УНИВЕРЗИТЕТ У БЕОГРАДУ

ПРАВНИ ФАКУЛТЕТ

Милана М. Писарић

ПОСЕБНОСТИ ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

докторска дисертација

Београд, 2016

UNIVERSITY OF BELGRADE

FACULTY OF LAW

Milana M. Pisarić

SPECIFITIES OF PROVING CYBER CRIME

Doctoral Dissertation

Belgrade, 2016

Ментор:
Проф. др Милан Шкулић, редовни професор Правног факултета Универзитета у Београду

Чланови комисије:

1. Проф. др Милан Шкулић, редовни професор Правног факултета Универзитета у Београду;
2. Проф. др Бранислав Симоновић, редовни професор Правног факултета Универзитета у Крагујевцу;
3. Проф. др Татјана Бугарски, ванредни професор Правног факултета Универзитета у Новом Саду;
4. Доц. др Вања Бајовић, доцент Правног факултета Универзитета у Београду.

Датум одбране:

ПОСЕБНОСТИ ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Резиме

Предмет дисертације је уочавање и анализа посебности откривања и доказивања кривичних дела обухваћених појмом високотехнолошког криминала.

У раду је указано је на одређене аспекте високотехнолошког криминала који га чине у значајној мери комплексном темом за проучавање од стране правника, а њихово неразумевање, односно неузимање у обзир представља озбиљну препреку институционалном одговору од стране надлежних органа. Наиме, поједине појавне облике карактерише просторна удаљеност између учиниоца и оштећеног која може бити прилично екстремна чиме се под местом извршења кривичног дела може сматрати неколико локација укључујући и неколико држава. Осим тога, вероватноћа откривања учинилаца је далеко мања него код традиционалних кривичних дела услед могућности сакривања идентитета у кибер простору при чему су средства извршења у домену високе технологије које се непрестано мења и учиниоци имају широк избор инструментаријума. С обзиром на то да се ради о релативно новој појави за надлежне органе, у погледу које су неопходна специјализована знања, кроз анализу прописа и примера добре праксе уочени су облици специјализације надлежних органа у супротстављању високотехнолошком криминалу. Уопште, размотрена су овлашћења која је потребно дати надлежним органима како би се створили одговарајући механизми за улажење у траг учиниоцима кривичних дела и обезбеђење доказа за потребе покретања и вођења кривичног поступка.

Полазећи од тога да се природа електронских записа који би се могли употребити као доказ у кривичном поступку и потребан форензички рад у прикупљању и обради тих података веома разликују у односу на уобичајене трагове и доказе, посебна пажња је посвећена правилима криминалистичке тактике и технике прилагођеним специфичностима података у рачунарима, рачунарским системима и рачунарским мрежама (тзв. дигитална форензика).

У циљу давања предлога *de lege ferenda*, сагледани су проблеми са којима се суочавају надлежни органи, анализиран је позитивноправно оквир у Репблици Србији и упоређен са релевантним прописима на међународном и

наднационалном нивоу и одредбама одговарајућих прописа у појединима државама. Резултати рада представљају доринос теоријском и практичном разјашњењу проблематике која је предмет докторске дисертације, па постоји могућност њихове практичне примене с обзиром ма то да је ово област у константном развоју и отворена и подложна модификовању.

Кључне речи: кривични поступак, доказивање, доказ, високотехнолошки криминал, електронски докази, заштита приватности
Научна област: правна
Ужа научна област: кривичноправна
УДК: 343.533::004

SPECIFITIES OF PROVING CYBER CRIME

Summary

The subject of the dissertation is the identification and analysis of specifics of detecting and proving criminal offenses covered by the concept of cyber-tech crime.

The paper points to certain aspects of cybercrime that make it significantly complex subject for the study by lawyers, and which lack of understanding or not taking into account, constitutes a serious obstacle to the institutional response by the competent authority. In fact, some forms of cyber crime are characterized by the spatial distance between the perpetrator and the victim, which can be quite extreme, while under the place of commission of the crime several locations, including several states, may be considered. In addition, the probability of detection of offenders is far smaller than in case of traditional crimes, due to the possibility of hiding the identity in cyber space, where the means of execution are in the field of high technologies constantly changing which provides offenders with a wide variety of instruments and tools. Given that this is a relatively new phenomenon for the competent authorities, in respect of which the necessary specialized knowledge is needed, through the analysis of the regulations and good practice the forms of specialization of competent authorities in fighting cybercrime are observed. In general, the author reviewed the powers that should be given to the competent authorities in order to create appropriate mechanisms for tracing offenders and securing evidence for the purpose of initiation and conduct of criminal proceedings.

Starting from the fact that the nature of electronic records that could be used as evidence in criminal proceedings and necessary forensic work in collecting and processing these data are very different compared to the usual clues and evidence, particular attention was paid to the rules of criminal tactics and techniques adapted to specific data in computers, computer systems and computer networks (the so-called. digital forensics).

In order to make certain de lege ferenda proposals, the problems faced by the authorities are analyzed, as well as positive legal framework in Republic of Serbia which was compared to the relevant regulations at the international level and the provisions of relevant legislation in individual countries. Results of the work represent

contribution to theoretical and practical clarification of the problem which is the subject of doctoral dissertations and therefore have the possibility of practical application with respect to matter that this is an area in constant development and open and subject to modification.

Keywords: criminal procedure, proving, evidence, cyber-crime, electronic evidence, privacy protection.

Scientific field: law

Specific scientific field: criminal law

UDK: 343.533::004

САДРЖАЈ

УВОД

Током протеклих педесетак година технолошки напредак је радикално променио личне и пословне активности појединаца, те функционисање друштва и државе. Од изума у касним 40-им годинама двадесетог века, рачунар и са рачунаром повезана технологија данас имају доминантну улогу у савременој култури, па се друштво тешко може замислити без постојања и ослањања рачунаре, чему је посебно допринела широка доступност за јавну употребу Интернета и других рачунарских мрежа које повезују рачунарске системе из целог света. Са развојем технологије производње рачунара, мобилних телефона и других преносивих електронских уређаја за обраду и пренос података, омогућен је приступ подацима преко рачунарских мрежа са сваког места у сваком тренутку. Појава и распрострањеност савременог концепта „рачунарство у облаку“, у оквиру ког се подаци складиште и њима се приступа у потпуности преко Интернета и других рачунарских мрежа (тзв. *cloud computing*), додатни је фактор повећања свеопште зависности од информационих технологија у свакодневном животу. Како се све више података о личности, од електронске поште до банковних рачуна, као и података од значаја за функционисање привреде и државе складиште у „облаку“, а који у сваком тренутку могу бити објект напада злоупотребом информационих система, оправдано је очекивање појединаца и привредних субјеката и других правних лица да се правно уреди заштита тих података у смислу очувања њихове безбедности. Сходно томе, државе настоје да одрже корак са технолошким напретком и заштите физичка и правна лица од злоупотреба информационих система, а *ultima ratio* у заштити наведених добара је прописивање одређених понашања као кривичних дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система и мрежа, а која се могу обухватити појмом високотехнолошког криминала. Да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских система и мрежа, разумљиво је опредељење држава да прилагоде, односно употпуне постојеће кривичне законе новим одредбама. За стварање одговарајућег правног оквира за супротављање овој врсти криминала путем кривичног права, осим што се у прописима кривичног материјалног права

одређена понашања инкриминишу, те предвиђају као кривична дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система и мрежа, неопходно је да прописи кривичног процесног права садрже одговарајућа овлашћења надлежних органа у циљу откривања извора недозвољене радње, односно прикупљања података о учињеном кривичном делу и учиниоцу, који могу бити коришћени као доказ у кривичном поступку, а водећи рачуна о специфичностима високотехнолошког криминала и окружења у ком се недозвољене активности предузимају.

Као ***предмет*** дисертације одређено је *поимање високотехнолошког криминала и уочавање специфичности* које представљају изазов за откривање и обезбеђивања доказа потребних за вођење кривичног поступка за кривична дела код којих су рачунарски подаци, рачунарски системи или рачунарске мреже средство извршења или објект напада, а које произлазе из карактеристика коришћених информационих технологија. Полазећи од тога да се природа рачунарских података, који би могли имати значај доказа у кривичном поступку, и потребан форензички рад у прикупљању и обради тих података у знатној мери разликују у односу на уобичајене трагове и доказе (с обзиром на брзину којом се радња може предузети а трагови у електронском облику изменити, сакрити или уништити), посебна пажња је посвећена *правилима дигиталне форензике* прилагођеним специфичностима података у рачунарима, рачунарским системима и рачунарским мрежама. Полазећи од тога да је вероватноћа откривања радње и учинилаца далеко мања него код „традиционалних“ кривичних дела, услед могућности прикривања трагова у рачунарским системима и мрежама (при чему су средства извршења у домену високе технологије које се непрестано мења, а учиниоци имају широк избор инструментаријума за извршење дела и прикривање трагова), у дисертацији су *разматрана овлашћења* која је потребно дати надлежним органима како би се створили одговарајући механизми за улажење у траг учиниоцима кривичних дела и обезбеђење тзв. *електронских доказа* за потребе кривичног поступка. Како је једна од јединствених карактеристика високотехнолошког криминала то да се радња извршења предузима у виртуелном свету у ком не постоје границе територијалне надлежности одређених држава, јер извршиоци имају могућност да усмере напад на рачунаре или мреже било где у

свету и да напад спроводу посредством рачунара или мреже који се налазе на различитим локацијама у односу на државу у којој се налази рачунар извршиоца или рачунар који је објект напада, један од предмета дисертације је сагледавање постојећих *механизама међународне правне помоћи и сарадње у кривичним стварима,* као и разматрање потребе ангажовања посебних механизама прилагођених специфичностима високотехнолошког криминала. Осим тога, разматрани су минимални услови и гаранције које је потребно узети у обзир, како би се обезбедила адекватна заштита одређених људских права и слобода у складу са принципом владавине права и спречило арбитрерно поступање надлежних државних органа, приликом законског регулисања, односно одређивања и извршења одређених процесних радњи у циљу откривања и обезбеђивања електронских доказа.

Предмет истраживања проучаван је темељно и свеобухватно, како би се у потпуности разумела проблематика откривања и обезбеђења доказа за потребе кривичног поступка за дела високотехнолошког криминала. Сложеност и комплексност предмета истраживања захтевала је адекватан и са комплексношћу предмета усклађен истраживачки процес, што првенствено подразумева да је истраживање спроведено у неколико фаза. Након прикупљања научне и стручне литературе, те њихове анализе, уочена су општа и специфична питања у оквиру појединих предмета истраживања. Након тога, анализирани су одговарајући прописи, како би се пронашли одговори на питања постављена у претходној фази, а потом је уследило синтетизовање најбољих решења. Овом задатку приступило се применом нормативног, историјског, логичког, језичког и упоредно-правног метода, како би сви аспекти и специфичности предмета истраживања били обухваћени, а посебан значај имао је правно-догматски метод, тј. позитивно-правни метод чијом применом је у дисертацији дата синтетичка оцена предмета истраживања, на који начин је дат допринес постојећим позитивно-правним решењима која се односе на предметну проблематику, давањем одговарајућих предлога *de lege ferenda*. Ради сагледавања обима високотехнолошког криминала, анализирани су подаци добијени статистичким истраживањима који се спроводе у оквиру рада Републичког завода за статистику, као и подаци из Извештаја о раду одељења за борбу против високотехнолошког криминала Вишег јавног

тужилаштва у Београду у периоду од 2011. до 2014. године[1]. Одговарајући закључци у вези са предузимањем оперативних и кривичнопроцесних радњи и мера од стране органа унутрашњих послова изведени су на основу стручног интервјуа са представником Одељења за борбу против високотехнолошког криминала у оквиру Министарства унутрашњих послова Републике Србије. Вођење стручног интервјуа са Тужиоцем за високотехнолошки криминал резултирало је потпунијим сагледавањем стања законодавног оквира за поступање надлежних органа, те је препозната нужност његовог прилагођавања сходно потребама праксе у супртотстављању кривичним делима из надлежности Одељења, односно Тужилаштва. Такође, анализирана је судска пракса доступна у базама података Службеног гласника и *Paragraf*-а, на службеним Интернет страницама и у билтенима судске праксе Вишег суда у Београду, Апелационог суда у Београду и Врховног касационог суда, као и иностранa судскa праксa.

Што се тиче ***структуре***, дисертација, поред увода и закључка, садржи осам делова. У *првом делу* су најпре у оквиру првог поглавља сагледани савремено информационо окружење и могућности злоупотреба информационих технологија, па је одређен појам високотехнолошког криминала и указано је на његове карактеристике и обим. Посебно поглавље је посвећено правном оквиру за супротстављање високотехнолошком криминалу. *Други део рада* посвећен је основним изазовима у супротстављању високотехнолошком криминалу са којима се суочавају надлежни државни органи и претпоставкама за ефикасност поступка за дела високотехнолошког криминала, и то питањима у вези са надлежношћу за гоњење и суђење за дела високотехнолошког криминала, као и специјализацији надлежних државних органа. *Трећи* део носи назив доказивање дела високотехнолошког криминала, у оквиру ког су одређени појам и карактеристике електронских доказа, а потом је пажња посвећена посебним радњама за обезбеђење електронских доказа полазећи од Конвенције о високотехнолошком криминалу. У *четвртом* делу аутор анализира нормативни оквир за доказивање високотехнолошког криминала у Републици Србији, уз оцену усаглашености са одредбама Конвенције о високотехнолошком криминалу. *Пети део* представља

[1] Извештај о раду одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду у периоду од 2011. до 2014. године аутору је достављен на основу молбе упућене Тужиоцу за високотехнолошки криминал.

упоредноправни приказ решења из националних законодавстава који се односе на доказивање дела високотехнолошког криминала. *Шести део* посвећен је међународној сарадњи надлежних државних органа у супротстављању високотехнолошком криминалу. У овом делу су најпре анализирани општи оквири за пружање међународне правне помоћи у кривичним стварима и недостаци постојећих механизама, а потом је разматрана потреба примене специфичних правних механизама ради убрзавања прекограничне сарадње надлежних органа у откривању и доказивању. У *седмом делу* рада приказан је пут од електронских записа, као трагова, до електронских доказа. У оквиру *осмог дела* супротстављање високотехнолошком криминалу је доведено у везу са основним људским правима и слободама, а нарочита пажња посвећена је заштити права на приватност и заштити података о личности у вези са кривичним поступком. *Завршни део* дисертације је посвећен изношењу закључака (у смислу преиспитивања постављене опште претпоставке из које су биле изведене посебне и појединачне претпоставке) и формулисању предлога *de lege ferenda* (као резултата анализе позитивноправног оквира у Републици Србији и поређења са релевантним прописима на међународном и наднационалном нивоу, као и са одредбама одговарајућих прописа у појединим државама).

Научна оправданост избора теме заснива се на чињеници да наведена питања до сада нису била предмет целовите научне обраде у домаћој теорији, док практичан значај обраде предмета истраживања произлази из низа спорних питања која се јављају приликом настојања да се његови домети унапреде на нормативно и организационом нивоу, а услед непостојања адекватних одговора на иста. Проучавањем постојеће ***литературе*** о високотехнолошком криминалу дошло се до закључка да су се наслови бавили следећом проблематиком: одређивањем појма високотехнолошког криминала, његовим узроцима и појавним облицима (домен кривичног материјалног права и криминологије), кибер безбедношћу и превентивним деловањем ради повећања резилијантности рачунарских система на нападе употребом информационих технологија (домен безбедности), те појединим специфичностима поступања овлашћених државних органа на лицу места по сазнању да је учињено дело употребом рачунарских система и мрежа (домен криминалистике). Што се тиче наслова *кривичног*

материјалног права и криминологије, неколико имена су препозната као најзначајнији аутори у смислу оригиналног научног доприноса, па су њихови радови навођени у делу који се односи на појмовно одређење високотехнолошког криминала. Постоји велики број радова који обрађују питања *кибер безбедности*, али су они били релевантни за предмет дисертације само у мери у којој обрађују дигиталну истрагу као реакцију на угрожавање доступности, целовитости и поузданости рачунарских података. За сагледавање и анализу одређених аспеката криминалистичке тактике и технике повезане са обрадом дигиталног лица места консултовани су најрепрезентативнији наслови *дигиталне форензике*, но као проблем у вези са њима уочено је да обилују високософистицираним техничким детаљима, па је циљ аутора био да их прилагоди правничком резоновању. Чињеница је да постоје бројне књиге и приручници из области дигиталне форензике, али нису у довољној мери адекватни, односно чак су неподесни за употребу од стране надлежних органа откривања и доказивања, који су, ипак, лаици у овој области. Осим тога, у овим радовима нису обрађивана веома важна правна питања у вези са истрагом дела високотехнолошког криминала, а која морају бити узета у обзир и доведена у везу са криминалистичким аспектима, јер представљају оквир за предузимање појединих радњи за прикупљање електронских доказа. Технички је изводљиво доста тога што је приказано у овим насловима, али како право поставља ограничења за технологију, нарочито када је користе надлежни државни органи, значај појединих наслова који нису доводили правила дигиталне форензике са правом је тиме знатно умањен. Као изазов у обради теме указали бисмо на веома битну чињеницу да су *кривичнопроцесна питања* у вези са откривањем и доказивањем дела високотехнолошког криминала *предмет недовољног броја научних и стручних радова*. У том смислу, за сагледавање посебних аспеката доказивања дела високотехнолошког криминала од изузетног значаја су били релевантни међународноправни прописи, законска решења појединих држава, као и одређене публикације настале у оквиру појединих институција и организација на регионалном и међународном нивоу.

Резултати рада представљају ***допринос*** теоријском и практичном разјашњењу проблематике која је предмет дисертације, али имају и могућност практичне примене с обзиром на то да је ово област која је у константном развоју и отворена

и подложна модификовању. У дисертацији је аутор настојао да укаже на одређене аспекте високотехнолошког криминала који га у значајној мери чине комплексном темом за проучавање, а чије неразумевање, односно неузимање у обзир представља озбиљну препреку институционалном одговору, у смислу прописивања овлашћења надлежних државних органа за предузимање радњи откривања и доказивања. Проучавањем посебних аспеката високотехнолошког криминала у оквиру истраживања на изради дисертације и настојањем да се разуме њихова суштина, међусобна веза и утицај на откривање и доказивање, обогаћена је постојећа научна и стручна литература која се недовољно бавила предметном проблематиком. Осим тога, узимање у обзир у закључку изнетих предлога *de lege ferenda* може допринети употпуњавању позитивноправних решења а тиме и супротстављању делима високотехнолошког криминала.

Први део
ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

Постиндустријско друштво се под утицајем развоја технолошких и економских услова трансформисало у информационо друштво које карактерише глобализација производње и трговине, те прекогранични проток робе и услуга, а између осталог и информација и комуникација посредством рачунарских мрежа. Савремени теоретичари социологије користе различите термине за означавање оваквог друштва: кибер-друштво, друштво ризика, глобално друштво, дигитално друштво[2]. Предвиђања утицаја развоја информационе технологије на информатичко друштво могу се пронаћи у литерарним и научним радовима аутора из прошлог века[3]. Писац научне фантастике Вилијам Гибсон (*William Gibson*), за кога се везује настанак кованице *cyber space*[4], је у краткој причи објављеној 1982. године (десетак година пре настанка Интернета) предвидео да ће постојати „потпуно умрежен свет у виду јединственог конзистентног интерфејса без потребе за постојањем рачунара, чиме ће се окончати еволуција човечанства" јер ће настати „виртуелна реалност у којој ће корисници рачунарских мрежа из

[2] M. Goncalves, „Technological Change, Globalization and the Europeanization of Rights", *International review of Law Computers& Technology* 3/2002, 302.

[3] Термин информационо-комуникационе технологије је некоректан, јер постоје две технологије: рачунарска (чији садржај се првенствено односи на складиштење и обраду података и презентовање информација) и комуникациона технологија (која се односи на пренос података и информација). Ове две технологије имају различите садржаје и у првој фази су се користиле одвојено. Каснијом интеграцијом рачунарске технологије, којој је примарна аутоматска обрада података, и комуникационе технологије, којој је примаран пренос комуникационим линијама података и информација, настала је информациона технологија. Из тих разлога, оправдано је користити или независно термине: рачунарска технологија и комуникациона технологија или уместо њих њихову заједничку супституцију: информациона технологија. Види С. Петровић, „Дилема: сајбер или кибер", *Страни правни живот* 2/2012, 371-372.

[4] Све шира примена информационе технологије уводи и нову терминологију, која се олако, некритички, а често и без елементарног разумевања суштине значења појединих термина, олако уводи у наш језик, и тиме изазива проблеме и дилеме у њиховој употреби. Међу погрешно коришћеним терминима је и термин *сајбер* простор. Исправније је користити префикс *кибер-* који потиче од корена речи кибернетика, научне дисциплине која је изучавала информационо-управљачке функције система, а коју је амерички научник *Norbert Viner* назвао по грчкој речи *κυβερνητική* (што значи управљач, кормилар). Термин *сајбер* је скраћеница од транскрибоване речи *Cybernetics* [sajbÁ(r)'netiks]). Вид: С. Петровић, *op. cit*, 373. Према оксфордском речнику енглеског језика префикс *cyber-* означава повезаност са Интернетом (*Oxford English Dictionary*, http://www.oed.com/).

целог света комуницирати“[5]. Професор кривичног права Џин Стивенс (*Gene Stephens*) је у чланку „Криминал у години 2000-ој“ (“*Crime in the Year 2000*”) објављеном 1981. године у часопису *The Futurist* написао да ће „подаци из свих сектора система кривичног правосуђа бити компјутеризовани и међусобно повезани, што ће у многоме олакшати рад полиције“. Исти аутор је за поменути часопис објавио 1995. године чланак под називом „Криминал у сајбер простору“(“*Crime in Cyber space*”) у коме је изнео мишљење да ће „генерације извршилаца кривичних дела у кибер простору незапажено проузроковати штету од више милијарде долара, при чему ће већина проћи незапажени и неоткривени“, предвиђајући „кибер нападе на државне органе и привредне субјекте, масовне крађе са кредитних картица, компјутерске преваре, крађе идентитета...“ као и „употребу биометрије и енкрипције у заштити података“[6]. Разумевање онтолошких основа *концепта кибер простора* (који је потекао из тзв. *cyberpunk* покрета током 1980-их[7]) је потребно због тога што су ова дистопијска схватања током 1990-их превазишла домен научне фантастике и у великој мери утицала и утичу на развој информационе технологије, а готово ниједно предвиђање даљег развоја виртуелног окружења није до сада остало неостварено. Пре само двадесет и пет године рачунарска мрежа била је позната и доступна само уском кругу јавности: прве рачунарске мреже користила је војска, а потом научне и академске установе[8]. Даљи технолошки развој, превасходно рачунара и протокола за

[5] Кратка прича „*Burning Chrome*“ доступна је на следећем линку: www.williamgibsonbooks.com. Кованица *cyberspace* први пут је употребљена 1982, али су реч и концепт који означава популаризовани од издавања класика научне фантастике дела *Neuromancer* 1984. године.

[6] G. Stephens, „Cybercrime in the Year 2025“, наведено према: M. Pittaro, *Cybercrime: Current Perspectives from InfoTrac,* 2nd edition, Wadsworth Publishing, Andover 2009, 44.

[7] Овај покрет се заснивао на веровању да се информационе технологије треба користити за подржавање и култивацију индивидуализма, а нарочито за подстицање самоопредељења појединаца. Више о томе D. Wall, „Criminalizing cyberspace: the rise of the Internet as a crime problem“, *Handbook of Internet Crime* (eds. Y. Jewkes, M. Yar) Willan, Devon 2010, 89-94; S.Brown, „Fiction, fantasy and transformation in the imaginaries of cybercrime: the novel and after“, *Handbook of Internet Crime*, 145-167.

[8] Први рачунар у САД је настао 1946. године (*ENIAC*) у оквиру истраживања Министарства одбране, а као одговор на совјетско лансирање првог сателита у свемир 1957. године, створено је тело (*Advanced Research Project Agency*: *APRA*) са циљем да се мобилизује академска заједница ради помоћи америчкој војсци у доба Хладног рата. У оквиру овог тела повезани су рачунари са циљем размене информација и тако је 1969. године настала прва рачунарска мрежа *APRANet.* Током 1970-их је Војска покушала да уступи мрежу појединим комерцијалним актерима, али услед недостатка средстава приватног сектора да одржава мрежу, она је била финансирана од стране државе. САД су током 1980-их финансијски подржавале произвођаче да модификују нове моделе рачунаре како би се створила основа за њихово умрежавање. Више о томе J. Curran,

комуникацију умрежених рачунара, довели су до стварања Интернета, чијег експоненцијалног ширења (како у квантитативном, тако и у квалитативном смислу) смо сведоци. Од појаве *World Wide Web*-а[9] који је омогућио стварање Интернета, као јавно доступне глобалне мреже састављене од рачунарских мрежа, експоненцијално расте број корисника ове мреже[10]. Смањење значаја *dial-up* конекција и ширење *broadband* услуга довело је до стварања окружења у ком је потребно континуирано одржавање конекција, па телекомуникационе компаније улажу у мрежну експанзију чиме се повећавају капацитети мреже и доступност конекција, што доприноси даљем развоју бежичне и мобилне технологије[11]. Лакоћа приступа информацијама похрањеним у рачунарским системима преко рачунарских мрежа и њихова размена електронским путем омогућава државним органима и пословним субјектима да се са јавношћу повежу и путем *online* сервиса, па појединци могу употребом Интернета да приступе бројним услугама у

"Reinterpreting Internet history", *Handbook of Internet Crime* (eds. Y. Jewkes, M. Yar), 18-25; Н. Путник, Сајбер простор и безбедносни изазови, Београд 2009, 22-25.

[9] Током 1990. године *CERN* је повезан са *APRANet* мрежом, а 1991. године је створен *World Wide Web*, што је у ствари назив за први *browser* - графички интерфејс (*Graphic User Interface:GUI*). Творац концепта је *Tim Berners-Lee.* Ли је створио програмски код (*hypertext transfer protocol: HTTP*) као средство које је омогућило размену података у мрежи и обраду текста у реалном времену. Код је пуштен у оквиру *CERN-a* чиме је неограниченом броју људи омогућено да приступе, повезују се и остварују комуникацију у једној глобалној мрежи информација, односно Интернету као рачунарској мрежи (прва створена веб странице била је http://info.cern.ch). Ли је овај код сматрао „бесплатним поклоном за заједницу" па је својим изумом допринео стварању јавно доступних рачунарских мрежа - током 1993. године *World Wide Web* платформа је постала доступна јавности, те је уследила приватизација мреже у јавном власништву, и Интернет је до 1995. године постао комерцијализован систем. Више о томе G. Ferrera, *CyberLaw: Text and Cases*, Cengage Learning, Independence 2011, 10-13; M. Rustad, *Global Internet law in a nutshell*, St. Paul, MN: West, Boston 2013, 12-13.

[10] За свега три године од стварања, Интернет је почело да користи 50 милиона корисника. Да би се разумело колико је велики потенцијал *www* технологије, може се указати на податак да је телевизији као новој технологији било потребно 15 година да би достигла овај број корисника, а радију чак 37 година (J. Naughton, *A Brief History of Future: Origins and History of the Internet*, London, Weidenfeld and Nicolson 1999, 12). Од 1994. до 2008. године број земаља које су биле повезане на Интернет се од 83 попео на 200. Почетком 1996. било је регистровано 16 милиона корисника, до 2008. године је тај број порастао на 1.59 милијарди, што је око 20% глобалног становништва. Средином 2014. године је 42% становника (преко 3.2. милијарде) користило Интернет. У Европи 70.5% становника користи Интернет, на северноамеричком континенту чак 87.7% (http://www.internetworldstats.com/stats.htm), а дневно се пошаље преко 210 милијарди порука електронске поште (*Internet Statistics*, http://www.statisticbrain.com/internet-statistics/).

[11] Током 2012. године 1.58 милијарди корисника су приступали Интернету преко својих мобилних телефона, што је око 67% корисника Интернета - тај проценат је у 2014. години износио око 79%, а предвиђа се да ће до 2017. године чак 2.97 милирајди лица приступати Интернету преко мобилних телефона, што ће представљати 91% од укупног броја корисника Интернета, односно 58% корисника мобилних телефона (*A. Srivastava, 2 Billion Smartphone Users By 2015 : 83% of Internet Usage From Mobiles*, http://dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017/#ixzz2rcbChM tk).

све већем обиму и са све већом брзином и ефикасношћу (електронска трговина, електронска управа, електронско гласање и слично). Широкопојасне конекције, технолошке иновације и смањење цене коштања уређаја допринеле су дигитализацији информација, што је имало утицаја и на банкарски и финансијски сектор, нарочито у погледу услуга које се нуде клијентима (нпр. системи за електронско плаћање) и пословних трансакција (нпр. електронски клиринг). Пословни процесни, посебно у оквиру електронске трговине, постају све више глобализовани и међусобно повезани, те зависни од великих информационих система и платформи који подржавају остваривање пословних активности (нарочито *cloud computing*[12]). Као последица наведеног утицаја информационих технологија уочава се све већа количина дигиталног садржаја, тј. података који су похрањени у електронском облику, односно екстраховани из рачунара и других уређаја за складиштење, обраду и пренос података[13].

Неспорно је да је развој информационе технологије донео савременом друштву безброј погодности, јер су корисницима пружене значајне могућности у погледу приступа дигиталним садржајима и олакшано обављање свакодневних активности. Ипак, истовремено растућа зависност друштва и појединаца од информационих технологија условила је настајање ризика са потенцијално врло озбиљним консеквенцама у информатичкој ери. Полазећи од максиме да „криминалитет „користи“ прилику“ [14], сасвим је јасно што су са олакшаном могућношћу приступа и размене дигиталног садржаја, уследиле и злоупотребе информационих технологија у криминалне сврхе.

[12] Извештај о коришћењу *cloud* услуга у 2012. години показао је да око 375 милиона корисника Интернета користи ове сервисе, а предвиђено је да ће тај број до краја 2013. години износити преко 625 милиона (*ISM Projected To Cost U.S. Cloud Computing Industry $35B*, http://www.forbes.com/sites/louiscolumbus/2013/08/08/prism-projected-to-cost-u-s-cloud-computing-industry-35b/, 44.). Друго истраживање предвиђа да ће до краја 2017. године чак 1.3 милијарде лица користити ове услуге (*Cloud Services Users Will Hit 625 Million in 2013: IHS*, http://slashdot.org/topic/cloud/cloud-services-users-will-hit-625-million-in-2013-ihs).

[13] У студији из 2003. године је наведено да подаци похрањују и архивирају у електронском облику у уделу од 92%, нарочито на хард-дисковима. Количина створених дигиталних садржаја у 2006. године је износила 161 милијарди гигабајта што је еквивалентно са 230 милијарди стандардних компакт дискова капацитета од 700 мегабајта. Пораст дигиталног садржаја је у периоду од 1986. до 2007. износио 67% на годишњем нивоу. Наведено према: M. Hilbert, „How to Measure "How Much Information"? Theoretical, Methodological, and Statistical Challenges for the Social Sciences“, *International Journal of Communication* 6/2012, 1044.

[14] U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society* (COMCRIME Study), European Commission, 1998, 19.

1. ТЕОРИЈСКА РАЗМАТРАЊА ПОЈМА И КАРАКТЕРИСТИКА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

У поимању високотехнолошког криминала могу се разликовати три дискурса:

А. Академски - научници настоје да објасне узроке и појавне облике овог феномена интердисциплинарним приступом у оквиру разних научних дисциплина: рачунарства, социологије, криминологије, кривичног права (уз тенденцију да се сваки облик злоупотребе информационе технологије означи као високотехнолошки криминал);

Б. Експертски - стручњаци за рачунарску безбедност истражују трендове и тенденције у развоју злоупотреба информационе технологије ради проналаска објашњења узрока и осмишљавања стратешких и техничких решења за супротстављање постојећим и потенцијалним ризицима (често нудећи своје производе и услуге);

А. Легислативни – регулаторна тела постављањем одређених правила одређују границе између прихватљивог и неприхватљивог понашања и у кривичним законима прописују кривична дела извршена злоупотребом информационе технологије.

У погледу термина за означавање злоупотреба информационих технологија, може се уочити да су они еволуирали упоредо са развојем могућности злоупотреба. Током 1970-их година је објављено неколико научних радова посвећених систематичном изучавању појаве злоупотребе рачунара који се означавају као „компјутерски криминал“ (*computer crime*)[15] и „кривична дела извршена употребом компјутера“ (*crime by computer*)[16]. У првој академској студији коју је 1977. године израдио немачки професор Урлих Зибер (*Urlich Sieber*) употребљен је термин компјутерски криминалитет (*die Computerkriminalität*) за означавање „кривичних дела повезаних са рачунарима“[17]. Термин „криминал повезан са компјутерима“ (*computer-related crime*) је коришћен за означавање кривичних дела код којих је рачунар средство извршења или објект

[15] G. McKnight, *Computer Crime*, Joseph, London 1973. Наведено према: J. Clough, *Principles of Cybercrime*, Cambridge University Press, Cambridge 2010, 4.
[16] D. B. Parker, *Crime by Computer*, Scribner, New York 1976. Наведено према: Clough, *op.cit*, 4.
[17] U. Sieber, *Computercriminalitat und Strafrecht*, Carl Heymanns Verlag KG, Köln 1977. Наведено према: S. Schjolberg, *The History of Cybercrime: 1976-2014*, Koln 2014,18.

напада или је извршење радње последица стручног знања из области рачунарске и информационе дисциплине. У вези са стручним знањем као конститутивним елементом кривичних дела је и термин „криминал у области информационе науке“ (*la criminalite informatique*[18]) и „криминал информационе ере“ (*information-age crime*). Међутим, термин компјутерски криминал[19] и његове варијације у условима технолошког развоја постао је неодговарајући (јер не обухвата рачунарске мреже), а данас се користи за означавање прве генерације злоупотреба. За означавање кривичних дела извршених злоупотребом рачунарских мрежа користе се и термини Интернет криминал (*Internet crime*[20]) и бежични криминал (*wireless crime*[21]). У употреби су и следећи термини: високотехнолошки криминал[22] (*hi-tech crime*[23]*/high-technology computer crime*[24]), електронски криминал (*electronic crime*[25]), рачунарски криминал (*computing crime*[26]), дигитални криминал (*digital crime*[27]) и виртуелни криминал (*virtual crime*[28]). Терминологија углавном потиче из криминолошке литературе, док је у смислу кривичног права, с обзиром на заштитни објекат који се штити прописивањем одређене групе кривичних дела, одговарајући термин „кривична дела против доступности, поузданости и целовитости рачунарских података“[29].

[18] D. Martin, *La Criminalite Informatique*, Presses Universitaires De France, Paris 1997, 196.
[19] Овај термин у домаћој литератури користе поједини аутори. Види З. Цветковић, „Компјутерски криминал“, *Бранич* 2-3/2001, 7; И. Фејеш, *Савремени криминалитет и доказно право*, Нови Сад 2002, 28; В. Николић, „Откривање и праћење компјутерског криминала“, *Безбедност* 2/2004, 262; М. Милошевић, „Актуелни проблеми сузбијања компјутерског криминала“, *Наука, безбедност, полиција* 1/2007, 60; Б. Лепојевић, М. Ковачевић-Лепојевић, „Међународни стандарди у супротстављању компјутерском криминалу и њихова примена у Србији“, *Зборник Института за криминолошка и социолошка истраживања* 1-2/2007, 268.
[20] Jewkes, Yar, *op.cit*, 42.
[21] G. Kipper, *Wireless Crime and Forensic Investigation*, Auerbach Publications, New York 2007, 5.
[22] Овај термин у домаћој литератури користе поједини аутори. Види М. Рељановић, „Високотехнолошки криминал - појам, регулатива, искуства“, *Страни правни живот* 3/2007, 77; Д. Прља, М. Рељановић, „Високотехнолошки криминал - упоредна искуства“, *Страни правни живот* 3/2009, 167; С. Живановић, „Практични аспекти високотехнолошког криминала“, *Криминалистичко форензичка истраживања* 1/ 2011, 140-141.
[23] M. Knetzger, J. Muraski, *Investigating High-Tech Crime*, Prentice Hall, New Jersey 2007, 44.
[24] R. Moore, *Cybercrime: Investigating High-Technology Computer Crime*, Anderson, Oxford 2011, 47.
[25] P. Grabosky, *Electronic Crime* , Pearson Prentice Hall, New Jersey 2007, 15.
[26] L. Garicano, P. Heaton, „Computing Crime: Information Technology, Police Effectiveness, and the Organization of Policing“, CEPR Discussion Paper 5837/2006, 7.
[27] R. Bryant, S. Bryan (eds.), *Policing Digital Crime*, Ashgate Publishing Limited, Surrey 2014, 12.
[28] T. Grivna, „Virtual crimes“, *Masaryk University Journal of Law and Technology* 1/2008, 98.
[29] М. Вићентијевић, „Кривична дела против безбедности рачунарских података”, *Избор судске праксе* 7-8/2008, 14.

Сматрамо да је, с обзиром на могуће злоупотребе информационе технологије у савременом кибер окружењу, најадекватнији термин „кибер криминал“ *(cyber crime*[30]), који је истовремено и најзаступљенији термин у научној и стручној литератури. Ипак, определили смо се да у раду користимо термин „високотехнолошки“ [31] криминал[32] с обзиром на то да: 1) информационе технологије имају круцијалан утицај на развој и суштину овог појма, имајући у виду улогу високе технологије при извршавању појединих радњи кривичних дела обухваћеним овим обликом криминала без које те радње не би биле могуће); 2) законодавац Републике Србије користи овај термин[33].

Различити термини обухватају, сходно томе, и различите садржаје. Постоји више дефиниција појма високотехнолошког криминала[34] а заједничко им је поимање да у високотехнолошки криминал спадају кривична дела повезана на одређени начин са информационим технологијама. Тако, високотехнолошки криминал обухвата радње код којих је рачунарски систем/мрежа објект напада или средство извршења[35], односно незаконите/неовлашћене радње које се

[30] Термин први пут је употребљен у раду: S. Brenner, „Cybercrime metrics: Old wine, new bottles?“, *Virginia Journal of Law and Technology* 1/2004, 1-52. У домаћој литератури се користи некоректан термин „сајбер“ криминал. Види В. Спасић, „Актуелна питања у области сајбер криминала“, *Билтен судске праксе Врховног суда Србије* 1/2006, 108; В. Спасић, „Сајбер криминал у светлу нове регулативе“, *Правни живот* 9/2005, 949.

[31] Термину високотехнолошки би се могло приговорити, јер у високу технологију осим информационе технологије спадају и биомедицина и генетски инжењерство, нанотехнологије, нуклеарне технологије и друго.

[32] У теорији се паралелно користе термини *криминалитет* и *криминал*. *Криминалитет* означава скуп кривичних дела у одређеном времену и простору или скуп одређене врсте кривичних дела, у зависности од атрибута који иде уз именицу (Т. Лукић, Посебности кривичног поступка за организовани криминал, тероризам и корупцију, Нови Сад 2008, 9). Тако, на пример, атрибут *организовани* одређеним кривичним делима „даје заједничко и у односу на остала кривиминална понашања битно дистинктивна обележја“. (М. Шкулић, *Организовани криминалитет: појам и кривичнопроцесни аспекти,* Београд 2015, 105-106). Ипак, определили смо се за термин *криминал,* јер обухвата укупност негативних друштевних појава и шири је појам од *криминалитета* (Лукић, *op.cit*, 10). Истовремено, употреба овог термина је „ради одређене терминолошке коректности сасвим пожељна“ (Шкулић, *op.cit*, 106) у контексту анализе позитивноправних решења у Републици Србији, која ће бити приказана у даљем тексту.

[33] Ратификујући Конвенцију Савета Европе, приликом доношења Закона о потврђивању Конвенције употребљен је погрешан превод термина *cybercrime* у наслову Конвенције – уместо правилног „кибер“ употребљен је термин „високотехнолошки“. Осим тога, према мишљењу појединих аутора у домаћој литературу, високотехнолошки криминал и сајбер криминал имају исто значење (Комлен Николић Л. et al, *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавних тужилаца Србије, Београд 2010, 30).

[34] О прегледу наслова који за предмет имају одређивање појма високотехнолошког криминала више видети: K. Jaishankar, „Establishing a Theory of Cyber Crimes“, *International Journal of Cyber Criminology* 2/2007, 5.

[35] Carter D.L, „Computer Crime Categories: How Techno-Criminals Operate“, *FBI Law Enforcement Bulletin,* 1995, (http://www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-

предузимају посредством рачунарске технологије (*computer-mediated*) у оквиру глобалне електронске мреже[36], односно кривична дела чије радње извршења су омогућене или извршене употребом рачунара, рачунарске мреже или хардверског уређаја[37]. Обухват појма се од првих злоупотреба рачунара ширио са развојем рачунарске и комуникационе технологије, па се могу уочити три „генерације" дела високотехнолошког криминала[38]. У прву генерацију спадају дела чије радње карактерише употреба рачунара[39] за извршење традиционалних (*traditional*[40])/обичних (*ordinary*[41]) кривичних дела[42]- рачунари се користе обично у фази припреме (као средство комуникације или за прикупљање информација потребних за планирање извршења радње кривичног дела). У другу генерацију спадају дела учињена употребом рачунарских мрежа – то су својеврсни хибриди традиционалних кривичних дела, прилагођени новонасталим приликама за извршење радње које је умрежавање рачунара омогућило[43]. Трећу генерацију чине облици кибер криминала, у правом смислу речи – ради се о делима чије радње карактерише аутоматизована и дистрибуирана природа напада омогућена у потпуности развојем информационих технологија, првенствено Интернетом[44].

%20Types%20of%20computer%20crime.pdf); N Kshetri, *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer, Amsterdam 2010, 7.

[36] C. Hale, „Cybercrime: Facts & Figures Concerning this Global Dilemma", *Criminal Justice International* 18/2002, http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.

[37] S. Gordon, Ford R., „On the definition and Classification of cybercimes", *Journal in Computer Virology* 1/2006, 14.

[38] Више о томе D. Wall, *Cybercrime:The Transformation of Crime in the Information Age*, Cambridge University Press, Cambridge 2010, 44-49.

[39] Тако се под појмом компјутерског криминалитета подразумева посебан вид инкриминисаних понашања код којих се рачунарски систем (схваћен као јединство хардвера и софтвера) појављује као средство извршења или као објект кривичног дела, уколико се дело на други начин, или према другом објекту, не би могло извршити или би оно имало битно другачије карактеристике. Игњатовић Ђ, „Појмовно одређење компјутерског криминалитета", Анали Правног факултета у Београду 1-3/91, 142.

[40] D. Wall, *Crime and the Internet*, Routledge, London 2001, 6.

[41] S. McQuade, *Understanding and Managing Cybercrime*, Allyn & Bacon, Boston 2005, 46.

[42] Кривично дело се сматрало компјутерским криминалом, уколико је знање рачунарске технологије било неопходно за извршење кривичног дела. S. Schjolberg, *Computers and Penal Legislation – A Study of the Legal Politics of a new Technology*, Scandinavian University Press, Oslo 1984, 16. Упор. U.S. Department of Justice, *The Criminal Justice Resource Manual on Computer Crime*, 1989, *https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf;*

[43] McQuade, *op.cit*, 48.

[44] О еволуцији високотехнолошког криминала више вди S. Brenner, *Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture)*, Praeger, Santa Barbara 2010, 10-29.

Осим тога, појам високотехнолошког криминала се може посматрати као трипартитна структура која обухвата кривична дела[45]: 1. чија радња је подржана рачунарима (*Computer-supported crimes*), односно код којих је рачунар инцидентални аспект извршења радње али може представљати потенцијални извор доказа; 2. Чија радња извршења је рачунарима омогућена, потпомогнута, односно са рачунарима повезана (*Computer facilitated/assissted/related crimes*), тј. кривична дела код којих су рачунарски систем/мрежа средство извршења радње (нпр. повреда ауторског права на Интернету); и 3. усмерена против интегритета рачунара (*Computer integrity crimes*) код којих је рачунарски систем/мрежа објект напада (нпр. неовлашћен упад у рачунарски систем). Оваква класификација се може посматрати и у вези са питањем да ли је високотехнолошки криминал потпуно нови облик преступништва или постоји аналогија са кривичним делима у *offline* окружењу, у смислу да се ради о „старим облицима криминала који су почињени на нове начине (*old wine, new bottles*[46]). Полазећи од заштитног објекта сматрамо да не би било исправно прву групу кривичних дела (*Computer-supported crimes*) третирати као високотехнолошки криминал, а да другу групу чине дела којима нови квалитет даје само употреба информационе технологије као средства које ствара нове могућности за извршење радње, што није довољно да их третирамо као посебне облике криминала. *Сходно томе, само она кривична дела чије су радње извршења усмерене против безбедности, доступности и целовитости рачунарских система и мрежа, а која без употребе информационх технологија не би биле могуће предузети, могу се сматрати новим обликом криминала*.

На основу наведеног, можемо се запитати која се то кривична дела сматрају високотехнолошким криминалом. Уколико се мушкарац и жена упознају и комуницирају преко *online* друштвене мреже, посредством које договоре састанак на ком мушкарац лиши живота жену, да ли је то кибер-убиство? Да ли се може сматрати високотехнолошким криминалом ситуација у којој лице нанесе другом лицу тешке телесне повреде а као средство извршења употреби тастатуру? Наравно да се у ова два примера не ради о високотехнолошком криминалу, већ су

[45] Clough, *op.cit*, 10. и 40. Исто: Wall, *Crime and the Internet*, 7-8; R. Bryant, S. Bryan (eds.), *Policing Digital Crime*, 35-36.
[46] Brenner, „Cybercrime metrics: Old wine, new bottles?“, 15.

посреди кривична дела чија радња извршења у реалном свету је просто омогућена употребом информационе технологије, односно део рачунарског система је употребљен као средство извршења. С друге стране, радња може бити извршена у виртуелном окружењу: рачунарска превара има више појавних облика – аукцијска превара, превара кредитним картицама, превара употребом лажног идентитета, фишинг итд. Ипак, превара је увек само превара а информациона технологије је употребљена као ново средство извршења кривичног дела које постоји годинама уназад. Међутим, уколико се компромитовани, малвером заражени рачунари употребе за стварање мреже „зомбија“ (тзв. *botnet*[47]) а ради остваривања одређених циљева (нпр. за слање порука нежељене поште[48]), посреди је ситуација која представља по свом квалитету нешто потпуно. Из ових примера би се могло доћи до закључка *да појам високотехнолошког криминала обухвата инкриминисана понашања код којих се рачунарски систем или рачунарска мрежа појављује као средство извршења или као објект кривичног дела, уколико се дело на други начин, или према другом објекту, не би могло извршити или би оно имало битно другачије карактеристике*[49], па сматрамо да би се само радња из последњег примера могла сматрати кривичним делом обухваћеним појмом високотехнолошког криминала. У том смислу се користи термин „дигитални криминал“ за означавање кривичних дела код којих постоји нов квалитет употребе дигиталне технологије (*digitality/novelty*[50]). Тако Грабовски (*Grabovsky*) сматра да већина дела учињена употребом рачунара представља само модификацију „терестријалних“ кривичних дела (*Old wine, new bottles*), док дела омогућена карактеристикама кибер простора означава термином електронски криминал, како би обухватио кривична дела које без употребе дигиталне технологије не би била могућа (*new wine, no bottles*)[51]. *Стога смо мишљења да се само кривична дела чије радње имају наведене специфичне карактеристике могу*

[47] Више о томе J. Kristoff, “Botnets and Packet Flooding DDoS Attacks on the Domain Name System”, *International Journal of Computer Forensics Science*1/2007, 15-16; C. Ard, „Botnet Analysis“, *International Journal of Computer Forensics Science* 1/2007, 67; N. Ianelli, „Botnets as a Vehicle for Online Crime“, *International Journal of Computer Forensics Science* 1/2007, 25.

[48] Тако је, примера ради, у 2009. години 85% нежељене поште (*spam*) последица коришћења ботнетова. P. Hunton, „Data attack of the cybercriminal: Investigating the digital currency of cybercrime“, *Computer Law and security Review* 28/2012, 205.

[49] Упореди са Игњатовић, *op.cit*.

[50] Bryant, Bryan, *op.cit*, 25.

[51] Grabosky, *op.cit*, 15.

сматрати високотехнолошким, односно кибер криминалом (то су sui generis облици треће генерације злоупотребе информационе технологије).

Одређени аспекти високотехнолошког криминала чине га у значајној мери комплексном темом за проучавање, а њихово неразумевање, односно неузимање у обзир представља озбиљну препреку институционалном одговору од стране надлежних органа. Полазећи од става да „што се ствари више мењају, све више остају исте“ (*plus ca change, plus c'est la meme chose*[52]), указујемо да не постоји јасна дихотомија између аналогног и дигиталног криминала нити је основана тврдња да су „кривична дела из реалног света просто мигрирала у кибер простор“[53] што „компликује примену традиционалних законских решења и еродира ефективност контролних механизама суверених држава“[54]. Ради потврђивања тезе да је високотехнолошки криминал *sui generis*, *потребно је утврдити конститутивне разлике између „преддигиталног/ аналогног“*[55] *и дигиталног криминала* имајући у виду улогу нових информационих технологија у трансформисању криминала у анонимне, аутоматизоване и виртуелне облике, а неколико карактеристика високотехнолошког криминала чине га специфичним и посебним у односу на „традиционалне“ облике[56]:

А. Док се радње традиционалних кривичних дела извршавају у физичком свету, виртуелност окружења омогућава извршиоцу да брзо, са великим бројем понављања предузима радњу извршења, уз могућност паралелног извршења, при чему се више лица/објекта напада може симултано оштетити по веома малим трошковима. У виртуелном простору је услед умрежености и огромне количине података који се преносе лако и по великој брзини, далеко већа приступачност и избор објеката напада, криминалних могућности и *modus operandi* (својство виртуелности);

Б. Поједине облике високотехнолошког криминала карактерише *просторна удаљеност* (између учиниоца и објекта напада, као и између саучесника) која

[52] Brenner, *op.cit*,.15.
[53] Brenner, *Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture)*, 10.
[54] S. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Northeastern University Press, Boston 2012, 2.
[55] B. Sandywell, „On the globalization of crime: the Internet and new criminality“, Jewkes., Yar, *op.cit*, 42.
[56] Тако, M. Yar, *Cybercrime and Society*, SAGE Publications, New York 2006, 5. и 42; Clough, *op.cit*, 5-8; Sandywell, *op.cit.*, 44; Bryant, Bryan, *op.cit*, 26-27.

може да буде далеко већа у поређењу са ситуацијом у физичком свету, па се не може применити Локардов принцип о контактним траговима. Једна од јединствених карактеристика високотехнолошког криминала је да се радња извршења предузима у кибер свету у ком не постоје границе територијалне надлежности држава, јер извршиоци имају могућност да усмере напад на рачунаре или мреже било где у свету и да напад спроводу посредством рачунара или мреже који се налазе у потпуности на различитим локацијама у односу на државу у којој се налази рачунар извршиоца или рачунар који је објект напада. Просторна удаљеност може бити прилично изражена, тако што се под местом извршења кривичног дела може сматрати неколико локација укључујући и неколико држава, па није реткост ситуација у којој надлежни органи више држава конкуришу са својом надлежношћу (својство делокализованости/детериторијализације социјалних сусрета, у смислу да за извршиоца готово не постоје просторна ограничења за приступ објекту напада);

В. Вероватноћа откривања учинилаца је далеко мања него код традиционалних кривичних дела, услед могућности прикривања идентитета учиниоца и радње извршења у рачунарским мрежама, при чему су средства извршења у домену високе технологије која се непрестано мења, па учиниоци имају широк избор инструментаријума за извршење дела и прикривање трагова (својство анонимности/безличности).

Из свега наведеног произашло је ширење различитих географски децентрализованих облика криминалних активности омогућених употребом глобализованих информационих технологија. Бројне дигиталне платформе су омогућиле превазилажење традиционалних физичких граница заснованих на дистанци и стварање једног јединственог умреженог простора[57] што је допринело томе да високотехнолошки криминал постане транснационални феномен, супротстављању коме је било потребно створити одговарајући правни оквир.

[57] M. Goodman, S. Brenner, „The emerging Consensus in on Criminal Conduct in Cyberspace“, *International Journal of Law and Information Technology* 2/2002, 183.

