.

У погледу претпоставки за претресање и поступка претресања Законик не садржи више ниједну одредбу која би се односила на претресање рачунара нити предвиђа сходну примену правила о претресању стана и других просторија.

Иако је похвално то што је законодавац поменуо да уређаји за аутоматску обраду података и опреме могу бити предмет претреса, потребно је унети поједине одредбе које би омогућиле ефективно предузимање претреса тих уређаја и опреме узимајући у обзир правила дигиталне форензике, а не претпостављати примену општих правила о вршењу претреса. Аналогно посматрање претреса у физичком свету и у виртуелном окружењу је поједностављивање које игнорише чињеницу да се претрес рачунарског система, који садржи енормне количине података, извршава применом метода и техника које су у далеко већој мери интрузивне од оних које се примењују током претреса у физичком свету, па је потребно додатно обезбедити заштиту права приватности корисника рачунара[36], како у погледу услова и претпоставки, тако и поступка претресања. Да ли овлашћење за претрес рачунара ради претраге електронских доказа треба да подразумева право органа да прегледа и анализира сваку датотеку ради проналаска доказа и могућност одузимања свих евентуално инкриминишућих података? Сматрамо да не. Иако је Законик прописао да предмети који нису у вези са кривичним делом због кога је претресање предузето, али који указују на друго кривично дело за које се гони по службеној дужности, могу привремено одузети, није прихватљива проста сходна примена правила на рачунарске податке. Сматрамо да је наредбом за претрес потребно ограничити могућност претреса ради проналаска рачунарских података потребних за конкретно кривично дело, тако да се у наредби одреди одговарајући метод којим се врши претрес спрам околности случаја, односно начин извршавања којим се откривају само они докази поводом којих се наредба и издаје.

С обзиром на природу рачунарских података похрањених у рачунару, било би корисно омогућити и да се претрес уређаја из разлога хитности може предузети у појединим случајевима када то налажу разлози хитности и без одлуке суда, као и овластити јавног тужиоца или полицију да приликом вршења увиђаја лица места за кривично дело које се гони по службеној дужности може спровести претрес уређаја одмах, уколико је то преко потребно ради осигурања трагова и доказа који су у непосредној вези с кривичним делом због којег се обавља увиђај (осим ако се ради о претресу дома), уз обавезу обавештавања суда подношењем извештаја са свим при-

[36] Више о разликама претреса у физичком и виртуелном окружењу вид: M. Adler, „Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search", *The Yale Law Journal* 4/1996, 1093-1120; J. Saylor, „Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches", *Fordham Law Review* 6/ 2011, 2822-2824; B. Weir, „It's (Not So) Plain To See: The Circuit Split On The Plain View Doctrine In Digital Searches", *Civil Rights Law Journal* 1/2010, 83-121.

купљеним доказним материјалом ради накнадног одобрења радње и могућности коришћења прикупљених доказа.

Осим прописивања обавезе лица да омогуће приступ рачунару и пруже потребна обавештења, потребно је предвидети санкције за лице које без оправданог разлога одбије да поступи у складу са поменутим обавезама (предвидети сходну примену члана 148. став 2.).

У вези са одузимањем предмета потребно је предвидети сходну примену правила о одузимању предмета и на похрањене рачунарске податке. Осим тога, потребно је прописати начин на који се рачунарски подаци одузимају, као и овлашћење органа да захтева предају потребних рачунарских података, похрањених у рачунару и оних којима се може приступити из просторије обухваћене наредбом за претрес, и то у целовитом, изворном, видљивом и опипљивом облику подобном да се изузме са лица места или у облику из ког се може провести у видљиву и читљиву форму, уколико постоји оправдан разлог да верује да могу представљати доказ. При томе, потребно је ограничити могућност одузимања појединих категорија рачунарских података, с обзиром на њихов садржај као и ограничити могућност обавезивања окривљеног као и одређених категорија лица (лица која нису дужна да сведоче у кривичном поступку услед постојања обавезе чувања државне, службене и професионалне тајне или одређеног степена сродства са окривљеним). Такође, било би целисходно предвидети санкције за лица која одбију да предају потребне податке, односно сходну примену правила о санкцијама за непоступању по дужности предавања предмета. Осим тога, потребно је прописати које податке надлежни органи могу тражити од пружалаца услуга електронских комуникација. Од пружалаца услуга би се могло тражити *предавају комуникације које су ускладиштене у електронском комуникационом систему* само на основу одобрења суда а у складу са правилима кривичне процедуре којом се одобрава претрес рачунара, док би се *подаци о кориснику* (име и презиме, адреса, дужина коришћења и врста комуникационих услуга које користи и начин плаћања и сл) могли захтевати посебном наредбом суда. Из тог разлога је потребно предвидети могућност да јавни тужилац до добијања наредбе суда може наредити пружаоцима услуга да задрже, односно обезбеде у неизмењеном облику одређене податке.