2. ПРАВНИ ОКВИР ЗА СУПРОТСТАВЉАЊЕ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Потреба за инкриминисањем радњи извршених против, односно употребом рачунара настала је у време када су рачунари постали доступни широј јавности. Током 1960-их године појавили су се извештаји о манипулацијама рачунара, рачунарским саботажама и шпијунажама, и другим облицима незаконите употребе рачунарских система[58]. С обзиром на релативно ограничену употребу рачунара у свакодневном животу од стране малог броја појединаца, ти први појавни облици су се односили на крађу телекомуникационих услуга и преваре у вези са трансфером електронских фондова[59]. *Еволуција законодавних решења је сукцесивно пратила развој технологије, одражавајући сагласност о потреби заштите појединих добара*[60]. У почетку је пажња била усмерена на инкриминисање неовлашћеног приступа приватним информацијама, али се временом појавила потреба за санкционисањем употребе рачунара за извршење кривичних дела против привреде. Током 1970-их је постало евидентно да постојеће инкриминације, настале у времену када се такав напредак технолошког окружења није могао ни замислити, нису адекватно решење, а битан допринос у указивању на потребу санкционисања злоупотреба рачунара прописивањем посебних инкриминација може се приписати закључцима са неколико научних скупова одржаних током 1980-их година[61]. У том периоду усвајају се први закони који су предвиђали посебне инкриминације: у америчкој држави Флориди 1978[62], Италији 1979, Аустралији 1981, Уједињеном Краљевству 1984, на нивоу САД

[58] Sieber, *op.cit*, 19.
[59] Goodman, Brenner, *op.cit*, 12.
[60] Више о томе, Sieber, *op.cit*, 25–32, 39.
[61] Од скупова који су резултирали идејом о кривичноправном регулисању злоупотреба рачунара као најзначајнији се означава скуп одржан 1992. године у Вирцбургу у Немачкој, јер су том приликом представљени извештаји из 29 држава на основу који су усвојене смернице за развој националног законодавства. Више о томе, U. Sieber, *Information Technology Crime – National Legislations and International Initiatives*, Carl Heymanns Verlag, Köln 1994, 25-28.
[62] *Florida Computer Crimes Act* усвојен је након инцидента у ком су запослени у предузећу *Flagler Dog Track* искористили рачунаре за штампање лажних добитних листића у наградној игри, па је овај Закон предвидео као кривично дело неовлашћену употребу рачунара. E. Casey, *Digital evidence and computer crime: forensic science, computers and the Internet*, Academic Press, Amsterdam-Boston 2011, 35.

1985, Данској 1986, Немачкој и Шведској 1987, Аустрији и Норвешкој 1988, Француској 1990, Финској 1992, Холандији 1993, Шпанији 1995. године итд[63].

У деценијама које су уследиле, *умрежавање рачунарских система и унапређење перформанси персоналних рачунара трансформирали су компјутерски криминал*. Са развојем технологије рачунара, развијале и облици и начини злоупотреба, а као неопходност се појавила потреба за уношењем специфичних одредаба у кривично законодавство. Са повећаном међуповезаношћу рачунара, омогућено је дистрибуирање дечје порнографије и повреде ауторских права на до тада неслућене начине. Даљи технолошки развој условио је појаву нових облика угрожавања безбедности дигиталних садржаја: стална повезаност рачунара са Интернетом учинила је рачунаре рањивим у погледу спољних напада преко рачунарске мреже, а употребе *peer-to-peer* технологије омогућила је извршавање дистрибуираног напада ускраћивања услуга *(Denial of Service:DoS*) и ширења малициозних кодова[64]. Конвергенција телекомуникација и рачунарства је претворила мобилне телефоне у мале умрежене рачунаре који услед недовољног обезбеђења представљају ризик по заштиту приватности корисника.

Да би се осигурало несметано одвијање свакодневних активности физичких и правних лица која се ослањају на поменуте технологије, *потребно је било пронаћи одговарајуће механизме за остваривање и очување безбедности дигиталних садржаја*. *Безбедност дигиталних садржаја* подразумева *заштиту доступности, поверљивости и потпуности података похрањених, преношених и обрађиваних у кибер простору*. *Доступност* је карактеристика података у електронском облику да им се може приступити и да се могу користити на потребан начин, *поузданост* (поверљивост) подразумева да подацима не могу приступити неовлашћена лица, док се *потпуност* (интегритет/целовитост) односи на очување тачности информација и на неизмењеност садржаја података у електронском облику. Како се све више података, од електронске поште до банковних рачуна, као и података од значаја за функционисање привреде и

[63] Schjolberg, *The History of Cybercrime: 1976-2014*, 24-31.
[64] Taylor M. et al, „Digital evidence from peer-to-peer networks“, Computer law & security review 27/2011, 648.

државе складиште у „облаку“, а који у сваком тренутку могу бити објект напада злоупотребом информационих система, оправдано је очекивање појединаца и привредних субјеката да се правно уреди заштита тих података у смислу очувања њиховог потпуности, доступности и поверљивости.

Интеграција телекомуникационих и информационих система у савременом друштву омогућава складиштење и пренос података о свим врстама комуникација чиме је створен низ нових могућности за злоупотребе у оквиру кибер простора. Те злоупотребе се односе на угрожавање интегритета, доступности или поверљивости рачунарских мрежа и телекомуникационих система и са њима повезаним података или се односе на употребу таквих мрежа и система за извршавање „традиционалних“ кривичних дела. Сходно томе, државе настоје да одрже корак са технолошким напретком и заштите појединце, привреду и друштво од злоупотреба информационих система, *a ultima ratio у заштити наведених добара је прописивање одређених понашања као кривичних дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система*. Да би се путем кривичног права пружила заштита безбедности дигиталних садржаја, одредбе кривичног закона треба да са довољно јасноће и прецизности дефинишу која понашања се имају сматрати кривичним делом, али на начин да буду у технолошком смислу неутрална, како би се могле примењивати на нове технолошке изазове. Без одређених прилагођавања специфичностима високотехнолошког криминала, као појаве глобалних размера, откривање и доказивање, ове врсте криминала готово да је немогуће. Стога је уочена потреба за стварањем правног оквира супротстављања високотехнолошком криминалу, састављеног од материјалноправних и процесноправних правила прилагођених овој врсти криминала као и за унапређењем међународне сарадње, у оквиру глобалног и регионалног приступа борби против кибер криминала. За стварање одговарајућег правног оквира за супротстављање овој врсти криминала путем кривичног права, осим што се у прописима кривичног материјалног права одређена понашања инкриминишу, те предвиђају као кривична дела против поверљивости, целовитости и доступности рачунарских података и рачунарских система, *неопходно је да прописи кривичног процесног права садрже одговарајућа овлашћења надлежних органа у циљу*

откривања извора недозвољене радње, односно прикупљања података о учињеном кривичном делу и учиниоцу који могу бити употребљени као доказ у кривичном поступку, а водећи рачуна о специфичностима високотехнолошког криминала и окружења у оквиру ког се недозвољене активности предузимају. Имајући у виду све 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 кривичне законе новим одредбама[65].

Из свих до сада наведених карактеристика високотехнолошког криминала, произлази недвосмислени закључак да је *велики проблем уколико различити правни системи различито приступају регулисању одговора државе на поменуте изазове и уколико не постоји јединствен став о томе које се то неовлашћене активности злоупотребом информационих технологија сматрају високотехнолошким криминалом и којим радњама и мерама превентивно и репресивно реаговати на њих*. Наиме, конвергенција рачунарства и комуникација и експоненцијални раст дигиталне технологије створили су ризике по безбедност рачунарских система, како у оквиру једне државе, тако и у прекограничном контексту[66], *па се као неопходност указала потреба за деловањем и на регионалном и међународном нивоу ради омогућавање ефикасне сарадње између надлежних државних органа*. Као основне *препреке ефикасном међународном деловању* на сузбијању високотехнолошког криминалу као глобалној појави, могу се означити *следећи фактори*: различито правно дефинисање радњи извршења појединих кривичних дела; неусклађеност процесних правила у националном законодавству у погледу истраге кривичних дела високотехнолошког криминала и неусклађеност или одсуство механизама међународне правне[67]. *Солидну основу за превазилажење ових препрека, односно за приближавање националног кривичног материјалног и процесног права и за остваривање ефективне прекограничне сарадње у супротстављању кибер криминалу* представља регулатива усвојена у

[65] N. Foggetti, „Transnational Cyber crime, differences between national laws and developments of European legislation: by repression?“, *Masaryk University journal of Law and technology* 2/2008, 37.
[66] Cassim F., „Formulating specialized legislation to address the growing spectre of cybercrime: a comparative study“, *Potchefstroom electronic law journal*, 12/2009, 42.
[67] Комлен Николић *et al*, *op.cit*,31.

оквиру Уједињених нација[68] и Савета Европе (с обзиром на то да је Република Србија чланица ових организације), те Европске уније (с обзиром на то да је Република Србија кандидат за чланство у овој регионалној организацији).

2.1. Савет Европе

Прва међународна иницијатива која се односила на рачунарски криминал потекла је са Конференције Савета Европе о криминолошким аспектима привредног криминала одржане 1976. године у Стразбуру и већ тада је препознато неколико облика злоупотреба рачунара[69]. Након тога, 1985. године формирана је стручна комисија са циљем разматрања правних питања у вези са компјутерским криминалом. Као резултат рада ове комисије, резиме смерница националним законодавствима представљен је у *Препоруци која се односи на кривична дела*

[68] У оквиру УН не постоји извор права од већег и непосредног значаја за супротстављање високотехнолошком криминалу. Током 2000-их усвојено је неколико резолуција, вредних помена, које се односе на злоупотребе информационих технологија, али које су упућујућег карактера, односно у виду препорука. Што се тиче препознавања проблема високотехнолошког криминала у оквиру УН, најпре бисмо поменули да је у тзв. Миленијумској декларацији, односно Резолуцији бр. 55/2 из 2000. године као један од приоритетних циљева утврђена и потреба да се нове технологије, а нарочито информационе и комуникационе технологије, учине безбедним и доступним свима (*United Nations Millennium Declaration*, 2000, http://www.un.org/millennium/declaration/ares552e.pdf). Осим тога, Генерална скупштина УН је усвојила две резолуције у циљу промовисања међународне сарадње у области хармонизације и примене кривичних закона. У Резолуцији бр. 55/63 о борби против злоупотребе информационих технологија, која је усвојена 2001. године, утврђени су основни принципи на којима би требало да почива борба против високотехнолошког криминала. Инсистира се на хармонизацији прописа, у смислу да би државе требало да својим синхронизованим законодавством онемогуће „стварање безбедних подручја“ за извршиоце кривичних дела кроз прописивање кривичних дела против поверљивости, интегритета и доступности рачунарских података и система (*Combating the criminal misuse of information technologies*, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf). У Резолуцији бр. 56/121 о криминалној злоупотреби информационих технологија, усвојеној 2002. године, указује се на потребу узимања у обзир резултата рада комисије Савета Европе (*Combating the criminal misuse of information technologies*, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf). Економско-социјални савет УН је у Резолуцији бр. 2070/20, усвојеној 2007.године, препоручио државама да, ради остваривања сарадње у спречавању и истрази превара и крађе идентитета употребом информационих система, те гоњењу и санкционисању учинилаца кривичних дела, размотре потребу за модернизацијом постојећег националног законодавства, а указано је на корисност приступања Конвенцији Савета Европе (*ECOSOC Resolution 2007/20 International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related crime* http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf). Из наведеног произлази да се у инструментима УН државе чланице недвосмислено упућују на Конвенцију Савета Европе.

[69] *Criminological aspects of economic crime*: Reports Presented to the Twelfth Conference of Directors of Criminological Research Institutes, Strasbourg 1977, 225-229.

повезана са компјутерима, усвојеној 1989. године[70]. У овој препоруци су наведене две листе кривичних дела, као смерница државама у регулисању ових појава на националном нивоу: обавезујућа листа минималних захтева у погледу кривичних дела које би државе требало да предвиде у кривичноматеријалним прописима[71], и опциона листа кривичних дела чије предвиђање је препуштено диспозицији држава[72]. Што се тиче процедуралних питања, значајна је *Препорука која се односи на проблеме кривичног процесног права у вези са информационом технологијом*, усвојена 1995. године [73]. Препорука садржи 18 принципа, категоризованих у 7 поглавља (претрес и заплена; технички надзор; обавеза сарадње са истражним органима; електронски докази; коришћење кодирања; истраживање, статистика и обука; међународна сарадња), а који су касније разрађени и инкорпорисани у Конвенцију.

Европски комитет за проблеме криминала (*European Committee on Crime Problems:CDPC*) је у новембру 1996. године образовао комисију састављену од стручњака за компјутерски криминал (*Committee of Experts on Crime in Cyberspace: PC-CY*) са задатком да састави нацрт конвенције[74]. **Конвенција о високотехнолошком криминалу**[75] (у даљем тексту: КВК) је усвојена на Конференцији Савета Европе 23. новембра 2001. године у Будимпешти, а на снагу је ступила 1. јула 2004. године[76]. Уз Конвенцију је 2003. донет, а ступио је на снагу 2006. године, Додатни протокол који се односи на инкриминацију дела

[70] *Computer-related crime: Recommendation No. R. (89) 9,* https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 .

[71] На листи су следећа кривична дела: рачунарска превара, компјутерски фалсификат, оштећење компјутерских података или компјутерских програма, рачунарска саботажа, неовлашћени приступ, неовлашћено прислушкивање, неовлашћено умножавање заштићеног компјутерског програма и неовлашћено умножавање топографије.

[72] На опционој листи су следећа кривична дела: измена компјутерских података и компјутерских програма, компјутерска шпијунажа, неовлашћена употреба компјутера, неовлашћена употреба заштићених компјутерских програма.

[73] *Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995,* https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2.

[74] Наведено према: *Explanatory Report of the Convention on Cybercrime (185), No. 10, http://conventions.coe.int.*

[75] *Council of Europe Convention No. 185 on cybercrime,* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[76] Услов за ступање Конвенције на правну снагу се односио на ратификацију од стране пет земаља, од чега су најмање три земље чланице СЕ.

расистичке и ксенофобичне природе извршених употребом рачунарских система[77].

Разматрањем листе потписница[78], може се уочити следеће: Конвенцију је од 47 чланица потписало 45, а ступила је на снагу у 39 држава чланица. Република Србија је КВК потписала 2005. године (као и Додатни протокол) а ратификовала 2009. године.[79] Од држава чланица једино Русија и Сан Марино нису потписнице Конвенције. С друге стране, Конвенцију су потписале и поједине земље не-чланице СЕ, а ступила је на снагу у Аустралији, Доминиканској републици, Јапану, Маурицијусу и САД[80]. Може се рећи да је тиме Конвенција превазишла регионални значај и стекла универзални карактер.

Што се тиче структуре, Конвенција поред Преамбуле, садржи четири поглавља. У *првом поглављу* дефинисани су основни појмови (рачунарски систем, рачунарски подаци, пружаоци услуга, проток података). *Друго поглавље* предвиђа легислативне мере које треба предузети на националном нивоу, а односе се на кривично материјално право и кривично процесно право. У оквиру 1. одељка кривична дела су категоризована у четири групе[81], а ова типологија је од изузетног значаја јер је усвајају међународни и национални прописи који уређују високотехнолошки криминал (иста је преузета и у актима ЕУ)[82]. Конвенција пред потписнице поставља захтев за увођењем истражних овлашћења, а ради

[77] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,* http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm. Потписивањем и ратификовањем Додатног протокола држава се обавезује да инкриминише одређена штетна понашања: ширење расистичког и ксенофобичног материјала преко рачунарских система; претњу мотивисану расизмом или ксенофобијом; порицање, значајно умањење, одобравање или оправдавање геноцида или злочина против човечности. Како Додатни протокол не садржи процесноправне одредбе, већ предвиђа сходну примену одредаба Конвенције, неће бити предмет даље обраде у раду.

[78] Листа потписница (стање у марту 2016. године) може се пронаћи на интернет страници: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

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

[80] Канада и Јужноафричка република су, такође, потписнице али Конвенција, у овим државама није још увек ратификована.

[81] Конвенција разликује четири групе кривичних дела: прву групу чине кривична дела усмерена против поверљивости, интегритета и доступности података и информационих система; другу групу чине кривична дела у вези са компјутерима (*computer-related crimes*) у извршењу којих се компјутер појављује као средство (као што су фалсификовање и превара); трећу групу чине кривична дела у вези са садржајем (као што је дечја порнографија); четврту групу чине повреде ауторских и сродних права.

[82] Сагледавање и анализа овог дела Конвенције није предмет рада. Више о усклађености материјалноправних одредаба Конвенције и законодавства Републике Србије (односно, одредаба Кривичног законика РС), више о томе, Комлен Николић *et al, op.cit,* 76-79. и 86-129.

модернизације „алата“ који стоје на располагању органима истраге и гоњења у вези са високотехнолошким криминалом. Наиме, у оквиру 2. одељка (чланови 14-21) су одредбе које се односе на процесно право, а садрже одређене смернице за кривични поступак, који се води у вези са кривичним делом које извршено употребом рачунарских система и мрежа, и смернице за прикупљање доказа у електронском облику о извршеном кривичном делу (чак и о кривичном делу које не спада у високотехнолошки криминал у смислу Конвенције)[83]. Успостављање, спровођење и примена овлашћења и поступака наведених у делу који се односи на процесно право захтева од државе да обезбеди адекватну заштиту људских права и слобода – првенствено права на приватност. При том треба да се поштују уобичајени стандарди, тј. минималне мере заштите, укључујући међународне инструменте о људским правима[84]. *Треће поглавље* тиче се међународне сарадње и поставља принципе који се односе на надлежност, екстрадицију, основне принципе међународне помоћи - процедуре које се односе на међусобне захтеве за помоћ у недостатку важећих међународних споразума, узајамну помоћ у вези са привременим мерама, те узајамну помоћ у вези са истрагом[85]. *Четврто поглавље* садржи завршне одредбе[86].

Циљ Конвенције је хармонизација националних законодавстава држава потписница. Ратификовањем или приступањем Конвенцији, држава се обавезује да одговарајућим механизмима имплементације обезбеди да у домаћем законодавству буду као кривична дела предвиђена одређена понашања (наведена у материјалним одредбама Конвенције), те да предвиде одређена овлашћења надлежним органима ради откривања и доказивања дела високотехнолошког криминала и прикупљања електронских доказа (у смислу процесних одредаба Конвенције). Конвенција представља свеобухватан оквир за прилагођавање кривичног материјалног и процесног законодавства специфичностима високотехнолошког криминала, а с обзиром на неадекватност традиционалних

[83] Ова проблематика је предмет обраде у Трећем делу рада.
[84] Ова проблематика је предмет обраде у Осмом делу рада.
[85] Ова проблематика је предмет обраде у Шестом делу рада.
[86] У складу са чланом 40, свака држава може изјавити да оставља могућност захтевања додатних елемената, како је предвиђено, по одређеним члановима. Слично је са стављањем резерви у складу са чланом 42. по ком свака држава може изјавити да ће искористи могућност стављања резерви како је то предвиђено у појединим члановима. Република Србија није ставила ниједну резерву на Конвенцију.

истражних овлашћења и одсуство у већини земаља посебних процедуралних правила која су се примењивала у кибер простору, Конвенција има за циљ да се у домаћем кривичном процесном праву обезбеде овлашћења надлежним органима која су неопходна за истрагу кривичних дела учињених у вези са рачунарским системима као и других кривичних дела за гоњење којих је неопходно прикупити доказе у електронском облику[87]. Осим тога, предвиђена су значајне процедуралне гаранције, што представља један од главних доприноса Конвенције[88]. И поред могућих и оправданих критика појединих решења[89], не треба занемарити значај Конвенције као првог и јединог међународног уговора глобалног домета који се односи на високотехнолошки криминал. Конвенција садржи минимална правила која треба да се угради у материјално и процесно законодавство држава потписница (директна имплементација – имплементација као обавеза) или која могу да послуже као модел за израду прописа међународним организацијама и државама које нису у обавези имплементације (индиректна имплементација – имплементација као модел). До сада је Конвенција као узор за регулисање компјутерског криминала послужила законодавствима у преко 100 земаља[90]. Свакако да би пун смисао Конвенције био постигнут када би је потписале и ратификовале, а тиме и имплементирале у своја законодавства све државе света, међутим, за сада, реалност је другачија – Русија, као једна од најзначајнијих земаља чланица Савета Европе није је ни потписала[91], а од десет земаља које имају највећи број корисника Интернета по становнику, само три су је ратификовале (САД, Немачка, Француска), док Кина, Бразил и Индија нису ни позване да приступе Конвенцији[92]. Ипак, Конвенција је значајна за европски

[87] M. Gercke, „Europe's legal approaches to cybercrime“, *ERA forum* 10/2009, 58.
[88] M. Miquelon-Weismann, “The Convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process?” *John Marshall Journal of Computer & Information Law* 2/2005, 333.
[89] S. Hopkins, „Cybercrime Convention: a positive beginning to a long road ahead“, *The Journal of High technology Law* l/2002, 105.
[90] Cybercrime Model Laws, 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Reports/2014_Zahid/3021_model_law_study_v15.pdf.
[91] О разлозима непотписивања/неприступања Русије Конвенцији, види S. Borisevich et al, „A comparative review of cybercrime law and digital forensics in Russia, the United States and under the Convention on cybercrime of the Council of Europe“, *Northern Kentucky Law Review* 39/2012, 298.
[92] F. Calderoni, „The European legal framework on cybercrime: striving for an effective implementation“, *Crime, Law and Social Change*, 5/2010, 350.

простор јер је послужила као модел/ узор са састављање референтних правних аката ЕУ.

2.2. Европска унија

Први извор права који се односио на регулисање злоупотребе нформационе технологије усвојен је 1991. године. Са циљем хармонизације прописа држава чланица у погледу заштите ауторског права аутора рачунарског софтвера, Комисија Европских заједница је усвојила Директиву о правној заштити компјутерских програма[93] (која се не односи на заштиту одредбама кривичног права). Европска комисија је у априлу 1998. године представила Студију о правним аспектима компјутерског криминала у информационом друштву[94], у којој је указано на специфичне проблеме и опасности криминала повезаног са компјутерима. У мају 1999. године Комисија је у вези са преговорима око нацрта КВК заузела становиште по ком земље чланице ЕУ у потпуности подржавају будућу Конвенцију[95] (што се понавља и у каснијим саопштењима, јер је значај Конвенције препознат у оквиру стратешког опредељења ЕУ). На почетку новог миленијума супротстављање високотехнолошком криминалу уврштено је међу политичке приоритете Европске уније у неколико стратешких докумената, од којих су најзначајније Саопштење Комисије ЕУ *Стварање безбеднијег информационог друштва кроз унапређење безбедности информационих инфраструктура и борбом против криминала повезаног са компјутерима* из 2001. године [96] и Саопштење Комисије ЕУ *Према зајединчкој политици у борби*

---

[93] *Council Directive 91/250/EEC on legal protection of computer programs,* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31991L0250.

[94] Ова студија позната је као *„COMCRIME study“,* а приредио је, за потребе и по налогу Европске комисије, Проф. др. Улрих Зибер са Универзитета у Вирцбургу.

[95] B. Ruyver, G. Vermeulen, T. Beken, *Strategies of the EU and the US in combating transnational organized crime*, Maklu 2002, 219.

[96] Указано је да на нивоу ЕУ не постоји ниједан легислативни акт који се директно односи на компјутерски криминал, те је уочена потреба за стварањем одговарајућих легислативних инструмената. С тим у вези Комисија је утврдила да ће предложити одређене легислативне мере са циљем приближавања националних материјалноправних и процесноправних прописа у вези са компјутерским криминалом. У погледу материјалноправних мера, изражена је намера да се следи типологија кривичних дела и стандарди које поставља Конвенција СЕ, а у погледу процесноправних мера, утврђено је да је неопходно уређење следећих питања: пресретање комуникација, међусобно признавање судских наредби у вези са истрагама компјутерског криминала, задржавање информација о преносу података, анонимни приступ и употреба,

против компјутерског криминала из 2007. године[97]. У *Стокхолмском програму* који је представљао политичку агенду ЕУ за период 2010-2014[98] истакнуто је да би државе чланице требало што је пре могуће да ратификују КВК[99]. Конвенција би требало да постане референтни правни оквир за борбу против високотехнолошког криминала на глобалном нивоу, који је препознат као једна од највећих изазова надлежних органа држава чланица и у програму 2015-2019[100]. Резултат таквог става је потписивање Конвенције од стране свих чланица ЕУ у овом периоду (Конвенције је ратификована и ступила на снагу у свим земљама чланицама, осим у Грчкој, Ирској и Шведској).

практична сарадња на међународном нивоу, надлежност, доказна снага компјутерских података, и сл. Ово саопштење је заправо представљало иницијативу за касније усвајање Оквирне одлуке о нападима на информационе системе из 2005. године, као обавезујућег извора права у оквиру некадашњег трећег стуба ЕУ (*Communication Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*, http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf.)

[97] Након што су препознати основни трендови компјутерског криминала, Комисија је за основне правце развоја политике супротстављања таквом облику криминала поставила: побољшање прекограничне сарадње између полицијских и судских органа држава чланица, између јавног и приватног сектора и међународне сарадње уопште. Из тих разлога Комисија се и у овом саопштењу залаже за подстицање држава чланица да ратификују Конвенцију СЕ – чак се помиње разматрање могућности да Заједница постане потписница Конвенције. Кључна активност се свакако огледа у успостављању оперативне сарадње између националних органа гоњења и процедура размене података, стручности и примера добре праксе на свим нивоима, као и између јавног и приватног сектора (првенствено се мисли на пружаоце услуга електронских комуникација). (*Towards a general policy on the fight against cyber crime*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF*). Широка подршка ратификовању Конвенције препознаје се и у ледећим документима:* Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, *http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf;*

[98] Official Journal of European Union C 115/1, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF*. Пред Комисију је Савет поставио захтев да да предлоге за разраду правног оквира за истраживања у кибер простору унутар Уније, те да предузима мере за унапређење/ побољшање партнерства јавног и приватног сектора. С тим у вези, унутар Уније би такође требало се да разјасне правила о надлежности и утврди законски оквир који се примењује на кибер простор унутар Уније, укључујући уређење прибављања доказа у циљу промоције прекограничне истраге. Услед значаја прекограничне сарадње, Европски савет је позвао државе чланице да унапреде међусобну правосудну сарадњу у предметима високотехнолошког криминала, нагласивши потребу сарадње и са земљама ван Уније. Такође, Савет је позвао државе чланице да дају пуну подршку националним платформама за обавештавање задужене за борбу против високотехнолошког криминала. Истакнуто је да би ЕУРОПОЛ могао да игра улогу ресурсног центра, стварањем Европске платформе за идентификацију дела која би требало да помогне националним платформама за упозоравање, те разменом релевантних података и најбоље праксе у вези са борбом против високотехнолошког криминала између држава чланица.

[99] H. Buono, „Gearing up the fight against cybercrime in the European Union: a new set of rules and the establishment of the European cybercrime center (ec3)“, *New journal of European criminal Law* 3/2012, 244.

[100] *Building an open and secure Europe, 2014*, http://europa.eu/pol/pdf/flipbook/en/borders_and_security_en.pdf.

Осим поменутих стратешких документа, јасно опредељење супротстављању високотехнолошком криминалу се манифестује и у донетим изворима права, од којих су најзначајнији: Директива о борби против сексуалне злоупотребе и искоришћавања деце и дечје порнографије[101] и Оквирна одлука о нападима на информационе системе[102].

Препознавши да је за супротстављање порнографском материјалу на ком су приказана деца а који су доступни путем Интернета, неопходно постојање правног оквира[103], да је степен регулисаности био различит од државе до државе, те да ефикасна борба против *online* дечје порнографије захтева хармонизацију националних прописа и успостављање одговарајуће међународне сарадње, на нивоу Европске уније је 2004. године усвојена Оквирна одлука о борби против сексуалног искоришћавања деце и дечје порнографије[104]. Како је Оквирна одлука и поред задовољавајућег нивоа имплементације имала незанемарљиве недостатке, у циљу унапређења правног оквира, након што су ступањем на снагу Уговора из Лисабону[105] створене нове легислативне могућности[106], децембра 2011. године

---

[101] *Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF.

[102] *Framework Decision 2005/222/JHA on attacks against information systems,* Official Journal of the European Union, L 69/67, *http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF*.

[103] Правни оквир би требало да садржи правила о инкриминисању одређених штетних понашања, идентификовању деце која су жртве, откривању и кривичном гоњењу учинилаца кривичних дела, уклањању садржаја са Интернета, односно онемогућавање приступа страницама на којима се ти садржаји налазе.

[104] *Council Framework Decision 2004/68/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography,* OJ L 13, 20.1.2004, p.44; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:NOT.

[105] *The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:EN:PDF.

[106] Уговором из Мастрихта (потписан 7. фебруара 1992. године, ступио на снагу 1. новембра 1993. године) у структури Европске уније предвиђен је тзв. Трећи стуб, као институционални оквир за правосудну и полицијску сарадњу у кривичним стварима (регулисан у поглављу 6). Важно је напоменути да у овој области институције ЕУ нису имале никакве надлежности и нису могле да усвајају уредбе и директиве као изворе права. Уговором из Амстердама (потписан 2. октобра 1997. година, а ступио на снагу 1. маја 2009. године) као један од циљева Европске уније прокламована је изградња простора слободе, безбедности и правосуђа, а Савет је добио овлашћење да на предлог Комисије и уз претходне консултације са Парламентом доноси одлуке и оквирне одлуке. Од ступања на снагу Уговора из Лисабона (потписан 13. децембра 2007. године, ступио на снагу 1. децембра 2009. године) структура ЕУ се више не заснива на „стубовима“ а органи ЕУ се овлашћују да правно уређују и питања из оквира некадашњег Трећег стуба, и то у четири области: 1. Сарадња у вези са контролом граница, питањима азила и имиграција; 2. Правосудна сарадња у грађанским стварима; 3. Правосудна сарадња у кривичним стварима; 4. Полицијска сарадња. На

усвојена ***Директива о борби против сексуалне злоупотребе и искоришћавања деце и дечје порнографије***[107]. Директива има за циљ да створи правни оквир за заштиту деце[108] од свих облика сексуалне злоупотребе и искоришћавања, унапређење међународне сарадње, те предузимање мера превенције и мера заштите деце жртава тих кривичних дела[109]. Члан 5. Директиве обавезује државе да предузму потребне мере да се *наведене радње у вези са online дечјом порнографијом*[110] *које су предузете с умишљајем и неовлашћено*[111] *предвиде као кривично дело и за њих пропишу казне затвора* у одређеном трајању[112]. Осим тога,

---

тај начин европске институције су добиле овлашћење да утврђују минимум правила која се односи на инкриминисање одређених понашања као кривичног дела, кривични поступак и облике сарадње надлежних органа држава чланица у кривичним стварима.

[107] Државе чланице су биле дужне да донесу законе, подзаконске акте и друге прописе у циљу усклађивања са одредбама Директиве до 13. децембра 2013. године, а Комисија ће до 18. децембра 2015. године саставити, те Парламенту и Савету поднети, извештај у ком ће проценити у којој мери су државе чланице предузеле потребне мере у циљу усаглашавања са одредбама Директиве.

[108] *Дететом* се сматра лице млађе од 18 година (што одговара појму малолетног лица у кривичном праву Републике Србије), с тим што Директива предвиђа могућност да држава у складу са националним прописима одреди узраст у ком је малолетно лице способно да сагласност за ступање у сексуалне односе, док је ступање у сексуалне односе са малолетним лицем млађим од тако одређеног узраста забрањено чак и уз његов пристанак (што одговара постављању границе између детета и малолетника у домаћем кривичном праву).

[109] У том смислу, Директива садржи минимум правила којих су државе дужне да се придржавају у прописивању кривичних дела и санкција у вези са сексуалном злоупотребом и искоришћавањем деце и дечјом порнографијом, а осим тога садржи и одредбе које су од значаја за спречавање ових појава као и заштиту жртава поменутих кривичних дела. У члановима 3-6. Директиве наведене су радње у вези са сексуалном злоупотребом и искоришћавањем деце и дечјом порнографијом које су државе чланице дужне да инкриминишу у својим законодавствима. За сваку од ових радњи прописани су и минимуми најтеже казне затвора које је држава дужна да испоштује приликом предвиђања санкције за одређено кривично дело.

[110] У смислу Директиве *термин дечја порнографија односи се на*: материјал који визуелно осликава дете укључено у праве или симуловане експлицитне сексуалне односе; приказ сексуалног органа детета, који примарно служи у сексуалне сврхе; материјал који визуелно осликава лице које изгледа као да је дете, укључено у праве или симуловане експлицитне сексуалне односе или приказ сексуалног органа лица које изгледа као да је дете, који примарно служи у сексуалне сврхе; реалистични приказ детета укљученог у експлицитне сексуалне односе или реалистични приказ сексуалног органа детета која примарно служи у сексуалне сврхе. Државама се оставља могућност да инкриминишу поменуте радње и у случајевима да порнографски материјали садрже приказе лица које изгледа као дете, а у ствари је имало 18 или више година у време настанка порнографског материјала. Више о томе, "Cybercrime" Provisions in The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, The Cybercrime Convention Committee (T-Cy), 2008, *http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20%282008%29%2003%20E%20-%20Sexual%20exploitation%20of%20children.PDF.*

[111] Употреба термина „неовлашћено" у овој одредби оставља државама чланицама могућност да из криминалне зоне и уопште одређивања појма „дечја порнографија" искључе одређене приказе, на пример, оне који су настали у медицинске, научноистраживачке и сличне сврхе, као и овлашћено поседовање одређених приказа од стране надлежних органа у вези са кривичним поступком или са спречавањем, откривањем и доказивањем кривичних дела.

[112] Предвиђа се инкриминисање следећих радњи то: 1. прибављање или поседовање дечје порнографије (максимална казна затвора у трајању од најмање 1 године); 2. свесно приступање

државе би требало да предвиде да је *кажњив и покушај* да се изврши нека од радњи предвиђених у члану 5. на тај начин што пунолетно лице средствима информационо-комуникационих технологија дете наводи да му пружи материјал порнографског садржаја у ком је дете приказано[113]. У вези са *откривањем и доказивањем наведених кривичних дела и гоњењем учинилаца*, Директива садржи изузетно битне одредбе[114]. Једна од најважнијих одредаба Директиве односи се обавезу држава да предвиде могућност да се у откривању и доказивању поменутих кривичних дела користе посебне истражне радње (које се користе у откривању и доказивању дела организованог криминала и других тежих кривичних дела). Ефикасне истражне радње односе се на пресретање комуникација, тајно праћење, укључујући електронски надзор, праћење банковних рачуна, за чије одређивање се узимају у обзир, између осталог, принцип пропорционалности, природа и озбиљност дела под истрагом. У случајевима у којима је то могуће и у складу са националним законодавством, такве радње подразумевају овлашћење службених лица да користе прикривени, тј. лажни идентитет на Интернету. Такође, да би се утврдио идентитет жртава поменутих кривичних дела, државе треба да омогуће употребу одређених техника

дечјој порнографији коришћењем информационо-комуникационих технологија (максимална казна затвора у трајању од најмање 1 године); 3. ширење, растурање или преношење дечје порнографије (максимална казна затвора у трајању од најмање 2 године); 4. нуђење, снабдевање или на други начин чињење доступном дечје порнографије (максимална казна затвора у трајању од најмање 2 године); 5. производња дечје порнографије (максимална казна затвора у трајању од најмање 3 године). Такође, државе могу да одлуче да ли ће се инкриминације односити и на случајеве у којима је креатор материјала порнографске садржине исте произвео и поседује само за сопствене потребе а да при томе не постоји ризик од ширења тог материјала.

[113] Успостављање контакта пунолетног лица са дететом у сврху задовољавања сексуалног нагона постало је нарочита претња у Интернет окружењу (коришћењем разних социјалних мрежа, форума, причаоница и других комуникационих канала) које пружа могућност анонимности и прикривања личних карактеристика (као што је узраст). Таква појава се назива *grooming.* Више о томе, F. Monterosso, "Protecting The Children: Challenges That Result In, And Consequences Resulting From, Inconsistent Prosecution Of Child Pornography Cases In A Technical World", *The Richmond Journal of Law and Technology* 3/2010, 5-7.

[114] Наиме, државе се обавезују да предузму неопходне мере да обезбеде да откривање, доказивање и гоњење не зависи од постојања кривичне пријаве, предлога за гоњење, односно кривичне тужбе жртве и њених заступника, као и да поступак може да се настави и у случају да жртва повуче предлог за гоњење, тужбу, односно своје исказе. Такође, државе би требало да предвиде да кривично гоњење учинилаца већине поменутих кривичних дела (члан 3, члан 4. става 2, 3, 5, 6 и 7. и из члана 5. става 6.) буде могуће и када је порнографски материјал коришћен одређени временски период након пунолетства жртве, узимајући у обзир тежину учињеног кривичног дела. У вези са подношењем кривичних пријава, државе би требало да предузму све мере да дужност чувања професионалне тајне код одређених занимања које подразумевају рад са децом не представља препреку тим лицима да пријаве кривично дело, у случају када имају оправдан разлог да верују да су деца жртве неке од поменутих кривичних дела. Види A. Reid, „Online protection of the child within Europe", *International Review of Law, Computers & Technology* 3/2009, 222.

у анализи порнографског материјала који су доступни или се преносе средствима информационе технологије. Осим тога, Директива од државе чланице захтева да би требало *да успоставе, односно унапреде сарадњу и са трећим државама* како би заједничким напорима уклониле порнографске садржаје са сервера који се налазе ван територије ЕУ[115], што је често тешко или из разлога што држава у којој се сервери налазе не жели да сарађује или се поступак уклањања показује као превише дуготрајан[116]. У складу са наведеним, члан 25. Директиве предвиђа да су државе дужне да предузму мере којим се обезбеђује *хитно уклањање Интернет страница* које садрже или служе за ширење материјала порнографског садржаја на којима су деца, а које се налазе на серверима како на територијама држава чланица тако и ван територије ЕУ[117].

[115] Полазећи од тога да борба против дечје порнографије захтева онемогућавање, односно ограничење могућности за циркулисање порнографског материјала (ни у ком случају се не може и не сме довести у вези са слободом мишљења и изражавања) и да је потребно пронаћи механизме да се лицима укљученим у активности производње и дистрибуирања тих штетних садржаја отежа да их чине доступним на Интернет страницама, да се уклоне постојећи садржаји и да се учине кажњивим ширење и преузимање тих садржаја.

[116] Из тог разлога, приликом доношења Директиве дошло се на идеју да се уведу механизми за блокирање приступа са територије ЕУ Интернет страницама за које је утврђено да садрже или служе за ширење дечје порнографије, при чему мере које државе чланице могу предузети ради уклањања, односно блокирања приступа таквим Интернет страницама могу бити легислативне, нелегислативне, судске и друге. Директива подржава самоиницијативне акције пружалаца Интернет услуга (*Internet service provider*) у циљу спречавања злоупотребе њихових услуга, односно све активности које би државе чланице предузеле, с тим што су државе чланице, без обзира на одабрану акцију или метод, дужне да обезбеде да оне буду у складу са принципом правне сигурности и унапред познате како корисницима тако и пружаоцима Интернет услуга. Из тог разлога неопходно је успостављање и унапређење сарадње државних институција и приватног сектора, нарочито у погледу стварања заједничке комплетне листе Интернет страница и избегавања дуплирања посла, а све то уз поштовање права крајњих корисника и усаглашавање са постојећим правним процедурама и стандардима и Европском конвенцијом о основним људским правима и слободама и Повељом ЕУ о основним људским правима. Упор. T.J. McIntyre, "Blocking child pornography on the Internet: European Union Developments", *International Review of Law, Computers & Technology* 3/2010, 213; R. Kleinschmidt, „An International Comparison of ISP's Liabilities for Unlawful Third Party Content", *International Journal of Law and Information Technology* 4/2010, 335-336.

[117] Осим тога, државе могу да предузму мере којима се *блокира приступ Интернет страницама,* које садрже или служе са ширење материјала порнографског садржаја на којима су деца, а које се налазе *на или ван територије* држава чланица, корисницима Интернет услуга који се налазе на територији држава чланица, с тим да се такве мере могу предузети само на основу транспарентних процедура које обезбеђују довољно адекватних гаранција (укључујући и могућност обраћања судским органима) нарочито у смислу да се ограничења предузимају само као потребна и сразмерна и да су корисници упознати са разлозима таквог ограничења. Упор. W.Ph. Stol et al., „Governmental filtering of websites: the Dutch case", *Computer law & security review* 25/2009, 257; P. Schumacher, „Fighting illegal Internet content - May access providers be required to ban foreign websites? A recent German approach", *International Journal of Communications Law and Policy*, 8/2004, 17.

Савет ЕУ је 24. фебруара 2005. године, на основу предлога Комисије предлог да се донесе оквирну одлуку који би се односила на незаконит приступ и поступање у вези са информационим системима, усвојио ***Оквирну одлука о нападима на информационе системе***. Сврха поменуте одлуке је приближавање националног законодавства и унапређење међународне полицијске и правосудне сарадње држава чланица у вези са најзначајнијим формама употребе информационих система у криминалне сврхе. Оквирна одлука је створила заједнички скуп правних дефиниција и одредила кривична дела која се односе на криминалне активности у вези са електронским мрежама, компјутерима и другим уређајима повезаним са мрежом (нпр. мобилни телефони), као и у вези са подацима и програмима у тим уређајима и мрежама[118]. Што се тиче надлежности, преузета су правила из Конвенције СЕ, па је држава надлежна за кривично дело извршено на њеној територији[119], критеријум држављанства се предвиђа као алтернативни за одређивање надлежности, док ће се случају сукоба, надлежност одредити споразумевањем између држава чланица да се централни поступак води у једној од држава које конкуришу на јурисдикцију[120]. У вези са унапређењем међусобне сарадње, у циљу побољшања размене података, од држава чланица се тражи да успоставе мрежу на принципу "24/ 7 " у оквиру које је 24 сата дневно, 7 дана у недељи, могућа размена информација о нападима на информационе системе. Остали аспекти процесног права нису преузети из Конвенције СЕ[121]. Поменута Оквирна одлука заправо је први корак ка уређењу кривичних дела у вези са нападима на информационе системе у оквиру ЕУ. Услед недовољног

[118] У типологији кривичних дела, Оквирна одлука се држи типологије успостављене Конвенцијом СЕ, па пред државе чланице поставља захтев да предузму мере да се као кривична дела предвиде и казне: 1. незаконит приступ информационим системима (чл. 2); незаконито ометање система (чл. 3), и незаконито ометање података (чл. 4). Државе чланице се обавезују да за ова кривична дела предвиде максималне казне између 1 и 3 године затвора (чл.6), односно између 2 и 5 година затвора, уколико су кривична дела почињена у оквиру криминалне организације, што је предвиђено као отежавајућа околност (чл.7). За кривичну одговорност за ова дела неопходно је утврдити постојање умишљаја код учиниоца, а подстицање, помагање, подржавање као и покушај извршења тих дела такође ће би требало да буду кажњени (чл.5).

[119] Држава ће бити надлежна уколико је извршилац физички присутан на њеној територији без обзира да ли се информациони систем који је нападнут налази или не налази на истој територији или ако се на њеној територији налази информациони систем који је предмет напада, без обзира где се налази извршилац.

[120] То ће бити држава на чијој територији је кривично дело извршено, или држава чији је држављанин извршилац или држава у којој је извршилац пронађен. R. Rahman, „The legal measure against Denial of Service (DoS) attacks adopted by the United Kingdom legislature: should Malaysia follow suit?“, *International Journal of Law and Information Technology* 2/2012, 95.

[121] M. Gercke, P. Brunst, *Praxishandbuch Internetstrafrecht*, Kohlhammer Auflage, Stuttgart 2010, 412.

нивоа имплементације и услед технолошког напретка и појаве нових облика извршавања компјутерских кривичних дела, уочена је потреба за изменом постојећих правила (чему је у прилог ишла је и „комунитаризација“ Трећег стуба ЕУ[122]), па је Комисија 2010. године Савету упутила предлог Директиве о нападима на информационе системе, која би требало да замени постојећу Оквирну одлуку[123]. Међутим, предлог директиве је још увек у процедури усвајања.

2.3. Република Србија

У домаћој кривичноправној теорији најзатупљенији је став по ком се компјутерски криминалитет може одредити као вршење одређених кривичних

[122] Дакле, право које је извирало из делокруга трећег стуба Уније није имало дејства комунитарног права, као што су непосредна примењивост и принцип првенства, а са друге стране, комунитарно право има директно дејство и примат у односу на национално право и оно је једино подлегало контроли Европског суда правде. Наиме, правила ЕУ која се односе на уређење одређених области у оквиру бившег Трећег стуба ЕУ пре Лисабонског уговора доношена су у форми оквирних одлука које немају директно дејство у државама чланицама, него је потребна њихова имплементација у национална законодавства. При том Комисија има само могућност надгледања нивоа имплементације правила из оквирних одлука, без могућности изрицања било какве санкције држави чланици која не приказује задовољавајући ниво имплементације или одговарања државе због неиспуњења обавеза из оквирне одлуке пред Европским судом правде због неиспуњења обавеза из оквире одлуке. Ступањем на снагу Лисабонског уговора 1. децембра 2009. године створене су могућности за олакшано усвајање нових легислативних мера у области правосудне и полицијске сарадње (квалификованом већином чланова Савета ЕУ уз учешће Парламента) и то у форми директиве (која има директно дејство), док је Комисији дато овлашћење да надгледа да ли се земља чланица придржава директиве, те уколико не поступа у складу са директивом, Комисија може да се обрати Европском суду правде. E. Kerlin- Karnell, „The Treaty of Lisbon and the Criminal Law: Anything New Under the Sun?“, *European Journal of Law Reform*, 3/2008, 8.

[123] Предлог Комисије доступан је јавности преко интернет странице *http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/463&format=HTML&aged=0&language=EN&guiLanguage=en*. У односу на Оквирну одлуку, предлог Директиве: поред незаконитог приступа информационим системима, незаконитог ометања система и незаконитог ометања података, предвиђа инкриминацију употребе одређених алата (као што су малициозни софтвери – нпр. ботнет – или незаконито прибављање компјутерских лозинки) за извршавање кривичних дела; уводи незаконито ометање информационог система као кривично дело; предвиђа подизање минимума затворске казне на 2 године; подиже висину максималне казне затвора за кривична дела почињена под отежавајућим околностима на најмање пет година (уместо на две године, како је предвиђено у Оквирној одлуци) уколико је кривично дело извршено: (а) у оквиру криминалне организације; (б) употребом алата који могу да изазову било нападе на велики број информационих система, било нападе који са собом повлаче знатна оштећења, у смислу поремећаја системских услуга, финансијских трошкова или губитка личних података (отежавајућа околност која није била предвиђена у Оквирној одлуци); (в) прикривањем правог идентитета починиоца и изазивањем штете законитом власнику идентитета (отежавајућа околност која није била предвиђена у Оквирној одлуци); предвиђа побољшањање полицијске/судске сарадње јачањем постојећег система размене података на бази 24/7, укључујући обавезу одговора на хитан захтев најкасније у року од 8 сати од постављања захтева; уводи обавезу прикупљања статистичких података о компјутерском криминалу.

дела злоупотребом рачунара, односно рачунарском система, што значи да само вршење кривичних дела подразумева употребу рачунара, односно рачунарског система као средства или циља извршења кривичног дела[124]. Овакав став је заузео и законодавац приликом одређивања која су то кривична дела у важећем извору кривичног материјалног права. Наиме, ***Кривични законик Републике Србије*** садржи одређен број кривичних дела који би могла бити обухваћена појмом високотехнолошког криминала. Занимљиво је да су у домаће кривично законодавства ове инкриминације биле први пут уведене 2003. године изменама и допунама Кривичном закона Србије, тако што су прихваћена решења из Нацрта КЗ СР Југославије из фебруара 2000. године, чиме је Србија инкриминисала поједина штетна понашања у кибер простору пре усвајања Конвенције у оквиру Савета Европе и пре него што је као потписница Конвенција била на то обавезана (Србија је тек 2005. године потписала Конвенцију)[125].

Ради сузбијања недозвољених понашања у вези са употребом информациних технологија као *ultima ratio* у Кривичном законику у глави 27. је прописано ***осам кривичних дела против безбедности рачунарских података***:

1. Оштећење рачунарских података и програма (члан 298);
2. Рачунарска саботажа (члан 299);
3. Прављење и уношење рачунарских вируса (члан 300);
4. Рачунарска превара (члан 301);
5. Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302);
6. Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303)[126];
7. Неовлашћено коришћење рачунара или рачунарске мреже (члан 304);
8. Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података (члан 304а).

[124] З. Стојановић, Н. Делић,, *Кривично право, Посебни део*, друго издање, Београд 2014, 260.
[125] З. Стојановић, *Коментар Кривичног законика*, Београд 2006, 663.
[126] У називу овог кривичног дела у трећој речи постоји словна грешка, па уместо „ограничавање“ стоји „органичавање“.

Од доношења Кривичног законика 2006. године у погледу ове групе кривичних дела извршене су измене и допуне 2009. године доношењем Закона о изменама и допунама Кривичног законика 2009. године[127], и то једино у законском опису кривичног дела неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. став 2) проширењем појма радње извршења. Осим тога, прописано је и ново кривично дело у овој глави у члану члан 304а[128].

Кривично дело ***оштећење рачунарских података и програма*** има три облика: основни и два тежа. Радња *основног облика* је одређена алтернативно, те може бити извршена на различите начина: брисањем, изменом, оштећењем, прикривањем или на други начин чињењем неупотребљивим рачунарског податка или програма. Било који од наведених облика извршења чини се неовлашћено, односно без сагласности власника рачунарског података или програма (без одговарајуће дозволе[129]). Кривично дело је извршено уколико је услед предузете радње извршења рачунарски програм или податак постао неупотребљив, односно не служи својој сврси. Дакле, *објект радње* су рачунарски подаци или рачунарски програм, а значење ових термина одређено је у члану 112. Тако је рачунарски податак свако представљање чињеница, информација или концепта у облику који је подесан за њихову обраду у рачунарском систему, укључујући и одговарајући програм на основу кога рачунарски систем обавља своју функцију (став 17), док се рачунарским програмом сматра уређени скуп наредби који служе за управљање радом рачунара, као и за решавање одређеног задатка помоћу рачунара (став 19). Законик је предвидео и два тежа облика, а квалификаторна околност је висина проузрокована штете (уколико је проузрокована штета у износу који прелази четристопедесет хиљада динара, односу у износу који прелази милион и петсто хиљада динара). *Субјективно обележје* за ово кривично дело је умишљај, а извршилац кривичног дела, сходно законској одредби, може бити било које лице.

Кривичним делом ***рачунарска саботажа*** штите се електронски сиистеми и мреже за електронску пренос и обраду података који имају посебан друштвени

[127] „Службени гласник РС“, бр. 79/2009.
[128] Н. Делић, *Нова решења у посебном делу КЗ Србије*, Београду 2014, 134.
[129] Стојановић, Делић, *op.cit*, 263.

значај[130]. Кривично дело има два основна облика. Радња извршења првог одновног облика кривичног дела је алтернативно одређена као уношење, уништење, брисање, измена, оштећење, прикривање или на други начин чињење неупотребљивим рачунарског податка или програма. Радња извршења другог облика је уништење или оштећење рачунара или другог уређаја за електронску обраду и пренос података. Објект радње је рачунарски података или рачунарски програм, док је објект друге радње, пак, оштећење рачунара или други уређај за електронску обраду и пренос података. У погледу субјективног обележје, за ово кривично дело је поред умишљаја, потребно да постоји одређена намера. Намера се састоји у томе што се радња извршења предузима ради онемогућавања или знатног ометања поступка електронске обраде и преноса података[131], но да би кривично дело било довршено није потребно да намера буде реализована. Осим тога, намера мора да обухвати и то да се ради о подацима који су од значаја за државне органе, јавне службе, установе, предузећа или друге субјекте.

Постоје два облика кривичног дела ***прављење и уношење рачунарских вируса.*** *Радња основног облика* састоји се у креирању рачунарског програма или неког другог скупа наредби унетих у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података (члан 112. став 20). Потребно је да радња извршења буде учињена у намери уношења рачунарског вируса у туђ рачунар или рачунарску мрежу (прављење вируса без постојања те одређене намере представљало би некажњиви покушај[132]). Постојање намере подразумева постојање директног умишљаја. Радња извршења тежег облика подразумева уношење рачунарског вирус у туђ рачунар или рачунарску мрежу. Кривично дело је довршено када је услед уношења рачунарског вируса у туђ рачунар или рачунарску мрежу дошло до наступања штете која се утврђује у сваком конкретном случају[133].

[130] Стојановић, Делић, *op.cit*, 264.
[131] Стојановић, *Коментар Кривичног законика*, 665
[132] Стојановић, *op.cit*, 666.
[133] Стојановић, Делић, *op.cit*, 266.

Иако кривично дело ***рачунарска превара*** представља посебан облик преваре, од кривичног дела преваре се разликује по томе што не постоји довођење или одржавање у заблуди неког лица, па се не може подвести под опште кривично дело преваре[134]. Кривично дело има основни, два тежа и један привилегован облика. Радња извршења основног облика огледа се у уношењу нетачног податка, пропуштању уношења тачног податка или прикривању тачног података на други начин или лажном приказивању податка. Нужно је да последица неке од алтернативно наведених радњи буде измењен резултат електронске обраде и преноса података. Уколико радње не би проузроковале наведену последицу, радило би се у конкретном случају о некажњивом покушају. Субјективно обележје је постојање директног умишаја, те намере да извршилац себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету (што значи да је нехат искључен као могући облик кривице). Намера обухвата не само прибављање противправне имовинске користи, него и наношење другом имовинске штете. Уколико је, пак, радња учињена само у намери да се други оштети, постојаће привилегован облик дела. За постојање кривичног дела, међутим, није потребно да је намера и остварена. Предвиђена су и два квалификована облика, одређена висином проузроковане имовинске штете (тежи облик постоји уколико је делом прибављена имовинска корист која прелази износ од четристопедесет хиљада динара, а најтежи уколико имовинска штета прелази износ од милион и петсто хиљада динара).

Кривично дело ***неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података*** има основни и два тежа облика. Радња основног облика је неовлашћено укључивање у рачунар или рачунарску мрежу или неовлашћено приступање електронској обради података. Укључивање, односно приступање је неовлашћено, односно без сагласности држаоца рачунара или контролора процеса обраде података и то кршењем одређених мера заштите. Субјективно обележје је постојање умишљаја, док је намера ирелевантна. Први тежи облик постоји уколико је податак добијен извршењем основног облика снимљен или употребљен на други начин, при чему није од значаја у коју сврху и на који начин је податак употребљен (што може бити од значаја за одмеравање

[134] Стојановић, *Коментар Кривичног законика*, 667.

казне[135]). Други тежи облик постоји уколико је услед основног облика проузрокована последица која се огледа или у застоју или озбиљном поремећају функционисања електронске обраде и преноса података или мреже или су наступању неке друге тешке последице. Тешка последица се не односи само на директне последице настале у рачунару, рачунарској мрежи или другом уређају за електронску обраду података, него обухвата и друге последице проузроковане неовлашћеним приступом.

Прописивањем кривичног дела ***спречавање и ограничавање приступа јавној рачунарској мрежи*** се штити право грађана на међусобно комуницирање и информисање путем рачунара. Радња кривичног дела је спречавање или ометање приступа јавној рачунарској мрежи, што се чини неовлашћено. Тежи облик, као и код других кривичних дела којима се угрожавају слободе и права грађана, постоји уколико радњу основног облика учини службено лице у вршењу службе. Рачунарском мрежом сматра се скуп међусобно повезаних рачунара, односно рачунарских система који комуницирају размењујући податке (члан 112. став 18), док је под јавном рачунарском мрежом подразумева она рачунарска мрежа која је, под одређеним условима, доступна свима. Субјективно обележје овог кривичног дела јесте умишљај.

Радња кривичног дела ***неовлашћено коришћење рачунара или рачунарске мреже*** подразумева употребу рачунара или рачунарске мреже без постојања сагласности држаоца рачунара, односно контролора рачунарске мреже. Ради се о најлакшем кривичном делу из ове главе. Субјективно обележје овог кривичног дела је умишљај, али је за постојање кривичног дела потребна да је радња извршена у намери да се себи или другом прибави противправна имовинска корист (али није потребно да је та намера и остварена). С обзиром на природу дела и значај, предвиђено је да се гоњење предузима се по приватној тужби.

Иако припремање кривичног дела не улази у зону кажњивости, законодавац је поједине припремне радње прописао као засебна кривична дела, као што је случај и са кривичним делом ***прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.*** Тако, припремне радње за извршење кривичних дела против безбедности рачунарских

[135] Стојановић, *op.cit*, 668.

података чине радњу овог кривичног дела и састоје се у поседовању, прављењу, набављању, продаји или давању другом на употребу рачунара, рачунарских система, рачунарских податке и програма ради извршења. Да би постојало кривично дело, потребно је да једна од алтернативно прописаних радњи буде предузета ради извршења кривичних дела против безбедности рачунарских података[136]. Стога субјективна страна кривичног дела подразумева директан умишљај и намеру да се делатности предузимају у одређеној намери.

Осим прописивања појединих кривичних дела у извору кривичног материланог права, ради доприноса успешној борби против ове врсте кривичних дела усвојен је ***Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*** 2005. године[137], који се примењује ради откривања, гоњења и суђења за кривична дела обухваћена појмом високотехнолошког криминала.

Закон у члану 2. одређује ***високотехнолошки криминал*** као вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. Члан 3. Закона проширује појам високотехнолошког криминала одређујући групе кривичних дела која се под одређеним околностима сматрају високотехнолошким криминалом. Предвиђено је да се Закон примењује на откривање, гоњење и суђење за 1) кривична дела против безбедности рачунарских података одређена Кривичним закоником; 2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара; 3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због *начина извршења* или *употребљених средстава* могу сматрати кривичним делима високотехнолошког криминала. На основу приказаног, могло би се рећи да је законодавац у значајној мери

[136] Делић, *op.cit*, 135.
[137] „Сл.гласник РС“, бр. 61/2005 и 104/2009.

прилагодио одредбе кривичног материјалног права решењима из Конвенције Савета Европе, док у погледу извора права Европске уније постоје одређена одступања. Ипак, за потпуно сагледавање проблема високотехнолошког криминала, осим разматрања теоријског одређења појма и кривичноправног оквира, потребно је сагледати и затупљеност овог облика криминала.

3. ОБИМ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Док је пре неколико деценија претња високотехношког криминала као вискософистиране криминалне активности била у домену научне фантастике, та претња данас представља реалност и кривична дела обухваћена овим обликом криминала проузрокују стварну штету појединцима, друштву и држави[138]. *Ипак, доступни извештаји о стању високотехнолошког криминала у медијима и стручној јавности се углавном заснивају на процени ризика од стране компанија из приватног сектора које се баве безбедношћу рачунарских система*. Истраживања показују да је глобална штета у 2013. години износила између 110 и 113 милијарди долара, при чему је просечна штета по појединцу износила је 197-298 долара[139] (штету трпе појединци чији подаци о личности су украдени – њих преко 550 милиона[140]). Процењује се да је у 2014. години високотехнолошки криминал глобалној економији нанео штету између 375 и 575 милијарди долара годишње, а просечна штета коју компаније трпе од напада на њихове информационе системе износила је 7.6 милиона долара.[141]. Други извор наводи цифру од преко 800 милиона у 2013. години (нпр. 40 милиона у САД, 54 милиона

[138] Да би се проценила укупна стварна штета коју узрокује високотехнолошки криминал, потребно је најпре одредити која кривична дела су обухваћена овим појмом. Осим тога, потребно је одредити да ли се под штетом посматрају само директне или индиректне последице високотехнолошког криминала (губитак интелектуалне својине, крађа финансијских средстава и осетљивих пословних информација, додатни трошкови за обезбеђење рачунарског система, трошкови опоравка од напада на информациони систем и слично).

[139] Током 2013. године извршено је *online* анктерирање 13,022 лица старости 18-64 године из 24 државе. (*Net Losses: Estimating the Global Cost of Cybercrime*, 2014, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf).

[140] http://www.symantec.com/about/news/release/article.jsp?prid=20131001_01

[141] *2014 Global Report on the Cost of Cyber Crime*, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf. Студија је израђена на основу података из САД, Велике Британије, Немачке, Аустралије, Јапана, Француске и Руске федерације и обухватала је 257 компанија.

у Турској, 16 милиона у Немачкој) [142], чиме је причињена штета око 160 милијарди годишње[143]. У 2013. години је преко 3000 компанија пријавило неовлашћен упад у информациони систем у САД, две банке у Персијском заливу су за неколико сати изгубиле милиона долара[144], док је једна британска компаније пријавила штету од 1.3 милијарде фунти само од једног напада[145] , а бразилске банке да њихови клијенти губе милионе долара годишње услед рачунарских превара[146]. Када је *Google* био хакован 2010. године, 34 компаније у различитим секторима су претрпеле штету због повреде права интелектуалне својине[147].

Поставља се *питање да ли се ове информације могу третирати као поуздане*? Сматрамо да ове процене нису реалне, јер се не заснивају на потпуном чињеничном субстрату[148], а подаци су прикупљени без утврђене методологије и за различите потребе[149]. Мишљења смо да се проблем огледа и у поимању високотехнолошког криминала, јер су поменути приступи некохерентни и често контрадикторни. Уколико се посматрају сензационалистички наслови у медијима и доведу у везу са извештајима о стању криминала који се заснива на злоупотреби информационих технологија, могло би се доћи до закључка да је реална опасност од високотехнолошког криминала постала од већа од свих дистопијских предвиђања. Међутим, треба имати у виду да *подаци из званичних статистичких извора у појединим државама указују на другачије стање ствари*[150], односно да

[142] J. Hawes, "2013 An Epic Year For Data Breaches With Over 800 Million Records Lost," Naked Security, February 19, 2014, http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-withover-800-million-records-lost/

[143] http://www.ponemon.org/news-2/23

[144] "Six Arrested Over 45 Million Cyber Heist on Middle East Banks," Al Arabiya, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Sixarrested-over-45-million-cyber-heist-on-Middle-East-banks.html

[145] T. Whitehead, "Cyber Crime A Global Threat, MI5 Head Warns," The Telegraph, June 6, 2012, http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crimea-global-threat-MI5-head-warns.html

[146] J. Robertson, "Why Are Hackers Flooding Into Brazil?" Bloomberg, September 13, 2013, http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html

[147] Укључујући следеће компаније: *Yahoo, Symantec, Adobe, Northrop Grumman* и *Dow Chemical*. (A. Cha, E.Nakishima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," The Washington Post, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html).

[148] A. Zavrsnik, „Cybercrime - definitional challenges and criminological particularities", *Masaryk University Journal of Law and Technology* 2/2008. 4-5.

[149] Више о методолошким, концептуалним логичким и статистичким проблемима у процени високотехнолошког криминала, види Kshetri, *op.cit*, 7-10.

[150] У Европским изворницима о криминалитету и статистици кривичног правосуђа (*European Sourcebook of Crime and Criminal Justice Statistics*) публикују се најпотпунији подаци о криминалитету на европском континенту, и као такви представљају поудан извор података који

број пријављених кривичних дела, оптужених и осуђених лица не расте експоненцијално и драматично као што се тврди[151].

У ***Србији*** број поднетих кривичних пријава за кривична дела против рачунарских података (у периоду од прописивања ове групе кривичних дела до 2014. године) није прешао 1% у односу на укупан број поднетих кривичних пријава за све групе кривичних дела, а тај проценат је осцилирао од 0.01 до 0.04 (0.03 % у 2006. години , 0.01% у 2007. години, 0.02% у 2008. години, 0.04% у 2009. години, 0.03 % у 2010. години, 0.02% у 2011. години, 0.02% у 2012. години и 0.03 % у 2013. години[152]). Током 2013. и 2014. године спроведено је истраживање високотехнолошког криминала, његовог обима и појавних облика, као и примене информационо-комуникационих технологија за вршење кривичних дела у Републици Србији[153], а резултати овог истраживања показали су да је више од четвртине кривичних дела почињених употребом информационих технологија управо из групе кривичних дела против рачунарских података [154] (27.1%) али су заступљена и друга кривична дела код којих су рачунар и рачунарске мреже средство, циљ и место извршења, и то кривична дела против слободе и права

омогућава увид у стање криминалитета. Стопа кривичног дела које је регистровала полиција изражена је у релевантним бројевима, и то рачунањем у односу на 100.000 становника. Тако је у 2006. години за 29 држава које су доставиле податке просечна стопа за дело угрожавање рачунарских података (дело против поверљивости, интегритета и доступности компјутерских података и система износила 7 (при томе је стопа у седам земаља била нула, у шест је била један, а двоцифрена је била само у Немачкој (66) и Белгији (53). Наведено према: Ђ. Игњатовић, Компарација криминалитета и казнене реакције: Србија- Европа, Правни факултет Универзитета у Београду, Београд 2013, 43.

[151] Тако је, на пример, у Великој Британији од усвајања Закона о злоупотреби рачунара 1990. до 2001. Осуђено свега 70 (наведено према: Fafinsky S., „The UK Legislative Position on Cybercrime: A 20-Year Retrospective“, *The Journal of Internet Law* 10/2009, 5.), односно 150 лица до 2010. године (наведено према: D. Wall, „Criminalizing cyberspace: the rise of the Internet as a crime problem“, *Handbook of Internet Crime* (eds. Y. Jewkes, M. Yar), 88.

[152] Републички завод за статистику, «Пунолетни учиниоци кривичних дела у Републици Србији, 2013. – Пријаве, оптужења и осуде», Билтен 588/2014, http://webrzs.stat.gov.rs/WebSite/repository/documents/00/01/62/77/SB-588-PunoletniUciniociKD.pdf

[153] Истраживања је спроведено у оквиру Одељења за високотехнолошки криминал Одељења за борбу против организованог криминалаУправе криминалистичке полиције и Управе пограничне полиције Министарства унутрашњих послова, а у оквиру твининг пројекта „Успостављање ефикасног система за спречавање и сузбијање илегалних миграција на територији Републике Србије“, који је спроводи од стране Влада Велике Британије и Републике Чешке. Резултати истраживања представљени су у публикацији В. Урошевић (ур.), *Везе cyber криминала са иррегуларном миграцијом и трговином људима*, Министарство унутрашњих послова Републике Србије, Београд 2014.

[154] При томе су рачунарска превара и неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској бради података извршена у чак 88.09 % случајева.

човека (16.1%), интелектуалне својине (15.5%), полне слободе (32.3%), имовине (2.6%), уставног уређења (1.9%) и привреде (3.9%)[155].

Подаци о броју и структури пријављених кривичних дела обухваћених појмом високотехнолошког криминала у смислу члана 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала садржани су у Извештају о раду одељења за борбу против високотехнолошког криминала Вишег јавног тужилаштва у Београду у периоду од 2011. до 2014. године. У току ***2014.*** године, у уписнику познатих учинилаца заведено 294 предмета а кривичне пријаве су поднете против 333 позната учиниоца, при чему је кривична пријава поднета због кривичних дела *против безбедности рачунарских података* против 56 лица[156], што представља *16.8%* од броја лица против којих је поднета кривична пријава. Од кривичних пријава које су поднете Тужилаштву од укупног броја пријављених лица чак њих *83.2%* пријављено је због кривичних дела *из других глава Кривичног законика*, при чему су против лица у значајнијем броју поднете кривичне пријаве због кривичних дела из следећих глава КЗ[157]: због кривичних дела из главе XIV (Кривична дела против слобода и

[155] Урошевић, *op.cit*, 4.

[156] Кривичне пријаве су поднете због кривичног дела Оштећење рачунарских података и програма из чл. 298 КЗ против 2 лица, због кривичног дела Рачунарска саботажа из чл. 299 КЗ против 3 лица, због кривичног дела Прављење и уношење рачунарских вируса из чл. 300 КЗ против 2 лица, због кривичног дела Рачунарска превара из чл. 301 КЗ против 14 лица, због кривичног дела Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из чл. 302 КЗ против 34 лица и због кривичног дела Спречавање и ограничавање приступа јавној рачунарској мрежи из чл. 303 КЗ против 1 лица.

[157] Кривичне пријаве су поднете и због кривичних дела из главе XXII КЗ (Кривична дела против привреде) против 16 лица (и то због кривичног дела Фалсификовање и злоупотреба платних картица из чл. 225 КЗ против 2 лица, због кривичног дела Пореска утаја из чл. 229 КЗ против 3 лица, због кривичног дела Неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга из чл. 233 КЗ против 3 лица, због кривичног дела Одавање пословне тајне из чл. 240 КЗ против 2 лица и због кривичног дела Недозвољена трговина из чл. 243 КЗ против 6 лица), што представља 4.8% од укупно пријављених лица; због кривичних дела из главе XX КЗ (Кривична дела против интелектуалне својине) против 12 лица (и то због кривичног дела Неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199 КЗ), што представља 3.6% од укупно пријављених лица; због кривичних дела из главе XXVIII КЗ (Кривична дела против уставног уређења и безбедности Републике Србије) против 8 лица (и то због кривичног дела Изазивање националне, расне и верске мржње и нетрпељивости из чл. 317 КЗ), што представља 2.4% од укупно пријављених лица; због кривичних дела из главе XVII КЗ (Кривична дела против части и угледа) против 4 лица (и то због кривичног дела Увреда из чл. 170 КЗ) што представља 1.2% од укупно пријављених лица; због кривичних дела из главе XXXIV КЗ (Кривична дела против човечности и других добара заштићених међународним правом) против 4 лица (и то због кривичног дела Расна и друга дискриминација из чл. 387 КЗ), што представља 1.2% од укупно пријављених лица; због кривичних дела из главе XXXIII КЗ (Кривична дела против службене дужности) против 2 лица (и то због кривичног дела Злоупотреба службеног положаја из чл. 359 КЗ против 1 лица и због кривичног дела Давање мита из чл. 368 КЗ против 1 лица), што

права човека и грађанина) против 139 лица[158] (што представља 41.7% од укупно пријављених лица); због кривичних дела из главе XXI КЗ (Кривична дела против имовине) против 37 лица[159] (што представља 11.1% од укупно пријављених лица); због кривичних дела из главе XXXI КЗ (Кривична дела против јавног реда и мира) против 30 лица[160] (што представља 9% од укупно пријављених лица); због кривичних дела из главе XVIII КЗ (Кривична дела против полне слободе) против 23 лица[161] (што представља 6.9% од укупно пријављених лица). У току ***2013.*** године, поднете су кривичне пријаве против 185 познатих учинилаца, при чему је кривична пријава поднета због кривичних дела *против безбедности рачунарских података* против 15 лица[162], што представља *свега 8.1%* од броја лица против којих је поднета кривична пријава, док је у *81.9% случајева* кривична пријава поднета *због кривичних дела из других глава Кривичног законика.* При томе против познатих учинилаца у значајнијем броју поднете су кривичне пријаве због кривичних дела из следећих глава КЗ[163]: због кривичних дела из главе XIV

представља 0.6% од укупно пријављених лица; због кривичних дела из главе XXX КЗ (Кривична дела против правосуђа) против 1 лица (и то због кривичног дела Повреда тајности поступка из чл. 337 КЗ), што представља 0.3% од укупно пријављених лица.

[158] Кривичне пријаве су поднете због кривичног дела Злостављање и мучење из чл. 137 КЗ поднета је кривична пријава против 1 лица, због кривичног Угрожавање сигурности из чл. 138 КЗ против 125 лица, због кривичног дела Неовлашћено прислушкивање и снимање из чл. 143 против 1 лица, због кривично дела Неовлашћено објављивање и приказивање туђег списа, портрета и снимка из чл. 145 КЗ против 11 лица, због кривичног дела Повреда слободе говора и јавног иступања из чл. 148 КЗ против 1 лица.

[159] Кривичне пријаве су поднете због кривичног дела Превара из чл. 208 КЗ против 36 лица и због кривичног дела Прикривање из чл. 221 КЗ против 1 лица.

[160] Кривичне пријаве су поднете због кривичног дела Изазивање панике и нереда из чл. 343 КЗ против 11 лица, због кривичног дела Насилничко понашање из чл. 344 КЗ против 1 лица, због кривичног дела Неовлашћено организовање игара на срећу из чл. 352 КЗ против 3 лица и због кривичног дела Неовлашћено бављење одређеном делатношћу из чл. 353 КЗ против 15 лица.

[161] Кривичне пријаве су поднете због кривичног дела Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из чл. 185 КЗ против 21 лица и због кривичног дела Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из чл. 185б против 2 лица.

[162] Кривичне пријаве су поднете због кривичног Оштећење рачунарских података и програма из чл. 298 КЗ поднете су кривичне пријаве против 2 лица, због кривичног дела Рачунарска саботажа из чл. 299 КЗ против 2 лица, због кривичног дела Рачунарска превара из чл. 301 КЗ против 6 лица и због кривичног дела Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из чл. 302 КЗ против 5 лица.

[163] Кривичне пријаве су поднете и због кривичних дела из главе XXVIII КЗ (Кривична дела против уставног уређења и безбедности Републике Србије) против 4 лица (и то због кривичног дела Изазивање националне, расне и верске мржње и нетрпељивости из чл. 317 КЗ), што представља 2.2% од укупно пријављених лица; због кривичних дела из главе XXXIII КЗ (Кривична дела против службене дужности) против 2 лица (и то због кривичног Давање мита из чл. 368 КЗ), што представља 1.1% од укупно пријављених лица; због кривичних дела из главе XVII КЗ (Кривична дела против части и угледа) против 1 лица (и то због кривичног дела Повреда угледа због расне,

(Кривична дела против слобода и права човека и грађанина) против 66 лица[164] (што представља 35.7% од укупно пријављених лица); због кривичних дела против имовине из главе 21. КЗ против 21 лица (што представља 11.4% од укупно пријављених лица); због кривичних дела против јавног реда и мира из главе 31. КЗ против 21 лица (што представља 11.4% од укупно пријављених лица); због кривичних дела из главе XX КЗ (Кривична дела против интелектуалне својине) против 19 лица[165], што представља 10.3% од укупно пријављених лица; због кривичних дела против привреде из главе 22. КЗ против 17 лица[166] (што представља 9.2% од укупно пријављених лица) због кривичних дела из главе XVIII КЗ (Кривична дела против полне слободе) против 16 лица[167] (што представља 8.5% од укупно пријављених лица). У току ***2012***. године у уписнику познатих учинилаца заведено је 114 предмета, а поднете су кривичне пријаве против 140 познатих пунолетних учинилаца, при чему је кривична пријава поднета због кривичних дела *против безбедности рачунарских* података против 28 лица[168], што представља *20%* од броја лица против којих је поднета кривична пријава. Од кривичних пријава које су поднете Тужилаштву од укупног броја пријављених лица чак њих *80% пријављено је због кривичних дела из других глава* Кривичног законика, при чему су против лица у значајнијем броју поднете кривичне пријаве због кривичних дела из следећих глава КЗ[169]: због кривичних

верске, националне или друге припадности из чл. 174 КЗ) што представља 0.5% од укупно пријављених лица; због кривичних дела из главе XXX КЗ (Кривична дела против правосуђа) против 1 лица (и то због кривичног дела Спречавање и ометање доказивања из чл. 336 КЗ), што представља 0.5% од укупно пријављених лица; због кривичних дела против правног саобраћаја из главе XXII КЗ против 1 лица, што представља 0.5% од укупно пријављених лица); због кривичних дела из главе XXXIV КЗ (Кривична дела против човечности и других добара заштићених међународним правом) против 1 лица (и то због кривичног дела Међународни тероризам из чл. 391 КЗ), што представља 0.5% од укупно пријављених лица.

[164] Од чега је кривична пријава поднета због кривичног дела Угрожавање сигурности из чл. 138 КЗ против чак 62 лица.

[165] Кривичне пријаве су поднете због кривичног дела Неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199 КЗ.

[166] Од чега је кривична пријава поднета због кривичног дела Фалсификовање и злоупотреба платних картица из чл. 225 КЗ против 9 лица.

[167] Кривичне пријаве су поднете због кривичног дела Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из чл. 185 КЗ.

[168] Кривичне пријаве су поднете због кривичног дела рачунарска саботажа из чл. 299. КЗ против 2 лица, због кривичног дела прављење и уношење рачунарских вируса из чл. 300 КЗ против 1 лица, због кривичног дела рачунарска превара из чл. 301. КЗ против 17 лица, због кривичног дела неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из чл. 302. КЗ против 8 лица.

[169] Кривичне пријаве су поднете и због кривичних дела против привреде из главе XXII КЗ против 7 лица (што представља 5% од укупно пријављених лица); у вези кривичних дела против имовине из

дела из главе XVIII КЗ (Кривична дела против полне слободе) против 44 лица[170] (што представља 31.4% од укупно пријављених лица); због кривичних дела из главе XIV (Кривична дела против слобода и права човека и грађанина) против 34 лица[171] (што представља 24.3% од укупно пријављених лица); због кривичних дела из главе XX КЗ (Кривична дела против интелектуалне својине) против 24 лица[172] (што представља 17.1% од укупно пријављених лица); због кривичних дела против јавног реда и мира из главе XXXI КЗ против 20 лица (што представља 14.3% од укупно пријављених лица). У току ***2011.*** године, у уписнику познатих учинилаца заведено 130 предмета, а поднете су кривичне пријаве против 153 позната пунолетна учиниоца, при чему је кривична пријава поднета због кривичних дела *против безбедности рачунарских података* против 29 лица[173], што представља скоро *19%* од броја лица против којих је поднета кривична пријава, док је у скоро *81% случајева* кривична пријава поднета *због кривичних дела из других глава* Кривичног законика. При томе, против познатих учинилаца у значајнијем броју поднете су кривичне пријаве због кривичних дела из следећих глава КЗ[174]: у вези кривичних дела из главе XXI (Кривична дела против привреде) против 47 лица[175] (што представља 30.7% од укупно пријављених лица); због кривичних дела из главе XVIII (Кривична дела против полне слободе) против 39 лица[176] (што представља 25.5% од укупно пријављених лица); због кривичних

главе XXI КЗ против 6 лица (што представља 4.3% од укупно пријављених лица), те због кривичних дела из главе XXVIII КЗ (Кривична дела против уставног уређења и безбедности Републике Србије) против 1 лица (што представља 0.7% од укупно пријављених лица).

[170] Кривичне пријаве су поднете због кривичног дела приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из чл. 185. КЗ против 20 лица и због кривичног дела неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199. КЗ против 24 лица.

[171] Кривичне пријаве су поднете због кривичног дела угрожавање сигурности из чл. 138. КЗ.

[172] Кривичне пријаве су поднете због кривичног дела неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199. КЗ

[173] Кривичне пријаве су поднете због кривичног дела оштећење рачунарских програма и података из чл. 298. КЗ против 1 лица, због кривичног дела рачунарска превара из чл. 301. КЗ против 21 лица и због кривичног дела неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података из чл. 302. КЗ против 7 лица.

[174] Кривичне пријаве су поднете и због кривичних дела против имовине из главе XXI против 3 лица (што представља 1.96% од укупно пријављених лица), те због кривичног дела фалсификовање исправе из чл. 355. КЗ против 3 лица (што представља 1.96% од укупно пријављених лица).

[175] Од чега је пријава поднета због кривичног дела Неовлашћено бављење одређеном делатношћу из чл. 353. КЗ против 46 лица.

[176] Кривичне пријаве су поднете због кривичног дела приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из чл. 185. КЗ

дела из главе XIV (Кривична дела против слобода и права човека и грађанина) против 21 лица[177] (што представља 13.7% од укупно пријављених лица); због кривичних дела из главе XX (Кривична дела против интелектуалне својине) против 11 лица[178] (што представља 7.2% од укупно пријављених лица).

Из приказаних података могу се извести одређени закључци:

1. У укупном броју кривичних пријава који се подносе против познатих учинилаца, у погледу кривичних дела поводом којих се кривичне пријаве подносе, процентуално учешће кривичних дела против безбедности рачунарских података не прелази 20%, односно кривичне пријаве се подносе претежно због кривичних дела из других глава Кривичног законика[179].

2. Кривичне пријаве су подношене и због кривичних дела из других глава КЗ, али су оне одбачене јер се односе на кривична дела која нису у надлежности

против 20 лица и због кривичног дела неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199. КЗ против 24 лица.

[177] Кривичне пријаве су поднете због кривичног дела угрожавање сигурности из чл. 138. КЗ.

[178] Кривичне пријаве су поднете због кривичног дела Неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199 КЗ.

[179] У погледу тих других кривичних дела, кривичне пријаве су током периода обухваћеног извештајем подношене због:

- кривичних дела *против интелектуалне својине* у просеку од 9.55%; при томе, у највећем броју случајева кривичне пријаве су подношене због кривичног дела Неовлашћено искоришћавање ауторског дела или предмета сродног права из чл. 199 КЗ;
- кривичних дела *против имовине* у просеку од 7.34%; при томе, може се уочити драстичан пораст заступљености ове групе кривичних дела од 1.96% у 2011. до 11.1% у 2014. години;
- кривичних дела *против привреде* у просеку од 26.7%; ипак, треба приметити да је на почетку извештаваног периода тај проценат износио 30.7% (јер су биле поднете кривичне пријаве против 46 лица због кривичног дела Неовлашћено бављење одређеном делатношћу из чл. 353. КЗ) али се у наредном периоду смањио и просечно износи 6%; може се такође уочити да се повећава разноликост у погледу кривичних дела из ове групе због којих се подносе кривичне пријаве; кривичних дела *против правног саобраћаја* у просеку мањем од 1%, и због кривичног дела Фалсификовање исправе у 2011. и 2013. години;
- кривичних дела *против слобода и права човека и грађанина* у просеку од 28.8%; може се уочити тенденција сталног пораста заступљености од заступљености у проценту од 13.7% у 2011. години до чак 41.7% у 2014. години; при томе, кривичне пријаве су у највећем броју случајева подношене због кривичног дела Угрожавање сигурности из чл. 138 КЗ;
- кривичних дела *против полне слободе* у просеку 18%, при чему се може уочити пад просечне заступљености са 28.5% у прве две године на 7.7% у току последње две године ; при томе, кривичне пријаве су у највећем броју случајева подношене само због два кривичног дела: Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из чл. 185 КЗ и Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу из чл. 185б;
- кривичних дела *против јавног реда и мира* у просеку од 11.6%; при томе, кривичне пријаве су у највећем броју случајева подношене због кривичног дела, при томе, ниједна кривична пријава није поднета због ових кривичних дела током 2011. године, а касније кривичне пријаве поднете су због разноврсних кривичних дела;

Тужилаштва у смислу Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала[180].

Може се поставити питање, *да ли подаци државних органа о ниској стопи заступљености високотехнолошког криминала у укупном броју кривичних дела указују на одсуство доказа о постојању или, пак, представљају доказ о непостојању високотехнолошког криминалу*? При томе, приликом разматрања статистичких података који потичу из извештаја суда, тужилаштва и полиције треба имати у виду да постоји велика тамна бројка извршених, а непријављених кривичних дела. *Може се поставити питање* да ли схватање високотехнолошког криминала као јасне и постојеће опасности од стране стручне јавности које се презентује општој јавности *служи да оправда активирање механизама за сузбијање злоупотреба информационих технологија, пре свега кроз прописивање интрузиваних овлашћења надлежних државних органа*[181], с обзиром на то да се поменути извештаји наводе и у документима у којим се истиче потреба за увођењем ефикаснијих мера за сузбијање високотехнолошког криминала, између осталог и у извештајима Савета Европе и Европске уније[182].

Оваква диспропорција података о обиму високотехнолошког криминала се може објаснити на три начина. Проблем високотехнолошког криминала предимензиониран је кроз извештаје медија о појединим драматичним случајевима а то погодује индустрији информационе безбедности, као и потреби

---

[180] Ради се о кривичним делима из групе кривичних дела *против части и угледа* (и то, због кривичног дела Увреда из чл. 170 КЗ и Повреда угледа због расне, верске, националне или друге припадности из чл. 174 КЗ), против *правосуђа* (и то због кривичног дела Повреда тајности поступка из чл. 337 КЗ); против *службене дужности* (и то, због кривичног дела Злоупотреба службеног положаја из чл. 359 КЗ и Давање мита из чл. 368 КЗ против 1 лица), те *против човечности и других добара заштићених међународним правом* (и то, због кривичног дела Расна и друга дискриминација из чл. 387 КЗ, те Међународни тероризам из чл. 391 КЗ).

[181] Појава да приватне компаније из области рачунарске безбедности драматизују извештаје о стању кибер криминала и тактички изазивају и шире страх, несигурност и сумњу назива се „трговина страхом“ (тзв. *FUDmongering* од *Fear Uncertainty Doubt).* Wall, *Cybercrime:The Transformation of Crime in the Information Age*, 9.

[182] Cybercrime: current threats and trends, *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp;* Cybercrime: where we are and where could go (Food for thought), *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Update/cyber_octopus_PS_alexander_mosaic1e.pdf;* European Union: Council conclusions on a concerted work strategy and practical measures against cybercrime, *http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf*); Proposed Cybercrime Prevention Act Hand Out, *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/if2008replist_en.asp;*

да се кроз подржавање културе страха[183] обезбеди легитимитет појачане контроле од стране државе. Друго објашњење односи се на недовољну *post-hoc* способност надлежних органа да реагују на глобализоване виртуелне проблеме високотехнолошког криминала[184], док се треће своди на проблем неразумевања високотехнолошког криминала. Иако сматрамо да је стање предимензионирано, неспорно је да опасност од високотехнолошког криминала постоји[185]. Штета коју поједина кривична дела обухваћена појмом овог криминала причињавају појединим оштећеним лицима посматрано у извештајима надлежних органа појединих држава можда и указују да је занемарљива у смислу заступљености у свеукупном броју кривичних дела у тој држави. Али, опасност од високотехнолошког криминала се налази у његовом „минималистичком захвату" на глобалном нивоу (*de minimism*[186]): велики број оштећених лица који се налазе на територији више држава трпи занемарљиву штету радњом извршења али учинилац ипак остварује велику имовинску корист. Примера ради, да би противправно одузео милион еура, извршилац не одузима ту своту новца са рачуна једног лица, него од милион лица која се налазе у различитим државама узима по један еуро, полазећи од претпоставке да ако много оштећених трпи „малу" штету, мала је вероватноћа да ће оштећени, ако и примете штету, исту пријавити, а тиме је мало вероватно и да ће надлежни органи повезати случајеве проузроковане једном радњом извршења (тзв. *salami technique*[187]). Стога је за супротстављање овом облику криминала потребно, ***реално сагледавајући бројне специфичне изазове*** који поставља пред надлежне органе откривања и доказивања и узимајући их у обзир, ***предвидети одговарајуће механизме реаговања***.

[183] У делима социолога се култура страха помиње као врста идеолошког „страха од страха" који води претераној бојазни јавности од криминала, без обзира да ли ризик реално постоји, при чему државе тактички користе и свесно подстичу тај страх од криминала да би контролисале широк спектар ризика. Више о томе, S. Furedi, *Culture of fear*, Continuum, London 2002, 12, 73; D. Garland, *The culture of control*, Oxford University Press, Oxford 2001, 141.

[184] D. Wall, „Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime", *International Review of Law Computers & Technology* 1-2/2008, 46.

[185] Постоји мишљење против покушаја да се квантификује високотехнолошки криминал јер се ради о парадигми која не представља реалан ризик. Више о томе, M. McGuire, *Hyper-crime: the New Geometry of Harm*, Abingdon, Oxford 2007, 15-20.

[186] Wall, *Cybercrime:The Transformation of Crime in the Information Age*, 3.

[187] Wall, *op.cit*, 40.

Други део

ОСНОВНИ ИЗАЗОВИ И ПРЕТПОСТАВКЕ ЗА ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Изазови откривања и обезбеђивања доказа за потребе кривичног поступка за кривична дела код којих су рачунарски подаци, рачунарски системи или рачунарске мреже средство извршења или објект напада произлазе из карактеристика коришћених информационих технологија. Наиме, одређене специфичности кибер простора, као инфраструктуре транснационалне природе, која обухвата Интернет, телекомуникационе мреже и рачунарске системе[188], представљају погодност за учиниоце кривичних дела у смислу извршења радње и прикривања трагова кривичног дела, али истовремено и озбиљну препреку за надлежне органе откривања кривичних дела и гоњења учинилаца. Могуће је предочити неколико фактора који су допринели томе да је Интернет као децентрализована мрежна структура омогућио развој високотехнолошког криминала. Кибер простор није фиксно, детерминисано окружење, него принципе и динамику аутономно контролишу и мењају корисници информационих технологија[189]. Дигитализација садржаја, анонимност, међуповезаност, децентрализација и међузависност су препознати као карактеристике Интернета[190] које су омогућиле извршиоцима интеракцију на даљину са објектом напада[191], односно приступ великом броју повезаних рачунара и корисника који се налазе било где у свету, без потребе да напусте просторију у којој се рачунар преко ког остварују конекцију налази. Тако је уношењем једног софтвера у рачунарску мрежу који се сам умножава (вирус) могуће у исто време покренути аутоматизован напад према великом броју информационих система који се налазе на различитим местима. При томе, извршилац може употребом разних техника за прикривање идентитета или трагова који воде до рачунара који користи (нпр.

[188] A. Aldesco, „The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime“, *Loyola of Los Angeles Entertainment Law Review* 1/2002, 99.
[189] S. Brenner, B. Koops, „Approaches to cybercrime jurisdiction“, *Journal of High Technology Law* 1/2004, 3.
[190] A. Sofaer, S. Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution Press, Stanford 2001, 7.
[191] B. Koops, „The Internet and its Opportunities for Cybercrime“, Tilburg Law School Legal Studies Research Paper Series 9/2011, 738-739.

употребом *online* бесплатних софтвера за измену и/или анонимизирање *IP* адресе[192]), као и садржаја комуникација које остварује (нпр. енкрипцијом[193]), да постане „невидљив, недоступан и много теже му се може ући у траг него извршиоцима у физичком свету“[194]. Осим тога, како је Интернет структуиран као отворена мрежна инфраструктура заснована на дигитализованом представљању података, извршилац може да, уз мале трошкове манипулише подацима, без умањења њиховог квалитета, као и да их мења без видљивих трагова[195]. Комбинација поменутих карактеристика Интернета и савремених информационих технологија условила је *транснационалну и динамичну природу високотехношког криминала* што представља основни изазов у супротстављању овом облику криминала.

Као најзначајнији изазови у вези са откривањем дела високотехнолошког криминала са којима се суочава полиција у Србији могу се навести следећи: неусклађеност правне регулативе са савременим облицима извршења кривичних дела; недовољна техничка опремљеност и оспособљеност полицијских службеника везана за откривање извршилаца у *online* окружењу; недостатак операционалних обука које би омогућиле да полицијски службеници који се баве спречавањем високотехнолошког криминала буду довољно обучени и технички опремљени за вршење ових задатака; потешкоће у откривању извршилаца кривичних дела који користе лажне идентитете у *online* окружењу, посебно када се у обзир узме чињеница да је у великом броју случајева међународна полицијска сарадња лоша, а да у некима чак и не постоји; потешкоће у откривању тачне локације извршења кривичног дела, пошто се ова кривична дела врше са многих места широм света, а у великом броју случајева извршиоци кривичних дела користе мреже са јавним приступом[196].

---

[192] Видети на пример: http://online-anonymizer.com/. Ови програми извршиоцима омогућавају анонимно слање електронских порука, без остављања трага о правој *IP* адреси извршиоца кривичног дела, на тај начин што се целокупан Интернет саобраћај према одређеним Интернет адресама и страницама остварује преко сервиса који, потом, као траг оставља своју *IP* адресу, а адреса правог корисника се налази на серверу ових сервиса.

[193] Видети на пример: http://www.encryptedcommunications.com/.

[194] N.K. Katyal, „Criminal Law in Cyberspace“, *University of Pennsylvania Law Review* 4/2001, 1042.

[195] A. Kamal, *The Law of Cyber-Space: An Invitation to the Table of Negotiations*, United Nations Institute for Training and Research, New York 2005, 26.

[196] В. Урошевић, З. Ивановић, С. Уљанов, *Мач у World Wide Web-у: изазови високотехнолошког криминала*, *Eternal mix*, Београд 2012, 105-106.

Неспорно је да је за стварање правног оквира, адекватног за супротстављање делима високотехнолошког криминала, потребно одредбе кривичног процесног права, које се односе на откривање и доказивање ових кривичних дела, прилагодити поменутим специфичностима окружења у ком се радње извршења предузимају[197]. Операције у оквиру рачунарских система и мрежа карактерише одређена непостојаност и брз проток података који веома лако, брзо и бесповратно могу бити измењени, прикривени или избрисани, па је за спровођење радњи ради проналажења и обезбеђења доказа потребно да надлежни органи гоњења имају посебна овлашћења. Међутим, стварна, ефективна примена тих овлашћења на основу одговарајућих процесних одредаба *захтева претходно испуњење две претпоставке* које проистичу из основних карактеристика високотехнолошког криминала, а које се односе на *могућност* и *способност* надлежних органа да поступе по прописаним овлашћењима. Наиме, *транснационална природа* кибер простора *условљава решавање питања надлежности* за предузимање радњи откривања, а *оспособљеност надлежних органа* за *суочавање са динамичном технолошком компонентом* овог облика криминала представља неопходан елемент њиховог ефикасног реаговања.

Дакле, осим што се прописивањем овлашћења постави правни оквир за супротстављање, претходно питање је да ли надлежни органи могу (надлежност) и да ли умеју (оспособљеност/специјализација) да предузму потребне радње за откривање и доказивање дела високотехнолошког криминала.

1. НАДЛЕЖНОСТ ЗА ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

У складу са принципом једнакости суверенитета држава утврђених у чл. 2. Повеље Уједињених нација, надлежност државе је ограничена на њену територију и становништво[198], што значи да држава има право да врши власт тако што: а) суверено уређује унутрашње односе прописивањем правних норми, б) у судским и поступцима пред другим државним органима утврђује одговорност адресата

[197] Радње надлежних органа које се предузимају ради откривања и доказивања дела високотехнолошког криминала предмет су Трећег дела рада.
[198] *Charter of United Nations*, http://www.un.org/en/documents/charter/ .

правних норми за непоступање по истим, и в) примењују правне норме и санкционише правне субјекте који не поступају у складу утврђеним правним нормама[199]. Осим што сопственим прописима уређује унутрашње односе (радње предузете на целој или делу њене територије, правни положај лица на њеној територији и заштиту својих и интереса њених држављана), може се поставити питање *да ли и у којим случајевима држава може* да ради заштите сопствених интереса и интереса њених држављана *прошири надлежност на радње које су предузете ван своје територије,* али које производе дејство у оквиру њених граница. С тим у вези је и питање *да ли и у ком обиму држава може да уређује односе у кибер простору* (који формирају Интернет као својеврсна рачунарска мрежа на глобалном нивоу и са њим повезане информационе технологије) а који превазилази границе суверених држава[200].

Да би се пронашао одговор на питање да ли се поменута правила могу применити и на кривична дела чије радње се предузете у кибер простору, односно да ли Интернет и глобализација употребе информационих технологија представљају праве концептуалне изазове по територијални суверенитет држава, потребно је сагледати онтолошке карактеристике кибер простора.

1.1. Важење права у кибер простору

Кибер простор као глобални медијум за комуникацију је рачунарска мрежа појединачних рачунарских мрежа за електронску комуникацију (међусобно повезаних усвајањем одређених протокола чиме је омогућен пренос информација) и као *такав, нема физичке оквире, већ представља виртуелно окружење* у ком не постоји централизовано управљање, него функционише на логичким, а не на географским принципима[201]. Ипак, виртуелном окружењу кибер простора се приступа преко рачунарског хардвера, који је лоциран у физичком свету, и

[199] Разликују се три елемента надлежности суверене државе: „*jurisdiction to prescribe*“, „*jurisdiction to adjudicate*“ и „*jurisdiction to enforce*“. Више о томе, S. Brenner, “Cybercrime jurisdiction”, *Crime, Law and Social Change* 46/2006, 189–206.

[200] G. Quirchmayr, „Internet, WWW and beyond“, *Information Technology and Lawyers* 1/2006, 140. Исто: D. Hunter, „Cyberspace as place and the Tragedy of the Digital Anticommons“, *California Law Review* 2/2003, 440.

[201] T. Berg, „The Impact of the Internet on state power to enforce the law“, *Brigham Young University Law Review* 4/2000, 1310.

софтвера који виртуелни свет трансформише у реалан свет видљив корисницима[202], у оквиру ког се могу разликовати операције које немају никакав ефекат на физички свет и које то имају. Од мишљења да прописи територијално суверених држава нису подесни да уређују Интернет (с обзиром на аутономност и децентрализованост мреже[203]), преко става да је потребно стварање регулаторног механизма ради спречавања штетних активности корисника[204] и заштите „кибер-слобода"[205], те да активности у оквиру кибер простора треба да буду предмет регулисања у прописима свих држава на чијој територији електронске комуникације могу произвести одређене ефекте[206], *уређење односа у кибер простору и управљање Интернетом је актуелно питање у научној литератури*[207]. Полазећи од максиме „код је закон" (*code is law*)[208] професора Лесига, најутицајнијег теоретичара кибер права (*cyber law*), основна идеја ових проучавања је разматрање на који начин право које стварају државе и правила рачунарског кода могу заједнички регулисати виртуелни свет кибер простора[209]. У том смислу, више субјеката уређују активности на Интернету: корисници[210] и

[202] C. Atchison, „Emerging Styles of Social Control on Internet: Justice denied", *Humanities, Social Sciences and Law, Critical Criminology* 1-2/2000, 88.

[203] У Декларацији о независности кибер простора (*A Declaration of the Independence of Cyberspace*) усвојеној 1996. године било је наведено да кибер простор представља потпуно одвојен свет од физичког света (и територијалних оквира државе) и да интервенције државе нису добродошле, јер оне немају надлежност у овом окружењу. Многи од креатора Интернета су веровали да се глобалном мрежом може управљати неформално кроз консензус између инжењера информационе технологије, пре него правилима које би наметала држава. Наведено према: O. Kerr, „Enforcing Law Online", *The University of Chicago Law review* 2/2007, 746.

[204] M. Williams, „Policing and Cybersociety: The Maturation of Regulation within an Online Community", *Policing & Society* 1/ 2007, 71.

[205] N. Strossen, „Cybercrime v. Cyberliberties", *International journal of Law, Computers and Technology* 1/2000, 15-16; Упор. D. Wall, „Introduction to Cybercrime, Cyberspeech and Cyberliberties", *International journal of Law, Computers and Technology* 1/2000, 6.

[206] G. Zekos, „State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction", *International Journal of Law and Information Technology* 1/2005, 4.

[207] О томе више, R. Spinello , *Regulating Cyberspace: The Policies and Technologies of Control*, Praeger ,Westport 2002, 15-18; S. Drucker, Gumpert G., *Real law @ virtual space : communication regulation in cyberspace*, Cresskill, NJ: Hampton Press, Hampton 2005; M.L. Mueller, *Networks and States: the Global Politics of Internet Governance*, MIT Press, Cambridge 2010, 127-159; C.T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge 2011, 46-48;

[208] L. Lessig, Code and Other Laws Of Cyberspace, 1999. Наведено према: T. Schulz, „Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", *The European Journal of International Law* 4/2008, 805.

[209] Право Интернета као нова правна дисциплина проучава међузависност и међутицаје правила Кода, тржишта и регулативе државе. Више о томе, Rustad, *op.cit*, 27-49.

[210] Више о томе, M. Rustad, „Private Enforcement Of Cybercrime on the Electronic Frontier", *Southern California Interdisciplinary Law Journal* 11/2001, 68; M. Shah, „The Case for a Statutory Suppression

пружаоци услуга мрежне структуре (преко улова коришћења услуга као саставног дела уговора са корисницима)[211], одељења за информациону безбедност компанија, невладине организације (као нпр. *Internet Watch Foundation: IWF*) и држава[212].

Регулисање односа у кибер простору од стране државе се огледа у доношењу више врста прописа из разних грана права, али је за предмет рада релевантно питање реаговања на штетне и недозвољене активности. Осим надлежности државе да репресивно делује поводом кривичних дела у кибер простору, постоји тенденција државне контроле активности на Интернету која се правда превенцијом безбедносних ризика, међу којима у политичкој агенди држава на глобалном нивоу нарочито истиче високотехнолошки криминал[213]. При томе, постоји бојазан да би „борба" против високотехнолошког криминала могла еродирати концепт отворености на ком се Интернет заснива и угрозити права и слободе у кибер простору[214].

Без обзира на изнете ставове, потребно је имати на уму да конфигурација Интернета ствара два сета околности: један заснован на физичкој а други на виртуелној реалности, па се може уочити тзв. проблем перспективе (*problem of perspective*[215]). Да би се право применило на чињенице, потребно је водити рачуна да ли се чињенице посматрају: а) из перспективе физичке стварности – Интернет се посматра као мрежа рачунара који су лоцирани у различитим деловима света

Remedy to Regulate Illegal Private Party Searches in Cyberspace", *Columbia Law Review* 1/2005, 250-278.

[211] Више томе вид: S. Stalla-Bourdillon, „Chilling ISPs. when private regulators act without adequate public framework", *Computer Law and security Review* 26/2010, 294; S. Stalla-Bourdillon, „The flip side of ISP's liability regimes: The ambiguous protection of fundamental rights and liberties in private digital spaces", Computer Law & Security Review 5/2010, 499; Y. Akdeniz, „New Privacy Concerns: ISPs, Crime Prevention and Consumers' Rights," *Journal of Law, Computers and Technology* 1/2001, 55-61.

[212] D. Wall, „Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace", *Police Practice and Research* 2/2007, 189. Упор. Bryant, Bryan, *op.cit*, 84-89.

[213] A. Zavrsnik, „Towards an overregulated cyberspace: criminal law perspective", *Masaryk University Law and Technology journal* 2/2010, 174. О еволуцији развоја контроле државе над Интернетом види W. Murdoch, "The Evolution of Legal Regulation of the Internet to Address Terrorism and Other Crimes", *The Journal of South African Law* 1/2007, 495.

[214] О ризику да државна контрола активности на Интернету угрози основне вредности савременог друштва види P. De Filippi, L. Belli, „Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation", *European Journal for Law and Technology* 2/2012, 14. Осим потребе заштите гарантованих људских права и у кибер простору, указали бисмо на зачетак „новог" људског права у вези са виртуелним окружењем, а то је право на приступ Интернету. Види P. De Hert, D. Kloza, „Internet (access) as a new fundamental right. Inflating the current rights framework?", *European Journal of Law and Technology* 3/2012, 5.

[215]. O. Kerr, „ The problem of perspective in Internet Law, Georgetown Law Journal 2/2003, 359.

преко хардвера који шаље, складишти и прима комуникације употребом стандардних протокола, а који се налази на територији државе (екстерна перспектива), или б) из перспективе Интернета - Интернет представља државним границама неомеђен простор у ком постоји могућност прикривања стварне локације, као и локације рачунара изменом *IP* адреса и слично (интерна перспектива). Посматрајући Интернет из интерне перспективе, појединци заиста комуницирају у оквиру виртуелног кибер простора, али споља гледано (екстерна перспектива) они се увек налазе на територији неке државе, јер „нису електронска бића која постоје у електронском окружењу“ [216]. *У том смислу кибер простор није одвојен од реалног света, не може се посматрати одвојено од територијалног суверенитета држава и стога не постоји потреба за стварањем неких посебних принципа за утврђивање надлежности, те регулисање активности корисника*.

1.2. Проблеми у вези са надлежношћу за дела високотехнолошког криминала

Да би се разумео проблем у вези са надлежношћу за дела високотехнолошког криминала, потребно је направити разлику између „локалних“ и „транснационалних“ кривичних дела[217]. У случају „локалних“ кривичних дела, учинилац употребом рачунара врши напад на рачунар који се налази на територији исте државе, па се ова ситуација од радњи „традиционалних“ кривичних дела разликује само по томе што је кибер простор искоришћен као окружење за извршење радње. Примера ради, извршилац кршећи мере заштите неовлашћено приступи рачунару који се налази у истој држави. Другу групу чине кривична дела са прекограничном димензијом у којој се извршилац и оштећени и/или рачунарски систем који је објект/средство напада налазе на територији различитих држава, односно код којих се место предузимања радње извршења и наступања последице налазе у различитим државама. Примера ради, извршилац у држави А искористи рачунар у држави Б да шаље мејлове који су инфицирани рачунарским вирусом на аутоматски генерисане адресе електронске поште

[216] C. Atchison, „The Internet and the State: Instrument of Social Control or Subversive Technology“, *Humanities, Social Sciences and Law, Critical Criminology* 1-2/2000, 167.
[217] S. Brenner, J. Schwerha, “Introduction—Cybercrime: A Note on International Issues”, *Information Systems Frontiers* 2/2004, 112.

лицима која се налазе на територији држава В и Г ради прикупљања лозинки за приступ, помоћу којих врши трансфер новца за банкарских рачуна оштећених лица на рачун који је отворен у држави Д. У вези са наведеним примером, јасно је колико је важно, а изузетно сложено питање одређивања надлежности државе да инкриминише одређене радње предузете у оквиру кибер простора и санкционише учиниоце тих радњи применом одредаба домаћег кривичног права, а ради откривања и доказивања дела.

Међу компонентама државног суверенитета су репресивна власт државе (у виду овлашћења државе да одређено антидруштвено понашање инкриминише као кривично дело и на исто реагује кривичном санкцијом) и јурисдикација (у смислу овлашћења судова једне државе да примењујући домаће законе реше одређену кривичну ствар)[218]. У погледу кривичног права, питање кривично законодавство које државе се примењује у конкретном случају *решава се правилима просторног важења кривичног законодавства,* што зависи од начина одређивања шта се подразумева под *местом извршења кривичног дела*. Утврђивање места је од нарочитог значаја код кривичних дела код којих је радња извршења предузета на једном месту, а последица наступила на другом месту (дистанциона кривична дела), каква су у великом броју случајева дела високотехнолошког криминала. Постоје три приступа у решавања питања шта се сматра под местом извршења кривичног дела: теорија делатности (релевантно је место извршења радње кривичног дела), теорија последице (релевантно је место наступања последица) и теорија јединства, односно убиквитета (местом извршења сматра се и место извршења радње кривичног дела и место наступања последица)[219]. Прихватање последњег приступа има за последицу да се у конкретном случајеву више места може сматрати местом извршења кривичног дела – уколико је више аката који чине радњу извршења предузето на различитим местима или је, пак, последица наступила на неколико различитих места. Овај проблем се може јавити наричито код дистанционих кривичних дела, код којих је радња предузета у једном месту, а последица је наступила на другом месту. Решавање овог питања је од посебног

[218] Д. Радуловић, *Кривично процесно право*, Подгорица 2002, 53.