У погледу могућности проширења иницијалног претреса рачунара на други рачунар који није обухваћен наредбом а ком се преко претресаног рачунара може приступити, неопходно је унети изричиту одредбу у Законик, а ту могућност условити оправданим разлозима (ако је испуњен услов у виду постојања вероватноће да ће у супротном доћи до губитка тих података).

## 5. Закључна разматрања

На основу наведеног, процесна законодавства која предвиђају да се одредбе о претресу и одузимању предмета примењују на рачунаре и рачунарске податке *нису у складу са чланом 19. Конвенције*, јер не омогућавају обезбеђење рачунарских података ни на који начин осим обезбеђења уређаја који је извор електронских доказа, што није довољно. Уколико би се направила аналогија између претреса ради проналаска и одузимање исправе и претреса рачунара ради проналаска електронских доказа (уколико се електронски докази посматрају само као врста исправа), могле би се разликовати две ситуације. "Традиционални" претрес и одузимање исправа подразумева потрагу за подацима који су регистровани у прошлости у неком опипљивом облику (нпр. записи на папиру), те преглед садржаја исправе и одузимање са лица места, при чему се прикупљају подаци који постоје у време претреса. Међутим, за претрес рачунара ради проналаска електронских доказа *потребне су додатне одредбе* како би се обезбедило да се рачунарски подаци прикупе на једнако ефективан начин као приликом прикупљања исправе као покретног предмета, и то *из више разлога*: подаци су у неопипљивом облику и могу бити читани само кроз употребу рачунарског уређаја; услед непостојане природе података, а ради очувања интегритета електронских доказа, ствара се клон уређаја, односно копија података још на лицу места, поред одузимања уређаја; подаци могу услед повећане умрежености рачунарских система бити похрањени на неком другом рачунару а ком се може без тешкоћа приступити преко рачунара који се претреса. *Из тог разлога је потребно створити механизам да се рачунарски подаци приликом претреса рачунара обезбеде у складу са својом природом.* Иако се тај циљ остварује применом правила дигиталне форензике, поједина правила је нужно инкорпорисати међу одредбе које уређују кривичну процедуру.

*Milana M. Pisarić, Assistant*
*University of Novi Sad*
*Faculty of Law Novi Sad*

# Search of Computers for Discovery of Electronic Evidence

***Abstract:*** *In order to address the specific nature of criminal activities committed using computer networks and systems, the efforts of states to adapt or complement the existing criminal law with purposeful provisions is understandable. To create an appropriate legal framework for supressing cybercrime, except the rules of substantive criminal law predict certain behavior as criminal offenses against the confidentiality, integrity and availability of computer data, computer systems and networks, it is essential that the provisions of the criminal procedure law contain adequate powers of competent authorities for detecting sources of illegal activities, or the collection of data on the committed criminal offense and offender, which can be used as evidence in criminal proceedings, taking into account the specificities of cyber crime and the environment within which the illegal activity is undertaken. Accordingly, the provisions of the criminal procedural law should be designed to be able to overcome certain challenges in discovering and proving high technology crime, and the provisions governing search of computer for discovery of electronic evidence is of special importance.*

***Key words:*** *Cyber crime, computer, search, electronic evidence.*

Датум пријема рада: 22.04.2015.