[219] У Кривичном законику РС прихваћена је теорија убиквитета, па се као место извршења кривичног дела сматра како оно место где је предузета (или пропуштена) радња, тако и место где је у целини или делимично последица наступила (члан 17. став 1).

значаја код дистанционих кривичних дела учињених путем Интернета, па чак и у погледу делатностих кривичних дела (уколико се радњом кривичног дела учињених на тај начин обухвате и радње које у једном техничком смислу чине целину)[220].

Кривично процесно право нема универзалну вредност и не важи неограничено, него има своју примену и важи у одређеном времену на одређеној територији у односу на одређена лица и у погледу одређених предмета[221]. Овакво право вршења власти се *традиционално везује за територију омеђену утврђеним границама државе* у оквиру које држава суверено предвиђа кривична дела и санкције за та дела, води кривични поступак против лица ради утврђивања да ли су учинила кривично дело и изриче кривичне санкције утврђене прописима кривичног права[222]. Отуда држава, по правилу, не може да прописује и примењује правне норме кривичног материјалног и процесног права на радње које су извршене на територији друге суверене државе. За просторно важење у основи важи *територијални принцип*, што подразумева да се у кривичним поступцима који се воде на територије једне државе примењује домаће кривично процесно право, без обзира на то ко је учинилац кривичног дела (домаћи држављанин, странац или лице без држављанства), где је дело учињено (на домаћој територији или у иностранству) и према коме је учињено[223]. Примена овог принципа подразумева, такође, да се у поступку пред домаћим судовима не могу примењивати страни прописи нити да страни органи могу предузимати кривичнопроцесне радње на домаћој територији[224].

---

[220] З. Стојановић, *Кривично право, Опште део,* двадесет друго издање, Београд 2015, 226.

[221] *Ibidem.*

[222] Поступци за утврђивање одговорности за непоступање по прописима једне државе могу се водити само против лица које је присутно, односно има пребивалиште или боравиште или обавља пословне активности на територији државе, а у погледу радњи предузетих ван територије државе само уколико је лице држављанин, или је радња има значајан, директан ефекат у оквиру граница државе.

[223] Наиме, свака држава тежи да њено законодавство буде примењено уколико за то постоје одређени интереси, а тај интерес постоји не само када је кривично дело извршено на *територији* државе, него и када је дело извршено у иностранству а учинилац је *њен држављанин* или дело учињено *против њених интереса и њених држављана*, док у одређеним случајевима постоји *општи интерес* свих држава да извршиоци одређених кривичних дела не избегну кривичну санкцију.

[224] Оваква примена кривичнопроцесног закона произлази из принципа државног суверенитета, према ком државна власт на својој територији не може бити ограничавана законима и актима других држава. Искључива примена домаћег кривичног процесног права је обавезна, не само у

Дакле, за примену територијалног принципа важно питање је одређивање шта се под *државном територијом* уопште сматра. Државна територија се може схватити као простор одређен државним границама, а чине га део површине земље и одговарајући појас мора (обално море), са припадајућим делом подземља и ваздушног простора изнад сувоземне и водене површине[225]. Од принципа територијалног важења кривичног процесног права могућа су одређена одступања, у смислу да се појам територије проширује или сужава и тада се говори о *екстериторијалном важењу права*[226], па се с тим у вези може поставити питање да ли територија државе обухвата и кибер простор.

Владајући став у литератури у почетним стадијумима развоја високотехнолошког криминала са специфичном прекограничном димензијом био је да је потребно развити нове/ додатне принципе за одређивање надлежности адекватне кибер простору[227], полазећи од тога да се ради о „супратериторијалном" електронском простору[228] независном од било које физичке локације[229], у потпуности одвојеном од реалног простора, у ком корисници рачунара и рачунарских мрежа комуницирају електронски и преко граница надлежности држава[230]. Међутим, *важење кривичноправних прописа* у односу на радње предузете у кибер простору по територијалном принципу *није ништа мање*

поступку по главној кривичној ствари, већ и за предузимање сваке друге процесне радње. Види, М. Грубач, *Кривично процесно право*, Београд 2011, 54.

[225] С. Бејатовић, *Кривично процесно право*, Београд 2014, 40.

[226] Случајеви проширења појма територије односе се, углавном, на домаће бродове без обзира на то где се налазе у време извршења кривичног дела, на цивилне ваздухоплове док су у лету а на домаће војне ваздухоплове без обзира где се налазио у време извршења кривичног дела. Осим проширења важења домаћег кривичног процесног права, постоје одређена места и објекти на која се не могу примењивати домаћи кривичнопросецни закони (види, Бејатовић, *op.cit*, 40). Дакле, изузетно, кривично процесно право једне државе или међународне организације може да се примењује на територији друге државе у следећим случајевима: а) уколико се државе споразумеју да се на територији једне државе кривично правосуђе применом свог права врши друга држава у погледу својих грађана који се ту налазе; б) у случају окупације; в) на основу међународних прописа се домаће кривично процесно законодавство не примењује на делове домаће територије на којим се налазе просторије одређених дипломатских установа; г) домаће кривично процесно законодавтсво не примењује на ратне бродове и ратне ваздухоплове стране државе кад се по дозволи власти друге државе нађу на њеној територији (Грубач, *op.cit*, 2011, 55. Упореди: Бејатовић, *op.cit*, 40).

[227] H. Kaspersen, Cybercrime and jurisdiction, 2009, *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/IF_2009_presentations/default_en.asp*, 4.

[228] Zekos, *op.cit*, 2-3.

[229] M. Brand, „Internet and the Law: An Article Examining the Problems and Questions Concerning the Regulation of Cyberspace", *Tilburg Foreign Law Review* 3/2002, 262.

[230] Brenner, Koops, *op.cit*, 36.

легитимно, него уређење односа у физичком свету, јер се приступ овом простору остварује преко уређаја који се налазе у оквиру територијалних граница државе[231], а *потребно је* из разлога да учиниоци не би избегли одговорност за радње извршене у неомеђеном виртуелном простору[232]. Но, питање је, како применити територијални принцип на радње у кибер простору, с обзиром на то да се локација у виртуелном простору односи се на виртуелну адресу рачунарских система између којих се остварује комуникација[233] а која може бити независна од физичке локације уређаја, тако да не постоји веза између *IP* адресе и надлежности државе на којој је физички лоциран рачунар[234].

У том смислу, у складу са територијалним принципом, држава је надлежна да уређује радње везане за злоупотребу информационих технологија на њеној територија, а своју надлежност заснива над радњама у кибер простору уколико се у оквиру њених граница налази место извршења кривичног дела и/или место на ком се наступила последица или место боравишта извршиоца или оштећеног лица чији рачунар је објект напада или се територијална надлежност повезује са свим овим околностима[235].

Залагање за примену територијалног принципа у погледу кривичних дела са транснационалном димензијом (чије радње извршења су предузете у кибер простору) потврђена је и *Конвенцији о високотехнолошком криминалу*. Наиме, у члану 22. Конвенција предвиђа два основа за успостављање надлежности државе, и то су територија (као примарни основ) и држављанство учиниоца дела (као секундарни основ). Истовремено, Конвенција не ограничава државу да у складу са националним законодавством предвиди додатне основе. Тако држава заснива надлежност за регулисање дела високотехнолошког криминала предвиђених Конвенцијом, *уколико је место извршења кривичног дела на њеној територији.* При томе се под *територијом* сматра и брод под заставом државе, као и ваздухоплов регистрован у складу са прописима те државе. У погледу *места*

[231] D. Koepsell, "An emerging ontology of jurisdiction in cyberspace", *Ethics and Information Technology* 2/2000, 101.
[232] J. Goldsmith, „The Internet and the Abiding Significance of Territorial Sovereignty", Indiana Journal of Global legal studies 2/1998, 475.
[233] R. Wittzack, „Principles of International Internet Law*", German Law Journal* 11/2010, 1245-1263.
[234] L. Lessig, , "The Path of Cyberlaw", *The Yale Law Journal* 7/1995, 1747.
[235] Више о томе, K. Darell, *Issues in Internet Law: Society, Technology, and the Law*, Amber Book Company, London 2013, 6-11.

извршења кривичног дела, Конвенција прихвата теорију убиквитета и проширује *locus delicti*, тако да државе имају надлежност и уколико се рачунарски систем који је објект напада (на ком су наступиле последице) налази у оквиру њених граница, али не и извршилац[236]. У случају да је дело извршено ван територије државе, њена надлежност се може засновати и уколико је извршилац њен држављанин, под условом да је дело кажњиво и по кривичном закону земље где је извршено (дакле, не и уколико је дело извршио странац у иностранству). Осим тога, држава може бити надлежна и уколико њен држављанин изврши кривично дело на месту изван територијалне надлежности било које државе[237].

У *кривичном законодавству Србије* основни принцип за одређивање просторног важења кривичног материјалног законодавства је територијални принцип (постоје и супсидијарни принципи, и то реални (заштитини) принцип, персонални и универзални принцип) [238]. У погледу просторног важења кривичног процесног права, такође, важи територијални принцип (*locus regit actum*), према ком се на територији једне земље примењују кривичнопроцесни закони те земље[239]. Дакле, у складу са *територијалним принципом*, за сва кривична дела *учињена на територији државе*, независно од држављанства учиниоца, примењује се домаће кривично законодавство (материјално и процесно). За примену овог принципа, важно је одредити значење *појма територије*. Под територијом се подразумева сувоземна територија, водене површине унутар граница, као и ваздушни простор над њима (члан 112. став 1 КЗ), а територијални принцип је проширен принципом заставе брода и принципом регистрације авиона (члан 6. ставови 2. и 3. КЗ). Осим тога, за разумевање територијалног принципа битно је и схватање шта се под местом извршења кривичног дела подразумева. Кривични законик одређује да је дело учињено на територији Републике Србије ако је на њој извршена радња кривичног дела, а под местом извршења кривичног дела, сматра се како место где је извршилац радио или био дужан да ради, тако и место где је у целини или делимично наступила последица дела (члан 17. КЗ).

---

[236] http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[237] A. Cottim, "Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime", *European Journal of Legal Studies* 3/2010, 15.
[238] Стојановић, *Кривично право (општи део)*, 70-74.
[239] С. Бркић, *Кривично процесно право I*, Центар за издавачку делатност Правног факултета у Новом Саду, Нови Сад 2014, 35.

У случајевима када се не може применити територијални принцип, односно када је дело извршено у иностранству примењују се други, субсидијарни принципи. Међутим, нису сви примењиви у погледу дела високотехнолошког криминала. Наиме, у складу са чланом 7. КЗ, *примарни реални принцип* се примењују само ако лице (домаћи држављанин или странац) у иностранству учини одређена кривична дела против добара која представљају нарочити интерес за државу[240]. При томе, страно кривично право нема значај (важи принцип апсолутне примене нашег права), односно домаће кривично право ће бити примењено чак и да је лице осуђено и казну издржало, но, мало је вероватно да страна држава у наведеним случајевима штити наведене интересе друге државе. Осим примарног реалног принципа, постоји и *супсидијарни*, по ком домаће кривично законодавство важи и за странца који у иностранству учини према нашој држави неко друго кривично дело (осим претходно наведених) или било које кривично дело против држављанина Србије, али под условом да се странац затекне на територији наше државе или да јој буде екстрадиран (као и да буду испуњени посебни услови за кривично гоњење за кривично дело чињено у иностранству из члана 10. КЗ), но, с тим у вези је питање спремности државе да изручује сопствене држављане другој држави ради вођења кривичног поступка за дела учињена против интереса те друге државе. Уколико, пак, домаћи држављанин у иностранству учини било које кривично дело (осим претходно наведених), у складу са *персоналним* принципом, на њега се примењују домаће кривично законодавство, али, такође, под условом да се затекне на територији наше државе или да јој буде екстрадиран (као и да буду испуњени посебни услови за кривично гоњење за кривично дело чињено у иностранству из члана 10. КЗ), па се персонални принцип може применити на учиниоце дела високотехнолошког криминала који су домаћи држављани. *Универзални* принцип има за циљ да се према учиниоцу увек може применити кривична санкција, а подразумева да домаће кривично законодавство важи за странца који према страној држави или

[240] Кривична дела против уставног уређења Републике Србије (изузимајући кривично дело изазивања националне, расне и верске мржње и нетрпељивости из члана 317. КЗ), кривично дело фалсификовања новца које се односи на домаћу валуту (члан 223), као и кривична дела тероризма (члан 391), јавног подстицање на извршење терористичких дела (члан 391 а), врбовања и обучавања за извршење терористичких дела (члан 391 б), употребе смртоносне направе (члан 391 в), уништења и оштећење нуклеарног објекта (члан 391 г), угрожавања лица под међународном заштитом (члан 392) и финансирања тероризма (члан 393).

према странцу учини у иностранству кривично дело за које се према законодавству у којој је учињено може изрећи затвор у трајању од пет година или тежа казна, а овај услов не мора бити испуњен ако се ради о кривичном делу које се према начелима признатим од стране међународне заједнице сматра кривичним делом. У том смислу се може поставити питање, да ли су дела високотехнолошког криминала препозната као таква. Имајући у виду широку прихваћеност Конвенције о високотехнолошком криминалу, могло би се тврдити да је то тако, међутим, за кривична дела која предвиђа Конвенција нису прописане толико строге кривичне санкције.

Неспорно је да држава настоји да обезбеди екстериторијално важење сопственог кривичног законодавства, али се поставља питање, које решење би било оправдано: а) примену примарног реалног принципа проширити и на друге групе кривичних дела, водећи рачуна о појединим објектима кривичноправне заштите који по природи ствари могу бити угрожени, односно повређени радњом дела која је предузета посредством информационих технологија, односно искоришћавањем рачунарске мреже или комуникације другим техничким средствима за извршење, а који се налазе ван територије државе; б) уколико је домаћи држављанин предузео радњу кривичног дела искоришћавањем рачунарске мреже или комуникације другим техничким средствима за извршење који се налазе ван територије државе (односно у иностранству)[241], уклонити услов

[241] У обзир би долазила поједина кривична дела из групе кривичних дела против слобода и права човека и грађанина из главе четрнаесте КЗ (нпр. кривично дело угрожавања сигурности (члан 138), повреде тајности писама и других пошиљака (члан 142), неовлашћеног прислушкивања и снимања (члан 143), неовлашћеног фотографисања (члан 144), неовлашћеног објављивања и приказивања туђег списа, портрета и снимка (члан 145), неовлашћеног прикупљања личних података (члан 146); кривична дела против части и угледа из главе седамнаесте КЗ; поједина кривична дела из групе кривичних дела против полне слободе из главе осамнаесте КЗ (нпр. кривично дело приказивања, прибављања и поседовања порнографског материјала и искоришћавање малолетног лица за порнографију (члан 185), искоришћавања рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу (члан 185 б); кривична дела против интелектуалне својине из главе двадесете КЗ; поједина кривична дела из групе кривичних дела против привреде и главе двадесет друге КЗ (нпр. кривично дело фалсификовања хартија од вредности (члан 224), фалсификовања и злоупотребе платних картица (члан 225), фалсификовања знакова за вредност (члан 226), прања новца (члан 231), злоупотребе монополистичког положаја (члан 232), неовлашћене употребе туђег пословног имена и друге посебне ознаке робе или услуга (члан 233), нарушавања пословног угледа и кредитне способности (члан 239), одавања пословне тајне (члан 240), обмањивања купаца (члан 244), фалсификовања знакова, односно државних жигова за обележавање робе, мерила и предмета од драгоцених метала (члан 245); поједина дела из групе кривичних дела против против општи сигурности људи и имовине из главе двадесет пете КЗ (нпр. кривично дело изазивања опште опасности (члан 278), уништење и оштећење јавних уређаја (члан 279), злоупотребе

предвиђен за примену персоналног принципа (да се кривично гоњење може предузети само ако се за кривично дело кажњава и по закону земље у којој је оно учињено) што би омогућило да се према домаћем држављанину може применити кривично законодавство и ако је дело учинио коришћењем информационе технологије која се налази у иностранству; в) у погледу универзалног принципа одредити одређена кривична дела[242]; г) проширити појам територије специфичним принципом (као за брод и ваздухоплов); или д) ништа од поменутог није потребно, с обзиром на то да је Законик прихватио теорију убиквитета, по којој је довољно да последица наступи на територији државе, да би се сматрало да је дело извршено на територији те државе и да се на томе заснива надлежност.

При свему томе не сме се превидети транснационални карактер високотехнолошког криминала. Будући да електронске комуникације производе ефекте по интересе држављана и интереса државе и преко граница[243], јер конфигурација кибер простора омогућава извршиоцу да коришћењем инфраструктура у неколико држава изврши кривично дело према лицу који се може налазити на територији друге државе, *државе су настојале да што је више могуће прошире надлежност по основу територијалног принципа*. Оправдање за

телекомуникационих знакова (члан 284); поједина дела из групе кривичних дела против безбедности јавног саобраћаја (нпр. кривична дела угрожавања саобраћаја опасном радњом и опасним средством (члан 290), угрожавање безбедности ваздушног саобраћаја (члан 291), угрожавање безбедности ваздушног саобраћаја насиљем (члан 292); кривична дела против безбедности рачунарских података из главе двадесет седме КЗ; кривично дело изазивања националне, расне и верске мржње и нетрпељивости; поједина дела из групе кривичних дела против јавног реда и мира из главе тридесет прве (нпр. кривично дело изазвања панике и нереда (члан 343), неовлашћеног организовања игара на срећу (члан 352); кривична дела против правног саобраћаја из главе тридесет друге КЗ; поједина дела из групе кривичних дела против човечности и других добара заштићених међународним правом из главе тридесет четврте КЗ (нпр. кривично дело недозвољене производње, промета и држања оружја чија је употреба забрањена (члан 377), расне и друге дискриминације (члан 387), поједина дела из групе кривичних дела против Војске Србије из главе тридесет пете КЗ (нпр. кривично дело подривања војне и одбрамбене моћи (члан 491).

[242] Тако на пример, члан 6. немачког Кривичног закона предвиђа да ће се немачко законодавтсво применити и ако је у иностранству учињено дело против одређених изричито наведених међународним правом заштићених правних интереса (између којих су у тачки 6. наведена кривична дела дистрибуција, прибављање и поседовање дечје порнографије (члан 184б), дистрибуција, прибављање и поседовање малолетничке порнографије (члан 184ц) уколико су почињена употребом телекомуникационих система (члан 184 д), односно у складу са тачком 9. и за друга кривична дела поводом којих се држава на основу међународног уговора обавезала да предузме кривично гоњење иако су учињена у иностранству. При томе треба имати у виду да чак ни Конвенција о високотехнолошком криминалу не предвиђа основ за заснивање надлежности за дела која странац учини у иностранству.

[243] D. Bradbury, „When borders collide: legislating against cybercrime“, *Computer Fraud & Security* 2/2012, 14.

проширење важења прописа на радње које су предузете на територији друге државе произлази из концепта да држава представља и штити интересе својих држављана, али докле год таква примена не угрожава сувереност друге државе[244]. *Државе различито приступају прописивању правила надлежности за кривична дела високотехнолошког криминала проширујући екстериторијални домет својих кривичноправних норми*. У појединим државама постоје посебна правила за одређивање надлежности у погледу кривичних дела код којих су рачунарски систем/мрежа објект извршења или средство напада. Тако, у америчкој држави Арканзас може се кривично гонити извршилац уколико „трансмисија која је конститутивни елемент радње, има извор или одредиште у држави", у Оклахоми је прописано да се „лице које је остварило недозвољен приступ рачунару или рачунарској мрежи у јурисдикцији друге државе може гонити и у једној и у другој држави", док надлежни органи државе Охајо могу гонити лице чија је „употреба рачунара, рачунарске мреже, телекомуникационих уређаја или услуге произвела рачунарски податак или комуникацију која се преноси или је похрањена на територији државе" [245]. Осим наведеног, у теорији се може уочити неколико модификација територијалног принципа које проширују његово дејство ван граница државе, а с обзиром на природу кибер простора:

1. Доктрина квалификованог дејства (*Qualified Effects Doctrine*) проширује надлежност државе уколико се на њеној територији произведене значајне последице дела учињеног у иностранству[246],
2. Тзв**.** *Top Level Domain* се сматра кибер територијом државе (слично екстратериторијалном важењу принципа заставе брода/авиона),
3. Доктрина проширеног дејства (*Wide Effects Doctrine*) проширује надлежност у погледу дела извршених путем Интернета на сваку државу са чије територије се одређеној страници може приступити[247].

Да би се *ограничило дејство поменутих доктрина*, *судска пракса* појединих држава препознаје неколико *критеријума* који се заснивају на постојању додатне

[244] J. Reidenberg, „Technology and Internet Jurisdiction", University of Pennsylvania Law Review 6/2005, 1961-1962.
[245] B. Koops, S. Brenner, (eds.), *Cybercrime Jurisdiction: A Global Survey*, T.M.C. Asser Press, Amsterdam 2006, 17-21.
[246] Више о томе, B. Craig, *Cyberlaw: The Law of the Internet and Information Technology*, Prentice Hall, New Jersey 2012, 13-16.
[247] Wittzack, *op.cit*, 1254.

везе између радње учињене посредством Интернета и последица произведених у држави (нпр. језик, садржај, публицитет објављеног садржаја). Тако је Регионални суд Париза заузео став да понуда нацистичких ознака преко америчког сервера представља кривично дело према француском кривичном праву. Савезни суд Немачке осудио је аустралијског држављана који је на аустралијској веб страници порицао холокауст из разлога што, осим што у Немачкој представља кривично дело, овакво поступање у значајној мери погађа немачку државу и нацију (случај *Toeben*)[248]. Британски суд је осудио француског држављана за постављање недозвољеног материјала на вебсајт који је похрањен на америчком серверу, јер је полиција у лондонској полицијској станици остварила увид у материјале, али и зато што је извршилац боравио у Великој Британији у време извршења радње (случај *Perrin*)[249], док је шведски суд искористио физичку локацију сервера за осуду у одлуци против *Pirate Bay*[250]. Овакви додатни услови су потребни, јер би у супротном: а) неограничена унилатерална примена доктрине *wide effects doctrine,* односно *qualified effects doctrine* за заснивање надлежности могла да угрози суверенитет других држава и истовремено да доведе до честих сукоба надлежности, и б) *World Wide Web* би се морао ускладити са правним поретком свих држава из које се остварује приступ Интернету, што није могуће без поништавања основних концептуалних карактеристика ове глобалне мреже, а нарочито слобода изражавања.

Наиме, уколико више држава тежи да успостави екстериторијално важење домаћег права, односно да прошири надлежност да уређује односе на територији друге државе применом поменутих принципа, то може довести *до сукоба надлежности*, како позитивног, тако и негативног. На основу хипотетичког примера може се указати на проблем сукоба надлежности који изазивају транснационални елементи дела високотехнолошког криминала. Учинилац који се налази у држави А је употребом рачунара лоцираних у држави Б и В извршио напад на информационе системе у државама Г и Д из чега произлази да радња извршења није предузета на територији једне већ су „делови“ радње извршени на

[248] Wittzack, *op.cit*, 1255.
[249] Wittzack, *op.cit*, 1256.
[250] G. Heissl, „Jurisdiction for Human Rights Violations on the Internet“, *European Journal of Law and Technology* 1/2011, 2-3.

територији више држава. Применом традиционалног принципа надлежности могуће је више сценарија: а) може се десити да ни држава у којој се налази извршилац нити државе у којима су оштећена лица не могу засновати надлежност за гоњење учиниоца кривично дело, б) држава заснива надлежност за гоњење учиниоца али се он налази у држави у којој радња није предвиђена као кривично дело, или в) да држава у којој се налази извршилац и друге државе у којима се налазе оштећени међусобно конкуришу да гоне учиниоца, па постоји проблем одређивања која од њих има приоритет, а осим тога како решити поштовање принципа *ne bis in idem* [251]. Конвенција као метод решавања сукоба надлежности између две државе потписнице предвиђа договор између држава, односно консултације у циљу проналажења најадекватнијег решења у конкретном случају[252]. Поједини аутори у вези са решавањем позитивног сукоба надлежности предлажу стварање принципа *ne bis in idem* у кибер простору[253], док се за превазилажење негативног сукоба надлежности указује на корисност универзалног принципа који проистиче из међународне солидарности[254].

У вези са превазилажењем поменутих проблема, и то применом универзалног принципа, вредни помена су предлози за формирање међународног суда који би био надлежан да суди учиниоцима најтежих облика дела високотехнолошког криминала са транснационалном димензијом[255]. Као оправдање за оснивање таквог суда наводи се повећан број случајева напада на критичне информационе инфраструктуре и немогућност „локалног процесуирања“[256].

---

[251] F. Pocar, „New challenges for international rules against cyber crime“, *European Journal on Criminal Policy and Research* 1/2004, 28.

[252] О предлогу за решавање позитивног сукоба надлежности, види Brenner, *op.cit*, 197-198

[253] О томе више, Kaspersen.,*op.cit*, 22-25.

[254] О аргументима за примену универзалног принципа види K. Gable, „Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent“, *Vanderbilt Journal of Transnational Law* 1/ 2009, 67-68. и A. Gillespie, *„*Jurisdictional issues concerning online child pornography*“, International Journal of Law and Information Technology* 3/2012, 156.

[255] A. Zavrsnik, The absence of body in Cyberspace Criminal Justice Impact, *Masaryk University Journal of Law and Technology* 1/2007, 43-52.

[256] Наводи се пример напада на информациону инфраструктуру Естоније 2007. године, као и оптужбе САД да Русија и Кина користе напредне рачунарске технологију за шпијунажу 2011. године –N. Cade, „An adaptive approach for an evolving crime: the case for an International cyber court and penal code“, *Brooklyn Journal of International Law* 37/2012, 1141; M. Watneym, „The Way Forward in Addressing Cybercrime Regulation on a Global Level“, *Journal of Internet Technology and Secured Transactions* 1-2/ 2012, 65.

Тако је у Нацрту Споразума Уједињених нација о оснивању међународног трибунала за кибер простор (*International Criminal Tribunal for Cyberspace*)[257] наведено да је Трибунал потребан како извршиоци *најтежих облика* дела високотехнолошког криминала не би услед проблема у вези са утврђивањем надлежности избегли кривичну одговорност. Нацрт Споразума садржи и предлог Статута Трибунала са неколико интересантних решења[258]. Надлежност за истрагу и гоњење кривичних дела припадала би Међународном тужилаштву за кибер простор, као посебном органу (*separate organ*) Трибунала (?). Даље се предвиђа да је Трибунал надлежан да гони (?) лица која су учинила следећа кривична дела: глобални напад на критичне информационе и комуникационе инфраструктуре (члан 2: *Global cyberattacks against critical communications and information infrastructures*)[259], остале облике глобалних размера (члан 3: *Other cybercrime of the most serious global concern*)[260], крађу идентитета и друга тешка кривична дела учињена на друштвеним мрежама (члан 4: *Social networks and identity theft*), као и припремне радње, односно стварање информационих и комуникационих алата и услова потребних за извршење поменутих дела (члан 5: *preparatory acts of provisions in the global statute on cyberattacks and cybercrime*). Може се уочити покушај стварања новог облика међународног кривичног права (у односу на сада већ традиционално схватање појма ове гране права), јер сва четири члана садрже формулацију „ко...кршећи одредбе међународног кибер кривичног права“ (*violations of international cybercrime law*) као својеврсни објективни услов инкриминације[261]. Претпостављамо да таква формулација има за циљ да повеже

[257] S. Schjolberg, *Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace*, 2014, http://www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf. Ради се о деветој верзији нацрта, а мандат за састављање нарта и заговарање идеје поверен је судији *Schjolberg* који је заједно са професором Зибером израдио прву студију о компјутерском криминалу. Нацрт предвиђа да би Трибунал формирала Генерална скупштина УН или Савет безбедности поступајући по поглављу Повеље УН.

[258] Поједина решења заслужују критику, што није чудно с обзиром на то да је за израду предлога Статута употребљен Статут Трибунала за бившу Југославију

[259] Напад подразумева оштећење, онеспособљавање или уништење критичне информационе и комуникационе инфраструктуре, што је довело до значајног угрожавања националне безбедности, јавног здравља, банкарских и финансијских сектора.

[260] Таксативно су наведени: неовлашћен приступ, недозвољено пресретање, ометање података, ометања система, злоупотреба уређаја, кривотворење, превара, дела повезана са дечјом порнографијом.

[261] Што се не може довести у везу са међународним кривичним правом, које је настало и развијало се у потпуно другачијим историјским околностима и са другачијим оправдањем, М. Шкулић, Међународни кривични суд – надлежност и поступак, Београд 2005, 23-29.

надлежност Трибунала првенствено са Конвенцијом СЕ о високотехнолошком криминалу[262]. Предлог Статута предвиђа приоритетну надлежност Трибунала у односу на националне судове (за разлику од принципа комплементарности предвиђеном у Римском статуту), при чему Трибунал може у свакој фази поступка који се води пред судовима у оквиру држава тражити уступање кривичног поступка. Осим тога, остављена је могућност да се надлежност Трибунала прошири и на друга кривична дела, и то одлуком Савета безбедности УН о измени Статута (?). Реализација идеје о оснивању посебног Трибунала на легитиман начин била би могућа само уколико би се постигао консензус суверених држава у оквиру Генералне скупштине УН и довољан број држава прихвато надлежност Трибунала[263].

Осим овог предлога, поједини аутори могуће решење проблема у вези са надлежношћу виде у оснивању суда у оквиру Савета Европе који би био надлежан за суђење учиниоцима *тешких* облика кривичних дела предвиђених у одредбама Конвенције о високотехнолошком криминалу а који су извршени на или са територије држава потписница. Оснивање Суда би било предвиђено амандманом на Конвенцију којој би било потребно да приступи довољан број потписница[264].

Мишљења смо да је мало вероватно да ће се ови предлози реализовати, јер државе нису спремне да се својевољно одрекну дела свог суверенитета (права сувереног вршења власти у смислу усвајања прописа и гоњења учинилаца), а нарочито из разлога што у погледу високотехнолошког криминала не постоји консензус да се ради о глобалној и универзалној претњи, односно кривичним делима која угрожавају међународну заједницу у довољној мери да би било оправдано оснивање неког међународног кривичног суда (односно, поверавање надлежности за суђење ових кривичних дела постојећим телима), тим пре, што се то до сада није догодило чак ни за тероризам и организовани криминал. Такође, сматрамо да остварљивост оваквих предлога није у складу са претпоставком да је

[262] Више о томе, B. Harley, „A global convention on cybercrime?“, *Columbia Science and Technology Law Review*, http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/.
[263] Истог мишљења је и судија *Schjolberg* који је креатр предлога Статута. Види Schjolberg, *The History of Cybercrime: 1976-2014*,189.
[264] W. Kraft, *Ideas on the Establishment of an International Court for Cyber Crime*, 2011, 8-9, http://www.wclf.de/cybercrime_court_en.html?file=tl_files/Media/Download/FINAL-CYBER-COURT-ENGLISH.pdf.

најбоље решење да у предметима високотехнолошког криминала поступају надлежни органи суверених држава[265].

Осим проширења надлежности државе да у кибер простору регулише злоупотребу информационих технологије, може се поставити питање да ли је могуће проширење надлежности за деловање надлежних органа, односно *да ли је место предузимања радњи надлежних органа у откривању и доказивању дела високотехнолошког криминала омеђено границама територије државе или је под одређеним условима могуће њихово екстериторијално деловање* у циљу прикупљања доказа о делима високотехнолошког криминала који се налазе у кибер простору који не познаје границе. У складу са правилима међународног јавног права[266], физичко присуство и активности органа државе/међународне организације на територији друге државе, а без њене претходне сагласности представљају повреду територијалног суверенитета. У случају потребе да у вези са кривичним поступком надлежни органи једне државе на територији друге државе предузму радње, нужно је ангажовање механизама пружања међународне правне помоћи у кривичним стварима[267]. Једино реално решење јесте стога приближавање националних прописа у што већој мери како би се омогућила ефективна међународна сарадња у случајевима транснационалног високотехнолошког криминала, у том смислу је од изузетно значајна Конвенција СЕ о високотехнолошком криминалу.

2. СПЕЦИЈАЛИЗАЦИЈА ДРЖАВНИХ ОРГАНА НАДЛЕЖНИХ ЗА ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Поред законског уређења радњи за откривање и доказивање дела високотехнолошког криминала, да би њихова примена била ефективна и ефикасна, а с обзиром на техничке специфичности чињеничног супстрата поводом којих се одређују, потребно је да орган поступка има одређени ниво знања о информационим технологијама. „Високотехнолошки“ елемент у генусном

[265] Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes*, 187.
[266] Правила утврђена у одлуцу у Лотус предмету 1929.године (Cf. Case of the S.S. "Lotus" (France v. Turkey), PCIJ Series A, No. 10). Више о томе, Koops, Brenner, *op.cit*, 72.
[267] Питање међународне правне помоћи је предмет Шестог дела рада.

појму који обухвата кривична дела учињена против/посредством рачунарских података/система/мрежа чини откривање и доказивање ових дела отежаним без поседовања посебних знања и вештина потребних за примену посебних техничких и тактичких правила. У том смислу, *може се поћи од претпоставке да је формирање специјализованих организационих јединица у оквиру полиције и јавног тужилаштва један од кључних фактора у успешном супротстављању високотехнолошком криминалу*.

Не постоји униформно решење које би било одговарајуће за све државе јер потреба за формирањем специјализованих и унапређењем постојећих јединица зависи од неколико фактора: законодавства, степена зависности друштва од информационих технологија, учешћа високотехнолошког криминала у стопи извршених кривичних дела и другог[268]. Да би се утврдило да ли постоји оправдање за формирање специјализованих јединица, посматрана су решења у појединим националним законодавствима, као примери добре праксе, а ради анализе надлежности, делокруга рада и организације, те уочавања типова специјализације.

У вези са утврђивањем *улоге специјализованих органа*, уочавају се три функције које се у оквиру рада тих органа остварују[269]: 1. Истрага кривичних дела учињених против рачунарских података/система и гоњење учинилаца тих дела (у смислу чланова 2-6. КВК); 2. Истрага кривичних дела учињених посредством (употребом) рачунарских података/система и гоњење учинилаца тих дела (у смислу чланова 6-10. КВК); и 3. Поступање по техничким и тактичким правилима у вези са рачунарским подацима који су похрањени, обрађују се или преносе путем рачунарских система/мрежа, а који могу бити доказ у кривичном поступку за сва кривична дела[270].

Дакле, смисао постојања специјализованих органа огледа се у њиховој основној улози, а то је истрага дела високотехнолошког криминала и поступање

---

[268] *ACPO, Good Practice and Advice Guide for Managers of e-Crime Investigation*, 2011, http://www.npcc.police.uk/, 5-6.

[269] Specialised cybercrime units - Good practice study, 2011, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf, 4.

[270] Скуп техничких и тактичких правила којима се уређује поступање органа ради проналаска и анализе рачунарских података као трагова кривичног дела назива се *дигитална форензика*, што је предмет Седмог дела рада. Докази који настају као резултат обраде рачунарских података применом дигиталне форензике називају се *електронски (дигитални) докази*, а они су предмет обраде Трећег дела рада.

по правилима дигиталне форензике ради проналаска дигиталних доказа. Надлежност и делокруг рада специјализованих јединица могли би бити одређени тако да обухватају све ове улоге или да представљају комбинацију истраге, прикупљања и форензичке анализе рачунарских података и других задатака (нпр. праћења и анализе феномена високотехнолошког криминала[271]). У сваком случају, њихова улога зависи од организације и надлежности полиције, односно јавног тужилаштва, те оперативних и процесних овлашћења датих у циљу остваривања послова и задатака из делокруга рада[272]. У том смислу могу се разликовати: 1) посебне организационе јединице полиције; 2) посебна тужилаштва; 3) посебни форензички капацитети у оквиру ових јединица или као самосталне структуре.

Као примере добре праксе у погледу организације и састава специјализованих органа могу се навести приступи у три америчке државе, у којима је још током 1990-тих година прошлог века препозната потреба за формирањем посебних организационих јединица за високотехнолошки криминал. Наиме, у САД у оквиру Федералног бироа за истрагу (*Federal Bureau of Investigation: FBI*) постоји Национална јединица за истрагу високотехнолошког криминала (*National Cyber Investigative Joint Task Force: NCIJTF*[273]) надлежна за истрагу најтежих облика високотехнолошког криминала, док је истрага осталих кривичних дела против безбедности рачунарских података у надлежности федералних јединица, са различитим организационим решењима, од којих бисмо издвојили следеће моделе:

А. Представнички модел (*Statewide Cyber Crime Task Force*) постоји од 1999. године у држави Мејн. Јединицу са задатком да истражује случајеве високотехнолошког криминала чине представници државног и окружног јавног тужилаштва, државних и локалних полицијских одељења и форензичких лабораторија. Наиме, ови органи одредили су своје представнике који су одговорни за истрагу дела високотехнолошког криминала, па у састав Јединице улазе три полицијска истражитеља, три форензичара и два заменика јавног тужиоца. Јединица координира истрагама које се спроводе широм државе, пружа

[271] C. Mulligan, "Perfect Enforcement Of Law: When To Limit And When To Use Technology", *The Richmond Journal of Law and Technology* 4/2008, 15.
[272] *Specialised cybercrime units,* 16.
[273] http://www.fbi.gov/about-us/investigate/cyber/ncijtf

правну и техничку помоћ другим органима, остварује сарадњу са пружаоцима услуга електронских комуникација, те реализује програме обуке за запослене у полицији и тужилаштву[274].

Б. Централизовани модел (*Dedicated In-House Cyber Crime Unit*) у држави Мисисипи огледа се у постојању Јединице за високотехнолошки криминал у оквиру Одељења за заштиту јавног интегритета (*Public Integrity Division*) Државног јавног тужилаштва које је надлежно за територију целе државе. Јединицу чине заменик тужиоца, који је на челу Јединице, три полицијска истражитеља и један форензичар. У оквиру Јединице је формирана лабораторија за дигиталну форензику која врши форензичке анализе поводом захтева свих полицијских одељења у држави[275].

В. Дистрибутивни модел (*Model of Distributed Forensics/Prosecution of Cybercrime*) заступљен у држави Нови Хемпшир функционише тако што тужилаштво и полиција на локалном нивоу воде истрагу дела високотехнолошког криминала (а не државно јавно тужилаштво које је иначе надлежно за истрагу кривичних дела), док форензичку обраду врши лабораторија на државном нивоу. Државна форензичка лабораторија има задатак да прегледа одузете електронске уређаје и резултате форензичке анализе похрањује у заједничкој рачунарској мрежи преко које локална полиција приступа обрађеном материјалу[276].

У научној литератури су, пак, препознате следеће категорије специјализованих организационих јединица за високотехнолошки криминал[277]: 1. Јединице за стручну подршку, односно јединице за форензичку истрагу, које врше форензичку обраду одузетих рачунарских уређаја; 2. Одељења која прикупљају оперативне податке о значајнијим случајевима са прекограничним елементима, као што су посебна истражна одељења (*Specialist Investigations Departments*) или одељења за посебне доказне радње и прикупљање информација (*Intelligence and Specialist Operations*), 3. Посебне јединице надлежне за истрагу кривичних дела против

[274] National Center for Justice and the Rule of Law, *Combating cyber crime: essential tools and effective organizational structures a guide for policy makers and managers*, 2007, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf, 19-22.
[275] *Combating cyber crime: essential tools and effective organizational structures a guide for policy makers and managers*, 22-24.
[276] *Combating cyber crime: essential tools and effective organizational structures a guide for policy makers and managers*, 17-22.
[277] Jewkes,Yar, *op.cit*, 540; Упор. Moitra S., "Developing policies for cybercrime", *European Journal of Crime, criminal law and criminal justice,* 13/3, 2005, 450.

рачунарских система и других „традиционалних“ кривичних дела са високотехнолошким елементима, и 4. Јединице које истражују поједине облике високотехнолошког криминала (нпр. случајеве *online* дечје порнографије).

Анализом законских решења појединих држава, уочене се следеће специјализоване организационе јединице[278]:

1. Јединице у оквиру полиције, специјализоване за истрагу кривичних дела код којих су рачунарски системи/мреже објект напада, односно средство извршења (*cybercrime units*) и за обављање одређених послова дигиталне форензике.

Тако је у Шпанији 1995. формирана централна јединица у оквиру судске полиције као специјална структура за истрагу дела учињених против/употребом рачунарских система и мрежа. У састав јединице улазе једна централна (са 45 запослених) и три посебне секције (са по 4-7 запослених), од којих је једна надлежна за истрагу дела против лица (нпр. илегално пресретање комуникација учињено посредством рачунара), друга за истрагу дела у вези са привредним криминалом (нпр. компјутерске преваре, повреда права интелектуалне својине), и трећа у оквиру које се врши форензичка анализа рачунарских података и система а која координира радом одељења на локалном нивоу[279]. У Француској постоје две посебне организационе јединице: Национална јединица надлежна за истрагу кривичних дела која су учињена против/посредством рачунарских система, док је за истрагу дела *online* дечје порнографије, расизма и ксенофобије учињене злоупотребом информационе технологије надлежно посебно одељење у оквиру судске полиције[280].

2. Јединице у оквиру полиције, специјализоване за високотехнолошки криминал (*high tech crime units*) надлежне само за истрагу кривичних дела против безбедности рачунарских података и система, као и за форензичку обраду рачунарских уређаја (и пружање другим организационим јединицама техничке подршке у том смислу).

Тако у Аустрији у оквиру криминалистичке службе постоје два одељења у чијој надлежности је истрага кривичних дела против рачунарских система

[278] Specialised cybercrime units - Good practice study, 5,13-15
[279] Specialised cybercrime units - Good practice study, 94-96.
[280] Specialised cybercrime units - Good practice study, 75-79.

(неовлашћен приступ рачунарима и рачунарским мрежама, повреда приватности телекомуникација, недозвољено пресретање рачунарских података, оштећење података, ометање функционисања рачунарског система, злоупотреба рачунарског програма, фалсификовање рачунарских података, превара у вези са обрадом података)[281]. У Белгији је формирана јединица за компјутерски криминал на централном нивоу која пружа техничку подршку регионалним јединицама на нивоу округа (постоје 26 регионалних јединица) које истражују кривична дела код којих је рачунарски систем/подаци објект напада, а осим тога централна јединица може аутономно да истражује случајеве у којима постоји потреба за хитним интервенцијама или кад је извршен напад на критичне информационе инфраструктуре. Ове специјализоване јединице нису надлежне за истрагу кривичних дела које су извршено посредством рачунарских система/мрежа али надлежним јединицама пружају помоћ у виду форензичке обраде и анализе рачунарских података[282]. У Великој Британији је у оквиру полиције на централном нивоу основана Јединица за електронски криминал (*Metropoliten Police central e-crime unit*[283]) која је надлежна за истрагу дистрибуираних напада на информационе системе, дистрибуцију малициозних кодова и преваре на Интернету[284].

3. Јединице за дигиталну форензику, формиране са задатком да прикупљају и анализирају електронске доказе без обзира на врсту кривичног дела (*computer forensic units*).

Таква јединица, на пример, формирана је у Румунији 2003. године законом којим је ратификована КВК, а у оквиру Одељења за истрагу организованог криминала и тероризма Републичког јавног тужилаштва[285]. У Литванији постоји одељење за форенизичку анализу информационих технологија у Центру за форензичке науке коју чине две организационе јединице, једна формирана у оквиру Министарства правде а друга у оквиру полиције, обе са задатком да за

[281] Specialised cybercrime units - Good practice study, 61-63.
[282] Specialised cybercrime units - Good practice study,. 63-65.
[283] Ово је првооснована специјализована јединица за високотехнолошки криминал у Европи (основана 1985. године). P. Sommer, „The Future for the Policing the Cybercrime“, *Computer Fraud & Security* 1/2004, 8.
[284] Jewkes, Yar, *op.cit*, 541-542.
[285] Specialised cybercrime units - Good practice study, 88-90.

потребе органа у оквиру којих су образоване, врше форензичку обраду електронских уређаја без обзира на то о ком кривичном делу се ради[286].

4. Јединица на централном нивоу, без истражних овлашћења одговорна за координацију, стратешку и функцију прикупљања оперативних података у циљу помоћи другим полицијским структурама у истрази дела високотехнолошког криминала и криминалистичкој обради других кривичних дела.

Тако у Великој Британији у оквиру полицијске Агенције за борбу против тешких облика организованог криминала (*SOCA: Serious Organised Crime Agency*) постоји одељење за високотехнолошки криминал које првенствено има улогу прикупљања оперативних података, процене степена претње и иницирање истрага у конкретним случајевима које истражују локалне јединице полиције. Поменута јединица полиције (*Metropolitan Police central e-crime unit*) и ово одељење чине Националну јединицу за високотехнолошки криминал (*National cybercrime unit*) у оквиру Националне криминалистичке агенције (*National Crime Agency*) са задатком прикупљања оперативних података, проактивног деловања на спречавању извршења кривичних дела употребом информационе технологије и остваривања међународне сарадње[287].

5. Јединице у оквиру полиције, које се формирају са надлежношћу да спроводе истрагу појединих облика високотехнолошког криминала.

Таква је Јединица за заштиту деце од искоришћавања у порнографске сврхе употребом информационих технологија (*Child Exploitation Online Protection*) формирана 2006. године у Великој Британији[288].

2.1. Специјализација надлежниих државних органа у Републици Србији

У *Републици Србији* је постоји „уникатно“ законско решење. Наиме, Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала[289] усвојен 2005. године предвидео је формирање

[286] L. Novikoviene, Bileviciute E., „Application of IT Examination in Investigation of Crimes on Safety of Electronic Data and Information Systems“, *Jurisprudence* 1/2010, 321-322.
[287] *http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.*
[288] *Ibidem.*
[289] „Сл.гласник РС“, бр. 61/2005 и 104/2009.

специјализованих организационих јединица у оквиру полиције, јавног тужилаштва и суда надлежних за поступање за дела високотехнолошког криминала. Високотехнолошки криминал у смислу члана 2. овог Закона представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, а члан 3. Закона проширује појам високотехнолошког криминала одређујући групе кривичних дела која се под одређеним околностима сматрају високотехнолошким криминалом[290].

За поступање у предметима кривичних дела која су одређена као високотехнолошки криминал надлежно је Више јавно тужилаштво у Београду за територију Републике Србије (члан 4. став 1) у оквиру ког је образовано *посебно одељење за борбу против високотехнолошког криминала* (означено као Посебно тужилаштво, у смислу члана 4. став 2. Закона[291]). Радом Посебног тужилаштва руководи Посебни тужилац за високотехнолошки криминал, кога на период од 4 године поставља Републички јавни тужилац (и може бити поново постављен) из реда заменика јавних тужилаца који испуњавају услове за избор за заменика вишег јавног тужиоца (уз писмену сагласност лица које се поставља и доношење решења о упућивању тог лица у Посебно тужилаштво), при чему предност имају заменици јавних тужилаца који поседују посебна знања из области информатичких технологија (члан 5. Закона). Посебни тужилац се по сазнању да се у једном предмету ради о случајевима које предвиђа члан 3. Закона, обраћа

[290] Предвиђено је да се Закон примењује на откривање, гоњење и суђење за 1) кривична дела против безбедности рачунарских података одређена Кривичним закоником; 2) кривична дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, као и њихови производи у материјалном или електронском облику, ако број примерака ауторских дела прелази 2000 или настала материјална штета прелази износ од 1.000.000 динара; 3) кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због *начина извршења* или *употребљених средстава* могу сматрати кривичним делима високотехнолошког криминала.

[291] Ипак, Закон о јавном тужилаштву („Сл. гласник РС“, бр. 116/2008, 104/2009, 101/2010, 78/2011 – др.закон, 101/2011, 38/2012 – одлука УС, 121/2012, 101/2013, 111/2014 – одлука УС и 117/2014) у члану 13. став 2. наводи да су јавна тужилаштва посебне надлежности само Тужилаштво за организовани криминал и Тужилаштво за ратне злочине.

Републичком јавном тужиоцу захтевајући од њега да му повери или пренесе надлежност (члан 6. став 2)[292].

По захтевима Посебног тужиоца поступа Служба за борбу против високотехнолошког криминала (члан 9. став 2). Током 2007. године у Министарству унутрашњих послова у Служби за борбу против организованог криминала (СБПОК) у оквиру Управе криминалистичке полиције (при Дирекцији полиције) формирано је *Одељење за борбу против високотехнолошког криминала*. Закон предвиђа да је за поступање у предметима кривичних дела из члана 3. Закона надлежно *посебно одељење Вишег суда у Београду*, а предност у распоређивању у посебно одељење имају судије са посебним знањима из информатичких технологија (члан 11. став 2), но како одељење од 2009. године више не постоји, у предметима поступају судије Вишег суда у Београду.

> *Виши суд у Београду се огласио ненадлежним за поступање у кривичном предмету против окривљеног због кривичног дела из области високотехнолошког криминала, односно кривичног дела рачунарске преваре из члана 301. став 1. КЗ, јер је суд сматрао да из чињеничног описа дела у оптужном предлогу произилазе елементи бића кривичног дела издавање чека и коришћење платне картице без покрића из члана 228. став 3. У вези са ставом 1. КЗ, јер се окривљени терети да је коришћењем платних картица за које није имао покриће прибавио себи имовинску корист преко милион динара, а да је уношење нетачних података у систем које је утицало на резултате електронске обраде и преноса података само омогућило извршење радње кривичног дела из члана 228. КЗ. Међутим, Апелациони суд је оцењујући наводе жалбе Тужиоца за високотехнолошки криминал заузе став да се у конкретном случају не ради о простом коришћењу платне картице, већ о злоупотреби и изигравању рачунарског система у намери прибављања противправне имовинске користи и наношења штете банци, те су стога основани наводи тужиоца. Дакле, Одељење за борбу против високотехнолошког криминала надлежно је у*

[292] Иако се у Закону предвиђа да Тужилац има иста права и дужности као јавни тужилац, нејасно је из ког разлога Закон условљава поступање Посебног тужиоца одобрењем Републичког јавног тужиоца по упућеном захтеву за поверавање/преношење надлежности, нарочито имајући у виду да је Посебно тужилаштво одрђено као посебно одељење образовано у оквиру Вишег јавног тужилаштва у Београду.

поступцима који се воде због кривичног дела коришћења платне картице без покрића, када је дело извршено тако што је окривљени на банкоматима, ради изигравања рачунарског система, уносио нетачне податке чиме је утицао на резултате електронске обраде и преноса података. На основу члана 3. Закона о организацији и надлежности државних органа за борбу против високтехнолошког криминала, побијано решење је укинуто и предмет је враћен првостепеном суду на даљи поступак[293].

Тужилац за високотехнолошки криминал[294], мишљења је „да је формирање Тужилаштва за високотехнолошки криминал добро решење, јер је пре тога постојало хаотично поступање тужилаштава опште надлежности, незаинтересованост носилаца јавнотужилачке функције и тешко прихватање рада на предметима који обухватају употребу рачунара, с обзиром на то да је међу њима било заступљено „застарело“ схватање да се ради о облику криминалитета који ће се тек појавити и који не представља реалност.

Организација и надлежност државних органа за борбу против високотехнолошког криминала у Републици Србији у принципу су регулисани на одговарајући начин. У погледу решења из чл. 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Тужилац је мишљења да је, у циљу да стварна надлежност буде свеобухватна, потребно изменити Закон у смислу да се надлежност прошири на сва кривична дела учињена посредством информационих технологија или макар да се прошири на поједине групе кривичних дела (нпр. у погледу кривичних дела против живота и тела).

Постојање специјализованог Тужилаштва надлежног за територију целе Републике је адекватно решење, јер би парцијална надлежност довела до проблема у виду комуникације и размене података између тужилаштава као и неједнакости тужилачке праксе. Напоре би требало усмерити ка „јачању“

[293] Решење Апелационог суда у Београду Кж 2 ПО 3. Бр. 15/11 од 30.05.2011. и Решење Вишег суда у Београду КПО 3 бр. 44/10 од 11.02.2011. године.

[294] Марта 2015. године обављен је стручни интервју у вези са искуствима у поступању са делима из надлежнсти Тужилаштва са Бранком Стаменковићем, Тужиоцем за високотехнолошки криминал. Одговори Тужиоца наведена су у раду су по његовом одобрењу.

постојећег посебног тужилаштва, а не на „парцијализацији“ надлежности на више посебних тужилаштава.

Као основни организациони недостатак у функционисању Тужилаштва јесте недовољан број носилаца јавнотужилачке функције. Наиме, на предметима из надлежности Тужилаштва ради Тужилац, два заменика и три тужилачка помоћника, што је више него недовољан број, ако се узме у обзир да је повећање броја запримљених кривичних пријава у 2014. години повећан за чак 47% у односу на 2013. годину. Иако квантитативни састав (број запослених) Тужилаштва није одговарајући, у погледу квалитативног састава (структуре запослених) стање је задовољавајуће. За распоређивање у Тужилаштво се поред испуњења општих услова за избор заменика јавног тужиоца у вишем јавном тужилаштву у складу са Законом о јавном тужилаштву, тражи и поседовање знања и вештина из области информационе технологије, што се утврђује кроз усмени разговор са Тужиоцем (а у току је израда Правилника који ће прецизније регулисати услове и поступак за избор). Такође, обезбеђена је перманентне обука запослених, како кроз рад на предметима и консултације са Тужиоцем, тако и кроз програме обуке у земљи и иностранству.

На основу наведеног, решења у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала могла би бити унапређена тако да се Тужилаштву у складу са Уставом и Законом о јавном тужилаштву обезбеди права „посебност“, у смислу да Тужиоца не именује Републички јавни тужилац већ да се бира у Народној скупштини (како је предвиђено у погледу Тужиоца за организовани криминал и Тужиоца за ратне злочине[295]), што би, између осталог, омогућило проширење систематизације, како носилаца јавнотужилачке функције, тако и административног особља. Осим тога, потребно је створити материјалне услове (већим издвајањима из буџетских

[295] Наиме, члан 4. став 2. Закона о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела («Сл.гласник РС», бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 - др. закон, 45/2005, 61/2005, 72/2009, 72/2011 - др. закон, 101/2011 - др. закон и 32/2013) предвиђа примену Закона о јавном тужилаштву, уколико овим Законом нешто није решено, па се одредбе Закона о јавном тужилаштву примењују у погледу избора Тужиоца и његове могућности да уређује организацију унутар Тужилаштва. На основу члана 5. Закона о организацији и надлежности државних органа у поступку против учинилаца ратних злочина („Сл.гласник РС“, бр. 67/2003) Тужиоца за ратне злочине бира Надлежна скупштина, који на основу члана 6. доноси акте о унутрашњој организацији и систематизацији радних места у Тужилаштву (уз сагласност Министра надлежног за правосуђе).

средстава) ради појачања људских ресурса, али и за набавку техничке опреме потребне за рад Тужилаштва, што је кључни услов за рад који даје резултате.

У погледу осталих решења у Закону, проблем представља чињеница да од реформе правосуђа 2009. године не постоји у Вишем суду у Београду посебно одељење належано за поступање у предметима високотехнолошког криминала, па поступају судије Вишег суда у Београду без потребног информатичког знања, који не разумеју материју и код којих постоји одбојност према упуштању у разумевање специфичности доказивања дела високотехнолошког криминала. Из тог разлога је корисно искористити законску могућност за формирање Посебног одељења за високотехнолошки криминал, у оквиру ког би постојало довољно судија са потребним информатичким знањем, и то како судија за претходни поступак, тако и судија које би биле функционално надлежне за вођење главног претреса".

На сличне проблеме указао је и шеф Одсека за електронски криминал[296]. Према његовом мишљењу „надлежност државних органа за борбу против високотехнолошког криминала у Републици Србији регулисана је одговарајући начин, и не постоји потреба за проширивањем круга кривичних дела за која је надлежно Одељење. Ипак, постоји потреба за унапређењем решења у погледу организације, у смислу да Одељење не буде саставни део Службе за борбу против организованог криминала (јер због тога постоји обавеза поступања према захтевима и Тужилаштва за организовани криминал и Тужилаштва за високотехнолошки криминал). Стога би требало предвидети да Одељење буде посебна јединица у оквиру Управе криминалистичке полиција које би поступало само по захтевима Тужилаштва за високотехнолошки криминал.

Постојање Одељења које је надлежно за територију целе Републике је адекватно решење, али би било целисходно да поред Одељења, као централне јединице полиције, постоји и више подручних јединица чијим радом би се координирало из Одељења. Постојање јединица/одсека у оквиру појединих полицијских управа омогућило би брже и адекватније реаговање, јер би се тиме

[296] Марта 2015. године по одобрењу Министрства унутрашњих послова Републике Србије обављен је стручни интервју у вези са искуствима у борби против кривичних дела из надлежности Одељења са господином др Владимиром Урошевићем, Шефом Одсека за електронски криминал у оквиру Одељења за борбу против високотехнолошког криминала. Одговори Шефа Одсека наведени су у раду по његовом одобрењу.

превазишао проблем просторне удаљености и непознавања терена и локалних прилика (слично решење постоји у Чешкој и Словенији).

У погледу организације послова, у оквиру Одељења постоје два одсека: Одсек за сузбијање криминалитета у области интелектуалне својине и Одсек за сузбијање електронског криминала. Анализа података и информација врши у оквиру оперативне аналитике Управе криминалистичке полиције, а рачунарска форензика, односно оперативна вештачења се поверавају Служби за специјалне истражне методе (у оквиру СБОК-а).

Што се тиче интерних правила поступања у вези са предузимањем оперативних и процесних радњи, постоји Оперативна инструкција за прикупљање и поступање са електронским доказима, усклађена са добром праксом у упоредним решењима. У вези са инструкцијом је израђен Приручник о методологији прикупљања електронских доказа, који је дистрибуиран криминалистичкој полицији подручних полицијских управа.

У функционисању Одељења постоје одређени организациони недостаци, у смислу ограничења ресурса што је последица недостатка посебног оперативног буџета са специјалне потребе Одељења. Наиме, недовољно средстава се намењује за куповину хардверске опреме, продужење лиценци за софтвере, плаћање појединих *online* услуга и слично, што је потребно у конкретним истрагама. Као проблем се јавља и недостатак простора за одлагање електронских доказа и непостојања стандардног формата у ком се докази чувају.

Проблем постоји и у погледу људских ресурса. Квантитативни састав је далеко од задовољавајућег јер је у Одељењу систематизацијом Министарства одређено свега 19 места, што је мали број, а с обзиром на обим задатака из делокруга рада било би потребно минимум још толико лица. Структура запослених (квалитативни састав) није у потпуности одговарајућа. У погледу знања, вештина и искуства за запослење/ распоређење у оквиру Одељења, захтевано је, поред општих услова за рад у државним органима, испуњење следећих услова: завршен факултет из области друштвених наука, искуство у оперативном раду (3-5 година), знање страног језика, познавање рада на рачунару. Стога је неопходно у рад Одељења укључити више лица информатичке струке, и то различитих

профила (односно знања и вештина), но првенствено са знањима из безбедности информационих система.

Ипак, остварује се перманентна обука запослених кроз програме у међународно препознатим центрима за дигиталну форензику. Запослени у Одељењу су сертификовани тренери, а у Управи за образовање при Министарству унутрашњих послова је спроведена обука за 250 припадника Управе криминалистичке полиције и Управе граничне полиције којим су стекли основна знања о поступању са електронским доказима".

Од оснивања, Одељење је поднело више стотина кривичних пријава надлежном тужилаштву за борбу против високотехнолошког криминала у Београду за кривична дела из ове области, а за различите облике кривичних дела која су извршена уз помоћ рачунара, рачунарских система и рачунарских мрежа кривичне пријаве су надлежним тужилаштвима на територији Републике Србије подносиле и друге организационе јединице МУП-а Републике Србије, док је Одељење за борбу против високотехнолошког криминала пружало и стручну помоћ при вршењу истрага везаних за илегалну трговину дрогом, недозвољену трговину, тероризам, убиства и друго[297]. Одељење за високотехнолошки криминал „сарађује са другим линијама рада криминалистичке полиције (Службом за сузбијање криминала, Службом за сузбијање организованог криминала, Службом за специјалне истражне методе, посебно Одсеком за прикупљање и обраду дигиталних доказа) и осталим организационим јединицама полиције"[298], међутим, „Министарство унутрашњих послова Републике Србије такође има и потребу за приснијом и ефикаснијом сарадњом са државним институцијама које се у свом раду сусрећу са високотехнолошким криминалом или се баве истраживањем ове појаве. Поред државних институција са којима Министарство унутрашњих послова има сарадњу, потребно је и укључивање додатних институција које својим ангажовањем могу знатно да допринесу истраживању ове појаве и успостављању ефикаснијег система спречавања кривичних дела из ове области. Посебан проблем је што недостаје ефикасан систем надгледања Интернета у циљу откривања кривичних дела из области високотехнолошког криминала, као и ефикасна платформа за пријављивање ових

[297] Урошевић, Ивановић, Уљанов, *op.cit*, 88.
[298] *Ibidem*, 84.

кривичних дела у *online* окружењу“[299]. У том смислу значајно би било да се у Републици Србији формира национални тим за информациону безбедност (*Computer Emergency Response Team: CERT*)[300] чије би успостављање у великој мери допринело ефикаснијем спречавању дела високотехнолошког криминала, бржем и одговорнијем приступу у истраживању ове појаве и обједињеном одговору на изазове и претње које ова појава доноси[301].

Специјализација надлежних државних органа, првенствено полиције и тужилаштва, јесте добро решење[302]. Међутим, на основу свега изнетог, сматрамо да је оправдано постојање специјализоване организационе јединице у полицији на централном нивоу која би била надлежна само за теже облике високотехнолошког криминала (нпр. с обзиром на степен организованости или значај последица конкретног дела), док би откривање других кривичних дела учињених против безбедности рачунарских података/система и дела учињених посредством информационе технологије требало да буде у „редовној“ надлежности криминалистичке полиције у полицијским управама, а чијим радом на случајевима високотехнолошког криминала би се координирало из централне јединице (нарочито у смислу техничке и стручне помоћи и подршке). Осим тога, добро је решење да у оквиру такве централне јединице, или као самостална структура, буде формирана форензичка лабораторија која би пружала техничку подршку, како централној јединици за високотехнолошки криминал, тако и подручним одељењима криминалистичке полиције[303]. Међутим, формирање специјализованих органа, односно организационих јединица само по себи није ефикасно решење уколико то није учињено у оквиру свеобухватне стратегије за супротстављање високотехнолошком криминалу. Специјализована јединица не остварује смисао уколико делује изоловано ван редовног организационог оквира надлежних органа[304]. Зато јесте добро решење да се на националном нивоу створи јединица која би била надлежна за територију државе, али која би, с обзиром на

[299] *Ibidem*, 106.
[300] Нажалост, у Републици Србији још увек не постоји.
[301] Урошевић, Ивановић, Уљанов, *op.cit*, 107.
[302] A. Hoey, „Techno-Cops: Information Technology and Law Enforcement“, *International Journal of Law and Information Technology*, l/1998, 72.
[303] D. Schmitknecht, „Building FBI computer forensics capacity: one lab at a time“, *Digital Investigation* 1/2004, 179.
[304] D. Wall, „Catching cybercriminals: Policing the Internet“, *International Review of Law Computers & Technology* 2/1998, 209.

могуће улоге јединице (обављање задатака не само у погледу дела високотехнолошког криминала) сарађивала са другим организационим јединицама (нпр. за привредни криминал, за заштиту деце, за заштиту интелектуалне својине и слично) у смислу пружања техничке подршке, као и са другим институцијама.

Мишљења смо да ефикасност рада специјализованих јединица у многоме зависи не само од овлашћења утврђених прописима него и од квалитета/квалификованости особља, сарадње са тужилаштвом/судовима и другим органима и институцијама на државном нивоу као и међународне сарадње са надлежним органима других држава. Полазећи од националних прописа (законског основа за формирање јединице и одговарајућих подзаконских аката који уређују место јединице у оквире полиције/тужилаштва), да би специјализована јединица остварила пуни смисао постојања, потребно је да постоје интерна правила која уређују организацију и обављање послова и задатака у оквиру јединице. На основу аналаизе постојећих типова специјализованих јединица као добро решење се показује постојање три секције у оквиру јединице (а које би имале следеће задатке: истрага, анализа података и дигитална форензика) као и да буде обезбеђене одговарајуће особље (квалификовано за обављање задатака из делокруга рада јединице) и инфраструктура (потребан простор, те хардвер и софтвер адекватан за потребе форензичке обраде рачунарских система, односно прикупљања, обраде и анализе електронских доказа).

Трећи део
ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Супротстављање високотехнолошком криминалу применом прописа кривичног материјалног и процесног права остварује се тако што се у кривичном поступку применом радњи предвиђених у закону који уређује кривичну процедуру утврђује да је одређено лице извршило кривично дело предвиђено кривичним законом. Значај доказа у кривичном поступку произлази из тога што се путем доказивања утврђују и разјашњавају чињенице које чине садржину кривичне ствари и основ свих судских одулука у кривичном поступку[305]. Да би кривично право остварило своју заштитну функцију, дакле, потребно је у кривичном поступку употребити доказе.

У теорији кривичног процесног права се проблему ***појмовног одређења доказа*** приступа са различитих становишта. Већина дефиниција се заснива на одређивању појма доказа у материјалном смислу, но, постоје и процесни појмови доказа. *Доказ у материјалном смислу* је сваки доказни основ или разлог садржан у одређеном доказном средству који говори о истинитости неке чињенице важне за поступак[306]. Дакле, доказни основ је садржан у доказном средству и служи за утврђивање чињенице која је предмет доказивања, а доказивати значи прикупљати доказне основе. Доказни основи су многобројни, док је број доказних средстава одређен законом. Приликом одређивања појма *доказа у процесном смислу* полази се од кривичнопроцесних одредаба у којима се уопштено или појединачно наводе докази[307], па се под појмом доказа подразумевају процесне радње управљене на то да се утврди истинитост чињеница које су од важности за

[305] В. Бајовић, *О чињеницама и истини у кривичном поступку*, Београд 2015, 70.

[306] Упореди: Т. Васиљевић, *Систем кривичног процесног права СФРЈ*, Београд 1981, 294; Б. Марковић, *Уџбеник кривичног судског поступка Краљевине Југославије*, Београд 1937, 282, V.Bayer, *Jugoslovensko krivično procesno pravo, knjiga druga, Pravo o činjenicama i njihovom utvrđivanju u krivičnom postupku*, Zagreb 1989, 16;. Грубач, *op.cit,* 234. Према томе, предмет доказа су правнорелевантне чињенице које чине садржину кривичне ствари и које се утврђују у кривичном поступку (*thema probandi*), доказни основи (*argumentum probatio*) су чињенице којима се правнорелевантне чињенице утврђују (којима се утврђује предмет доказа), а доказна средства (*media probandi*) су извори из којих се добија доказни основ (Васиљевић, *op.cit,* 301), односно облици у којима су доказни облици садржани (Грубач, *op.cit,* 235).

[307] З. Јекић, *Кривично процесно право*, осмо измењено и допуњено издање, Београд 2003, 235.

судску одлуку. Из овога произлази да је појам доказа у процесном смислу изједначен са доказним поступањем[308]. Доказивање је сложена активност у којој учествује више кривичнопроцесних субјеката, а са циљем расветљавања и решавања кривичне ствари, односно утврђивања правно релевантних чињеница у конкретном кривичном поступку[309].

Узимајући у обзир значај доказа у односу на чињенице које се утврђују, као и субјекте које их утврђују, доказ би се могао одредити као чињеница помоћу које субјект који утврђује чињенице, утврђује постојање или непостојање релевантних и других чињеница на којима темељи одлуку у кривичном поступку. Сами докази представљају резултат извођења одређених радњи регулисаних законом који уређује кривичну процедуру. Другим речима, предузимањем доказних радња се прикупљају и изводе докази ради утврђивања чињеница које имају одређен степен кривичноправне релевантности[310].

У вези са делима високотехнолошког криминала државни органи надлежни да предузимају процесне радње у циљу доказивања да је дело извршено (односно, радње прикупљања и извођења доказа) суочавају се специфичним проблемима у вези са доказима. У овом делу рада пажња је посвећена „електронским“ доказима, посебностима доказних радњи којима се они *прикупљају и изводе* (кроз примену одговарајућег метода или технике прибављања доказа) и потреби њиховог прилагођавања специфичностима дела високотехнолошког криминала.

---

[308] Бејатовић, *op.cit*, 274.

[309] Могуће је разликовати доказивање у логичном смислу (одвија се у складу са законитостима логике) и доказивање у процесном смислу (одвија се у складу са правилима предвиђеним у процесном закону). Доказивање у процесном смислу састоји се из више међусобно повезаних активности: откривање (активност кривичнопроцесних субјеката усмерену ка проналажењу извора доказа), извођење -прихватање откривених извора доказа и процесно уобличавање на законом одређен начин, проверавање - испитивање веродостојности доказног средства и самог доказа, што се врши у случају сумње, а извођењем других доказа, и оцена доказа - одређивање вредности откривених и изведених доказа у односу на предмет чињеница које су предмет доказивања. (Бејатовић, *op.cit,* 280). Доказне радње се стога могу одредити као радње прикупљања или извођења доказа које се предузимају са циљем да код органа поступка формирају уверење о постојању или непостојању чињеница које су предмет доказивања (Бркић, *op.cit,* 285). Код сваког доказа могу се уочити активност која је правно регулисана одредбама кривичног процесног права, затим постоје правила криминалистичке тактике, као и активност која се састоји у оцени доказа која је у савременим правима ослобођена свих формалних доказних правила (Јекић, *op.cit,* 235).

[310] Радње доказивања су радње које суд предузима да би формирао своје убеђење о постојању или непостојању чињеница које могу бити од утицаја на његову одлуку (Марковић, *op.cit,* 281).

1. ЕЛЕКТРОНСКИ ДОКАЗИ

Савремено друштво се све више ослања на дигиталне изворе информација и рачунарске системе и мреже у којима се складиште, обрађују и преносе рачунарски подаци, што за последицу има даљи развој друштва у правцу унапређења коришћених технологија и повећања обима података. Развој Интернета и скоро неограничене могућности његове употребе са собом носе потенцијал проналаска трагова о активностима корисника на Интернет страницама, социјалним мрежама и бројним каналима комуникације, а тај скуп се квалитативно и квантитативно повећава са развојем концепта „рачунарство у облаку“ (*cloud computing*) у оквиру ког су апликације и подаци ускладиштени у серверима који се налазе на територији више држава. Експоненцијално повећање употребе технологије у свакодневном животу је историјски преседан у развоју друштва. Међутим, масовна употреба дигиталних уређаја и савремених облика информационе технологије као последицу је створила модификовање начин извршења радњи „традиционалних“ кривичних дела, а са повећаним учешћем измењених „традиционалних“ и по карактеру потпуно нових облика недозвољених активности, као неопходност настала је потреба за коришћењем нових начина за доказивање ових облика кривичних дела. У вези са делима високотехнолошког криминала у теорији се помињу „***електронски докази“*** као својеврсни резултат примене тих нових начина за доказивање. У овом поглављу настојаћемо да кроз разоткривање суштине и специфичности „електронског доказа“ утврдимо да ли се ради о посебној врсти доказа и у чему се огледа његов значај.

1.1. Појам и карактеристике електронских доказа

У последњих неколико деценија судови су *препознали електронске записе* генерисане у рачунарима и другим уређајима за електронску обраду података (у облику порука електронске поште, дигиталних фотографија, извода из финансијских трансакција на *ATM* апаратима, текстова у програмима за обраду текстуалних докумената, инстант порука, табела, историје Интернет

претраживача, база података, садржаја меморије рачунара, рачунарских бекапа (*back up*), рачунарских исписа, дигиталних видео и аудио датотека и слично) *као корисне доказе* о извршењу кривичних дела учињених злоупотребом информационих технологија. Рачунари и други уређаји за електронску обраду података пронађени на лицу места, а за које постоји вероватноћа да су повезани за извршењем кривичног дела, обезбеђују се и чувају као и сваки други предмет који је материјални доказ. Истовремено, трагови о извршеном кривичном делу су све више присутни у виртуелним окружењима, а поступање са њима разликује у односу на трагове у физичком свету. Наиме, у рачунарима се ствара, похрањује и преноси велики број података у облику електронских записа и сваки од њих представља *дигитални траг* о одређеним *аутоматским процесима у рачунару* или *о активностима корисника*. Дигитални траг се може означити као низ битова који настају као производ извршавања наредби у рачунару: одређени *input* (наредба) производи у дигиталном систему одређени *output* (резултат) и проузрокује промене у претходном стању, тако што *output* производи похрањене и/или новонастале низове битова и оставља траг о низу догађаја који су довели до њиховог настанка[311]. При томе, наредба може да потиче од корисника али и да буде резултат аутоматских процеса у рачунару. Приликом анализе уоченог дигиталног трага исправно је пратити фазе у процесу електронске обраде података (од наредбе до резултата), како би се дошло до доказа као крајњег резултата тог процеса[312]. Осим тога, кроз неколико суштинских примедаба се може довести у питање подобност „сирових“ електронских записа да буду доказ у кривичном поступку. Наиме, може се десити да електронски записи буду непотпуни, односно да не садрже довољно података за разумевање временског оквира одређеног дигиталног догађаја или да хардвер/софтвер који аутоматски ствара електронске записе пропусти да региструје поједине. Осим тога, електронски записи не могу да буду доказ о идентитету лица која је предузело одређене радње.

[311] J. Barbara, *Handbook of Digital and Multimedia Forensic Evidence*, Springer, Heidelberg-Dordrecht 2008, 128.
[312] J. Roberts, „A Practitioner's Primer on Computer-Generated Evidence“, *The University of Chicago Law Review* 2 /1974, 263.

Дакле, сам по себи *одређени рачунарски податак као својеврсан дигитални траг није сам по себи довољан нити подобан да буде доказ* одређене чињенице. Рачунарски подаци за лаике немају већу, односно никакву сазнајну вредност, *него је анализа рачунарски генерисаног електронског записа, а коју би извршило лице са стручним знањем, нужна*, да би се *дигитални траг могао користити као доказ у кривичном поступку*. Потребно је, наиме, да лице која поседује стручна знања из области информационе технологије пружи објашњења о томе шта се десило унутар рачунарског система и мреже на основу запажених записа о одређеним дигиталним догађајима (нпр. рачунар са *IP* адресом"xxx.yyy.zzz.1234" је покушао да успостави везу са портом 80 или корисник "littlejoe" је приступио директоријуму 3/3/15 у 01.50[313]).

Услед тога, надлежни органи су морали пронаћи начин да се носе са изазовима дигиталних трагова, као скупа електронских комуникација, датотека на рачунару или у другим облицима електронских уређају[314], који могу бити у најразличитијим облицима, од записа у рачунару до оних који се могу пронаћи у мобилним телефонима, који су сами по себи мали рачунари[315], а решење је пронађено у ангажовању лица информатичке струке. Та лица помажу надлежним органима да се по сазнању да је кривично дело учињено употребом информационих технологија, пронађу одговори 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 систем 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 ове 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***.

---

[313] C. Brown, *Computer Evidence: Collection and Preservation*, Charles River Media, Boston 2009, 20.
[314] R. Moore, *Search and seizure of digital evidence*, LFB Scholarly Pub., New York 2005, 66.
[315] О специфичностима прикупљања података из паметних мобилних телефона, више о томе, D. Bennett, „The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations", *Information Security Journal: A Global Perspective* 1/2012, 162–165.

Постоје различите дефиниције електронског, односно дигиталног доказа. Осим одређивања електронског доказа као *информације* која се чува или преноси у бинарном облику а која се може користити као доказ на суду[316], постоје и другачија мишљења. Иако је дигитални доказ мање опипљив од других облика материјалних доказа, ипак се ради о *материјалном доказу*, с обзиром на то да је састављен од магнетних поља и електронских импулса који се могу прикупљати и анализирати уз помоћ специјалних алата и техника[317]. Историјски посматрано, доказна средства као што су документи, фотографије и други записи, без обзира на то у ком су физичком облику, имали су статус исправа. Исправе представљају облик људске мисли која је писаним, графичким, звучним или другим знацима забележен на адекватној подлози[318]. Електронски записи у дигиталном облику у уређајима и опреми за електронску обраду пренос података (као што су рачунари и периферни рачунарски уређаји, рачунарске мреже, мобилни телефони, дигиталне камере, и други преносиви уређаји, укључујући преносиве носиоце меморије (*USB* стикови) као и подаци са Интернета) стога би се могли сматрати *исправама*. У теорији постоје различита становишта у погледу одређивања појма исправе, њихове садржине и квалификације. Могуће је исправу одредити у ужем и у ширем смислу. Под исправом у ужем смислу би се подразумевале писане белешке које садрже одређене податке, разне писане изјаве и саопштења у којима су садржане чињенице које се утврђују у кривичном поступку, као и цртежи и скице из којих се такве чињенице могу разабрати[319]. Осим оваквог схватања, постоји и шире схватање по ком се исправом идентификује са појмом материјалних доказа[320]. У теорији су подељена мишљења и о томе да ли је исправа по својој садржини посебна врста доказног средства (а не само „писмени облик“ другог доказног средства[321]) или просто средство за изражавање других доказних средстава (исправе су само облик у ком се јављају друга доказна средства и само су по форми доказно средство[322]). Заправо, исправа може бити

[316] *International Organisation on Computer Evidence http://www.ioce.org.*
[317] Casey, *Digital evidence and computer crime: forensic science, computers and the Internet*, 10.
[318] М. Шкулић, Т. Бугарски, *Кривично процесно право*, Нови Сад 2015, 299.
[319] Bayer, *op.cit*, 215.
[320] Радуловић, *op.cit*, 204.
[321] Bayer, *op.cit*, 211.
[322] Марковић, *op.cit*, 365; Васиљевић *op.cit*, 368. Исправе су самостално доказно средство искључиво по форми, док по садржини оне просто садрже у себи неко друго доказно средство

„материјални доказ сам по себи, *corpus delicti,* без обзира на садржину, а може се јавити као доказ и својим садржајем, било као самостални доказ (уверење, потврда) или као израз неког другог доказног средства које се јавља само у облику исправе“[323]. Постоји *више врста исправа*, с обзиром на средство изражавања чињеница, па се деле на графичке, фигуративне (слике, цртежи, рељефи), фонографске (садрже звучно регистроване чињенице) и аудиовизуелне (садрже чињенице које се сазнају чулима слуха и вида). Како се, дакле, под исправом подразумевају различити предмети *израђени од човека,* сазнавање садржаја врши се читањем, гледањем, слушањем или на други начин. За сазнавање садржаја исправе понекад није довољно знање органа поступка, него је потребна помоћ стручног лица, уколико је за опажање чињеница неопходна примена стручног знања и техника, у ком случају такве исправе (предмети и ствари) могу да буду предмет вештачења.

Сходно томе, рачунарски подаци као „електронски“ докази се не разликују од „традиционалних“ доказа у облику исправа. Међутим, иако би се „електронски“ докази могли сматртати исправама, потребно је указати на одређене ***специфичности рачунарских података*** (што су у основи):

1. Рачунарски подаци у уређајима и опреми за електронску обраду пренос података нису увек производ људске мисли нити су предмети израђени од човека, него су често резултат аутоматских процеса у уређајима;

2. Могу бити измењени пре, за време или након прикупљања, односно могу бити измењени или уништени и кроз редовне процесе у рачунару, тј. уобичајен рад рачунара: у електронским уређајима се стање меморије константно мења, било по наредби корисника (нпр. “сачувај овај документ“) или аутоматски, кроз функционисање оперативног система (нпр. „алокација простора за одређени програм“), па је због ове карактеристике потребно електронским уређајем руковати на одговарајући начин од тренутка уочавања истог као релевантног за кривични поступак;

3. Веома су непостојани: понекад рачунарски подаци могу бити у меморији уређаја у којој подаци буду избрисани, односно преко њих се пресниме неки

(увиђај, исказ сведока или вештака) или *corpus delicti* (фалсификовани новац и слично). Види С. Кнежевић, *Кривично процесно право, Општи део*, Ниш 2015, 313.

[323] Т. Васиљевић, М. Грубач, Коментар Законика о кривичном поступку, Београд 2011, 299.

други подаци сваки пут кад се одређени догађај деси, а то може бити: престанак електричног напајања или аутоматско преснимавање старих информација (да би се створио простор у меморији за чување нових информација), па је зато потребно уређаје у којима се налазе потенцијални електронски докази сачувати на одговарајући начин што је пре могуће;

4. Невидљиви су за нестручна лица: могу се пронаћи на местима на којима би само стручно лице тражило или која су доступна само употребом специјалних алата – као што електронски микроскоп са скенером омогућава ентомологу да уочи кључне морфолошке одлике ларве, тако постоје и специфични алати којом стручно лице прегледа и анализира податке на рачунару;

5. Значење електронских доказа може објаснити само стручно лице: рачунасрки подаци пронађени у рачунару могу бити од мале, односно готово ни од какве користи за лаика који није у могућности да издвоји податке на начин да релевантна информација буде целовита и да њом није манипулисано нити да је измењена[324];

6. Могу се умножавати (бити копирани) без икаквих ограничења: информација у дигиталном облику се може умножавати неограничено и свака копија је у потпуности идентична оригиналу. На овај начин је могуће створити више у потпуности идентичних копија које могу анализирати више стручњака у исто време, а копија се може представити на суду као оригинал приликом изношења налаза и мишљења вештака;

7. Количина података које се прикупља и анализира је немерљива у односу на било коју другу ситуацију у физичком свету, па се тражење електронског доказа може посматрати као тражење игле у пласту сена[325].

Како год да се рачунарски подаци који се преносе или чувају у рачунарском систему означавају и схватају, сама природа рачунарских података у електронском облику је узрок што је њима далеко лакше манипулисати и изменити их у односу на традиционалне физичке трагове. Из наведеног произлази да дигитални траг може постати дигитални доказ само ако са њиме поступа на

[324] Упореди R. Rockwood, „Shifting burdens and concealing electronic evidence: discovery in the digital era“, *Richmond Journal of Law & Technology* 16/2005, 1-19; Bryant, Bryan, *op.cit*, 13-21.
[325] E. Kenneally, C.Brown, „Risk sensitive digital evidence collection“, *Digital Investigation* 2/ 2005, 105.

одговарајући начин, тј. кроз употребу посебних метода и техника, које изворно потичу из рачунарских наука. Ипак, као и за друге типове *научних доказа*, прикупљање и руковање електронским доказима је веома осетљиво питање, па је на уму потребно имати следеће:

А. Сваки електронски уређај има своје специфичне карактеристике, па се одређне процедуре морају пратити да би се приступило његовој меморији у оквиру које се чувају потенцијални електронски докази. Један од највећих ризика у вези са електронским доказима је њихово ненамерна, односно случајна измена, до чега може доћи уколико уређајем рукује лице које не поседује адекватно знање. У таквој ситуацији може се поставити питање у вези са одређеним изменама електронског доказа и довести у сумњу, односно да ли је у доказима који иду у корист или на штету окривљеног нешто додато или одузето;

Б. Нове технологије се развијају веома брзо, па се тиме јављају нови извори електронских доказа и постоји потреба за константним усаглашавањем процедура и техника које је потребно применити како би се садржају из електронских уређаја приступулио и како би се исти анализирао;

В. Да би стручњак био у могућности да на задовољавајући начин пронађе и анализира електронске доказе, осим одговарајућег знања и вештина, потребно је и да располаже адекватним алатима и да примењује одговарајуће технике и процедуре које морају бити проверљиве и поновљиве, односно да њиховом применом и други стручњаци могу доћи до истих резултата, јер се само на тај начин може обезбедити да откривена информација има доказну вредност;

Г. С обзиром на то да је крајњи циљ да се откривени и анализирани електронски запис употреби као доказ у кривичном поступку, неопходно је да се приликом прикупљања дигиталних трагова поступа у складу са националним прописима и добром криминалистичком праксом, како би они били прихватљиви као доказ на суду. Прихватљивост подразумева најмање три особине: *аутентичност* – мора постојати могућност да се у непосредну везу доведе доказни материјал са конкретним догађајем који се истражује; *потпуност* – мора да казује целу причу а не само одређену перспективу; *поузданост* – не сме да постоји ништа у вези са начином прикупљања и руковања електронским доказима што би изазвало сумњу у аутентичност и истинитост.

Дакле, електронски записи, који могу имати значај доказа у кривичном поступку, непостојани су и лако се могу изменити или изгубити, уколико се са предметима који су њихови носиоци не поступа на адекватан начин, односно ако се одређене мере предострожности не поштују. Примера ради, уколико необучен службеник полиције приликом увиђаја и одузимања предмета укључен рачунар искључи пре него што га пошаље у лабораторију на форензичку обраду, уместо да је поступио у складу са принципима добре праксе, такво његово поступање може трајно угрозити потенцијалне електронске доказе садржане у рачунару. Из тога разлога је било ***нужно створити одређена правила*** којих је потребно придржавати се приликом руковања таквим подацима на начин да се континуирани интегритет (непрекидна целовитост) информација може одржати и доказати. Истраживање конкретног случаја је веома комплексно и да би било извршено на исправан начин, потребно је да се ***примене специфични алати, технике и методе***, који се разликују од оних које се користе у физичком свету приликом истраживања традиционалних кривичних дела. Окружење је техничко, алати и методи који се користе су технички и захтева се примена техничких знања како би се решио случај уз поштовање одговарајућих проверених научних принципа и правила криминалистичке технике и тактике, који се изучавају у оквиру посебне научне дисциплине (***дигиталне форензике)***[326]. Зато је *нужно* да се лица која предузимају мере првог захвата придржавају правила дигиталне форензике, *корисно* је да приликом предузимања тих радњи и мера на лицу места буде присутно стручно лице, а *неопходно* је да екстраховање, преглед и анализу рачунарских података врши само оно лице које има потребна стручна знања и то применом проверених научних метода и техника.

С обзиром на то су електронски записи веома склони изменама и/или губитку, услед намерне активности корисника или функционисања рачунарског система, сматрамо да не могу сами по себи бити доказ, већ просто траг којој валидност и доказни значај може дати само ***стручно лице које анализира процес електронске обраде података а којом анализом се долази од електронског записа до електронског доказа***. Заправо електронски записи и електронски докази су просто чињенице о којима стручно лице даје налаз и мишљење а који се

[326] Дигитална форензика је предмет Седмог дела рада.

користе као доказ у кривичном поступку. Сматрамо да је настојање да се електронски доказ одреди као посебна врста доказа само последица недовољног разумевања. Електронски доказ није прости електронски запис нити рачунарски податак, па се не може третирати ни као предмет ни као исправа, нити је то пак *неки sui generis* доказ.[327] Једино што се као доказ о извршеном кривичном делу употребом информационе технологије уноси у кривични поступак јесте извештај стручног лица које је прегледало рачунар и анализирало електронске записе применом техника и метода дигиталне форензике, и резултате тог процеса приказао у извештају (који може садржати налаз и/или мишљење). То лице потом у кривичном поступку својим стручним знањем помаже суду у својству вештака у утврђивању и/или оцени чињеница које су предмет доказивања. У том смислу, можемо упоредити електронске записе са ДНК, који је сам по себи невидљив, неопипљив, садржан у одређеном материјалу биолошког порекла, а тек екстраховањем из материјала и стручном анализом, односно вештачењем постаје доказ одређене чињенице у кривичном поступку – а ни у ком смислу се не ради о посебној врсти доказа.

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[328]. 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.

Дакле, 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

[327] Примера ради, мишљења о посебној врсти доказа могу се наћи код следећих аутора: O. Leroux, "Legal Admissibility of Electronic Evidence", *International journal of Law, Computers and Technology* 2/2004, 205; O. Kerr, „Digital Evidence and the New Criminal Procedure", *Columbia Law Review* 1/2005, 300; Б. Бановић, „Електронски докази", *Ревија за криминологију и кривично право* 3/2006, 224; Х. Хамидовић, „Основне карактеристике дигиталних доказа", *Криминалистичко форензичка истраживања* 1/ 2011, 362-372; Т. Лукић, „Дигитални докази", *Зборник радова Правног факултета у Новом Саду* 2/2012, 180.

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

електронских записа, односно да су записи представљени као доказ пред судом ни мање ни више у односу на тренутак 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 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.

На основу свега наведеног, ***електронске доказе*** бисмо могли одредити као рачунарске податке који су похрањени или се преносе у рачунарском систему, рачунарској мрежи или другом уређају и опреми за електронску обраду, пренос и/или складиштење података, а који, након што су прикупљени, обрађени и анализирани у складу са правилима дигиталне форензике а у законском оквиру који уређује правила кривичне процедуре, могу имати значај доказа у кривичном поступку.

2. Извори електронских доказа

Два основна циља откривања и расветљавања сваког кривичног дела јесу идентификовати учиниоца и прикупити релевантне податке и доказе да су се радњом осумњиченог лица стекли битни елементи бића кривичног дела. У погледу утврђивања идентитета лица осумњиченог да је радњу извршења предузело употребом информационих технологија, поставља се питање како довести у везу рачунарски податак (дигитални траг) са виртуелним идентитетом лица на које се податак односи (до ког води дигитални траг) и како повезати виртуелни са стварним идентитетом осумњиченог лица. Рачунарски подаци се могу пронаћи похрањени у рачунарској мрежи или у неком рачунарском систему у поседу осумњиченог, оштећеног или трећег лица (нпр. пружалаца услуга електронских комуникација), или се могу пресрести у току преноса кроз рачунарску мрежу, а услови и начин на који органи поступка могу доћи до

релевантних рачунарских података који могу бити доказ о извршеном кривичном делу, уређени су правилима кривичне процедуре.

Рачунарски подаци који могу бити електронски доказ, дакле, налазе се или ускладиштени у електронским уређајима (рачунарским системима) или се преносе путем рачунарске мреже. Свако лице запослено у државном органу који предузима радње откривања треба да буде свесно да као потенцијалне изворе доказа размотри све уређаје и опрему који могу да функционишу самостално или заједно са или везано за традиционалне рачунарске системе (користе се за побољшање приступа корисника или за проширење функционалности компјутерског система) а који могу бити присутни на лицу места. При томе треба имати у виду да напредак у информационој технологији условљава повећање броја и типова уређаја, који могу да садрже електронске доказе, скоро свакодневно. Када се уређајима и њиховим садржајем правилно рукује и одржава се интегритет рачунарских података, резултирајући електронски докази могу бити најуверљивији доказ и у одређеним околностима пружити информације које могу омогућити реконструкцију специфичног низа догађаја, односно потпуно и истинито утврђено чињенично стање.

Рачунарски подаци су ускладиштени на различитим медијумима, који се разликују по величини и начину употребе, начину складиштења података (на физичком и логичком нивоу) и меморијским капацитетима, што има утицаја на начин прикупљања података и анализу прикупљених података[329]. Следећи списак потенцијалних извора електронских доказа не би требало сматрати коначним – наведени су примери најчешћих извора који се могу срести у пракси. Рачунарски подаци се, спрам извора у којима су садржани, могу поделити на следећи начин:

1. ***Електронски докази који се могу прикупити из рачунарског система***

Рачунарски системи могу бити потенцијални докази, сами по себи, а могу садржати вредне доказе за истрагу било ког кривичног дела (а не само дела високотехнолошког криминала) у виду похрањених рачунарских података, које аутоматски генерише рачунар или их ствара корисник, као што су: текстуални документи, фотографије, сликовни прикази, електронска пошта са додацима, базе података, финансијске информације о кориснику који приступа *online* услугама,

[329] I. Walden, *Computer forensics and the presentation of evidence in criminal cases*, Jewkes, Yar, *op.cit*., 608.

историја посећених Интернет страница, разговори са другим корисницима, подаци о уређајима са којима је рачунар повезан и слично. Рачунарски системи могу бити у различитим облицима (као десктоп рачунари, лаптоп рачунари, торањ рачунари, таблет рачунари, минирачунари или *mainframe* рачунари[330]), састоје се од хардвера и софтвера, који функционишу заједно ради обраде података, а потенцијалне електронске доказе садрже:

а) *основне компоненте* (кућиште, у ком су матична плоча, микропроцесор, хард диск, меморија и везе са другим уређајима[331]);

б) *периферни уређаји* – иако нису интегрални део рачунара, са њиме повезују како би побољшале његову функционалност (примера ради: скенери, штампачи, микрофони, веб-камере, звучници, читачи меморијских картица итд), а такође имају сопствене капацитете за складиштење података који могу бити релевантни за истрагу (нпр. присуство читача картица може бити индиција у истрази клонирања кредитних картица)[332];

---

[330] Више о типовма рачунара, J. Hennessy, D. Patterson, *Computer Architecture: A Quantitative Approach*, Elsevier, Waltham 2011, 11-23.

[331] Више о основним компонентама, М. Хајдуковић, Ж. Живанов, *Архитектура рачунара (преглед принципа и еволуције)*, ФТН Издаваштво, Нови Сад 2013, 284-294.

[332] Уређаји за пријем гласовних порука садрже примљене поруке, податке за идентификацију позива, избрисане поруке. Дигиталне камере за снимање фотографија и видео записа у дигиталном облику са у сопственој меморији могу имати ускладиштене снимљене записе. Уређаји за слање факсова скенирају фотографије и текстуалне документе и шаљу их коришћењем телефонске линије и садрже податке о меморисаним и позиваним бројевима других уређаја са којима је остварена комуникација, историју послатих и примљених докумената, време слања и пријема докумената и слично. Штампачи у својој меморији садрже податке о корисницима, датуму и времену штампања, називу документа који су били штампани, док се у меморији скенера чувају документи у дигиталној форми који су настали као резултат скенирања текстуалних и графичких приказа. Модерни копир-апарати садрже податке о копираним документима, а постоје мултифункционални уређаји који комбинују разне функције, нпр. функција копирања, скенирања и слања факсова (а осим тога више ових функција може бити интегрисано у рачунарски систем). Пејџери као уређаји за слање и примање електронских порука у нумеричком и текстуалном формату могу бити користан извор доказа. Уређаји са системом за географско позиционирање (*GPS*) садрже информације о претходним дестинацијама, понуђеним и праћеним рутама, географским координатама... Види, Б. Милојковић, „Деловање полиције у спречавању злоупотребе савремених система за позиционирање и географских информационих система“ у: *Место и улога полиције у превенцији криминалитета - стање, могућности и перспективе, зборник радова*, Београд: Полицијска академија 2002, 501-518; Б. Милојковић, Д. Маринковић, „Системи за глобално позиционирање и њихов значај у откривању и доказивању кривичних дела“, *Наука, безбедност, полиција* 2/2007, 41-59. У меморији дигиталних сатова, који имају функцију пејџера, чувају се дигиталне поруке, могу садржати и додатне податке: именик, календаре, електронску пошту и белешке, а поједини модели имају могућност синхронизације информација са рачунаром. Читачи магнетних трака (односно *credit card skimmers*) користе се за очитавање информација које су сачуване на магнетној траци пластичних картица, па потенцијално могу садржати информације о имаоцу картице које су овим уређајем очитане (датум до ког картица важи, број картице, безбедносни код картице и сл.).Више о томе, види: *COE Electronic evidence guide: A basic guide for police officers, prosecutors and judges,* 2013,

в) *уређаји за складиштење података* - постоје у разним облицима и величинама, а разликују се по начину на који се подаци у њима складиште и чувају. Стога је потребно да лица која разматрају доказни потенцијал података у њима буду свесна њиховог постојања и капацитета складиштења. Најчешће су заступљени *hard дискови* и *solid state дискови* (*SSD*)[333], који су традиционално основни уређаји за складиштење података уграђени у рачунарски систем, *екстерни хард дискови*[334], те *преносиви уређаји за складиштење података*[335]: компакт диск (*Compact Disk:CD*), дигитални видео диск (*Digital Video Disk: DVD*) и блурej диск (*Blu-ray Disks: BD*). Иако изгледају веома слично, њихови капацитети за складиштење и начин складиштења се у великој мери разликују. Такође, подаци се складиште у *меморијским (flash) картицама* (користе се у многим електронским уређајима, као што су дигиталне камере, мобилни телефони, лаптоп рачунари, конзуле за видео игрице... а како за чување података није потребно електрично напајање, јављају се у разним облицима и величинама и лако се могу сакрити) и *USB уређаји за складиштење података* (*Universal Serial Bus:USB,* који се заснивају на стандарду који дефинише протокол за комуникацију, конекцију и извор напајања за уређаје који се повезују са рачунаром, а јављају се у великом броју облика, величина и капацитета за складиштење података[336]).

2. *Електронски докази који се могу прикупити из других електронских уређаја за аутоматску обраду, пренос и складиштење података*

Велики је број уређаја који могу садржати дигиталне доказе, а поменућемо оне који се најчешће користе.

---

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/2467_EEG_v18_short.pdf (у даљем тексту: *COE* водич), 16-26.

[333] *SSD* чувају податке на другачији начин у односу на првопоменуте (употребом микрочипова који немају покретне делове као хард дискови и због тога постоји мања вероватноћа за оштећење услед ударца а пружају и бржи приступ подацима).

[334] Екстерни хард дискови према подацима доступним у време писања рада, могу имати меморијски капацитет и по неколико терабајтова.

[335] Могући изазови у вези са екстерним дисковима су следећи: основна функција складиштења података је у појединим случајевима неопходна за функционисање, па се као проблематично може показати њихово одношење са лица места, а с друге стране, обрада на лицу места може бити отежана, чак немогућа с обзиром на њихов велики меморијски капацитет.

[336] Наведено према: M. Cross, D. L. Shinder, *Scene of the Cybercrime*, Syngress, Burlington 2008, 125-135.

а) *Мобилни телефони:* Време када је мобилни телефон једноставно био уређај за обављање телефонских разговора је прошлост, јер се данас користе за обављање многих других задатака, као што су слање и примање текстуалних или мултимедијалних порука, приступ Интернету и преглед електронске поште, комуникацију посредством *bluetooth* функције и обављање пословних активности и друго. Заправо, модерни мобилни телефони су прави мали рачунари. Важно је имати на уму да различити телефони имају различите могућности и оперативне системе који често захтевају специјализовану опрему за ефикасно издвајање информација, уз одржавање интегритета доказа;

б) *Уређаји за снимање аудио и аудио-видео записа:* Користе се за прављење аудио записа, фотографија или видео записа који могу бити похрањени у интегрисаним меморијским картицама или хард-дисковима а садрже и *USB* портове преко којих се садржај може преносити на рачунар;

в) *CCTV камере* (*Closed Circuit Television*): користе их компаније, државни органи, појединци за обезбеђење и надгледање активности у одређеном простору;

г) *Преносиви уређаји за репродуковање аудио и аудиовизуелних записа* (*Moving Picture Expert Group Audio Layer 3: MP3 players*): Служе за складиштење и репродуковање музике и других аудио и видео записа у различитим форматима, као и фотографија, документа и других података који се могу чувати у дигиталном облику у интегрисаној меморији или су повезани са преносивим уређајима за складиштење података;

д) *Конзоле за видео игрице*: веома су технички узнапредовале у односу на моделе из раних 1970-их и не треба их игнорисати јер могу садржати значајне информације, или у интегрисаној меморији или су повезани са преносивим уређајима за складиштење података што омогућава корисницима не само да играју видео игрице него и да приступају интернет страницама, да преузимају, складиште и гледају видео записе, фотографије, музику[337].

3. *Електронски докази који се могу прикупити из рачунарских мрежа*

Рачунарске мреже представљају конекцију два или више рачунара који су повезани кабловима за пренос података или бежично, тако да овако умрежени рачунари размењују податке и друге ресурсе између њих. Осим у самој

[337] S.Wang, „Measures of retaining digital evidence to prosecute computer-based cyber-crimes“, *Computer Standards & Interfaces* 29/2007, 218.

рачунарској мрежи, потенцијални докази налазе се и у другим хардверским компонентама, које омогућавају остваривање активности потребних за функционисање мреже[338]. Рачунарске мреже се јављају у разним облицима[339], а од изузетне важности је пажњу посветити Интернету као глобалној рачунарскј мрежи, која повезује рачунаре широм света путем одређених уређаја и протокола. Наиме, сваком рачунару се додељује одређена *IP (Internet Protocol)* адреса[340] што је основна „путања“ за слање пакета информација доступних на Интернету, при

[338] Потребно је на овом месту дати објашњење појединих појмова у вези са рачунарском мрежом: *Port* је крајња тачка у каналу мрежне комуникације и њихови бројеви омогућавају да више апликација на једном рачунару користе мрежне изворе; при томе портови нису утичнице у рачунару него су то виртуелне тачке; *Bandwidth* је количина информација која се може пренети преко телефонске линије, кабловске линије и сл.; *Media Access Control (MAC) address* је квази-јединствени идентификациони број који се додељује већини мрежних адаптера, у виду серијског броја, односно картице за мрежни интерфејс (*network interface cards:NIC*); *Network Attached Storage (NAS)* слично екстерном хард диску, с тим што се пружа услуга складиштења података целој мрежа а не појединачном рачунару (као својеврсни webserver); контролор мрежног интерфејса (*Network Interface Controller:NIC*) је матична плоча или картица која се инсталира у рачунар и омогућава му да се повезује на мрежу; *Network Hub* је уређај који повезује више мрежних уређаја тако да функционишу као један сегмент у мрежи; мрежни прекидач *(Network Switch*) је уређај који се користи да се међусобно повеже група мрежних уређаја (садрже интерну базу података о томе које *MAC* адресе користе његови портови и на тај начин могу циљано да прослеђују пакете података у саобраћају тачно одређеном порту); рутер *(Router)* је уређај који одређује тачку у мрежи према којој се пакети података у саобраћају даље упућују (рутери који се користе у домаћинствима у себи имају више функција: служе као мрежни прекидач, *access point, firewall*); сервер (*Server*) је рачунар у мрежи који је тако конфигурисан да буде стално доступан и да пружа информације или услуге (*web server, email server, file server, print server*) другим рачунарима у мрежи; *Firewall* је хардверски уређај или софтверска услуга која се користи да се повећа безбедност рачунарске мреже блокирањем или пропуштањем одређеног саобраћаја у мрежи; *Access Point* је уређај који управља мрежним саобраћајем у бежичним (*WLAN*) на тај начин што ствара мрежу за *WLAN* уређаје и међусобно их повезује. Функцију овог уређаја могу вршити како у ту сврху произведени уређаји, тако и рачунари одређених конфигурацији па и паметни мобилни телефони. Више о томе, *COE* водич, 27-31.

[339] Тако, примера ради, могу се разликовати следеће рачунарске мреже: 1) *Local Area Network (LAN)* – рачунарска мрежа која покрива малу географску област, као што је стан, канцеларија, или група објеката нпр. школа. Ову мрежу карактерише много већа брзина преноса података, покривеност мање локације и недостатак потребе за изнајмљивањем телекомуникационих услуга; 2) *Wide Area Network (WAN)* –рачунарска мрежа која покрива шире географско подручје, односно то је мрежа чије комуникационе везе превазилазе границе једног града, регије или државе, а која користи рутере и јавно доступне комуникационе везе; за разлику од мрежа које покривају мања географска подручја и не користе јавно доступне комуникационе везе, као што су: мрежа коју је креирао индивидуални корисник (*personal area networks:PAN),* мреже које постоје у оквиру универзитетског кампуса (*campus area networks (CANs))* или мрежа које покривају одрђене градове (*metropolitan area networks:MAN).* WAN мрежа која им највећи географски обухват је Интернет. Наведено према: Cross, Shinder, *op.cit*, 191-194. Више о врстама рачунарских мрежа, Kipper, *op.cit*, 4-10.

[340] Адресе додељује *Internet Assigned Numbers Authority* (*IANA*) преко регионалних ентитета и пружалаца Интернет услуга у оквиру њих (*RIPE* за Европу и одређене делове Азије, *APNIC* за Азију и Пацифички регион, *ARIN* за Северну Америку, *LACNIC* за Јужну Америку и *AfriNIC* за Африку), на тај начин што *IANA* обавештава регионалне организације о томе које *IP* адресе су доступне у њиховој „надлежности“, а од њих пружалац Интернет услуга захтева одређени распон *IP* адреса, а потом их дистрибуира међу корисницима, правећи своју мрежу за коју сноси одговорност.

чему не постоје две идентичне *IP* адресе повезане на Интернет у исто време, јер сваки чвор у мрежи мора да буде уникатан како би могао да шаље и прима податке[341]. Дакле, уређај се повезује у глобалну рачунарску мрежу преко *IP* адресе, али је потребно знати да уређај нема једну, заувек додељену адресу (статичке *IP* адресе се додељују одређеним уређајима/корисницима за које је потребно да *IP* адреса буде стално позната), него се уређају сваки пут када се повеже на мрежу додељује друга *IP* адреса (динамичка *IP* адреса). Пружалац услуга електронских комуникација може да идентификује која *IP* адреса је у одређеном тренутку била додељена ком уређају, али је потребно је имати на уму следеће: 1. Додељивање *IP* адреса не врши према лицу, тј. кориснику, него према уређају, 2. Потребно је знати тачно и прецизно време за које се тражи идентификација корисника чијем уређају је додељена *IP* адреса. Осим *IP* адресе, сваки чвор у мрежи има и своје име (*Fully Qualified Domain Name: FQDN*)[342], а *Domain Name System:DNS* је систем који повезује којој *IP* адреси, односно адресама је додељено које *FQDN* име, и обрнуто[343]. Употребом *IP* адреса рачунар се повезује са Интернетом и корисници приступају *World Wide Web (WWW)* који представља систем докумената, односно веб страница (које су хипертекстоване,

[341] Од 1982. био је заступљен систем *IPv4* адреса који се састоје од 4 низа бројева који су раздвојени тачком, при чему сваки низ може да има вредност од 0 до 255 (нпр. 192.168.1.252. Простом математичком операцијом може се утврдити да постоји свега 4.294.967.296 различитих комбинација, односно јединствених *IP* адреса наспрам више милиона рачунара, уређаја и корисника који се повезују на Интернет мрежу. Уопште, број додељених *IP* адреса које су доступне једном пружаоцу Интернет услуга је далеко мањи од броја корисника његових услуга. Дакле, *IPv4* адресе су исцрпљене услед повећања броја корисника рачунара који се укључују у глобалну мрежу. Како се не би ограничио приступ доступним *IP* адресама, развијене су технологије и протоколи за превазилажење проблема ограниченог броја доступних *IP* адреса, од којих је потребно поменути два Интернет протокола: *DHCP* и *IPv6*. Протокол *DHCP* (*Dynamic Host Configuration Protocol*) подразумева следеће: када се уређај повезује на Интернет, захтев се упућује пружаоцу Интернет услуга који му аутоматски додељује *IP* адресу из базена *IP* адреса које су у том тренутку доступне (односно нису додељене другом уређају у том тренутку) и моментом искључења са мреже, та *IP* адреса је поновно доступна и додељује се другом уређају који захтева повезивање на мрежу. Интернет протокол *IP*v6 је нови систем, који се састоји од 8 низова хексадецималних бројева и слова која су раздвојени двотачком (нпр. 2001:0db8:85a3:0042:0000:8a2e:0370:7334), чиме би се омогућило постојање 340,000,000,000,000,000,000,000,000,000,000,000,000 *IP* адреса. Једна од предности оваквог концепта је да би сваки уређај имао уникатну *IP* адресу чиме би се олакшао посао идентификације. Међутим, не постоје начин да регионалне организације за доделу *IP* адреса учине притисак на локалне пружаоце Интернет услуга да пређу на нови систем који при томе још увек није тестиран у погледу безбедносних ризика. Наведено према: E. Casey, *Handbook of Digital Forensics and Investigation*, Academic, Amsterdam-Boston 2010, 441-442.

[342] На пример: http://www.ius.bg.ac.rs/.

[343] Имена домена додељују национални регистри, акредитовани од стране *Internet Corporation for Assigned Names and Numbers: ICANN, http://www.icann.org*

писане *HTML* кодом и груписане у веб сајтове). Веб странице се чувају на рачунарима- серверима који се могу налазити било где у свету, а да би се одређеној веб страници могло приступити, потребно је знати *IP* адресу тог рачунара (чвора у мрежи), односно његово *FQDN* име (за веб странице се назива *Uniform Resource Locator:URL*[344] и садржи протокол који се користи за приступ одређеном извору и ближе одређује чему тачно се приступа на том извору)[345].

Осим *IP* адреса која је значајна за утврђивање везе између корисника и уређаја, податке који могу бити електронски докази садрже и следећи извори: вебсајтови[346] уопште, а нарочито корисни су вебсајтови социјалних мрежа[347], *Webmail* платформе[348], платформе за *online* складиштење података (с обзиром на то да се све већи број апликација заснива на *cloud computing* концепту[349]), *Peer-to-Peer (P2P)* мреже за размену садржаја[350] и слично.

---

[344] На пример: http://www.ius.bg.ac.rs/biblioteka/Default_cir.htm.

[345] C. Easttom, J. Taylor, *Computer Crime, Investigation, and the Law*, Course Technology, Boston 2010, 302-303.

[346] Осим видљивог садржаја вебсајта, користан извор информација је и његов „невидљиви" део. У суштини, ради се о програмском језику који је коришћен за креирање сајта (*HTML, CSS, Javascript* и др.) и о садржају који сервер шаље претраживачу који га интерпретира и део приказује у „видљивом" делу. У овом делу се као потенцијални докази могу прикупити подаци о кориснику/креатору сајта (лозинке, референце о идентитету и сл.), о скривеним пољима, референце о спољним сајтовима који могу бити независни извор доказа. Осим тога помоћу тзв. "*source code*" форензичар може пронаћи доказ да је са одређеног рачунара приступљено одређеном сајту чак и у случају да је корисник рачунара у потпуности избрисао податке о посећеним сајтовима (*Internet History*) преко претраживача на том рачунару. О анализи изворног кода, види C. Li, *Handbook of research on computational forensics, digital crime, and investigation : methods and solutions*, Information Science Reference, New York 2010, 470-496.

[347] Веома корисни подаци могу се пронаћи обраћањем пажње на интерни систем за идентификацију активности корисника социјалних мрежа (основни подаци о кориснику, чланство у групама, фотографије, *likes/dislikes* и сл.) који се у највећем броју случајева поклапа са системом за идентификацију пружалаца Интернет услуга, на који начин се утврђује да су активности на сајту социјалне мреже предузимане са одређеног рачунара. Нпр. *Facebook* користи "*fbid*" (*Facebook ID*) све време (нпр. *URL* за *FB* страницу на којој је одређена фотографија је http://www.facebook.com/photo.php?fbid=389359417758298.). Према томе, свакако да је корисно имати слику екрана (*screenshot*) на којој је приказана одређен *Facebook* профил, али је много поузданије интерни идентификациони број тог профила у *Facebook* бази података.

[348] Већина садржи у додатном заглављу *IP* адресу пошиљаоца мејла послатог преко тог сервиса, но *Gmail*, с друге стране, избегава откривање ове информације, у циљу заштите приватности својих својих корисника, али зато трајно чува копије прилога електронској пошти. Више о прикупљању и анализи података из електронске поште. Easttom, Taylor, *op,cit*, 307-308.

[349] О проблемима прикупљања електронских доказа који су похрањени у *cloud computing* системима види M. Taylor et al., „Digital evidence in cloud computing systems", *Computer Law& security review* 26/2010, 306; S. Mason, E. George, "Digital evidence and 'cloud' computing", *Computer law & security review* 27/2011, 525.

[350] Ради се о систему у ком су индивидуални рачунари повезани тако да сваки може истовремено да буде и сервер и клијент, а омогућава корисницима да претражују и деле датотеке похрањене у повезаним рачунарима, при чему се гарантује анонимност корисника. Наведено према: M. Britz, *Computer Forensics and Cyber Crime: An Introduction*, Prentice Hall, New Jersey 2008, 407. О

Да би знао које информације за потребе истраге да затражи од пружалаца услуга (који на располагању има базен *IP* адреса а које додељује корисницима у одређеном временском оквиру), потребно је да надлежни орган зна шта су *IP* адресе и како се додељују, шта су *DNS* и како се региструју, као и шта све у вези са рачунарском мрежом може представљати потенцијални извор електронских доказа.

4. ***Електронски докази који се могу прикупити од пружалаца услуга електронских комуникација***

Иако је у општој јавности широко заступљено мишљење да су активности на Интернету анонимне (коришћењем псеудонимних и псеудоанонимних података у комуникацији) и да им се не можеући у траг, правна лица која су регистрована за пружање услуга електронских комуникација поседују о корисницима услуга велики број података који се могу употребити за идентификацију лица и тиме као електронски доказ. Ти подаци су разноврсни: од података о спољашњим карактерситикама комуникације (нпр. дужини разговора) до садржаја комуникације која је остварена посредством пружалаца услуга; поједини подаци су ускладиштени у базама података пружалаца услуга на основу уговорног односа са корисником (нпр. подаци о кориснику услуга), док се други преносе кроз рачунарске мреже за време остваривања комуникације[351]. Ради се наиме о подацима о комуникацији (*communication data*), који се могу се поделити у три групе: 1. Подаци о кориснику (*subscriber data*): подаци које је сам корисник открио, као нпр. личне преференције, подаци о адреси електронске поште за потребе инсталирања или издавање рачуна за коришћене услуге, лозинке за приступ и сл. 2. Подаци о оствареном комуникационом саобраћају *(traffic data*): број телефона одлазних и долазих позива, *IP* адресе пошиљаоца и примаоце поруке електронске поште, подаци о инсталираној рачунарској мрежи корисника (нпр. *IP* адреса рутера) и сл. 3. Подаци о коришћењу услуге електронске

форензичкој обради овог типа рачунарских мрежа, више о томе, Li, *op.cit*, 355-379; Taylor et al, *op.cit*, 647-652.

[351] Пружаоци услуга електронских комуникација долазе у посед података из три извора: 1. Подаци које корисници услуга предају приликом заснивања уговорног односа у вези са коришћењем услуга; 2. Подаци које генеришу информационо-комуникациони системи и ресурси које користе приликом пружања услуга; 3. Подаци који се добијају од других правних субјеката, као што су други пружаоци услуга укључени у процес комуникације или субјекти преко којих се врши плаћање за коришћење услуга од стране корисника. Walden, *op.cit*, 612.

комуникације (*usage data*): време и дужина трајања коришћења услуге (нпр. дужина трајања одређене комуникације), подаци о количини података који су преузети или постављени у мрежу (даунлодовани или аплодовани), подаци о повезивању и прекиду везе са рачунарском мрежом, подаци о преусмеравању или прослеђивању услуга, подаци о коришћењу специфичних услуга (као нпр. коришћење услуга складиштења података у облаку) и слично[352]. Осим тога пружаоци услуга складиште и садржај саме комуникације *(content data).* Прикупљање наведених разноврсних података за потребе кривичног поступка је предмет регулисања различитих прописа, у зависности од природе података. Осим тога, једна од карактеристика модерног комуникацијског окружења је да пружаоци услуга електронске комуникације користе алтернативне технологије за приступ и одржавање мреже (*wireline* и *wireless*) а последица тога је да се подаци преносе путем различитих мрежа у власништву или под контролом различитих правних лица[353]. Услед тога, неретко постоји потреба да се подаци прикупљају од више пружалаца који су укључени у остваривање релевантне електронске комуникације.

Из наведеног се може уочити да постоји велики број потенцијалних извора електронских доказа. Да би се дошло до електронских доказа, према њиховим изворима се предузимају одређене специфичне радње доказивања, приликом чега је потребно поступати узимајући у обзир специфичности начина на који се подаци у њима похрањују/преносе, као и природу тих података.

2. СПЕЦИФИЧНЕ РАДЊЕ ЗА ПРИКУПЉАЊЕ ЕЛЕКТРОНСКИХ ДОКАЗА

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

[352] У погледу ових података важно је узети у обзир разлику у временским зонама, а која је релевантна због тога што поједине компоненте рачунарске мреже могу бити лоциране у географски удаљеним местима и тада се користи метод *Co-ordinated Universal Time (Greenwich Mean Time).*

[353] I. Walden, „Communication service providers: Forensic source and investigatory tool“, *Information security technical report* 11/ 2006, 15.

појединца, искоришћавање деце у порнографске сврхе и кршење ауторских права су недозвољене активности које су постојале и пре појаве рачунара и Интернета. Стога постојећи извори кривичног права могу представљати солидну основу за откривање и хватање лица која су извршила кривична дела слична наведеним али у кибер простору, односно доказивање дела високотехнолошкг криминала. Оно што, ипак, 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, у квантитативном и квалитативном смислу, другачији у односу на традиционална кривична дела. Наиме, глобална рачунарска мрежа повезаних рачунарских система, која обухвата целу земаљску куглу, омогућава појединцу да употребом рачунара у једној држави предузме одређене штетне радње са последицама у рачунару у било којој другој држави, докле год постоји одговарајући електронски уређај и Интернет конекција на оба места. Огроман домет и готово потпуна анонимност корисника на Интернету отежава задатак органа гоњења да уђу у траг учиниоцима и открију извор криминалне активности, а у случају да то успеју, границе територијалне надлежности могу да их спрече у прикупљању доказа потребних за изношење оптужбе пред суд. 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[354]. На структурном нивоу, с обзиром на то да се ради о својеврсној глобалној рачунарској мрежи, *сама конфигурација Интернета превазилази границе држава*, док према традиционалним принципима међународног јавног права државе имају надлежност само у оквиру својих суверених граница, па је самим тим и место предузимања радњи и мера надлежних органа за откривање, гоњење и вођење кривичног поступка за дела високотехнолошког криминала ограничено на територију државе. На техничком нивоу, операције у оквиру рачунарских система и мрежа карактерише одређена *непостојаност и брз проток података* који могу бити измењени, премештени, прикривени или избрисани за неколико секунди,

[354] 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.

што у принципу значи да предузимање радњи ради проналажења и обезбеђења дигиталних трагова и дигиталних доказа може бити, најблаже речено, отежано.

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*. За стварање одговарајућег правног оквира за супротављање 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. Сходно томе, *одредбама кривичног процесног права би требало омогућити да се превазиђу одређени изазови у откривању и доказивању дела високотехнолошког криминала*, а који се односе на: решавање ситуације у којој више држава има надлежност над гоњењем, давање одговарајућих овлашћења надлежним органима, задржавање и очување података који могу бити употребљени као доказ, проналажење одговарајућег механизма за пријављивање кривичних дела, координирање радом и разменом информација и података између надлежних органа, декодирање енкрипције и утврђивање идентитета учиниоца и слично[355].

Прописи који уређују кривичну процедуру би, дакле, требало да садрже овлашћења органа гоњења у циљу прикупљања електронских доказа, али је приликом одређивања сврхе и околности под којима се процесна овлашћења могу применити, неопходно водити рачуна о правним принципима домаћег кривичног процесног права, које представља неопходну спону између кривичног дела и

[355] I. Brown, „Communications Data Retention in an Evolving Internet“, *International Journal of Law and Information Technology* 2/2010, 100.

изрицања одређене кривичне санкције од стране суда. У том смислу прописују се одређена овлашћења надлежним органима ради остварења кривичноправног захтева, но у исто време циљ је спречавање примене кривичног закона према лицима за које се утврди да нису учинили претпостављено кривично дело, уз очување претпоставке невиности[356]. *Из тог разлога приликом прописивања овлашћења надлежним органима у вези са откривањем и доказивањем дела високотехнолошког криминала требало би да постоје одређена ограничења, чији је смисао спречавање самовоље у поступању од стране тих органа али и сразмерна примена радњи процесне принуде према лицима за које постоји одређени степен сумње да су учинила кривично дело и предметима (обухватајући и рачунарске податке) за које постоји вероватноћа да могу имати значај доказа (нарочито електронског доказа), имајући у виду потенцијално висок степен интрузивности појединих радњи и мера којима се докази прикупљају*. Како би се постигла неопходна равнотежа између интереса кривичног поступка и интереса (и права) окривљеног и других лица у поступку, релевантни су не само врста радњи које су органи овлашћени да предузму, него и ограничавање обима у прописивању овлашћења и начин остваривања тих овлашћења.

Подаци који се складиште, обрађују и преносе у рачунарским мрежама и системима су непостојани и подложни изменама, а како би се створио основ да се захтева очување ових података, у националном законодавству би било корисно предвидети *могућност експедитивног чувања ускладиштених рачунарских података*. Смисао ове привремене мере је својеврсно "замрзавање података" у циљу спречавања губитка или измена постојећих података који би могли имати значај доказа у кривичном поступку, до добијања судске одлуке на основу које би се једино могао *остварити увид у садржај података*. У ситуацији када је потребно рачунар ком се приступило прегледати, односно остварити увид у то који се подаци у њему налазе, поставља се питање да ли је могуће аналогно применити правила која уређују традиционалне мере процесне принуде према стварима у форми претресања и привременог одузимања физичких предмета. Да би се претражио рачунарски систем, те да би се утврдило присуство података неопходних за кривични поступак, неопходно је утврдити ко, под којим условима

[356] S. Brenner, „Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law“, *Murdoch University Electronic Journal of Law* 2/2001, 40.

и по ком основу је овлашћен да приступи рачунарском систему, те да ли могуће остварити приступ у одређеним хитним случајевима мимо утврђених правила[357]. Полазећи од претпоставке да је неопходно посебно регулисати предузимање радње претресања рачунара и прикупљање података који се у њима похрањени, пажњу је потребно посветити начину уређења следећих питања: јасном утврђивању разлике између претраге аутоматски обрађених података и података које је корисник створио; обавези обавештавања лица које је држалац рачунара о томе да је систем био предмет претресања и који подаци су прибављени у одговарајућем моменту; обиму и условима за претресање рачунарског система који је са рачунаром који је предмет претресања повезан преко рачунарске мреже. Осим што су надлежни органи овлашћени да претраже, односно на одговарајући начин приступе рачунарском систему, односно делу рачунарског система као и уређајима за складиштење података који се налазе на територији државе, уколико је вероватно да се подаци складиштени у другом рачунарском систему или делу система, а који се такође налазе на територији државе и могуће им је приступити, односно који су доступни преко рачунарског система који се предмет претресања, било би корисно размотрити овлашћење надлежних органа да у одређеним случајевима иницијално претресање прошире и на тај други рачунарски систем.

За кривични поступак од значаја су не само подаци ускладиштени у једном рачунарском систему, него и подаци који се генеришу у реалном времену, док сигнал кроз рачунарску мрежу пролази од извора до одредишта комуникације. У погледу прикупљања таквих података, оправдано је разликовати прикупљање у реалном времену података о комуникационом саобраћају и пресретање у реалном времену садржаја комуникација, те сходно томе надлежним органима дати одговарајућа овлашћења да прикупљају или снимају применом техничких средстава на својој територији, односно да наређе пружаоцима услуга електронских комуникација да у оквиру својих техничких могућности прикупљају ове податке. При томе је нужно постојање различитог правног режима у погледу ових врста података.

Што се правног уређења пресретања садржаја комуникација тиче, неопходно је у прописима на *одговарајући начин превазићи неколико дилема*: 1) како је дошло

[357] S. Trepel, "Digital Searches, General Warrants, And The Case For The Courts," *Yale Journal of Law and Technology* 10/2008, 138.

до конвергенције информационих и телекомуникационих технологија, поставља се питање да ли се постојећа овлашћења техничког надзора комуникација могу еквивалентно применити на случај пресретања различитих облика техничких комуникација, као што су комуникације између рачунара[358]; 2) да ли је оправдано, с обзиром на принцип пропорционалности, евентуално проширење могућности одређивања те радње у односу на сва кривична дела која су у кривичним законима одређена као дела против рачунарских система, на дела чије радње су предузете злоупотребом рачунара, или чак на дела за која је у конкретном случају потребно обезбедити доказ у електронском облику[359]; 3) да ли је потребно одредити различите услове за предузимање ове радње у зависности од врсте комуникације (комуникација између рачунара или између појединаца и рачунара) и природе мреже (јавна или приватна) у погледу којих се пресретање одређује; 4) које су то техничке мере које истражни органи морају да користе како би прикупљени подаци били обезбеђени на одговарајући начин; 5) како поставити услове и одредити гаранције о којима треба водити рачуна приликом пресретања како би се постигла одговарајућа равнотежа између права лица, погођених радњом, на приватност и интереса кривичног поступка; 6) код пресретања података о садржају комуникација, да ли предвидети да се мера примењује у односу на одређену комуникацију која се на територији те државе обавља путем рачунарског система или обавезати пружаоце електронских услуга да неселективно задржавају податке о свим комуникацијама за одређени временски период.

У вези са остваривањем поменутих овлашћења надлежних органа, потребно је обавезати одређене субјекте на сарадњу. Најпре се поставља питање, на који начин обавезати лица која имају приступ, односно контролу над рачунарским системом и мрежама у којима су ускладиштени, обрађени или се преносе подаци који могу бити доказ у кривичном поступку да надлежним органима омогуће приступ, односно претраживање тог система или мреже? Како обавезу предаје одређених предмета, а која је предвиђена традиционалним правилима кривичне

[358] W. Murdoch, "Regulation of State Surveillance of the Internet human rights infringement or e-security mechanism?", *International Journal of Electronic Security and Digital Forensics*, 1/ 2007, 44.
[359] J. Cannatacia, J. Mifsud, „The end of the purpose-specification principle in data protection?", *International Review of Law, Computers & Technology* 1/ 2010, 108.

процедуре прилагодити виртуелном окружењу и нематеријалној природи електронских доказа (примера ради, обавезивањем да се штампају подаци или да буду представљени у видљивој и разумљивој форми, а у случају да су подаци енкриптовани, откривањем лозинке и слично). Осим тога, да ли је потребно предвидети могућност издавања својеврсне наредбе за предавање података, као посебног правног основа за омогућавање приступа подацима ускладиштеним у рачунарском систему или уређају за складиштење података. Поставља се питање који би орган био надлежан за доношење такве наредбе и који би се подаци могли тражити, нарочито у вези са поштовањем права појединца на тајност комуникација, односно интереса заштите пословне тајне. У вези са обавезом држаоца рачунара, односно рачунарског система и мреже, поставља се и питање да ли је оправдано обавезати лице које поседује знања о функционисању система који се претражује да са надлежним органима сарађује, пружајући им неопходне информације, нарочито ако се ради о осумњиченом лицу, имајући у виду привилегију од самооптуживања или се пак та обавеза може односити само на администраторе система и друга стручна лица. Исто тако, које то специфичне обавезе могу бити наметнуте операторима јавних и приватних мрежа у смислу употребе неопходних техничких мера ради омогућавања пресретања електронских комуникација од стране истражних органа, односно на који начин обавезати пружаоце услуга електронских комуникација доступних јавности да по наредби истражних органа учине доступним податке потребне ради идентификовања корисника услуге а у погледу којих пружалац има приступ, односно контролу. С последњим у вези се поставља питање, који су то подаци? Неопходно и оправдано је направити разлику између идентификационих података, других података и осетљивих података. Стога нарочиту пажњу треба посветити правилима чија је сврха заштита података о личности, те стандардизовати процедуре и обавезати операторе да податке учине доступним на основу формалних писаних наредби, те избегавати неформално и усмено прикупљање како би се подаци могли користити као доказ. Како се не би компромитовала истрага, исти се могу обавезати да као тајну чувају чињеницу да извршавају те радње по налогу надлежних орагана као и све информације у вези са тим. Такође, битно је предвидети право лица на које се радња односи да у

одговарајућем тренутку буде обавештено у које сврхе и по ком правном основу су се подаци о њему прикупљали.

Као полазна основу за разматрање правног регулисања овлашћења надлежних органа неопходних за истрагу кривичних дела учињених у вези са рачунарским системима и мрежама узета је ***Конвенција о високотехнолошком криминалу***, која у члановима 16-21. уређује следеће радње: хитно чување похрањених рачунарских података (члан 16), хитно чување и делимично откривање података о саобраћају остварених комуникација (члан 17), издавање налога за предају рачунарских података (члан 18), претрес рачунара и рачунарске мреже и одузимања података (члан 19), прикупљање података о саобраћају у реалном времену (члан 20) и пресретање комуникација (члан 21). Изузетно битна одредба садржана је у члану 14. Конвенције који одређује обухват процесних одредаба на тај начин што се наводи да се овлашћења и процедуре примењују на откривање и доказивање како кривичних дела наведених у члановима 2. до 11. Конвенције (кривична дела против поверљивости, целовитости и доступности рачунарских података, рачунарских система и мрежа), тако и свих других кривичних дела која су извршена употребом рачунарског система, као и на прикупљање електронских доказа уопште (за сва кривична дела). На тај начин је постављен широк обухват процесних овлашћења предвиђених у одредбама Конвенције. Овлашћења предвиђена у Конвенцији, од којих су нека посебно иновативна, одговарају различитим циљевима (као што су лоцирање извора и идентификовање учинилаца кривичних дела, те прикупљање доказа) али су сва усмерена ка прикупљању података за потребе конкретне кривичне ствари, те нису проактивна у погледу свог ефекта или обима и не служе стварању „орвелијанског“ система електронског надзора у телекомуникационом окружењу[360]. Конвенција предвиђа могућност да се подаци прикупљају, те обавезује оне који поседују релевантне податке да их учине доступним, односно да их сачувају за потребе вођења истраге, али не садржи захтев нити оправдава свеобухватан и неселективан надзор комуникација појединаца од стране пружалаца услуга електронских комуникација нити државних органа, већ да се радње предузимају само ради откривања конкретног кривичног дела и учиниоца.

[360] M. Singh, „Cybercrime Convention and transborder Criminality“, *Masaryk University Journal of Law and Technology* 1/2007, 58.

У поглављима која следе, анализиране су одредбе Конвенције о високотехнолошком криминалу које уређују специфичне радње за прикупљање електронских доказа, и то: 1. Хитно чување похрањених рачунарских података, 2. Остваривање приступа и увида у садржај похрањених рачунарских података, и 3. Надзор електронских комуникација.

2.1. Хитно чување похрањених рачунарских података

Идентификација осумњиченог у великом броју случајева захтева анализу података о саобраћају, међу којима *IP* адреса може бити од нарочите користи за надлежне органе. Међутим, проблем постоји уколико се релевантни подаци о саобраћају у информационим системима пружалаца услуга електронских комуникација аутоматски бришу након кратког временског периода (нпр. након слања електронске поште или остваривања приступа Интернету). Подаци који су настали током одређеног процеса и који су омогућили остваривање комуникације више нису потребни и уклањају се из капацитета за складиштење података. Да би се надлежним органима омогућило да остваре приступ подацима потребним за идентификацију осумњиченог, неопходно је на одговарајући начин обавезати пружаоце услуга да потребне податке сачувају. У том смислу постоје два приступа: експедитивно чување похрањених рачунарских података у смислу Конвенције о високотехнолошком криминалу и задржавање података о саобраћају (нпр. у смислу Директиве ЕУ 2006/24 о задржавању 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 *похрањени* у оквиру рачунарских система, *нарочито у ситуацијама када постоји опасност да су рачунарски подаци* који би могли бити електронски доказ у конкретној кривичној ствари *посебно осетљиви, у смислу губитка или измене.* Уколико је предвиђено да се обезбеђење података остварује издавањем наредбе 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 деведесет 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 томе, 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 истраге конкретног кривичне ствари, 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 предвиђен законом.

Члан 16. заправо се односи на *привремену меру* која треба да омогући надлежним државним органима да нареде тренутно чување података који се већ налазе ускладиштени у рачунарском систему, као својеврсно „замрзавање“ у неизмењеном облику (*quick freeze procedure*[361]). Ова мера се може односити како на *податке о саобраћају*, тако и *на садржај остварене комуникације*, и може обухватати податке у поседу пружалаца услуга електронских комуникација, али и било ког другог физичког или правног лица. Мера хитног чувања ускладиштених рачунарских података се не односи на неке неодређене, *него на тачно одређене рачунарске податке* који могу бити од користи за конкретан случај, односно употребљени за проналажење и идентификацију осумњиченог, односно као електронски доказ у кривичном поступку. Интегритет потребних рачунарских података иначе може бити обезбеђен и предузимањем неких других радњи и мера, пре свега издавањем налога за предају података (на које се односи члан 18. Конвенције) или претресања рачунара и одузимања података (на које се односи

[361] ITU, *Understanding cybercrime: phenomena , challenges and legal response*, 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, 346.

члан 19. Конвенције), али процедура за предузимање тих радњи често захтева више времена и сложенија је (захтева се пстојање чињеница које чине предузимање радње оправданом, одобрење суда, обавештавање осумњиченог и његова одговарајућа права) у односу на експедитивно чување података које има карактер хитне мере. Дакле, имплементација 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 остваривање приступа садржају тих података*, предузимањем 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. 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. Конвенција), 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 у смислу 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 свим пружаоцима, за које се утврди да је коришћењем њихових услуга 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.

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[362]. Задржавање података о саобраћају односи се на формална обележја електронске комуникације (односно податке о саобраћају) а не и на њихов садржај, и обавезују се само правна лица која су регистрована за пружање услуга у овој области[363]. 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 података је у односу на задржавање података ужег обухвата, јер се односи на чување 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 чување података који ће тек настати. Истовремено, мера хитног чувања податка је у односу на задржавање податка ширег обухвата, 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, јер 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

[362] 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).

[363] Више о задржавању података, Т. Лукић, „Прислушкивање и задржавање телекомуникационих података“, *Правни живот* 9/2011, 840; Т. Бугарски, *Доказне радње у кривичном поступку*, друго измењено издање, Нови Сад 2014, 50-56.

принцип пропорционалности (у вези са истраживањем тешких кривичних дела). У погледу пружалаца услуга електронских комуникација, мера хитног чувања похрањених података је економски повољнија, јер се од њих не очекује да задржавају и чувају неодређени број података неодређеног броја лица за одређени временски период (што са собом носи велике финансијске трошкове у погледу складиштења и обезбеђења интегритета података) него се обавезују само да обезбеде да се подаци за потребе конкретног случаја не обришу аутоматски у кратком временском периоду.

Анализом прописа појединих држава потписница Конвенције, а узимајући у обзир одређене критеријуме, могуће је донети закључак о степену имплементације члана 16. и 17. Конвенције у њиховим законодавствима[364]. 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[365]. 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, но, 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 наређе или на „*други сличан начин обезбеде*“

[364] 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; 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.

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

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 података уколико се циљ може остварити нпр. претресањем рачунара или привременим одузимањем 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[366]; 2. у односу на било које физичко или правно лице[367]; 3. у погледу свих рачунарских података[368]; 4. на експедитиван начин.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

[366] 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, не би се могло констатовати да су на одговарајући начин испуниле обавезу предвиђену у члану 16. Конвенције.

[367] 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, који омогућавају надлежним органима да наређе пружаоцима услуга електронских комуникација 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 већини 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.

[368] 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 имплементирале овај члан.

електронски докази могу обезбедити под наведеним условима и неком другом мером или радњом[369]. 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. Овакво решење је смислено јер се на тај начин обезбеђује хитност поступања, а заштита права осумњиченог се накнадно осигурава потребном одлуком суда ради остваривања приступа садржају сачуваних података[370]. 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 користе, процедура се обично своди на претходно добијање судског 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 тужилац, па и полиција*.

2.2. Остваривање приступа и увида у садржај похрањених рачунарских података

Претходно поменуте мере привременог карактера имају за циљ да се постојећи подаци похрањени у рачунарским системима обезбеде од губитка и/или измена за време које је потребно док надлежни органи добију одобрење за упознавање са садржајем тих података, односно за предузимање одговарајућих радњи којима се остварује приступ и увид у садржај рачунарских података, у складу са прописима који уређује кривичну процедуру, а то су следеће радње: 1) предавање

[369] 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. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[370] *ITU, op.cit.* 246.

похрањених рачунарских података, и 2) претресање рачунара ради проналаска и одузимања похрањених рачунарских података.

2.2.1. Предавање похрањених рачунарских података

Члан 18. Конвенције обавезује државе да предвиде у својим прописима мере којима се надлежни органи овлашћују да наређе:

1. Лицу да преда одређене *рачунарске податке који су у поседу или под контролом* тог лица а који су *похрањени* у рачунарском систему или уређају за складиштење података;
2. Пружаоцу услуга електронских комуникација да преда *податке о кориснику* услуга, а који су у поседу или под контролом пружаоца (подаци о кориснику су подаци у облику рачунарског података или у другом облику које пружалац услуге чува о кориснику, а не подаци о саобраћају/садржају комуникација, као нпр. тип комуникационих услуга које је користио, технички услови и време коришћења услуге; идентификациони подаци корисника, поштанска или географска адреса, број телефона, подаци везани за наплаћивање услуге доступни на основу уговора о пружању услуге; као и други подаци о месту на ком је инсталирана опрема за пружање услуге и слично).

На основу овог члана, надлежни органи би требало да буду овлашћени да издају наредбу за предавање постојећих, у рачунарским системима похрањених података (не података који ће настати услед неких будућих комуникација или операција). Тако се лица која су била обавезана на хитно чување података, овом наредбом обавезују да сачуване податке предају надлежним органима. Међутим, наредба за предају података није само везана за члан 16. Конвенције. Ради о општем овлашћењу надлежних органа да захтевају од лица, која у поседу или под контролом држе похрањене рачунарске податке потребне за кривични поступак, да омогуће остваривање увида у садржај тих података. Ова радња је осмишљена као мање интрузивно средство за добијање података у односу на претрес и одузимање рачунара. Наиме, уколико би лице поступило по таквој наредби, надлежни органи не би имали потребе да одузимају хардвер на ком су подаци

похрањени (у смислу претреса и одузимања рачунара), што је нарочито значајно у дигиталним истрагама у којима није потребан приступ хардверу[371] нити је могуће одузимање великих информационих система (нпр. у банкама). Осим предавања података, радња из члана 18. Конвенције је релевантна у ситуацији када је надлежним органима потребно да на основу утврђене техничке адресе (нпр. *IP* адресе) идентификују лице које је ту адресу користило у време извршења кривичног дела, јер се наредбом пружаоци услуга обавезују да предају податке о кориснику услуга.

Наредба се може издати лицу које има потребне податке у поседу/под контролом, а под тим се подразумева како ситуација у којој су подаци физички присутни у рачунару, тако и ситуација у којој се подацима може приступити на начин да то лице контролише приступ подацима. Тако би, примера ради, лице било дужно да преда податке које чува *online* посредством удаљеног сервиса са складиштење података, а којима може приступити путем рачунарске мреже (нпр. у налогу на *Gmail.com*). Државама је препуштено да предвиде који надлежни органи су овлашћени за издавање наредбе у погледу појединих врста рачунарских података. Пример ради, полиција може наредити предавање података који су јавно доступни, док би судска наредба била потребна у погледу других врста података, а у складу са принципом пропорционалности и ради заштите гарантованих људских права. Међутим, наредба се ни у ком случају не може издати према окривљеном лицу, јер њега штити привилегија од самооптуживања.

2.2.2. Претресање рачунара ради проналаска и одузимања похрањених рачунарских података

Претресање рачунара и других уређаја за електронску обраду и пренос података још увек заузима централно место међу радњама које надлежни 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

[371] *ITU, op.cit,* 248.

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.

Члан 19. Конвенције 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[372];

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;
- 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.

[372] При тому 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 у складу са националним законодавством постоји довољно вероватноће 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. http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

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.

На основу наведеног, сматрамо да 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. Ако бисмо покушали да направимо аналогију између претреса ради проналаска и одузимање исправе и претреса рачунара ради проналаска електронских доказа (уколико бисмо електронске доказе посматрали само као врсту исправе), уочили бисмо да се ове две ситуације разликују. "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 уз употребу рачунарског уређаја; услед непостојане природе података, а ради очувања интегритета електронских доказа, ствара се клон уређаја, односно копија података још на лицу места пред 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.

2.3. Тајни надзор електронских комуникација

Конвенција у петом поглављу садржи два члана који се односе на обавезу држава да у националним законодавствима предвиде одредбе које омогућавају прикупљање рачунарских података у реалном времену, при чему се члан 20. односи на прикупљање података о саобраћају комуникације а члан 21. на прикупљање података о садржају комуникације, односно на пресретање комуникација. Ради имплементације члана 20, од држава се очекује да на одговарајући начин овласте надлежне органе да прикупљају или снимају у реалном времену применом техничких средстава *податке о саобраћају* одређене комуникације која се остварује употребом рачунарских система и мрежа, док се члан 21. односи на обавезу државе да у вези са *тешким* кривичним делима у складу са националним законодавством предвиди овлашћење надлежних органа да прикупљају или снимају у реалном времену применом техничких средстава *садржај* одређене комуникације која се остварује употребом рачунарских система и мрежа. Ради се, дакле, о прикупљању две врсте података који се преносе посредством рачунарских система и мрежа: података о саобраћају и података о садржају комуникације, а услед дивергенције информационих и комуникационих технологија, ове радње односе се на све видове електронске комуникације (фиксна и мобилна телефонија, електронска пошта, *VoiP* и др). Док Конвенција не дефинише податке о садржају комуникације, подаци о саобраћају су одређени у члану 1. као рачунарски подаци у вези са комуникацијом која се остварује употребом рачунарског система а које систем генерише (извор, одредиште и путања комуникације, време, датум, величина и трајање комуникације као и тип услуге којом је комуникација остварена).

Члан 14. Конвенције који одређује обухват процесних одредаба садржи два изузетка, у погледу радњи из члан 20. и члан 21. Наиме, с обзиром на то да се пресретање комуникација сматра најинтрузивнијом мером, од држава се очекује да примену мере ограниче у складу са принципом пропорционалности на најтежа кривична дела. У многим државама се подаци о саобраћају комуникација и подаци о садржају комуникација различито третирају, међутим, државе у којима се ова два типа података третирају на исти начин могу предвидети да се радња из

члана 20. примењује на одређена тешка кривична дела, докле год то ограничење није уже постављено у односу на ограничења из члана 21. Једна од нелогичности односи се на могућност ограничења овлашћења надлежних органа у погледу пресретања комуникација само на тешка кривична дела. Принцип сразмерности односи се на кривична дела за које је предвиђена казна затвора од најмање неколико година затвора, а што се утврђује у складу са националним законодавством. За кривична дела из чланови 2-11. КВК не предвиђа велику меру казне затвора, па их потенцијално искључује из обухвата процесне радње пресретања комуникација, но, овакво решење је неопходно и оправдано, јер се ипак ради о интрузивним радњама, које у значајној мери могу угрозити тајност комуникација.

Радње из члана 20. и 21. се односе на прикупљање ове две врсте података *у времену у ком се комуникације остварује* (*real time*), а не и на податке о већ оствареној комуникацији који су похрањене у рачунарском систему пружалаца услуга електронских комуникација (на њих се односе радње из члана 18. и 19). Даље, радње се предузимају *само у вези са конкретним комуникацијама* које се остварују (не и на задржавање неодређених података) и то само за потребе кривичног поступка за одређена кривична дела (а не за неодређена кривична дела).

Овлашћења надлежних органа у смислу ова два члана обухватају и могућност да се пружаоци услуга електронских комуникација обавежу да у оквиру техничких могућности омогуће прикупљање или снимање тих података или помогну надлежним органима у прикупљању или снимању података, и да чувају као тајну чињеницу да се примењује ова радња[373].

[373] У том смислу, постоји битно ограничење овлашћења да се пружаоци обавежу да омогуће односно помогну у пресретању комуникације а односи се на њихову тренутну расположивост ресурса – не може се очекивати од пружалаца да прилагођавају техничку или кадровску опремљеност за потребе извршавања обавезе пресретања комуникација. Може се рећи да оваква техничка и организациона неутралност Конвенције представља слабост јер није јасно из ког разлога би провајдеи самоиницијативно улагали у скупа и софистицирана средства потребна за пресретање комуникација, уколико их решење не обавеже на то. Cangemi D., „Procedural Law Provisions of the Council of Europe Convention on Cybercrime“, *International review of law computers & technology* 2/ 2004, 170.

Четврти део

ДОКАЗИВАЊЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ДОМАЋЕМ ПРАВУ

Доказивање у кривичном поступку се одвија предузимањем одређених процесних радњи у складу са основним доказним правилима и доказним начелима утврђеним у пропису који уређује кривичну процедуру. Доказивање у кривичном поступку је у Републици Србији уређено ***Законником о кривичном поступку***[374] (у даљем тексту: ЗКП).

Доказивање као *поступна делатност* суда и странака обухвата неколико *фаза*: предлагање доказа, одлучивање о извођењу доказа, извођење доказа, оцену доказа и образлагање оцене доказа, док су необавезне фазе поступања са доказима прикупљање доказа[375] и проверавање доказа[376]. У погледу *предлагања доказа*, у складу са начелом материјалне истине[377], које је важило у домаћем кривичном процесном праву до ЗКП из 2011, суд је био дужан да истинито и потпуно утврди чињеница које су од важности за доношење законите одлуке, па је сходно томе изводио доказе како по предлогу странака тако и по службеној дужности. Како је ЗКП утврдио да је терет доказивања на тужиоцу, суд по правилу одређује извођење само оних доказа које су странке предложиле[378]. Ипак, с обзиром да егзистира „лимитирано начело материјалне истине“, суд може изузетно да „изађе из оквира доказних предлога странака“[379]. *Одлучивање о извођењу доказа* зависи

[374] Законик о кривичном поступку, „Службени гласник РС“, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014. У даљем тексту: ЗКП.

[375] Осим што постоје доказне радње којим се докази изводе, постоје и доказне радње којим се докази само *прикупљају* (кроз примену одговарајућег метода или технике прибављања доказа) па се након тога приступа извођењу доказа (у ове радње спадају: претресање, привремено одузимање предмета и посебне доказне радње). Бркић, *op.cit,* 305.

[376] Бркић, *op.cit,* 298.

[377] Више о томе, Шкулић, Бугарски, *op.cit,* 131-138.

[378] Суд има рестриктивну и супсидијарну могућност предлагања доказа али само у функцији отклањања противречности или нејасноћа у вези са доказима који су већ изведени по предлогу странака (не и у погледу утврђивања чињеница у погледу којих нису претходно изведени докази). При томе, суд најпре даје налог странци да предложи допунске доказе, а тек уколико странка не поступи по том налогу, а суд процени да је ради свестраног расправљања предмета доказивања неопходно извести допунске доказе, одређује се извођење таквих доказа.

[379] Бркић, *op.cit,* 299.

од фазе поступка[380]. *Извођење доказа* је фаза у којој се доказна средства користе на начин прописан законом са циљем да се утврде чињенице које су предмет доказивања[381]. Што се тиче *оцене доказа*, иако је врше и други процесни субјекти, она се везује за суд, који се руководи начелом слободног судијског уверења током поступка када год утврђује чињенице, као и приликом доношења одлуке којом решава кривичну ствар[382].

Доказивање у кривичном поступку се одвија предузимањем одређених процесних радњи у складу са основним доказним правилима и доказним начелима утврђеним у Законику[383], који разликује две врсте процесних радњи које су доказно релевантне: *опште доказне радње* (начелно примењиве у сваком кривичном поступку без обзира на врсту кривичног дела које је предмет поступка[384]) и *посебне доказне радње*[385] (намењене за откривање и доказивање

[380] У истрази одлуку о извођењу доказа доноси јавни тужилац и предузима доказне радње по сопственој иницијативи, а окривљени и бранилац могу поднети предлог за предузимање одређене доказне радње корист одбране. Уколико јавни тужилац тај предлог одбије или не одлучи у року од 8 дана, окривљени и бранилац могу предлог поднети судији за претходни поступак који може, уколико усвоји предлог, да наложи јавном тужиоцу предузимање доказне радње у одређеном року (међутим, нису предвиђене последице непоступања по таквом налогу). Законик предвиђа установу припремног рочишта (које се обавезно одржава уколико се поступак води за кривична дела за која је прописана казна затвора преко 12 година, док је у осталим случајевима његово одржавање факултативно) на ком се планира ток доказног поступка на главном претресу, у смислу да су странке, бранилац и оштећени образлажу доказе које намеравају да изведу на главном претреду. На главном претресу суд (председник већа) доноси одлуку о извођењу доказа на предлог странака, браниоца и оштећеног, и може у одређеним случајевима доказни предлог ових лица одбити.

[381] У фази истраге доказе изводе како јавни тужилац, тако и полиција . На главном претресу је извођење доказа поверено странкама, док је суд задржао контролну функцију.

[382] Како би се предупредило арбитрерно и волунтаристичко поступање услед слободне оцене доказа, суд је дужан да своје одлуке аргументује. Иако се може говорити о ограничењу начела истине, значај доказивања је утврђен у Законику прописивањем да пресуду, или решење које одговара пресуди, суд може засновати само на чињеницама у чију је извесност уверен (члан 16. став 4).

[383] Законик о кривичном поступку не садржи систем доказних средстава, него садржи одредбе о извођењу доказа појединим доказним средствима, али се из тога не може извести закључак да се, осим доказа о чијем извођењу Законик посебно говори, не могу користити друга доказна средства (Грубач, *op.cit,* 239). Ипак, законодавац је у члану који уређује оцену доказа предвидео једно ограничење, у смислу да се судске одлуке се не могу заснивати на доказима који су, непосредно или посредно, сами по себи или према начину прибављања у супротности са Уставом, Законом, другим законом или општеприхваћеним правилима међународног права и потврђеним међународним уговорима, осим у поступку који се води због прибављања таквих доказа (члан 16. став 1).

[384] То су следеће радње: саслушање окривљеног, испитивање сведока, вештачење, увиђај, реконструкција догађаја, коришћење исправа, узимање узорака, провера рачуна и сумњивих трансакција, привремено одузимање предмета и претресање.

[385] То су следеће радње: тајни надзор комуникација, тајно праћење и снимање, симуловани послови, рачунарско претраживање података, контролисана испорука и прикривени иследник.

одређених посебних кривичних дела, која се иначе тешко или отежано откривају и доказују предузимањем само општих доказних радњи[386]).

У овом поглављу најпре ће бити приказане доказне радње релевантне за доказивање дела високотехнолошког криминала, а потом ће бити анализирина усклађеност одредаба Законика са одредбама Конвенције о високотехнолошком криминалу.

1. ДОКАЗНЕ РАДЊЕ РЕЛЕВАНТНЕ ЗА ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

За прикупљање електронских доказа релевантни су првенствено увиђај, претресање и привремено одузимање предмета, доказивање исправом, вештачење, те тајни надзор комуникација и рачунарско претраживање података.

1.1. Опште доказне радње

1.1.1. Увиђај

Код одређивања појма увиђаја у теорији се углавном полази од законског одређења овог појма. Тако Законик предвиђа да се увиђај предузима када је за *утврђивање* или *разјашњење* неке чињенице у поступку потребно непосредно опажање органа поступка. У теорији се акценат ставља на термин „чулно“ опажање, под тим истичући да се на ради само о опажању чулом вида него и осталих чула[387]. Увиђај, дакле, представља утврђивање релевантних чињеница путем *непосредног чулног опажања* органа који води поступак[388]. Ради се о хитној радњи која не трпи одлагање, па уколико се не предузме одмах, односно у најкраћем могућем року по сазнању да је извршено кривично дело, неће моћи да се предузме или ће то бити знатно отежано.

[386] М. Шкулић, Г. Илић, *Водич за примену новог Законика о кривичном поступку*, Београд 2013, 27.
[387] Марковић, *op.cit*, 347.
[388] Грубач, *op.cit*, 289.

Предмет увиђаја може бити лице, ствар или место. Иако је нарочито значајан увиђај места извршења кривичног дела, јер се на њему могу пронаћи трагови извршења кривичног дела и предмети којима је кривично дело извршено или су настали извршењем кривичног дела (као извори материјалних доказа), предмет увиђаја може бити и свако друго место на ком се могу опазити чињенице важне за кривични поступак[389]. Предмет увиђаја могу бити и ствари, међу којима су и предмети за извршење кривичног дела, на којима је дело извршено или су настали извршењем кривичног дела (*corpora delictorum*)[390].

Увиђај врши орган поступка, а то је, у зависности од фазе поступка увиђај јавни тужилац у фази истраге, суд у фази главног поступка или полиција у предистражном поступку. Орган поступка управља увиђајем, док га фактички спроводе стручна лица форензичке, саобраћајне, медицинске или друге струке, у зависности од конкретне потребе и самог кривичног дела, који заједно са органом поступка представљају увиђајну екипу. Због тога орган поступка мора да располаже потребним знањем из криминалистике које ће му омогућити да управља радом стручних лица и да би могао да постави потребне захтеве у вези са увиђајем[391].

Од свих доказних радњи, законодавац је најмање простора посветио увиђају. Законодавац није ни могао ићи даље, јер се вршење увиђаја врши по законитостима других наука[392]. Но, Законик садржи одређена правна правила која уређују спољашњу страну извођења ове процесне радње[393], односно одредбе којима се регулише регистровање резултата увиђаја, те право присуствивања одређених лица вршењу увиђаја. За вршење увиђаја није потребна никаква формална одлука суда, нити неког другог органа, већ се увиђај предузима по сазнању да је извршено кривично дело, с обзиром на бројне факторе који утичу на изглед лица места[394]. Увиђај се због своје непосредности узима као најпоузданији

[389] Радуловић, *op.cit,* 226.
[390] Грубач, *op.cit,* 290.
[391] Шкулић, Бугарски, *op.cit,* 297.
[392] О општим криминалистичко-тактичким правилима за вршење увиђаја види: Ж. Алексић, М. Шкулић, Криминалистика, Београд 2011, 43-53.
[393] Грубач, *op.cit* , 291.
[394] О извршеном увиђају се саставља записник уз који се прилаже документација која је настала вршењем увиђаја. У записник се морају унети сви подаци прописани Законником, а то су: назив органа поступка, место, дан и час када је предузета радња и када је она завршена, имена и презимена присутних лица и у ком својству присуствују, као и назначење кривичног предмета по

начин утврђивања чињеница и најбољи доказ, што би било тачно уколико се увиђај предузима и чињенице непосредно опажају на главном претресу од свих судија који одлучују у кривичној ствари. Уколико се, пак, увиђај врши ван главног претреса, што је најчешћи случај, његов резултат је посредан и користити се у фомри исправе – записника о резулататима и току увиђаја – као својеврсно сведочанство о туђем опажању. Као такво, резултат увиђаја може имати недостатке као и свако друго доказно средство, чија оцена зависи од слободне оцене доказа коју суд врши[395]. Због тога је од изузетне важности да опажање чињеница обавља плански усмерено од стране непристрасног државног органа, а непосредно од стране квалификованихи стручних лица са потребним знањима и вештинама, а све уз вођење записника и друге процесне гаранције за његову потпуност и тачност.

1.1.2. Претресање и привремено одузимање предмета

Претресање је материјално истраживање над лицима и стварима које се предузима са циљем проналажења трагова кривичног дела или предмета важних за кривични поступка или са циљем хватања окривљеног[396]. Предмет претресања може бити лице или стан и друге просторије[397], као и поједини предмети. Потребно је разликовати претресање стана и других просторија од прегледа места увиђајем, јер се увиђајем утврђују чињенице а претресање има за циљ проналажење и одузимање предмета који могу да послуже као доказ. С тим у вези, претреса се стан (као просторије у којој се трајно или привремено, стално или повремено борави или може да се борави) и са станом повезане просторије,

ком се увиђај предузима. У записник је потребно унети ток и садржину самог увиђаја, а уз записник прилажити предмети, скице, цртежи, планови, филмски или други технички снимци, фото документација и сав други материјал који је настао вршењем увиђаја.

[395] Грубач, *op.cit* 294.

[396] Код претресања, циљ је пронаћи предмет који су као средство послужили за извршење кривичног дела или били намењени том циљу; који су произашли из кривичног дела;који су прибављени кривичним делом; на којима се могу пронаћи трагови извршења кривичног дела, који помажу осветљавања личности учиниоца, његових веза у припремању и извршењу кривичног дела, као и други предмети који могу из извесних разлога бити важни за откривање извршиоца. В. Ђурђић, *Основи криминалистике*, Ниш 2012, 145.

[397] Станови и друге просторије могу припадати окривљеном и другим лицима (па и лицима ослобођеним од дужности сведочења).

док се остале просторије прегледају по правилима која важе за увиђај, јер Устав пружа само гаранцију неповредивости стана[398].

Законско уређење претресања обухвата: а) основне одредбе (чл. 152. до 154), б) претресање на основу наредбе (чл. 155. до 157) и в) претресање без наредбе (чл. 158. до 160).

Претресање се може вршити у било којој фази поступка. Но, основ за **претресање** је вероватноћа (не пуно уверење или основана сумња), тј. нешто више од простог, ничим непоткрепљеног очекивања да ће се постићи циљеви наведени у Законику. Вероватноћа је степен уверености о постојању чињеница који је јачи од степена уверења потребног за отварање истраге[399] - када постоје основи сумње, јавни тужилац доноси наредбу о спровођењу истраге, међутим, не може се предузети претресање да би се пронашли основи сумње - вероватноћи да ће се претресањем постићи одређени резултати мора да претходи основ сумње - у супротном би се могло претресати свако лице и свако место.

Постојање овакве вероватноће представља материјални услов, док се формални услов огледа у потреби постојања одлуке суда (правило је да се претресање предузима на основу наредбе суда, с тим да се у законом предвиђеним случајевима може изузетно предузети и без наредбе, но те изузетке би требало уско тумачити, Законик изузетно дозвољава одступање од овог услова). Претресање наређује суд на образложен предлог јавног тужиоца. Полиција, дакле, није овлашћена да се непосредно обраћа суду са захтевом, што значи да би свакако о потреби вршења претресања морала да обавести јавног тужиоца. Поред испуњености овог материјалног услова, неопходно је да јавни тужилац поднесе суду образложени предлог за претресање, у ком би требало означити предмет претресања и навести разлог претресања, што у основи подразумева изношење чињеница које указују на постојање вероватноће. У току истраге под одређеним условима може да дође до претресања и на предлог осумњиченог и његовог браниоца (члан 302). Ако јавни тужилац прихвати предлог одбране, поднеће предлог суду, а у случају да одбије предлог или не одлучи о њему, судија за

[398] Грубач, *op.cit,* 319-320.
[399] Васиљевић, Грубач, *op.cit,* 192.

претходни поступак ће, ако се сагласи с предлогом, донети наредбу о претресању[400].

С обзиром на то да претресање може да предузме орган поступка, ову доказну радњу може предузети и полиција, у складу с овлашћењем полиције да у предистражном поступку по налогу јавног тужиоца или самостално предузме одређене доказне радње (члан 285. став 3. и члан 287) или да у току истраге предузме доказне радње које јој повери јавни тужилац (члан 299. став 4). Јавни тужилац може од полиције да преузме вршење радње коју је она на основу закона самостално предузела, док у другим ситуацијама јавни тужилац може оценити да је и сâмо његово присуство претресању довољно, а да полиција треба да настави с претресањем. Околност да јавни тужилац није предузео претресање и да му, уз то, није ни присуствовао ствара обавезу за орган који је извршио претресање да о томе одмах обавести јавног тужиоца[401].

Законик одређује претпоставке за претресање[402], но, претресању се може приступити и без испуњавања ових претпоставки, уколико се претпоставља оружани отпор или друга врста насиља или ако се очигледно припрема или је отпочело уништавање трагова кривичног дела или предмета важних за поступак (или у фази припремања или извршења, с тим да припремање треба да буде очигледно, што значи да постоји разумно уверење да се припрема уништавање трагова кривичног дела или предмета важних за поступак) или је држалац стана и других просторија недоступан. Како законодавац у члану 152. изричито

[400] Садржај наредбе о претресању је детаљно уређен. Реч је о новини у нашем кривичном поступку чији је *ratio legis* постављање јасних граница у оквиру којих се орган поступка може кретати приликом. У наредби о претресању је потребно навести назив суда који је одредио претресање (тачка 1). Функционално надлежан за доношење наредбе по правилу би био судија за претходни поступак основног или вишег суда, с тим да не би требало искључити ни могућност да се претресање нареди у каснијим фазама поступка. Наредба о претресању би требало јасно да означи предмет претресања, односно да прецизно одредити стан, просторију или лице које треба претрести, као и тражена лица и предмете. Као обавезни елемент наредбе предвиђен је разлог претресања, који се односи на образлагање вероватноће да ће се пронаћи окривљени, трагови кривичног дела или предмети важни за кривични поступак. Поред назива суда који је наредио претресање, у наредби се наводи и назив органа који ће предузети претресање, што је, по правилу бити полиција или јавни тужилац, а након потврђивања оптужнице то би могао да буде и суд. У наредби о претресању се могу навести и други подаци који су од значаја за претресање, што зависи од околности конкретног случаја.

[401] Шкулић, Бугарски, *op.cit*, 310.

[402] Као претпоставке ЗКП предвиђа: предају наредбе држаоцу стана и других просторија или лицу на коме ће се претресање предузети, позивање лица да добровољно преда лице, односно предмете који се траже; те, поучавање лица да има право да узме адвоката, односно браниоца који може присуствовати претресању (уколико држалац или лице захтева присуство адвоката, односно браниоца, почетак претресања ће се одложити до његовог доласка, а најдуже за три часа).

разиликује стан и друге просторије или лице као предмет претресања и уређаје за аутоматску обраду података, а у одредби члана 156. то пропушта да уради (изиричито се помињу само стан и друга просторија или лице), а не предвиђа ни сходну примену ових правила на претресање уређаја и опреме, сматрамо да би требало изричито уредити претпоставке за њихово претресање.

Држалац стана и других просторија позваће се да присуствује претресању, а ако је он одсутан, позваће се да у његово име претресању присуствује неко од пунолетних чланова његовог домаћинства или друго лице. Такође, потребно је да претресању присуствују два пунолетна грађанина као сведоци који се пре почетка претресања упозоравају да пазе на ток претресања, као и да имају право да пре потписивања записника о претресању ставе своје приговоре на веродостојност садржине записника. Може се поставити питање на који начн сведоци, као лаици, могу пратити ток претресања уређаја за аутоматску обраду података с обзиром оно обухвата активностима за које је потребан одређен степен познавања информационе технологије. Из тог разлога сматрамо да би било целисходно предвидети обавезно фотографисање и снимање претресања уколико су предмет претресања уређаји и опрема 152. из став 3 (каква обавеза постоји ако се претресање врши без присуства сведока).

У погледу поступка претресања, Законик предвиђа да се претресање се врши обазриво, уз поштовање достојанства личности и права на интимност и без непотребног ремећења кућног реда, и то, по правилу дању, а ноћу (односно између 22 и 6 часова) само изузетно, ако је дању започето па није довршено или је то одређено наредбом за претресање. О сваком претресању ће се сачинити записник у коме ће се тачно описати предмети и исправе који се одузимају и место на коме су пронађени, а посебно ће се образложити због чега се претресање врши ноћу[403].

Законодавац је предвидео законски основ за предузимање два процесна овлашћења којима се омогућава улазак у стан и претресање без наредбе суда и мимо

[403] . У записник се уносе и примедбе присутних лица, а прилажу му се фотографије и снимци уколико је претресање снимано и фотографисано. Записник о претресању потписују присутна лица, а у случају да лице одбије да потпише записник, то ће се посебно навести. О одузетим предметима ће се сачинити потврда која ће се одмах издати лицу од кога су предмети, односно исправе одузете.

утврђених претпоставки[404]. Чак и да законодавац дозволи претресање уређаја за аутоматску обраду података, поменути основи за претресање без наредбе суда не би били примењиви. Да би се обезбедила судска контрола претресања предузетог без наредбе, предвиђена је обавеза подношења извештаја судији за претходни поступак, који цени да ли су били испуњени услови за претресање. Ову дужност имају јавни тужилац или овлашћена службена лица полиције, а она обухвата како претресање стана и других просторија, тако и претресање лица. Захтев да се извештај поднесе *одмах* по предузетом претресању представља стандард чија испуњеност представља *questio facti*.

Осим тога, предвиђено је да се закључане просторије, намештај или друге ствари отворају силом само ако њихов држалац није присутан или неће добровољно да их отвори или то одбије да учини присутно лице, као и да се приликом отварања избегава непотребно оштећење. Може се поставити питање да ли би се ова одредба могла аналогно примењивати и у односу на уређаје и опрему из члана 152. став 3, уколико су исти „закључани", односно уколико је приступ онемогућен енкрипцијом или применом других техничких средстава. Законик, међутим, садржи обавезу држаоца предмета или присутног лица да омогући приступ и да пружи обавештења потребна за њихову употребу. Од поменуте дужности је изузет окривљени (то је последица забране самооптужења о којој говори члан 68. став 1. тачка 2), као и лице које је искључено (члан 93) или ослобођено од дужности сведочења (члан 94. став 1) или од давања одговора на поједина питања (члан 95. став 2).

> *Одредбом члана 155. став 3. ЗКП прописано је да ће претресање из става 1. овог члана започети најкасније у року од осам дана од дана издавања наредбе. Одредбом члана 152. став 3. ЗКП прописано је да се претресање уређаја за аутоматску обраду података и опреме на којој се чувају или се*

[404] Наиме, прописано је да јавни тужилац или овлашћено службено лице полиције може без судске одлуке ући у стан и друге просторије и без присуства сведока обавити претресање стана и других просторија или лица која се ту затекну, и то: 1) уз сагласност држаоца стана и друге просторије; 2) ако неко зове у помоћ; 3) ради непосредног хапшења учиниоца кривичног дела; 4) ради извршења одлуке суда о притварању или довођењу окривљеног; 5) ради отклањања непосредне и озбиљне опасности за људе или имовину. Ако након уласка у стан и друге просторије није предузето претресање, држаоцу просторија или присутном лицу одмах ће се издати потврда у којој ће се назначити разлог улажења и унети примедбе држаоца или присутног лица. Ако је након уласка у стан и друге просторије предузето претресање, о уласку у просторије и извршеном претресању без наредбе суда и присуства сведока биће сачињен записник у коме ће се назначити разлози уласка и претресања.

могу чувати електронски записи предузима на основу наредбе суда и по потреби уз помоћ стручног лица. Како је одредба члана 155. ЗКП (па и става 3) одредба општег карактера, иста се односи и на претресање уређаја за аутоматску обраду података и опреме, а уколико претресање не отпочне у року од осам дана, мора се прибавити нова наредба[405].

Специфичност претресања уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи јесте у томе да се може предузети само на основу наредбе суда. Приликом претресања наведених ствари орган поступка може имати помоћ стручног лица. До претресања може да дође након привременог одузимања уређаја или опреме (члан 147. став 3), али оно може и да претходи њиховом привременом одузимању (члан 153).

У примени чланова 152. и 155. у вези са чланом 147. ЗКП, који се односе на издавање наредбе за претрес уређаја за аутоматску обраду података (мобилни телефон), у судској пракси је било спорно је да ли мобилни телефони спадају уређаје за аутоматску обраду података, као и да ли судија за претходни поступак треба да изда наредбу за претрес или тужилаштво треба да изда наредбу за вештачење, у случају када је истрага отворена наредбом тужилаштва? Врховни касациони суд је заузео став да се мобилни телефони се могу сматрати уређајима за аутоматску обраду података, у смислу члана 152. став 3. ЗКП, имајући у виду опремљеност мобилних телефона, могућности приступа интернету и размене мејлова и других електронских података а при чему се електронски записи могу чувати у различитим фајловима у самом телефону те по предлогу јавног тужиоца суд може наредити њихово претресање у смислу одредбе члана 155. ЗКП али истовремено, уколико се спроводи истрага, може се наредбом јавног тужиоца одредити вештачење мобилног телефона и његовог садржаја[406].

Приликом претресања ***привремено се одузимају предмети*** који су у вези са сврхом претресања, односно у вези с кривичним делом које представља основ за

[405] Одговори Кривичног одељења Врховног касационог суда на спорна правна питања нижестепених судова са седнице одржане 27.10.2014. године.
[406] Одговор кривичног одељења врховног касационог суда на спорна правна питања нижестепених судова са седнице одржане 04.04.2014. године.

предузимање ове доказне радње[407]. Изричито је наведено да у предмете који се привремено одузимају спадају и уређаји за аутоматску обраду пдатака и уређаји и опрема на којој се чувају или се могу чувати електронски записи (члан 147. став 3). Одлуку о одузимању предмета доноси орган поступка (у зависности од фазе поступка - полиција, јавно тужилаштво или суд).

Законик предвиђа дужност лица која су држаоци тих предмета да органу поступка омогући приступ предметима, пружи обавештења потребна за њихову употребу и да их на захтев органа преда, као и санкцију за непоступање по тој обавези (члан 148). При томе, од дужности да омогући приступ предметима ии да пружи обавештења потребна за њихову употребу није искључен окривљени (ослобођен је само у погледу обавезе предавања предмета), што је у супротности са привилегијом од самооптуживања.

Ипак, законодавац у члановима о привременом одузимању предмета у вези са претресањем, разликује предмете и исправе који се одузимају уколико су у вези са сврхом претресања. Уколико се приликом претресања нађу предмети који нису у непосредној вези са сврхом ове доказне радње, односно с кривичним делом због којег је она предузета (реч је о предметима који представљају случајни налаз), ти предмети се привремено одузимају, под условом да указују на друго кривично дело које се гони по службеној дужности (члан 153. став 3). Треба приметити та се оваквом одредбом не предвиђа могућност да се рачунарски подаци третирају као случајни налаз (јер Законик не наводи могућност одузимања исправа у овим околностима), па се не би могли одузети електронски докази који се не односе на кривично дело поводом ког је радња претресања предузета. С обзиром на природу електронских доказа, било би оправдано предвидети могућност одузимања и исправа у овом члану.Осим тога, Законик предвиђа да предмети, који су приликом претресања привремено одузети, могу бити враћени лицу од којег су одузети, уколико јавни тужилац нађе да нема основа за покретање кривичног поступка или ако престану разлози због којих су предмети привремено одузети, а не постоје разлози за њихово трајно одузимање (члан 153. став 4). Међутим, ова

[407] Иако служе истом процесном циљу, а то је обезбеђење доказа за кривични поступак, потребно је разликовати издавање од узапћења ствари. Издавање је добровољна привремена предаја ствари које се одузимају по кривичном закону или које треба да послуже као доказ у поступку, од стране држалаца ствари а на позив надлежног државног органа.

одредба се не односи и на исправе, самим тим ни на рачунарске податке, па би требало предвидети враћање исправа.

Раније важећи ЗКП садржао је коректну одредбу у члану 85, по којој је *истражни судија,* сам или на предлог јавног тужиоца, могао *наредити* да поштанска, телеграфска и друга предузећа, друштва и лица регистрована за пренос информација *задрже и њему, уз потврду пријема, предају* писма, телеграме и друге пошиљке које су упућене окривљеном или које он шаље, ако постоје околности због којих се са основом може очекивати да ће ове пошиљке послужити као доказ у поступку[408]. По важећем законском решењу заплена писама и других пошиљки реализује се у оквиру посебне доказне радње тајног надзора комуникације, што значи само у погледу одређених кривичних дела и под условима и поступку предвиђеном за ову посебну доказну радњу.

1.1.3. Доказивање исправом

Појам исправе одређује Кривични законик (члан 112. став 26) као сваки предмет који је подобан или одређен да служи као доказ какве чињенице која има значај за правне односе, као и рачунарски податак. На сличан начин то чини и Законик о кривичном поступку (члан 2. став 1. тачка 26) одређујући исправу као сваки предмет или рачунарски податак који је подобан или одређен да служи као доказ чињенице која се утврђује у поступку (члан 83. став 1. и 2).

Поступак доказивања исправом подразумева прикупљање и употребу исправе и оцену доказне снаге исправе. Законик предвиђа да се доказивање исправом врши читањем, гледањем, слушањем или увидом у садржај исправе на други

[408] Васиљевић, Грубач, *op.cit*, 208. Пошиљке је отварао истражни судија у присуству два сведока, а постојала је дужност да се при отварању пази да се не повреде печати, о чему се састављао записник. Ако интереси поступка дозвољавају, садржај пошиљке могао се саопштити у целини или делимично окривљеном, односно лицу коме је упућена, а може му се пошиљка и предати. Ако је окривљени одсутан, пошиљка ће се вратити пошиљаоцу ако се то не противи интересима поступка. Мере се преиспитивала на свака три месеца, а могла је трајати најдуже девет месеци, при чему се *с*провођење мера имало прекинути чим престану разлози за њихову примену. Одредба овог члана није се односила на прислушкивање и тонско снимање телефонских и других разговора, него се такво узапћење могло одредити за свако кривично дело за које се гони по службеној дужности. Јавни тужилац није био овлашћен да нареди задражавање нити су се задржане пошиљке могле њему предати, него је само био овалашћен да упути предлог судији. Битно је истаћи да се мера могла одредити само у погледу пошиљки које иду од окривљеног или ка окривљеном, што је претпостављало да је поступак већ почео а не да се на основу одузетих списа тек треба покренути кривични поступак.

начин. Како је рачунарски податак изједначен за исправом, доказивање оваквом исправом подразумева *увид у садржај на други начин, а то би било могуће само вештачењем*.

До исправа се долази или тако што их суду предају странке или се већ налазе у судским списима (као резултат претходно предузетих процесних радњи)[409]. У случају да је из неког разлога исправу немогуће приложити судском спису, битан садржај исправе се уноси у записник[410].

Пре него што приступи оцени исправе, па и рачунарског податка, као доказа, треба утврдити да ли се уопште може употребити као доказ, па је претходно потребно утврдити: а) ко је аутор исправе; б) одакле су аутору познате чињенице унете у исправу; в) који су субјекти, поред аутора, учествовали у стварању испарев; г) место и време настанка исправе (полазећи од чињенице да време и место настанка исправе могу бити важни елементи за утврђивање чињеница на основу исправе)[411]. Истинитост података садржаних у јавној исправи се претпоставља, јер веродостојност јавне исправе представља обориву претпоставку, за разлику од веродостојности приватних исправа за коју је најпре потребно утврдити аутентичност исправе (другим доказним средствима)[412]. При томе, с обзиром на то да постоји претпоставка аутентичности за јавне исправе, она се испитује само у случају сумње, док се утврђивање аутентичнсти приватне исправе врши у сваком случају[413]. Суд, дакле, мора да утврди аутентичност рачунарског податка као исправе извођењем других доказа (нпр. сведоцима, признањем издаваоца или вештачењем). Што се тиче оцене исправе као доказа, суд је врши по слободном судијском уверењу, а меродаван је њен садржај – како исправа садржи податак о бићу кривичног дела који је утврђен увиђајем, признањем окривљеног, исказом

[409] Грубач, *op.cit,* 293. Исправу по службеној дужности или на предлог странака прибавља орган поступка или подносе странке, по правилу, у оригиналу. Ако је оригинал исправе уништен, нестао или га није могуће прибавити, може се прибавити копија исправе. Орган поступка ће у записник унети садржај исправе и направиће њену копију, а у случају потребе оригинал ће вратити подносиоцу.Уколико лице или државни орган одбије да на захтев органа поступка добровољно преда исправу, поступиће се у складу са одредбама Законика које уређују одузимање предмета.

[410] Бејатовић, *op.cit,* 274.

[411] Bayer, *op.cit,* 218

[412] Исправа коју је у прописаном облику издао државни орган у границама своје надлежности, као и исправа коју је у таквом облику издало лице у вршењу јавног овлашћења које му је поверено законом, доказује веродостојност онога што је у њој садржано, но дозвољено је доказивати да садржај овакве исправе није веродостојан или да исправа није правилно састављена. Кнежевић, *op.cit,* 314.

[413] Грубач, *op.cit,* 294.

сведока ил вештака, суд исправу цени по истим правилима која важе за оцену увиђаја, признања окривљеног, исказа сведока или вештака, но, увек по слободном судијском уверењу[414].

Како исправа представља по својој природи објективније и непристрасније доказно средство у односу на остале, као својеврсни „неми сведок“ кривичног докагађа, „потребно је да се нађу лица који познају њихов језик, како би оне кроз ова лица проговорила“, што за последицу пак има да су „ови неми сведоци објективни, у оној мери у којој су објективна лица која рукују њима“[415], што нарочито важи за рачунарске податке. Стога је за доказивање употребом рачунарских података као исправе потребно остваривање увида у садржај, при чему је од изузетне важности вештачење.

1.1.4. Вештачење

Појава вештачења као доказне радње у кривичном поступку је последица развоја науке и технике и њихове примене у извршењу кривичног дела, те потреби да се лица са стручним знањима укључе у процес утврђувања чињеница у криивчном поступку. С обзиром на то да суд не поседује знања неопходна за расветљавање и решавање кривичне ствари, у појединим случајевимам потребно је ангажовање лица са стручним знањима у одређеним областима науке, струке или заната да помогне у у утврђивању чињеница које се без тог посебног знања не могу утврдити. Када се у кривичном поступку поставе питања од којих зависи доношење одлуке о кривичној ствари а на која судија не може да одговори јер излазе из сфере његовог општег и посебног правног образовања и за које не поседује потребно стручно знање и вештину, ангажују се вештаци.

Вештачење је поступак у коме вештак изводи своје закључке у односу на чињенице из садашњости које је чулно опазио, односно открио захваљујући научним методама којима влада, као и стручним средствима, примењујући своје стручно знање из одређене уже научне области. Суд се не може задовољити стручним испитивањем ствари које је извршено ван кривичног поступка за друге циљеве и тиме заменити вештачење јер је такво испитивање вршено без

[414] Грубач, *op.cit,* 294.
[415] Ч. Стевановић. В. Ђурђић, Кривично процесно право (Општи део), Ниш 2006, 259.

поступања по правилима кривичног поступка. Такође, вештачење извршено ван кривичног поступка у неком другом поступку (грађанском или управном, односно административно-казненом) не може се користити као доказ у кривичном поступку[416].

Вештачење је запажање чињеница важних за поступак или давање мишљења о запаженим чињеницама (односно и једно и друго) уз помоћ стручног знања или вештина одређених лица у оним случајевима када опште знање судије или његова стручна правнма спрема нису довољни[417]. Другим речима, налаз је констатација о постојању или непостојању чињеница, док је мишљење стручни закључако констатованим чињеницама.

Законик о кривичном поступку је детаљно регулисао вештачење као доказну радњу у одредбама чланова 113. до 132[418]. Вештачење се одређује када је за утврђивање или оцену неке чињенице у поступку потребно стручно знање (материјални услов) при чему је изричито наведено да предмет вештачења не могу бити правна питања. Стога чињеница да судија располаже посебним знањем потребним за решавање појединих техничких питања у процесу не искључује потребу вештачења[419].

Бранилац је уложио жалбу на пресуду у чијем образложењу суд као доказ да је окривљени на ДВД снимку наводи да, иако је снимак није баш најбољег квалитета, окривљени препознат од стране суда и заступника оптужбе. Бранилац је према мишљењу другостепеног суда основано указао да је закључак првостепеног суда неприхватљив јер судија не може својим мишљењем да замени мишљење судског вештака одговарајуће струке, с обзиром да не располаже потребним стручним знањем, те да је суд без јасних разлога одбио предлог јавног тужиоца да се у доказном поступку обави вештачење од стране вештака одговарајуће струке. Стога, када је спорно да ли се на ДВД снимку или фотографији види одређено лице или не,

[416] Васиљевић, Грубач, *op.cit*, 266.
[417] Васиљевић, Грубач, *op.cit*, 265.
[418] У првом делу у основним одредбама су предвиђени разлози за вештачење, одређивање вештака, дужност и изузеће од дужности вештачења, одређивање вештачења, наредба о вештачењу, заклетва вештака, налаз и мишљење вештака, а потом следе одредбе којима се уређују посебни случајеви вештачења.
[419] Васиљевић, *op.cit*,.328.

суд нема овлашћење да се упушта у утврђивање чињенице да ли је на снимку баш то лице или неко друго, већ то може оценити само судски вештак[420].

Субјект поступка који може да одреди вештачење је орган поступка, што је зависности од стадијума јавни тужилац у истрази или суд који одређује вештачење у судским фазама поступка, а пре свега на главном претресу, док у предистражном поступку вештачење може одредити и полиција[421]. Орган

---

[420] Решење Апелационог суда у Београду Кж. 1 бр. 3201/13 од 23. 01. 2014. године и решење Вишег суда у Београду К. Бр. 61/11 од 19.12.2012. године.

[421] У вези са одређивањем вештачења од стране полиције, на овом месту бисмо поменили ставове судске праксе у вези са вештачењем које није одредио овлашћени орган (у складу са ранијим законским решењем). *Вештачење извршено по налогу припадника полиције, а не суда, с обзиром на запрећену казну представља вештачење које је извршено супротно одредбама члана 238. став 3. ЗКП, али то представља релативну битну повреду кривичног поступка. Такво поступање није у супротности ни са једном начелном одредбом Законика о кривичном поступку о поступању државних органа у кривичном поступку када постоје основане сумње да је неко лице извршило кривично дело, па је наложено вештачење, са циљем ефикасности и благовременог прикупљања доказа у кривичном поступку. Имајући у виду одредбу члана 18. став 2. ЗКП која прописује да се судске одлуке не могу заснивати на доказима који су сами по себи или према начину прибављања у супротности са одредбама овог Законика, другог закона, Устава Србије или међународног права, Врховни суд је оценио да поступак органа унутрашњих послова не представља злоупотребу датих овлашћења према одредбама ЗКП, која би била на штету оптуженог и кривично правних начела укључујући и ову законску одредбу. Имајући у виду налаза и мишљења МУП-а који је извршио вештачење, спроведено без наредбе истражног судије, али свакако у циљу обезбеђења доказа, такав доказ може постављати само релативну битну повреду одредбе кривичног поступка прописане у члану 368. став 2. ЗКП, која не доводи безусловно до укидања првостепене пресуде, већ се у сваком појединачном случају испитује да ли је таква повреда била од утицаја на законитост и правилност првостепене пресуде. Стога поступањем припадника полиције није учињена повреда одредаба кривичног поступка која је прописана у члану 89. став 10. ЗКП, у члану 205. став 3. ЗКП, у члана 337. став 3. ЗКП или пак 116. став 1. ЗКП, на којим доказима се ни под којим условима не би могла засновати судска одлука, а што је децидирано прописано законом* (Пресуда Врховног суда Србије Кж. 1309/06 од 11. септембра 2006. и пресуда Окружног суда у Јагодини К. 185/05 од 27. јануара 2006. године). *Побијена пресуда донета је уз битну повреду одредаба кривичног поступка, јер је заснована на доказу на коме се не може заснивати. Првостепена пресуда заснована је на записнику о вештачењу Криминалистичко-техничког центра Управе криминалистичке полиције МУП-а Србије које је обављено на захтев МУП-а. Међутим, према одредби члана 238. став 3. ЗКП орган унутрашњих послова не може сам одредити вештачење које не трпи одлагање ако се ради о кривичном делу за које је прописана казна затвора до 10 година, тако да је у овом случају с обзиром на висину запрећене казне за предметно кривично дело вештачење је могао наложити само суд, а не и орган унутрашњих послова* (Решење Врховног суда Србије Кж. 1060/05 од 19. септембра 2005. и пресуда Окружног суда у Крушевцу К. 153/04 од 14. априла 2005. године). Интересантно је образложење решења другостепеног суда поводом жалбе на решење којим издвојена су из списа два вештачења Националног криминалистичко-техничког центра из разлога што вештачења нису обављена по наредби истражног судије. *Наиме, како вештачење није трпело одлагање и одређено је искључиво у сврху утврђивања околности, које су од значаја за постојање самог бића кривичног дела које се окривљенима ставља на терет, ова вештачења се могу користити као доказ у кривичном поступку иако су прибављена без наредбе истражног судије. У прилог оваквом схватању иде и став Европског суда за људска права, према коме радње које у моменту одређивања нису трпеле одлагање и вршене су у преткривичном поступку могу бити одређиване и без наредбе истражног судије, јер је суштина преткривичног поступка у томе да се на главном претресу омогући расправљање о околностима које су од значаја за постојање самог бића кривичног дела које се окривљенима ставља на терет. Дакле, према налажењу Апелационог суда у Београду, предметна*

поступка је субјект овлашћен да одреди вештачење, и то или по предлогу странака и браниоца[422] или по службеној дужности[423].

Уколико је испуњен материјални услов, орган поступка доноси писану наредбу о вештачењу (формални услов). Међутим, Законик предвиђа могућност одређивања вештачења без писане наредбе, уколико постоји опасност од одлагања, али тада постоји обавеза састављања службене белешке[424]. Наредба се може донети у свакој фази кривичног поступка, па и у предистражном поступку, а уколико постоји потреба, вештачење се може поновити или допунити. Од дана достављања наредбе вештаку почиње да тече рок за вештачење који је одређен у наредби, а вештак има неколико права и дужности у складу са Законником[425].

вештачења имају потребне формалне услове за коришћење у кривичном поступку, а да ли ће имати и суштинску доказну снагу зависи од контрадикторног кривичног поступка, односно резултата доказног поступка у којем могу бити оспорена или потврђена (Решење Апелационог суда у Београду Кж2. 3000/11 од 13. септембра 2011. и решење Вишег суда у Београду К. 1875/10 од 7. јула 2011 године).

[422] Када вештачење предложи окривљени и његов бранилац, оштећени као тужилац или приватни тужилац, од ових лица орган поступка може да тражи да се унапред положи новчани износ за трошкове вештачења. Када се вештачење одређује на предлог странака или браниоца, орган поступка може од предлагача да тражи да предложи и лице, односно стручну установу или државни орган коме треба поверити вештачење, као и да постави питања на која вештак треба да одговори.

[423] Стога се *не може се прихватити као доказ вештачење које је прочитано на претресу, а које је суду доставио бранилац оптуженог, јер вештаци нису одређени наредбом суда, нити су упозорени на своје дужности, нити су положили заклетву. Наиме, бранилац оптуженог доставио је суду експертизу Института, коју је суд извео као доказ и у образложењу пресуде навео да је на основу истог, уз остале доказе утврдио чињенично стање. Законом предвиђени услови да експертиза Института представља налаз и мишљење вештака нису испуњени, јер суд није писменом наредбом вештачење поверио овом Институту, а самим тим није одредио ни у погледу којих чињеница вештачење треба обавити (члан 114. ЗКП), аутори експертизе нису разгледали предмет вештачења, нити су испуњени остали услови предвиђени чланом 117. ЗКП, односно вештаци нису упозорени на своје дужности, нити су положили заклетву* (Решење Врховног суда Србије Кж. 2253/05 од 30. јануара 2006. и пресуда Окружног суда у Зрењанину К. 89/05 од 19. септембра 2005. године).

[424] Садржина наредбе утврђена је у члану 118. ЗКП и експлицитно су наведени следећи елементи: 1) назив органа који је наредио вештачење; 2) име и презиме лица које је одређено за вештака, односно назив стручне установе или државног органа коме је поверено вештачење; 3) означење предмета вештачења; 4) питања на која треба одговорити; 5) обавеза да изузете и обезбеђене узорке, трагове и сумњиве материје преда органу поступка; 6) рок за подношење налаза и мишљења; 7) обавезу да налаз и мишљење достави у довољном броју примерака за суд и странке; 8) упозорење да чињенице које је сазнао приликом вештачења представљају тајну; 9) упозорење на последице давања лажног налаза и мишљења. Поред ових елемената, предвиђен и један условни обавезан елемент а то је да се у наредби наведе име и адреса стручног саветника, под условом да га странка има. Потребно је истаћи да се наредба о вештачењу доставља и странкама уколико наредбу доноси суд, како би им се омогућило да упуте своје примедбе или питања у вези са предметом вештачења, као и да им се евентуално омогући да поднесу захтев за изузеће вештака који је одређен у наредби уколико сматрају да постоји неки од разлога за изузеће.

[425] Вештак има следећа права: право да се упозна са предметом вештачења; право да разматра списе и разгледа предмете; право да предложи прикупљање доказа или прибављање предмета који су од важности за давање налаза и мишљења; право да тражи да предложи да се приликом

С обзиром на функцију вештачења (а то је да стручна лица помогну утврђивању одређених чињеница у кривичном поступку) потребно је да орган поступка усмери вештака на одређени правац и одреди оквире вештачења. У техничку страну вештачења орган поступка се не упушта, али се вештаку мора одредити тачан садржај његовог рада и иницијатива се не сме препустити вештаку. У том смилу, сматрамо да су од изузетног значаја одредбе које као обавезне елементе наредбе предвиђа означење предмета вештачења и питања на које треба да да одговор.

Извођење вештачења се врши у складу са одредбама Законика о кривичном поступку и оно обухвата припрему вештачења, само вештачење (које се врши у складу са стандардима одређене струке) и давање исказа вештака[426]. Странке, оштећени и бранилац могу присуствовати испитивању вештака, из чега произлази да не могу присуствовати самом вештачењу. Међутим, мислимо да не постоје правне сметње да се, кад према оцени органа поступка прилике то дозвољавају и оцени као корисно, могло допустити окривљеном да присуствује раду вештака у циљу потпунијег и бржег утврђивања стања ствари[427], а не само приликом

предузимања друге доказне радње (нпр. увиђаја, реконструкције догађаја и друго) разјасне поједине околности или да се лицу које даје изјаву поставе поједина питања; право на накнаду трошкова; право на награду (одређује орган поступка). Основне дужности вештака су да се одазове на позив органа поступка[425] и да да свој налаз и мишљење у року који одреди орган поступка, а који се може из оправданих разлога на захтев самог вештака и продужити. Вештачење које мора да изврши по одлуци органа поступка обухвата обавезу брижљивог разматрања предмета вештачења, тачног навођења свега запаженог и давање мишљења непристрасно и у складу са правилима науке и вештине. Вештак одговара за свој рад, а лажно вештачење представља кривично дело Давање лажног исказа (члан 335. КЗ), на које се упозорава од стране суда. Види, Шкулић, Бугарски, *op.cit*, 286.

[426] По правилу, вештачењем руководи орган који је наредио вештачење и оно се изводи у његовом присуству, а само изузетно ће се вештачење обавити у његовом одсуству, када оно захтева испитивања која дуго трају, уколико се врше у државним органима или установама, као и када то захтевају морални разлози. Руковођење обухвата обавезу органа поступка да се вештаку покажу предмете које ће размотрити, право да вештаку поставља питања и по потреби тражи обајшњења у погледу датог налаза и мишљења. Пре него што приступи самом вештачењу, вештак мора да се упозна са предметом вештачења. Уколико је потребно тражиће од суда да му се достави потребна документација и да му се омогући увид у списе, а све ради свеобухватног сагледавања предметне проблематике и давања потребног налаза и мишљења. Уколико је за потребе вештачења потребно да се анализира нека материја, вештаку ће се ставити на располагање само део те материје уколико је то могуће, док ће се остатак обезбедити у потребној количини, за случај накнадних налаза. Вештачење врши сам вештак и то лично. Он је обавезан да да налаз и мишљење, али и да одговори на постављена питања. Уколико сматра да наука и струка, као и вештине којима располаже, могу да допринесу свестраном разјашњењу предмета вештачења под условом да се истраживања врше у другом правцу у односу на онај који је постављен у наредби, то мора да образложи судији.

[427] Налаз и мишљење се увек подносе у писаној форми када је испитивање предмета вештачења и завршено без присуства органа који је наредио вештачење. Уколико су налаз и мишљење дати

испитивања вештака[428]. Садржину исказа вештака чини налаз и/или мишљење[429]. Без обзира што се вештак може обавезати да да или налаз или мишљење или и једно и друго, налаз и мишљење представљају логичку и фактичку целину: налаз је предмет мишљења и нема мишљења без налаза[430]. Налаз вештака мора да садржи навођење метода и употребљених техничких уређаја којима се служио, а други вештаци који врше ново вештачење, морају бити упознати са ранијим вештачењем.

Наредбом председника већа Вишег суда у Београду одређено да Јединица за специјалне истражне методе МУП-а Републике Србије обави вештачење садржаја долазно – одлазних позива и порука са бројева телефона који су одузети од окривљених Ј.Д.В. и Б.В. Служба за специјалне истражне методе - Одељење за електронски надзор је првостепеном суду доставила извештај о прикупљању података из мобилних телефона и СИМ картица ових окривљених, који извештај је суд извео као доказ на главном претресу и потом га ценио како појединачно тако и у међусобној вези са осталим изведеним доказима и одбраном окривљених. Према наводима захтева за заштиту законитости који је поднео бранилац, недозвољен доказ на коме се пресуда не може заснивати је тумачење првостепеног суда извештаја Управе криминалистичке полиције – Службе за специјалне истражне методе

усмено, уносе се у записник одмах, а орган поступка може одобрити вештаку да у одређеном року поднесе писани налаз и мишљење.

[428] Пример ради, уколико се врши вештачење пословних књига може се поставити питање метода и организовања рада вештака. Могуће је да вештак ради сам без странака и органа поступка а извештај поднесе на крају и предочи странкама на који могу ставити примедбе. Осим тога, било би могуће да вештак након што је прегледао и испитао све што му јхе потребно, даје извештај у записник, а странке и бранилац могу постављати питања. Осим тога, могуће би било да вештак врши преглед пословања окривљеног у његовом присуству, при чему би се могао изјаснити о сваком документу, што је нарочито корисно за разјашњење ствари.

[429] Васиљевић, Грубач, *op.cit,* 275. *Налаз вештака* представља део исказа у ком вештак наводи чињенице које је чулима непосредно спознао, прегледом, односно истраживањем предмета вештачења, а уз примену посебне научне методе у истраживању, као и уз помоћ посебне техничке апаратуре. *Мишљење вештака* представља део исказа у ком вештак даје одговор на питања које је орган поступка поставио у наредби о одређивању вештачења, и то у виду сумирања резултата истраживања експертског истраживања и закључивања. Другим речима, налаз садржи констатацију чињеница важних за поступак, а мишљење стручни суд о констатованим чињеницама.

[430] Радуловић, *op.cit,* 233. Вештак може дати само налаз или само мишљење, а може и једно и друго, што зависи шта орган који наређује вештачење од њега тражи. У оба случаја вештак треба да наведе правила струке и да образложи како је дошао до својих закључака. Налаз и мишљење могу бити у писаној и у усменој форми презентовани органу поступка. По правилу, они се одмах уносе у записник, али постоји могућност да вештак и накнадно поднесе налаз и мишљење у писаној форми, наравно у року који одреди орган поступка.

Одељења за електронски надзор за шта суд није компентентан нити може да зна ко је слао поруке са телефона окривљене Ј.Д.В. нити на шта се ове поруке односе, већ је то требало да утврди стални судски вештак. Међутим, по налажењу Врховног касиционог суда, није у питању тумачење, већ оцена доказа прибављеног одговарајућим вештачењем, па су самим тим наводи захтева браниоца окривљеног Б.В. да се на овом доказу пресуда не може заснивати и да је на штету окривљеног повређен закон из члана 438. став 2. тачка 1. ЗКП, оцењени као неосновани[431].

Вештачење је од изузетног значаја за дела високотехнолошког криминала, што потврђује и судска пракса.

Апелациони суд у Београду је потврдио првостепену одлуку из разлога што је првостепени суд правилно утврдио да је окривљени извршио кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из члана 185. став 4. КЗ-а. Одбрана је тврдила да је тачно да је окривљени са програма Shareaza скидао обичну порнографију, али да није знао да је мрежа затворена и да његова намера није била да скида дечју порнографију, будући да наведен програм аутоматски „вуче“ претходно селектоване фајлове. Међутим, првостепени суд је правилно утврдио да је окривљени преузео и материјал на ком је дечја порнографија (просечан узраст малолетних лица око 12 година) укупног капацитета 6 гигабајта, а да је исти складиштио на хард диску рачунара што је доказано увидом о потврду о одузимању предмета (издатом приликом претреса стана окривљеног) и на основу извештаја о вештачењу МУП РС. Жалбени наводи окривљеног а није имао намеру да „скида“ дечју порнографију и да их је рачунар сам и аутоматски преузео из мреже оповргнути су исказом вештака МУП РС УКП Службе за специјалне истражне методе на основу ког је утврђено да програм скида видео клипове са рачунара других корисника (а да је услов да лице постане косриник ове затворене мреже да и то лице понуди неки порнографски садржај), те да се претрага материјала са злоупотребом деце у конкретном случају вршила претрагом по кључним речима и да не

[431] Пресуда у предмету Кзз 280/2015 од 26.03.2015. године.

постоји могућност да програм сам „гомила“ недозвољен материјал. Из тог разлога је потврђена првостепена пресуда[432].

Одлучујући о жалби против првостепене пресуде побијане због непотпуно утврђеног чињеничног стања Апелациони суд у Београду је утврдио да су пресуда не садржи јасне разлоге о одлучним чињеницама на основу којих је првостепени суд закључио да је скидање материјала порнографске садржине и смештање у меморију рачунара учинио управо окривљени, с обзиром да спорни рачунар користе још три укућана (супруга и двоје малолетно деце), да се у компјутере у кући најбоље разуме син окривљеног. Имајући у виду да је рачунар био доступан већем броју лица, нејасан је закључак првостепеног суда да је окривљени предузео противправне радње које му се стављају на терет. Наиме, то што је у рачунару који припада породици окривљеног пронађен предметни порнографски материјал са малолетним лицима не може по аутоматизму бити доказ да га је прибавио окривљени. Апелациони суд је ценећи одбрану окривљеног, исказе саслушаних сведока и писане доказе, нашао да у конкретном случају нема доказа да је окривљени извршио кривично дело прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију из члана 185. став 4. Кривичног законика, па га је услед недостатка доказа применом одредбе члана 432. тачка 3. ЗКП ослободио оптужбе[433].

У вези са дужношћу вештака да у складу са правилима науке или вештине, савесно, непристрасно и по свом најбољем знању, тачно и потпуно изнесе свој налаз и мишљење, сматрамо да би вештак информационе технологије требало да: прецизно објасни сваки корак у примењеној методологији, односно различите принципе који су довели до сваког појединачног закључка; предсатви извор за сваку чињеничну основу и све радне претпоставке које су довеле до потврђене хипотезе (као и друге чињенице и/или претпоставке које су биле на располагању, али које нису коришћене, као и разлоге зашто су искључени из разматрања); наведе да ли су коришћене методе и хипотезе потврђене и да ли постоји могућност да буду поново тестиране ради валидације резултата; и да наведе који

[432] Пресуда Апелационог суда у Београду Кж По3 8/2015 од 11.06.2015. године.
[433] Пресуда Апелационог суда у Београду Кж По3 5/2014 од 19.02.2014. године.

професионални стандарди су коришћени у поступању са материјалом и да ли је било одступања од уобичајене праксе[434]. Истовремено, потребно је да вештак критички приступи теоријама, приступима, методама и тестирањима које се уобичајено користе ради долажења до налаза и/или мишљења о предмету вештачења[435]. Да се не би поставило питање ко заправо спороводи анализу: стручно лице или софтвер, потребно је обезбедити поновљивост и транспарентност анализе.

Иако се претпоставља да вештак има, а да орган поступка нема одговорајуће стручно знање потребно за утврђивање одређених чињеница у случају да се одреди вештачење, орган поступка (а првенствено судија) не би требало да прихвата некритички и без икакве анализе излагања и закључке вештака, нити да стварну оцену замењује фразом да „прихвата мишљење вештака јер је убедљиво и логично“[436]. Постоје више разлога услед којих суд може да не прихвати мишљење вештака: непотпуност и квалитативни недостаци материјала којим је располагао вештак; одсуствo убедљивих аргумената који би говорили у прилог закључку вештака; недовољна развијеност односне гране стручног знања; недовољнас квалификованост самог вештака; повреда ЗКП у поступку вештачења[437]. Налаз вештака може бити непотпун због тога што није исцрпљен халог органа поступка у смислу шта треба вештачити и на која питања одговорити или због тога што обављене радње показују да су потребна даља испитивања ван оквира првобитног вештачења[438]. Суд оцењује налаз и мишљење као и остале доказе, по свом слободном уверењу, и може исказ вештака да прихвати или не прихвати, јер налаз и мишљење вештака не вежу суд, па се некритичко и аутоматско прихватање не би могло оценити као похвално. Суд може да одбије мишљење вештака и да пресуди потпуно супротно вештаковом мишљењу, ако за своју одлуку нађе

[434] Више о задацима стручњака, Casey, *op.cit*, 48-56.
[435] Barbara, *op.cit*, 121.
[436] Васиљевић, Грубач, *op.cit*, 282-283. Суд је дужан да савесно овени сваки доказ појединачно и у вези са осталим доказима и да на основу такве оцене изведе закључак о томе да ли је нека чињеница утврђена, јер на основу изведених доказа доноси пресуду, односно одлуку којом коначно решава предмет спора. Суд цени налаз и мишљење вештака као и сваки други доказ у кривичном поступку, по слободном судијском уверењу, појединачно и у вези са другим доказима. Суд не мора да прихвати мишљење вештака, може да га одбије и да пресуди потпуно супртоно вештаковом мишљењу.
[437] Бејатовић, *op.cit*, 331.
[438] Васиљевић, Грубач, *op.cit*, 281.

ослонац у другим доказима[439]. У Законику су садржане одредбе како суд треба да поступи у случају да налаз и мишљење имају неких недостатака[440]. Уколико се, међутим, наведени недостаци не могу исправити допунским, односно поновљеним вештачењем од стране истог вештака, орган поступка може да повери вештачење у погледу истог предмета другом вештаку (што значи да је одређење новог вештачења супсидијарно и условљено[441]).

У складу са Законником о кривичном поступку лице са стручним знањем из информационих технологија може се појавити у кривичном поступку осим у улози вештака, и у својству стручног лица и стручног саветника.

С***тручно лице*** помиње се у неколико одредаба. Приликом предузимања увиђаја 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, узима потребне узорке ради анализе или прикупља друге податке (члан 133. став 2). Такође, у члану 148. став 1. је предвиђено да орган поступка пре одузимања предмета, по потреби у присуству стручног лица прегледати предмете, а присуство стручног лица је предвиђено и као могућност приликом предузимања претресања уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи (члан 152. став 3). Лица која присуствују доказним радњама

---

[439] Упореди: *Сходно свом слободном судијском уверењу суд не мора да прихвати мишљење вештака, али и не може донети закључке супротне мишљењу вештака. Анализирајући оцену налаза и мишљења комисије судских вештака, како то утврђује и оцењује првостепени суд, долази се до закључка да је суд посумњао у тачност датог мишљења, али да није поступио у смислу одредбе члана 123. ЗКП. Сходно свом слободном судијском уверењу суд не мора да прихвати мишљење вештака, али и не може донети закључке супротне мишљењу вештака, односно мора га прихватити у целини, или одбацити, али га не може прихватити само делимично и заменити својим мишљењем. У колико суд допунским саслушањем вештака своју сумњу није отклонио одредиће ново вештачење и нове вештаке* (Решење Врховног суда Србије Кж. 1876/03 од 26. јануара 2004. и пресуда Окружног суда у Београду К. 52/03 од 11. јула 2003. године)

[440] Тако ЗКП прецизирано уређује два могућа облика корекције претходно обављеног вештачења, односно начина проверавања његовог стручног квалитета и доказне веродостојности, и то у виду: 1) допунског, односно поновљеног вештачења, или 2) новог вештачења. Наиме, орган поступка има могућност да, на предлог странака или по службеној дужности, одреди допунско, односно поновљено вештачење уколико постоје *недостаци у налазу вештака* (налаз је нејасан, непотпун, погрешан, у противречности сам са собом или са околностима о којима је вештачено или се појави сумња у његову истинитост) или пак постоје недостаци у мишљењу вештака (мишљење је нејасно или противречно). Налаз може бити нејасан као последица начина на који је вештак изложио утврђене чињенице, непотпун је уколико не садржи одговоре на сва питања или недовољно образложене одговоре,погрешан је уколико чињенице нису правилно утврђене, док је мишљење нејасно ако се не може са сигурношћу утврдити шта је вештак закључио, а противречно је уколико су садржани закључци међусобно противречни или нелогично повезани. Бркић, *op.cit,* 360-361.

[441] Шкулић, Илић, *op.cit*., 31.

могу предложити јавном тужиоцу да ради разјашњења ствари постави одређена питања осумњиченом, сведоку или вештаку, а по дозволи јавног тужиоца могу постављати питања и непосредно. Ова лица имају право да захтевају да се у записник унесу и њихове примедбе у погледу предузимања појединих радњи, а могу и предлагати прикупљање појединих доказа (члан 300. став 8). Осим тога, Законик предвиђа да уколико је то потребно ради разјашњења појединих техничких или других стручних питања која се постављају у вези са прибављеним доказима или приликом саслушања осумњиченог или предузимања других доказних радњи, јавни тужилац може затражити од стручног лица одговарајуће струке да му о тим питањима да потребна објашњења. Ако су приликом давања објашњења присутни осумњичени или бранилац, они могу тражити да то лице пружи ближа објашњења. У случају потребе, јавни тужилац може тражити објашњења и од одговарајуће стручне установе (члан 300. став 9). Такође, не постоји сметња да стручно лице буде позвано да у својству сведока да у исказу пренесе сазнања или опажања у вези са предметом сведочења (осим уколико би својим исказом повредило дужност чувања тајног податка, док надлежни орган, односно лице органа јавне власти не опозове тајност податка или га не ослободи те дужности у смислу члана 93. став 1. тачка 1).

Осим наведеног, у ЗКП је предвиђен још један користан вид контроле рада вештака, а то је установа ***стручног саветника***. Наиме, осим као вештака, орган поступка може лица са потребним стручним знањима ангажовати и у другим приликама, али се резултат њиховог ангажовања тада не третира као доказ. Стручна лица се ангажују ради разјашњења појединих техничких или других стручних питања која се постављају у вези са прибављањем доказа или предузамања других процесних радњи, али у тим случајевима стручна лица помажу органу поступка у утврђивању чињеница на тај начин што им кроз стручно расуђивање и стручно-технички рад дају савете у решавању стручне, ванправне проблематике. Не може се сматрати вештаком лице које је позвано да као стручњак изврши једну чисто материјалну радњу или ради давања обичног обавештења који помаже, на пример, приликом саслушања окривљеног, када је потребно стручно знање из одређених области[442].

[442] Васиљевић, Грубач, *op.cit,* 265.

Свака странка може слободно да изабере и пуномоћјем овласти стручног саветника када орган поступка донесе наредбу о вештачењу. Установа стручног саветника је новина у Законику о кривичном поступку. Стручни саветник је лице које располаже стручним знањем из области у којој је одређено вештачење. Међутим, стручно лице није посебно доказно средство као вештак, него пружа органу поступка у решавању питања из области за коју је стручан и не ради се о вештаку, него о учеснику у поступку који с обзиром да нема својство вештака нити права ни дужности као вештак, не обавља вештачење нити је резултат његовог представља налаз и мишљење. То је лице које се испитује као сведок јер поседује специфична знања у односу на одређено ванправно питање. Стручни саветник заправо има контролну функцију у односу на вештачење које је спроводи вештак одређен одлуком органа поступка. Како испољава одређену процесну иницијативу у односу на већ одређено вештачење, условно се може означити као „паралелни вештак“[443]. Наиме, када орган поступка одреди вештачење, странка може изабрати и пуномоћјем овластити стручног саветника са функцијом провере вештачења при чему не постоји „супер вештачење“ између исказа стручног саветника и налаза и мишљења вештака[444]. Ангажовањем стручног саветника, вештачење у ствари поприма контрадикторни карактер, јер стручњак одређен од странака парира вештаку одређеном од стране органа поступка[445].

Као стручни саветник се у поступку не може одредити лице које је искључено или ослобођено од дужности сведочења, а окривљени и оштећени као тужилац имају право да органу поступка поднесу захтев за постављање стручног саветника, јер је предвиђена сходна примена одредаба које уређују могућност постављања пуномоћника оштећеном као тужиоцу, и браниоца сиромашном окривљеном[446].

---

[443] М. Шкулић, Кривично процесно право, Правни факултет у Београду, Београд 2014, 230.
[444] Правно схватање посебних одељења Врховног касационог суда, са седнице 31.01.2012. године. Наведено према: Билтен Вишег суда у Београду 82/2012, 14.
[445] Кнежевић, *op.cit*, 303.
[446] *Међутим, нису испуњени услови да се оптуженом постави стручни саветник у ситуацији када он има четири изабрана браниоца, што указује да према свом имовном стању може да сноси и евентуалне трошкове награде стручног саветника. Решењем Вишег суда у Београду – Посебно одељење, одбијен је захтев за постављање стручног саветника економско-финансијске струке оптуженом. Против наведеног решења благовремено су изјавили жалбу браниоци, у којој су навели да је нејасно на основу чега је првостепени суд закључио да је оптужени у могућности да плати стручног саветника када је на основу приложених доказа правилно утврдио да оптужени нема имовине, да није порески обвезник и да је незапослен. По налажењу кривичног већа, правилно*

Стручни саветник у складу са чланом 126. располаже одређеним правима и дужностима: дужан је да положи заклетву, да странци пружи помоћ стручно, савесно и благовремено, да не злоупотребљава своја права и не одуговлачи поступак, а има право да буде обавештен о дану, часу и месту вештачења, присуствује и у току вештачења прегледа списе, предмет вештачења, предложи вештаку предузимање одређених радњи, да даје примедбе на налаз и мишљење вештака, на главном претресу да поставља питања, те да буде испитан о предмету вештачења. Осим тога, предвиђено је да стручни саветник, као и окривљени и његов бранилац имају право да присуствују вештачењу, а да није предвиђен изузетак од ове могућности. Управо у вези са последњим, у поступању у пракси су се појавиле одређене дилеме, јер су поједина вештачења до те мере специфична или задиру у приватност одређених лица, па је само по себи немогуће да бранилац и окривљени присуствују вештачењу а осим тога питање колико је то и неопходно кад могу ангажовати стручног саветника. Тако је у једном предмету пред Вишим судом у Београду суд одбио захтев одбране да бранилац и окривљени присуствују економско-финансијском вештачењу у установи са образложењем да је „сав материјал који је требало да прегледају вештаци достављен, као и све примедбе и сугестије које су имали окривљени и браниоци, записници и транскрипти са претреса, наредба је донета на претресу, а природа економско финансијског вештачења у установи од стране комисије, па чак и да је од стране појединца, таква је, да је по оцени суда могуће да окривљени и браниоци присуствују једино прегледању документације и констатовању шта се прегледа и на која питања треба одговорити вештачењем…а каснија стручна анализа у којој вештаци примењују методе анализе, упоређивања, рачуна и слично, представља мисаони, интелектуални процес, и сама по себи искључује било чије присуство“[447]. Да је одбрана ангажовала стручног саветника, он би имао право да присуствује

је поступио поступајући председник већа када је одбио захтев бранилаца да се оптуженом постави стручни саветник економско-финансијске струке јер, и по оцени већа, околност да оптужени у предметном кривичном поступку има више од једног ангажованог браниоца (укупно четири) указује да према свом имовном стању може да сноси и евентуалне трошкове награде стручног саветника. Решење већа Вишег суда у Београду – Посебног одељења Кв-По1. 682/12 од 25. октобра 2012. и решење председника већа Вишег суда у Београду – Посебног одељења К-По1. 302/10 од 5. октобра 2012. године.

[447] С. Николић Гаротић, „Неке дилеме у вези вештачења“, Билтен Вишег суда у Београду 85/2014, 137.

вештачењу, али је питање, узимајући у обзир образложење суда и специфичну природу вештачења, каква би била конкретно улога стручног саветника. Код вештачења од стране стручњака дигиталне форензике, питање је да ли право стручног саветника да присуствује вештачењу подразумева да он заједно са вештаком седи за рачунаром и прати кораке које предузима вештак користеће специфичне форензичке алате или је сврсисходније омогућити стручном саветнику да по обављеном вештачењу на клону уређаја предузима анализу користећи исте технике и методе коришћене од стране вештака што би било у функцији провере извршеног вештачења?

Стручни саветник је дужан да странци пружа помоћ стручно, савесно и благовремено, а у вези са електронским доказима, могући задаци се односе на проверу интегритета и континуитета електронских доказа; тестирање форензичке процедуре којим се дошло до доказа; објашњење суштине приказаних електронских доказа и њихове улоге у доказивању тврдњи супротне стране; идентификовање могућих релевантних доказе које иду у корист стране; помоћ странци приликом испитивања вештака[448]. Осим што има право да прегледа списе и предмет вештачења, било би корисно предвидети могућност не само да предложи вештаку предузимање одређених радњи, него да му буде омогућено да сам предузме одређене радње, односно да примени правила дигиталне форензике и форензичке алате, како би проверио резултате који су представљени као доказ у поступку и о њима да исказ.

1.2. Посебне доказне радње

Посебне доказне радње су изузетне и њихова примена се ограничава, по правилу, само на најтеже облике криминалитета, али и када се ова кривична дела откривају и доказују, посебне мере се користе само као *ultima ratio*, односно као последње средство за којим се посеже, уколико се редовним доказним радњама не постижу резултати, или би то било повезано са значајним тешкоћама, или чак немогуће. Посебне доказне радње могу се примењивати само под следећим условима: да су изричито предвиђене законским одредбама (*начело легалитета*);

[448] *ACPO,* 31.

да не постоје „блаже“ мере за остварење истог циља (*начело супсидијарности*); да се ради о веома тешким кривичним делима (*начело сразмерности*); да се спроводе на основу *одлуке надлежног судског органа*; да се прецизно *временски ограниче* и да се спроводе уз постојање *надзора над законитим вршењем*[449]. Законик о кривичном поступку садржи општа правила за примену посебних доказних радњи (односе се на: услове за одређивање посебних доказних радњи; кривична дела за која се могу одредити посебне доказне радње; поступање са прикупљеним материјалом; случајни налаз и тајност података) а која се примењују на све посебне доказне радње.

1.2.1. Тајни надзор комуникација

Одређивање тајног надзора комуникације претпоставља испуњеност одређених материјалних (члан 162) и формалних (члан 161) услова. Законик међу општим правилима којима уређује посебне доказне радње као материјални услов за предузимање посебних доказних радњи предвиђа кумулативну испуњеност две претпоставке: 1) да постоји основ сумње да је лице према коме се радње одређују учинило кривично дело које спада у категорију кривичних дела у погледу којих се могу одредити посебне доказне радње („посебно кривично дело“), и 2) да се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Чланом 162. ЗКП-а експлицитно је одређен круг кривичних дела за која се наведене посебне доказне радње могу одредити, а предвиђено је посебно да се, уколико су испуњени материјални услови предвиђени законом, посебна доказна радња тајни надзор комуникације може одредити и за следећа кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199. Кривичног законика), оштећење рачунарских података и програма (члан 298. став 3. Кривичног законика), рачунарска саботажа (члан 299. Кривичног законика), рачунарска превара (члан 301. став 3. Кривичног законика) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. Кривичног законика). Може се приметити да нису сва кривична дела високотехнолошког

[449] Бугарски, *op.cit*, 25.

криминала сврстана у категорију посебних кривичних дела- међутим, овај други елемент материјалног услова би могао начелно бити испуњен код свих облика извршења кривичних дела против безбедности рачунарских података, односно код кривичних дела која би могла бити обухваћена појмом високотехнолошког криминала.

Изузетно, посебне доказне радње се могу предузети и према лицу за које постоји основи сумње да припрема извршење посебних кривичних дела, уколико постоји један од алтернативно прописана разлога: а) уколико околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати, или б) уколико би то изазвало несразмерне тешкоће или велику опасност. „Могућност примене посебних доказних радњи и у односу на припремање, а посебно у односу на покушај кривичних дела, у погледу којих су такве радње и иначе могуће, није споран, без обзира што у кривичноправном смислу није увек могуће кажњавање за припремање, као и за покушај тих кривичних дела (мада је покушај у највећем броју случајева, с обзиром на прописану казну за та кривична дела, свакако кажњив)... јер основ за примену посебних доказних радњи није кажњивост одређеног стадијума у извршењу кривичног дела као таквог, већ потреба да се одређено кривично дело спречи“ [450]. Кривична дела против безбедности рачунарских података с обзиром на запрећену казну пак не спадају у кривична дела код којих је покушај кажњив у смислу члана 30. КЗ, јер за већину облика извршења кривичних дела против безбедности рачунарских података прописана казна затвора до 5 година а није прописано изричито кажњавање за покушај. Ипак, с обзиром да материјални услов може бити испуњен у великом броју случајева, сасвим је оправдано да се посебне доказне радње могу применити и уколико постоји само основ сумње да се дело припрема.

Посебне доказне радње се примењују као *ultima ratio* а законодавац је изричито предвидео да приликом одлучивања о одређивању и трајању посебних доказних радњи орган поступка ће посебно ценити да ли би се исти резултат могао постићи на начин којим се мање ограничавају права грађана.

[450] Шкулић, Илић, *op.cit*., 35.

Ако су испуњени формални и материјални услови на образложени предлог јавног тужиоца суд може одредити надзор и снимање комуникације која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки[451].

Посебну доказну радњу одређује стварно и месно надлежан суд образложеном наредбом, која обавезно садржи следеће елементе: расположиве податке о лицу према којем се тајни надзор комуникације одређује[452], законски назив кривичног дела, означење познатог телефонског броја или адресе осумњиченог, односно телефонског броја или адресе за коју постоје основи сумње да је осумњичени користи, разлоге на којима се заснива сумња[453], начин спровођења[454], обим и трајање посебне доказне радње. Функционална надлежност за доношење одлуке припада судији за претходни поступак који, ако прихвати предлог јавног тужиоца, доноси образложену наредбу о тајном надзору комуникације. У противном случају, судија за претходни поступак решењем одбија предлог.

Тајни надзор комуникације обухвата два аспекта: *надзор и снимање комуникације* која се обавља путем телефона или других техничких средстава, а други на *надзор* електронске или друге *адресе* осумњиченог и заплену писама и других пошиљки. Тајни надзор комуникације се може односити само на праћење комуникације или на надзор адресе, али може обухватити оба сегмента.

---

[451] Иако законодавац не говори о садржини предлога јавног тужиоца, осим што предвиђа да он мора да буде образложен, може се закључити да је јавни тужилац у обавези да наведе сличне елементе које садржи и наредба о одређивању тајног надзора. Реч је, пре свега, о расположивим подацима о лицу према којем се тајни надзор комуникације одређује, законском називу кривичног дела, означењу познатог телефонског броја или адресе осумњиченог, односно телефонског броја или адресе за коју постоје основи сумње да је осумњичени користи, и разлозима на којима се заснива сумња. У предлогу за одређивање тајног надзора комуникације требало би посебно навести да се докази не могу прикупити на други начин. Поред тога, могло би да буде предложено да се заплене писма и друге пошиљке.

[452] Важно је запазити да законодавац говори о расположивим подацима о лицу према којем се одређује тајни надзор, што представља нижи стандард у односу на онај који се захтева рецимо код наредбе за довођење (члан 195. став 2) или наредбе о спровођењу истраге (члан 296. став 3), код којих је потребно навести личне податке осумњиченог. Код наредбе о одређивању тајног надзора било би довољно да се наведе само име, презиме или надимак осумњиченог лица, или било који други податак који доприноси његовој индивидуализацији. То значи да се тајни надзор комуникација може одредити како према познатом, тако и према непознатом осумњиченом лицу.

[453] У наредби је потребно навести и разлоге на којима се заснива сумња, што значи да би требало образложити постојање основа сумње из члана 161. ст. 1. и 2.

[454] Судија за претходни поступак у наредби одређује и начин спровођења тајног надзора комуникације, а то подразумева одређивање органа који ће извршити наредбу, као и обавезу организације или лица које је регистровано за пренос информација да пружи потребну помоћ (члан 168. ст. 1. и 2).

Постојање могућности тајног надзора комуникације отвара и проблем доказне прихватљивости тзв. листинга телефонских разговора. Став наших судова је да листинг телефонских разговора представља доказ који се може изводити на главном претресу[455].

Како је у погледу спровођења тајног надзора комуникација у судској пракси дошло до промене става у вези с могућношћу да Безбедносно-информативној агенцији буде поверено извршење наредбе о тајном надзору комуникације[456], као и услед ограничене надлежности полиције да поступа у расветљавању одређених кривичних дела, прописано је да наредбу извршава полиција, Безбедносно-информативна агенција или Војнобезбедносна агенција. Орган који је одређен да спроведе тајни надзор комуникација је дужан да сачињава дневне извештаје који се заједно са прикупљеним снимцима комуникације, писмима и другим пошиљкама које су упућене осумњиченом или које он шаље, достављају судији за претходни поступак и јавном тужиоцу на њихов захтев. У том случају им се достављају и прикупљени снимци комуникације, писма и друге пошиљке које су упућене осумњиченом или које он шаље.

Тајни надзор комуникације се по правилу врши преко поштанских, телеграфских и других предузећа, друштава и лица регистрованих за преношење информација, али се може обавити помоћу посебне опреме. До њеног коришћења може да дође на јавном месту или на месту на којем је приступ ограничен. С тим у вези се отвара питање могућности постављања посебне опреме за надзор комуникација у стану и другим просторијама. С обзиром на то да наредба судије за претходни поступак не даје такво овлашћење државном органу који извршава ову посебну доказну радњу, треба прихватити мишљење да се надзор и снимање обавља у поштанским и другим предузећима коришћењем технике која у њима постоји. Због тога је у ставу 2. предвиђена дужност поштанских, телеграфских и других предузећа, друштава и лица регистрованих за преношење информација да омогуће спровођење надзора и снимања комуникације и да, уз потврду пријема, предају писма и друге пошиљке органу који извршава наредбу о тајном надзору комуникације.

[455] ВСС, *Кж. бр. 1547/04* од 22. новембра 2004.
[456] ВСС, *Кж1. бр. 493/05* од 8. јуна 2005; *Кж ОК. бр. 7/05* од 2. фебруара 2006.

Законик предвиђа могућност проширења тајног надзора комуникације, па уколико у току спровођења тајног надзора комуникације дође до сазнања да осумњичени, уместо телефонског броја или адресе који су означени у наредби о спровођењу ове посебне доказне радње, користи други телефонски број или адресу, државни орган који извршава наредбу може проширити тајни надзор комуникације и на тај телефонски број или адресу. Доношење нове наредбе носи ризик да у међувремену буду изгубљене корисне информације о претпостављеној криминалној активности учиниоца, па је из тог разлога за проширење тајног надзора комуникације и на новооткривени телефонски број или адресу овлашћен органи који спроводи тајни надзор комуникација. Овакво проширење је фактичког карактера, али је условљено и временски ограничено, јер до формалног проширења може доћи искључиво накнадним одобрењем од стране суда поводом испољене иницијативе јавног тужиоца[457]. Наиме, овај је дужан да о томе ће одмах обавестити јавног тужиоца. Законик јасно утврђује дужност јавног тужиоца да након што буде офоцијелно обавештен о томе фактичком проширењу тајног надзора[458], јер је по пријему обавештења дужан да одмах поднесе предлог да се накнадно одобри проширење тајног надзора комуникације. О предлогу одлучује судија за претходни поступак у року од 48 часова од пријема предлога и о томе саставља белешку у записнику, па уколико усвоји предлог, накнадно одобрава проширење тајног надзора комуникације, а ако одбије предлог, материјал који је прикупљен прошереним надзором се уништава.

Трајање тајног надзора је омеђено фактичким и формални роком. Наиме, предвиђено је да спровођење надзора се прекида чим престану разлози за његову примену, што је последица *ultima ratio* карактера посебних доказних радњи. Осим тога, Законик у месецима одређује колико најдуже може тајни надзор трајати (у оквиру ког рока егзистира фактички рок). Постоје два режима трајања тајног надзора комуникације, од којих се један односи на кривична дела општег криминала, док се други примењује за кривична дела за која је посебним законом одређено да поступа Тужилаштво за организовани криминал или Тужилаштво за ратне злочине.Тајни надзор комуникације може трајати три месеца, а због неопходности даљег прикупљања доказа се може продужити највише за три

[457] Шкулић, *op.cit.*, 249.
[458] Шкулић, Илић, *op.cit.*, 39.

месеца. Ако је реч о кривичним делима за која је посебним законом предвиђено да поступа тужилаштво посебне надлежности, тајни надзор може се изузетно продужити још највише два пута у трајању од по три месеца. То значи да је у погледу кривичних дела високотехнолошког криминала, која су у надлежности Тужиоца за високотехнолошки криминал а који није тужилац посебне надлежности, спровођење надзора може трајати најдуже 6 месеци. До окончања тајног надзора комуникације може, дакле, да дође протеком наведених рокова, али и пре тога, чим престану разлози за његово спровођење.

По завршетку тајног надзора комуникације орган који је спроводио надзор доставља судији за претходни поступак снимке комуникације, писма и друге пошиљке. Поред тога, уз материјал се доставља и посебан извештај[459]. Законик прописује на који начин судија за претходни поступак поступа с достављеним материјалом - приликом отварања писама и других пошиљки судија је дужан да пази да се не повреде печати и да се омоти и адресе сачувају, као и да о отварању састави записник. Након тога сав материјал добијеним спровођењем тајног надзора комуникације судија за претходни поступак доставља јавном тужиоцу, који одређује да ли ће материјал употребити, јер је основна сврха примене посебне доказне радње прикупљање доказа за доношење одлуке о даљем предузимању кривичног гоњења. Наиме, предвиђено је да јавни тужилац одређује да се снимци добијени употребом техничких средстава у целини или делимично препишу и опишу, а од његовог става зависи да ли ће прикупљени материјал бити употребљен као доказ или не. Законодавац предвиђа да се прикупљени материјал уништава одлуком суда уколико јавни тужилац не покрене кривични поступак у року од шест месеци од када се упознао са материјало прикупљеним коришћењем посебних доказних радњи или уколико изјави јавни тужилац експлицитно изјави да прикупљени материјал неће користити у будућем поступку или пак да против осумњиченог ни неће покренути поступак[460]. У случају таквог експлицитног или

[459] Извештај садржи: време почетка и завршетка надзора, податке о службеном лицу које је надзор спровело, опис техничких средстава која су примењена, број и расположиве податке о лицима обухваћеним надзором и оцену о сврсисходности и резултатима примене надзора.

[460] У Законику стоји формулација: „да против осумњиченог неће захтевати вођење поступка“, што би требало изменити, јер јавни тужилац више не захтева ни од кога покретање поступка, него он отвара поступак у складу са чланом 7. ЗКП.

имплицитног става јавног тужиоца, sudija za prethodni postupak ће doneti rešenje o uništenju prikupljenog materijala.

Међутим, у одређеним ситуацијама прикупљени материјал се не може користити као доказ јер су приликом спровођења тајног надзора начињене одређене грешке. Уколико су снимци прибављени противно одредбама о тајном надзору комуникације, односно супротно наредби судије за претходни поступак, Законик као процесну последицу предвиђа то да се на прикупљеним подацима не може заснивати судска одлука. У том случају, са прикупљеним материјалом се поступа у складу са чланом 84. став 3. ЗКП, односо издвајају се из списа.

У одредби 41. став 1. Устава Србије гарантовано је да је право на тајност писама и других средстава општења неповредиво, али и да се одступања од ове гаранције могу прописати законом ако је то неопходно за вођење кривичног поступка, под условом да да о томе одлучи суд у сваком конректном случају. Дакле, прислушкивање комуникације техничким средствима и њихова регистрација путем посебних техничких уређаја, без знања лица која учествују у комуникацији, може представљати дозвољен начин за стицање доказа за кривични поступак. Но, из Устава проозлази да се таква могућност може користити само ако је то *неопходно ради вођења кривичног поступка*, „под условом да други докази којима располажу органи гоњења нису довољни, али истовремено, да неки други докази постоје, не и да би се тек прибавио материјал за покретање поступка“[461]. Законик о кривичном поступку, пак, предвиђа, да се посебне доказне радње, могу одредити ако се на други начин не могу прикупити докази за *кривично гоњење* или би њихово прикупљање било знатно отежано. Иначе, Законик разликује моменат почетка кривичног гоњења (члан 5. став 2.) и почетка кривичног поступка (члан 7). Тако *кривично гоњење започиње* првом радњом јавног тужиоца, или овлашћених службених лица полиције на основу захтева јавног тужиоца, предузетом у складу са овим законником ради провере основа сумње да је учињено кривично дело или да је одређено лице учинило кривично дело, док *кривични поступак почиње* доношењем наредбе о спровођењу истраге или потврђивањем оптужнице којој није претходила истрага, односно за дела за која се води скраћени поступка доношењем решења о одређивању

[461] Васиљевић, Грубач, *op.cit,* 1001.

притвора пре подношења оптужног предлога или одређивањем главног претреса или рочишта за изрицање кривичне санкције у скраћеном поступку, те одређивањем главног претреса у поступку за изрицање мере безбедности обавезног психијатријског лечења. Ако је већ моменат почетка кривичног гоњења уопште одређен, а нарочито на овакав начин, нелогочно је да се везује материјални услов за предузимање посебних доказних радњи за немогућност да се прикупе докази за кривично гоњење. Осим тога, такво прописивање није у складу са уставном одредбом, јер се могућност одступања од уставне гаранције везује за потребе вођења кривичног поступка, а не кривичног гоњења. У том смислу, одређивање радње не би имало никакво оправдање кад јавни тужилац има довољно других доказа за покретање истраге.

1.2.2. Рачунарско претраживање података

Рачунарско претраживање података је посебна доказна радња која се састоји у компјутерском претраживању већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело. У оквиру ове посебне доказне радње спроводе се две врста активности: претраживање података (као претходна активност) и упоређивање података прикупљених претраживањем са релевантним подацима који се тичу осумњиченог и кривичног дела[462]. Претраживање је усмерено на две врсте података: а) личне и б) друге податке, а који су претходно обрађени и похрањени у одређене базе података, садржане у евиденцијама које воде различити органи, организације и установе[463]. Материјални услов за одређивање ове посебне доказне радње садржан је у члану 161. ст. 1. и 2, а заснива се на тешкоћама или немогућности прибављања доказа на

[462] Шкулић, *op.cit.*, 259.

[463] То могу да буду подаци о преласку границе, листинзи телефонских разговора, подаци о потрошњи (воде, струје, гаса), о осигурању живота и имовине, о приходима, о плаћеном порезу, о кретању новца на банковним рачунима, о промени адресе, о медицински третираним повредама, медицинским терапијама или дијагнозама, о завршеним школама, о туристичким путовањима, о хотелским рачунима, о купљеним и продатим аутомобилима, о саобраћајним прекршајима, о судским поступцима, о позивима за полицијску интервенцију, о дозволама за држање оружја, о обављању службе у посебним војним и полицијским јединицама, о добијеним дозволама за управљање превозним средствима. Прикупљени подаци се потом упоређују са подацима који се налазе у полицијским базама података, а односе се на извршена кривична дела одређене врсте, на одређена лица као осумњичене, или на одређене карактеристике које су уочене приликом извршења кривичног дела.

други начин, док је формални услов да суд на основу предлога јавног тужиоца изда наредбу за спровођење. Док је у погледу тајног надзора комуникације предвиђено да се радња може одредити и уколико постоји основ сумње да су извршена одређена кривична дела против безбедности рачунарских података (члан 162. став 3), рачунарско претраживање података се не може одредити ни према једном из ове групе кривичних дела. Сматрамо да би било сасвим оправдано предвидети могућност одређивања ове посебне доказне радње према делима која спадају у високотехнолошки криминал у смислу члана 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала.

Образложени предлог јавног тужиоца требало би да садржи податке о осумњиченом, законски назив кривичног дела, као и опис података које је потребно рачунарски претражити и обрадити. Наредба о рачунарском претраживању података садржи податке о осумњиченом, законски назив кривичног дела, опис података које је потребно рачунарски претражити и обрадити, означење државног органа који је дужан да спроведе претрагу тражених података, обим и време трајања посебне доказне радње. Одредба која одређује садржину наредбе (а између осталог предвиђа да се означава државни орган који спроводи радњу) није у складу са чланом 180, који уређује спровођење рачунарског претраживања података (одређујући да наредбу извршава полиција, Безбедносно-информативна агенција, Војнобезбедносна агенција, царинске, пореске или друге службе или други државни орган, али и *правно лице које на основу закона врши јавна овлашћења),* па је потребно усагласити ова два члана. Наиме, како само претраживање може вршити не само државни орган него и правно лице, док упоређивање са подацима може вршити само државни орган, потребно је у одредби која уређује садржај наредбе јасно назначити који субјект је овлашћен за претраживање (као претходну активност), а који за упоређивање (као накнадну активност).

Рачунарско претраживање података може трајати највише три месеца, због неопходности даљег прикупљања доказа може се изузетно продужити још највише два пута у трајању од по три месеца, а у оквиру тог формалног рока спровођење рачунарског претраживања података се прекида чим престану разлози

за његову примену. По завршетку рачунарског претраживања података државни орган, односно правно лице доставља судији за претходни поступак извештај, а судија за претходни поступак извештај доставља јавном тужиоцу.

Код примене одредбе члана 178. и члана 179. ЗКП који се односе на рачунарско претраживање података као спорно се међу нижестепеним судовима појавило питање ко издаје наредбу на основу тих прописа, када јавни тужилац преко ове мере, као посебне доказне радње, тражи да се преко рачунарског претраживања података прибаве подаци о телефонским комуникацијама и коришћење базних станица и њихово аутоматско упоређење са неким бројем телефона, односно да ли се кроз ову доказну радњу могу тражити телефонске комуникације и базне станице. Врховни касациони суд је дао тумачење наведених чланова у смислу да тужилац не може сам да прибавља податке у вези евиденције телефонске комуникације и коришћења базних станица ни рачунарско претраживање већ само да образложено предложи суду издавање наредбе у смислу одредбе члана 178. и 179. ЗКП[464].

Погрешно је било поступање у судској пракси у смислу да су се применом ове посебне доказне радње прибављали листинзи и тзв. задржани подаци. „У складу с тим, једино је суд, односно у конкретном случају судија за претходни поступак, функционално овлашћен да захтева достављање задржаних података. Иако се задржани подаци не односе на садржај комуникације, већ се ради о њеним формалним обележјима, којима се откривају врста, извор и одредиште комуникације, време њеног трајања и терминална опрема корисника комуникације, они потпадају под заштиту неповредивости тајности писама и других средстава комуницирања које су прокламоване у члану 41. Устава. Такође, подаци који се у конкретном случају наводе у предлогу тужилаштва за организовани криминал представљају податке у односу на које постоје обавезе задржавања, а у складу с одредбама чл. 128. и 129. ЗЕК, и који се као такви налазе у посебним базама података телекомуникационих оператера, односно који су похрањени у терминалној опреми претплатника или корисника“[465]. С обзиром на то да се посебна доказна радња *рачунарско претраживање података* може

[464] Одговор кривичног одељења Врховног касационог суда на спорна правна питања нижестепених судова са седнице одржане 04.04.2014. године.
[465] Пресуда Вишег суда у Београду, *Кв.По1 бр. 601/13* од 13. 08.2013.године.

предузети само у односу на кривична дела предвиђена у члану 162. став 1, измењена је одредба члана 286. ст. 3. и 5, тако да основ за прибављање „листинга“ телефонских разговора и тзв. задржаних података представља наредба коју, на захтев јавног тужиоца, доноси судија за претходни поступак. О прибављеним „листинзима“ и задржаним подацима полиција је дужна да обавести судију за претходни поступак.

2. УСКЛАЂЕНОСТ ЗАКОНИКА О КРИВИЧНОМ ПОСТУПКУ СА КОНВЕНЦИЈОМ О ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Узимајући у обзир обавезу Републике Србије да процесно законодавство усклади са одредбама Конвенције о високотехнолошком криминалу, у поднасловима који следе разматрали смо да ли и у којој мери одредбе Законика о кривичном поступку могу да послуже остварењу смисла одређених радњи из појединих чланова Конвенције.

2.1. Усклађеност са члановима 16. и 17. Конвенције

У Србији у погледу обезбеђења ускладиштених рачунарских података који могу имати значај електронског доказа, Законик о кривичном поступку 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 изузетно може предузети без наредбе* (у складу са члановима 158-160). 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 зајамченом 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 судије за претходни поступак, а на предлог јавног тужиоца, прибави евиденцију остварене телефонске комуникације, коришћених базних станица или изврши лоцирање места са којег се обавља комуникација. По предузимању радње, полиција је дужна да одмах а најкасније у року од 24 часа обавести јавног тужиоца (члан 286. став 4). Овлашћење дато полицији у циљу остварења дужности из члана 286.став 1, 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. У првобитном решењу у Законику је у члану 286. било предвиђено да полиција по налогу јавног тужиоца прибавља евиденције, међутим, због питања усклађености овог са чланом 41. Устава којим се гарантује тајност писама и других средстава комуникације, изменама Законика из 2014. године[466] предвиђено је издавање налога од стране суда. Ако је интенција законодавца била да обезбеди заштиту гарантованих људских права, у смислу да су одступања дозвољена само на одређено време и на основу одлуке суда и ако су неопходна ради вођења кривичног поступка на начин предвиђен законом (члан 41. став 2. Устава), изменењим решењем у Законику то није учињено на адекватан начин. Наиме, одлука суда којом би било омогућено ограничење тајности писама у складу са Законником могла би бити донета у облику пресуде, решења и наредбе (члан 269), док се налог не помиње као врста одлуке. Стога би било исправније да ова одредба садржи формулацију „по наредби судије за претходни поступак, а на предлог јавног тужиоца“. Ипак,

[466] Члан 6. став 1. Закона о изменама и допунама Законика о кривичном поступку („Сл.гласник РС“, бр. 55/2014).

мишљења смо да би ради омогућавања експедитивног деловања у нарочито хитним околностима било оправдано предвидети да јавни тужилац може издати налог, а евентуално за такво поступање обезбедити контролу суда у виду потврде законитости тако издатог налога, тим пре што се не ради о прикупљању података у реалном времену (прикупљање података у реалном времену покривено је посебном доказном радњом), него података о остваренoj комуникацији (што би се могло остварити издавањем одговарајуће наредбе).

Осим поменутих одредаба Законика о кривичном поступку, релевантан је и Закон о електронским комуникацијама[467]. Чланом 128. Закона о електронским комуникацијама[468] било је предвиђено да је оператор дужан да задржи податке о електронским комуникацијама за потребе спровођења истраге, откривања кривичних дела и вођења кривичног поступка, у складу са законом којим се уређује кривични поступак, као и за потребе заштите националне и јавне безбедности Републике Србије, у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова, као и да задржане податке без одлагања достави на захтев тих органа. Одредбе члана 128. у делу који је гласио: „у складу са законом којим се уређује кривични поступак“, „у складу са законима којима се уређује рад служби безбедности Републике Србије и рад органа унутрашњих послова“ и „на захтев надлежног државног органа“ престале су да важе на основу Одлуке Уставног суда[469]. Такође је престала да важи одредба члана 129. став 4. по којој је било предвиђено да министарство надлежно за послове телекомуникација и информационог друштва, по прибављеном мишљењу министарства надлежног за послове правосуђа, министарства надлежног за унутрашње послове, министарства надлежног за послове одбране, Безбедносно-информативне агенције и органа надлежног за заштиту података о личности, ближе прописује захтеве у вези са задржавањем података. Наиме, Уставни суд је прогласио неуставним ове одредбе члана 128. којима је била установљена обавеза оператора да задржане податке, без обзира што се њима не открива садржај комуникације, учине доступним на захтев

[467] Закон о електронским комуникацијама, „Службени гласник РС“, бр. 44/2010 и 62/2014 – одлука УС.
[468] "Сл. гласник РС", број 44/2010.
[469] ИУз број 1245/2010 од 13. јуна 2013. године, објављене у "Сл. гласнику РС", бр. 60/2013 од 10. јула 2013. године.

надлежног органа, а без претходно прибављене одлуке суда, јер се таквом одредбом нарушава неповредивост права на тајност комуницирања корисника електронских комуникација. Законом о изменама и допунама Закона о електронским комуникацијама[470], у целини је измењен члан 128, па је оператор[471] је дужан да задржи одређене податке о електронским комуникацијама као и да их чува 12 месеци од дана обављене комуникације[472]. Ради се о подацима потребним за: 1) праћење и утврђивање извора комуникације; 2) утврђивање одредишта комуникације; 3) утврђивање почетка, трајања и завршетка комуникације; 4) утврђивање врсте комуникације; 5) идентификацију терминалне опреме корисника; 6) утврђивање локације мобилне терминалне опреме корисника. При томе, обавеза задржавања података обухвата и податке о успостављеним позивима који нису одговорени, али не обухвата податке о позивима чије успостављање није успело, а изричито је забрањено задржавање података који откривају садржај комуникације (члан 129). Приступ тим задржаним подацима није допуштен без пристанка корисника, осим на одређено време и *на основу одлуке суда*, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. Одлука Уставног суда је за сваку похвалу, но задржавање података на начин предвиђен Законом о електронским комуникацијама само по себи могло би представљати предмет испитивања од стране Суда, имајући у виду да су уставни судови у неколико европских држава огласили законе којима је било одређено задржавање података у смислу Директиве о задржавању података (која решења су употребљена као инспирација за прописивање одредаба о задржавању у Закону о електронским комуникацијама), као и да је Уставни суд Европске уније поништио Директиву[473]. Иако би се задржавање података могло правдати потребом да надлежни органи могу у случају потребе да траже од пружалаца услуга одређене податке, сматрамо да прописивање обавезе задржавања бројних података за велики број лица у

[470] "Сл. гласник РС", бр. 62/2014.

[471] Односи се на оператора јавних комуникационих мрежа или оператора јавно доступних електронских комуникационих услуга (за значење израза, види члан 4. став1.).

[472] Подаци се задржавају у складу са релевантним међународним техничким стандардима, односно препорукама које се односе на задржане податке, у изворном облику или као подаци обрађени током обављања делатности електронских комуникација који морају бити истог квалитета и нивоа заштите као и подаци у изворном облику, а на начин да им се без одлагања може приступити, односно да се без одлагања могу доставити на основу одлуке суда.

[473] Више о томе, вид: Седми део.

неодређену сврху и то у пропису којим се не уређује кривична процедура није оправдано са становишта заштите гарантованих људских права и правне сигурности уопште. Важно питање у вези са наведеним је на који начин надлежни органи остварују приступ подацима о саобраћају, имајући у виду неповредивост тајности комуникација. С обзиром на то да Устав дозвољава одступање од тајности писама и других средстава општења само на одређено време на основу одлуке суда ако су неопходна за вођење кривичног поступка *на начин предвиђен законом* (члан 41. став 2), то значи да би се у сврху вођења кривичног поступка и просто задржавање података могло одредити само на основу одлуке суда и у складу са законом који уређује кривични поступак. Стога сматрамо да би у потпуности требало одустати од задржавања података на начин како предвиђа Закон о електронским комуникацијама, и унети одговарајуће одредбе у Законик о кривичном поступку. Да би се надлежним органима омогућило да остваре приступ подацима потребним за идентификацију осумњиченог, неопходно је на одговарајући начин обавезати не само пружаоце услуга него и сва лица која у поседу, односно контролом имају потребне податке да их сачувају, али само тачно одређених података за потребе конкретног кривичног поступка. 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 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 (издавањем одговарајуће наредбе од стране суда, и то или наредбе за предавање података или наредбе за претрес рачунара). 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, а ради постизања експедитивности.

2.2. Усклађеност са члановима 18. и 19. Конвенције

Српски Законик о кривичном поступку 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 над ствари и претресања предмета. Наиме, када је за утврђивање или разјашњење неке чињенице у поступку потребно непосредно опажање органа поступка, може се предузети увиђај над ствари, 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 други 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 обезбеђивање трагова у рачунарима и са њима повезаним уређајима, а које стручно лице треба да изврши не може да се 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 изложио 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 служи 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[474], 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

[474] 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, 1097; J. Saylor, *op.cit*, 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, 94.

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 прикупљеним 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 *предавање комуникације које су у 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.

Такође, 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).

2.3. Усклађеност са члановима 20. и 21. Конвенције

Тајни надзор комуникација у Србији је посебна доказна радња коју суд може одредити према лицу за које постоје основи сумње да је учинило кривично дело из члана 162. овог Законика о кривичном поступку, а на други начин се не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано, као и уколико постоје основи сумње да лице припрема неко од наведених кривичних дела, а околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Иако не одступају у великој мери од анализираних решења у другим државама, наведене одредбе Законика би се, ипак, могле побољшати.

Приликом одлучивања о одређивању и трајању посебних доказних радњи орган поступка је дужан да води рачуна о пропорционалности, односно да

посебно цени да ли би се исти резултат могао постићи на начин којим се мање ограничавају права грађана. Кривична дела у односу на која се примењују посебне доказне радње одређена су у члану 162. Законика, а ради се о кривичним делима за која је посебним законом одређено да поступа јавно тужилаштво посебне надлежности, као и таксативно наведеним кривичним делима. Осим тога, радња тајног надзора комуникација се може одредити и за следећа кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права (члан 199. Кривичног законика), оштећење рачунарских података и програма (члан 298. став 3. Кривичног законика), рачунарска саботажа (члан 299. Кривичног законика), рачунарска превара (члан 301. став 3. Кривичног законика) и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података (члан 302. Кривичног законика). Да би се испоштовао принцип сразмерности, оправдано је везивање могућности за одређење пресретања комуникације за тешка кривична дела (за која је запрећена казна затвора од најмање неколико година). У погледу кривичних дела у односу на која се у Србији може одредити тајни надзор комуникације, сматрамо да су неоправдано изузети поједини облици и поједина кривична дела из главе 27 (кривична дела против безбедности рачунарских података), и то: Оштећење рачунарских података и програма (члан 298.ставови 1.и 2), Прављење и уношење рачунарских вируса (члан 300), Рачунарска превара (члан 301. став 1. и 2), Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303) и Неовлашћено коришћење рачунара или рачунарске мреже (члан 304). Чак и да се прихвати резон да се у погледу Оштећења рачунарских података и програма и Рачунарске преваре, могућност спровођења посебне доказне радње везује за износ настале штете (преко 1.500.000 динара), законодавац је превидео да радња извршења изостављених кривичних дела може проузроковати, штету далеко већих размера. Осим тога, за доказивање кривичних дела против безбедности рачунарских података је потребно предвидети да се у случају да се претресом рачунара и применом других радњи и мера не могу прикупити докази може применити тајни надзор комуникација, а услед специфичности трагова и доказа о извршеној радњи кривичног дела. У погледу кривичних дела извршених употребом, односно против рачунарских система и мрежа може се приступити на тај начин што се

могућност одређивања радње проширује у погледу других кривичних дела која су извршена употребом информационих система и телекомуникационе технологије, као и других кривичних дела када је потребно прикупљање електронских доказа. У том случају треба још више инсистирати на неопходности такве радње, у смислу да су неопходне за утврђивање истине или да би то било немогуће или знатно отежано применом других радњи и мера/ када постоји вероватноћа да се њиховом применом може доћи до информација корисних за разјашњење кривичног дела, под условом да је њихова примена потребна и од изузетног значаја.

Ова посебна доказна радња обухвата надзор и снимање комуникације која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки. Ипак, узапћење се не односи на поруке електронске поште, односно других прука које се преносе коришћењем услуга електронских комуникација.

Радњу може одредити само судија за претходни поступак образложеном наредбом на образложени предлог јавног тужиоца. Иако је потребно да радњу одређује суд, оправдано је предвидети да у *изузетно хитним случајевима* радњу може одредити и *јавни тужилац*, али је у одређеном року (од неколико часова од одређивања) потребно да његову наредбу потврди, односно одобри судија, у супротном се извршење радње обуставља а резултати се не могу користити као доказ.

Спровођење надзора се прекида чим престану разлози за његову примену, може трајати три месеца, а због неопходности даљег прикупљања доказа се може продужити највише за три месеца. У погледу кривичних дела за која је посебним законом одређено да поступа јавно тужилаштво посебне надлежности, тајни надзор се може изузетно продужити још највише два пута у трајању од по три месеца, међутим, међу њима нису кривична дела из главе 27. КЗ.

Радњу извршава полиција, Безбедносно-информативна агенција или Војнобезбедносна агенција. Сматрамо да је оправдано у Законику о кривичном поступку овластити само полицију на предузимање ове радње, а да се резултати надзора које спроводе службе безбедности не би смели користити као доказ у кривичном поступку, јер је њихово поступање уређено другим прописима и

служи остваривању других циљева и заштите других интереса, тим пре што ове агенције нису "орган поступка" у смислу члана 1. тачка 15.

Поштанска, телеграфска и друга предузећа, друштва и лица регистрована за преношење информација дужна су да органима који извршавају наредбу, омогуће спровођење надзора и снимања комуникације и да, уз потврду пријема, предају писма и друге пошиљке. Међутим, за непоступање није предвиђена санкција (па би било целисходно предвидети сходну примену члана 282. став 2. и 3).

Законик предвиђа могућност проширење тајног надзора комуникације. Наиме, уколико се у току спровођења тајног надзора комуникације. дође до сазнања да осумњичени користи други телефонски број или адресу, орган који извршава наредбу може проширити тајни надзор комуникације и на тај телефонски број или адресу. Међутим, не постоји могућност проширења и на број и адресу коју у име или за рачун осумњиченог користи треће лице. Осим могућности проширења надзора током спровођења радње, оправдано би било предвидети *могућност проширења у погледу лица* према којима се радња одређује, тако да се наредба може односити како на осумњиченог тако и на лица за које се на основу одређених чињеница сумња да у име осумњиченог или од осумњиченог примају и прослеђују поруке или да осумњичени користи њихов прикључак, односно адресу.

Ради заштите приватности лица, од значаја би била одредба која предвиђа да уколико постоје чињенице које упућују на закључак да би се путем мере стекло само сазнање из приватног живота тих лица, таква мера није дозвољена. Такође, сва сазнања о приватном животу која стекну путем мере не смеју се даље користити, снимци о таквим сазнањима морају се одмах избрисати, а стицање таквих сазнања и брисање записа о истима мора се документовати у списима. Уколико би се приликом извршења мере прикупили лични подаци о трећим лицима, јер је то из техничких разлога неизбежно за постизање циља, такви се подаци се не би смели користити у друге сврхе осим сравњења података ради утврђивања траженог броја апарата и броја картице, а након окончања мере би се одмах се морали уништити.

Четврти део

ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ПОЈЕДИНИМ ДРЖАВАМА

Државе и међународна заједница су суочене са изазовима савремених облика криминала у последњих петнаестак година усвајале посебне материјалноправне, организационе и процесне прописе за спречавање, откривање и сузбијање специфичностима тих облика криминала, међу којима је и високотехнолошки криминал. Тим прописима се предвиђају битна одступања од устаљених и општеприхваћених ставова и установљавају органи са посебним надлежностима и са знатно ширим овлашћењима у односу на органе у редовном кривичном поступку, што је са собом донело опасност да се поремети равнотежа између општих интереса ефикасности кривичног гоњења и заштите људских права[475]. Појединим одступањима од класичне кривичне процедуре заустављена је надмоћ тенденције веће заштите слобода и права учесника поступка (карактеристичне за теорију и законска решења двадесетог века) у односу на захтев за повећањем ефикасности поступку, што је за последицу имало нужно ограничење слобода и права учесника у поступку[476]. Борба против савремених облика криминалитета захтева посебно процесно законодавство, јер су класична процесна средства и методи недовољно ефикасни, нарочито у области прикупљања доказа, па је било потребно предвидети нова средства и методе који се заснивају на употреби техничких достигнућа. Ради повећања ефикасности у спречавању, откривању и доказивању савремених облика криминала државе су измениле и допуниле своје кривичнопроцесне законе, но, поједина решења је потребно прихватити као нужду, уз аргументовану критику и скепсу, јер се лако могу претворити у средство нелегитимне репресије у друштву[477].

У поглављима која следе, анализиране су одредбе којима су поједине државе прилагодиле своја национална законодавства потреби да се створе правни механизми за превазилажење проблема доказивања савремених облике криминала у кривичном поступку, наравно са нагласком на дела високотехнолошког

[475] Грубач, *op.cit* 517.
[476] В. Ђурђић, Кривични поступак Србије, Ниш 2006, 200.
[477] Грубач, *op.cit*, 518-519.

криминала. У одабиру националних законодавстава аутор је руковођен намером да укаже на специфична решења у државама на европском континенту (уз настојање да постигне географску покривеност појединих региона), као и у САД. Стога је поглавље подељено на три дела: 1) Доказивање дела високотехнолошког криминала у државама англосаксонског кривичнопроцесног система; 2) Доказивање дела високотехнолошког криминала у државама континентално-европског кривичнопроцесног система[478]; 3) Доказивање дела високотехнолошког криминала у појединим државама бивше СФРЈ.

1. ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ДРЖАВАМА АНГЛОСАКСОНСКОГ КРИВИЧНОПРОЦЕСНОГ СИСТЕМА

1.1. САД

У САД је се експедитивно чување рачунарских података могуће одредити на основу члана 2703(ф) Савезног кривичног закона[479]. Ова мера омогућава истражитељима и тужиоцу да се не изгубе битни подаци похрањени код 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 пружаоци услуга електронских комуникација према компанијској политици имају слободу да избришу или сачувају податке о кориснику и његовим активностима, што значи да 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

[478] О подели у два велика позитивноправна кривичнопроцесна система и њиховим карактеристикама види: Шкулић, Бугарски,*op.cit*, 42-54.
[479] *The U.S. Federal Criminal Code*, http://www.law.cornell.edu/uscode/text/18/2703.

држаоцу података наредбу 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 оствареним комуникација, са временом трајања тих комуникација; врсту и време коришћења појединих услуга; телефонски број или други идентификациони број корисника, као и привремено додељену *IP* адресу (динамичке *IP* адресе); начин 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 временски период одређен у наредби (најдуже до деведесет дана, с тим што се овај период може наредбом додатно продужити за још деведесет дана). Међутим, истражитељи не добијају издавањем наредбе никакве податке о налогу корисника, укључујући и податак да ли налог постоји, јер пружалаоце услуга електронских комуникација у откривању оваквих података спречавају прописи о поверљивости података о корисницима, а што је могуће тек по добијању судског налога. Још један проблем произилази из односа поверљивости према кориснику, јер постоји дужност пружалаоца да корисника налога обавесте о издавању наредбе за чување података и поступању по тој наредби, а ово може трајно да нанесе штету истрази.

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 за претрес рачунара ради прикупљања података похрањених у електронском облику (*Warrant Seeking*

Electronically Stored Information[480]). 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[481], и то да се сагласи, између осталог, да се одриче од могућности позивања на тзв. *plain view doctrine*[482] 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)[483]. Примену ових ограничења судови правдају

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

[481] 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, J. Saylor, „Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches“, *Fordham Law Review* 6/ 2011, 2840.

[482] Четврти амандман 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.

[483] 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 конкретном случају) у потпуности искључују из вршења претреса рачунара (чак ни у виду надгледања или давања смерница), доводи се 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

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[484]. 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 другог 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[485], не постоји ниједан правни основ да суд у сваком конкретном случају приликом одобравања претраге рачунара унапред оглашава доказе до који се дошло поменутом доктрином недозвољеним, јер постоји механизам контроле појединачних доказа[486]

претреса непристрасном и незаинтересованом лицу. 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.

[484] 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 (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 генерални (уопштени) 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, R. Moore., "To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice* 1/2004, 55-57; O.Kerr, „Searches and Seizures in Digital World", *Harvard Law Review* 2/2005, 555). 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 налога за претрес не могу користити (иако законито прибављен). Simpson, " *op.cit*, 25.

[485] О потреби да се полицији на овај начин онемогуће коришћење широких дискреционих овлашћења, P. Ohm, „*Massive Hard Drives, General Warrants, and the Power of Magistrate Judges", Virginia Law Review* 1/2011, 99; J.Stinsman, „Computers and Searches, Rethinking the Applicability of the Plain View Doctrine", *Temple Law Review* 4/2011, 1099; M. Dodovich, „The Plain View Doctrine Strikes Out In Digital File Searches*", Journal of Law and Policy for the Information Society* 6/2011, 659.

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

(правило о издвајању незаконитих доказа, тзв. *exclusionary rule*[487]) применом ког би незаконито поступање полиције било санкционисано немогућношћу употребе доказа до ког се дошло на тај начин, односно противно налогу[488].

У САД је *прикупљање података о саобраћају у реалном времену* уређено у 206. поглављу 18. Закона[489]. Прикупљање података о саобраћају одобрава суд на основу захтева јавног тужиоца, при чему је у захтеву довољно да се укаже на чињенице које се применом ове радње могу прикупити а које су релавантне за истрагу кривичног дела (члан 3122). Ова радња се извршава тако што се инсталирају одређени уређај у информационом комуникационом систему било ког пружаоца услуга електронских комуникација (тзв. *pen register* или *trap and trace* уређај, дефинисани у члану 3127) који снимају податке о комуникацији која се остварује у реалном времену. Извршење радње траје најдуже 60 дана, уз могућност продужења уколико и даље стоје разлози због којих је радња одређена. Орган који је овлашћен да предузме ову радњу је законски ограничен у смислу да постоји дужност да приликом снимања или декодирања електронских и других импулса, те података о адреси и путањи комуникације која се преноси или обрађује у информационом комуникационом систему примени технику која не открива садржај електронске комуникације (члан 3121). Уколико овлашћени органи инсталирају сопствене уређаје у рачунарску мрежу пружалаца услуга, дужни су да саставе о томе записник који садржи податке о лицу које је инсталирало уређај, датум и време кад је уређај инсталиран и реинсталиран, време кад је уређају приступљено ради прикупљања података, као и конфигурацију

[487] 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.

[488] 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 (O. Kerr, „Ex Ante Regulation of Computer Search and Seizure“, *Virginia Law Review* 6/2010, 1250). Вредна помена 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 (Saylor, *op.cit*, 2854-2857).

[489] Тзв. *Pen Register and Trap and Trace statute*, http://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.

уређаја у тренутку инсталирања и евентуалне промене, а тај записник се у року од 30 дана од окончања радње предаје у судски депозит.

Пресретање комуникација уређено је у 119. поглављу 18. Закона[490]. Обезбеђује се заштита приватности комуникација и забрањује пружаоцима услуга електронских комуникација да трећој страни предају податке или омогуће приступ електронским комуникацијама, али се предвиђају дозвољени изузеци од овог правила. Тако је у члану 2516 предвиђено да је пресретање електронских комуникација дозвољено за потребе кривичног поступка уколико на захтев јавног тужиоца суд изда налог којим овлашћује или одобрава предузимање ове радње, јер је то потребно за прикупљање доказа да су учињена одређена кривична дела. Захтев за издавање налога се подноси у писаном облику и садржи, између осталог, чињеничне наводе који оправдавају предузимање радње (чињенични опис кривичног дела, податке који идентификују лице и одређивање комуникације поводом ког се захтев подноси) а нарочито опис претходно предузетих истражних процедура које нису дале потребне резултате, као и временски период за који се пресретање тражи. На основу поднетог захтева надлежни суд одобрава предузимање радње пресретања уколико утврди да постоји довољно вероватноће у смислу „оправданог разлога за веровање“ (*probale cause for belief*) да је учињено или да се припрема извршење одређеног кривичног дела и да се могу прикупити потребне информације из пресретане комуникације, те *да су уобичајене истражне процедуре покушане али да нису дале резултата*. У налогу суда се, осим података које садржи и захтев поводом ког се издаје, одређује и временски период за који се пресретање дозвољава, уз навођење да ли се извршење аутоматски обуставља по прикупљању очекиване комуникације. Пресретање траје колико је потребно за остваривање сврхе предузимања ове радње, али не дуже од 30 дана (с тим што је могуће продужење за још 30 дана уколико суд процени да и даље стоје разлози због којих је првобитно пресретање и одобрено). Како се

[490] Тзв. *Electronic Communication Privacy Act*, https://it.ojp.gov/default.aspx?area=privacy&page=1285. Овим Законом су 1986. измењене и допуњене одребе Закона о прислушкивању телефона и о скривеним микрофонима (*Federal Wiretap Act*) из 1968. Закон је неолико пута мењан, од којих су најзначајније измене и допуне учињене Законом о помоћи надлежним органима у вези са комуникацијама из 1994 (*Communications Assistance to Law Enforcement Act*), *USA PATRIOT Act* из 2001, Законом о потврђивању *USA PATRIOT* из 2006 и Законом о изменама и допуанама Закона о прикупљању страних обавештајних података из 2008. године. У току је законодавна реформа овог Закона у циљу повећања гаранција приватности електронских комуникација. Више о томе, http://www.gpo.gov/fdsys/pkg/BILLS-113s607rs/pdf/BILLS-113s607rs.pdf.

налогом може или одобрити већ започето или наредити пресретање које следи, рачунање овог рока почиње или од дана кад је полиција поднела захтев или десетог дана од издавања налога. На основу издатог налога, полиција може од пружалаца услуга електронских комуникација, као и држалаца рачунарских система преко којих се комуникација остварује, тражити да саопште све потребне информације као и техничку помоћ потребну за реализацију пресретања (члан 2518). Закон одређује да службена лица у полицији могу податке, који се односе на садржај електронске комуникације а који су сазнали као резултат предузимања радње пресретања, користити само у мери потребној за обављање службених дужности у вези са кривичним поступком, те да о томе могу сведочити под заклетвом пред кривичним судом (члан 2517). Осим пресретања садржаја комуникације, у складу са чланом 2703. надлежни органи могу *тражити од пружалаца услуга да предају* комуникације које су у ускладиштене у електронском комуникационом систему у последњих 180 дана, на основу одобрења суда а у складу са Федералним правилима кривичне процедуре којом се одобрава претрес рачунара. Осим тога, од пружалаца услуга електронских комуникација се могу тражити и подаци о кориснику (име и презиме, адреса, дужина коришћења и врста комуникационих услуга које користи и начин плаћања) али, такође, само на основу одлуке суда. Из тог разлога је предвиђена могућност да јавни тужилац до добијања налога суда може наредити пружаоцима услуга да задрже, односно обезбеде у неизмењеном облику одређене податке, и то до 90 дана (са могућношћу продужења рока за још 90 дана).

1.2. Велика Британија

У Великој Британији не постоје специфичне одредбе о мери хитног чувања података, али постоји низ овлашћења надлежних органа чијом применом 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[491], затим одговарајућих чланова Закона о уређењу истражних

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

овлашћења из 2000. године[492] и Закона о полицијским и кривичнопроцесним доказним радњама из 1984. године[493]. 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 складу са другим одељком Закона о полицији и кривичнопроцесним доказним радњама[494] 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 (*indictable offence*), да се у одређеној просторији могу пронаћи предмети од значаја за истрагу кривичног дела, тј. који могу бити релевантни докази, а на које се не односе законске привилегије или се не примењује 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

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

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

[494] *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. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117591/pace-code-b-2011.pdf.

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). Одузети предмети се одузимају ради форензичке обраде за потребе представљања у поступку пред судом (члан 22. став 3).

Трећи део Закона о уређењу истражних овлашћења[495] 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 (у члановима 49-56).

Пресретање комуникација се у Великој Британији врши у складу са 1. поглављем Закона о уређењу истражних овлашћења[496]. Након одређивања кривичног дела неовлашћеног пресретања (члан 1) и консенсуалног пресретања (члан 3), Закон регулише предузимање истражне радње *пресретање комуникација* на основу налога. Пресретање комуникације се може одредити уколико је то потребно за остваривање одређеног циља (између осталог и ради спречавања или доказивања озбиљних кривичних дела) и пропорционално је остваривању тог циља, тј. да се циљ не може остварити ни на један други начин (члан 5. ставови 3. и 4). На основу налога државног секретара, а поводом захтева одређених лица (наведених у члану 6) се може овластити или наредити лицу да предузме

[495] http://www.legislation.gov.uk/ukpga/2000/23/contents

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

прикупљање података о садржају комуникације која се остварује у реалном времену (а које су обухваћене налогом) као и предавање пресретаних комуникација и других података о комуникацији (члан 5. став 1). Налогом се пресретање одређује на период до 3 месеца, уз могућност продужења уколико и даље постоје разлози због који је првобитан налог издат (члан 9. став 6), а пружаоцима телекомуникационих услуга се може одредити накнада за трошкова насталих у вези са извршавањем налога (члан 14). Осим пресретања комуникација, Закон у 2. поглављу предвиђа и *прикупљање других података о комуникацији* (чланови 21-25). Под другим подацима се подразумевају подаци о саобраћају (односно подаци који могу да идентификују лице, уређај или локацију, као и подаци који идентификују рачунарски податак, датотеку или програм преко којих се комуникација остварује у смислу члана 2. става 9) као и подаци о кориснику услуга. Полиција може од пружалаца телекомуникационих услуга захтевати предавање података о комуникацији а који су у њиховом поседу или које могу на легалан начин прибавити, уколико је то потребно за остваривање одређених циљева (међу којима су и откривање и спречавање кривичних дела) и у сразмери за тим циљем (члан 22).

2. ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ДРЖАВАМА КОНТИНЕНТАЛНО-ЕВРОПСКОГ КРИВИЧНОПРОЦЕСНОГ СИСТЕМА

2.1. Немачка

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, јер немачки Закон о кривичном поступку[497] 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 Закона које се односе на обезбеђење и одузимање предмета уопште, као и одредбу члана 100г који даје основ за хитно

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

чување података о саобраћају у складу са принципом сразмерности[498]. 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). За одузимање предмета (и рачунарских података) потребна је, по правилу, наредба суда[499]. Поред тога, 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[500]. Законик не предвиђа никаква 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 је Немачка делимично 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, 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 тајног надзора комуникација) или да је покушало извршење таквог дела (у случају да је покушај кажњив) или *да је извршило било које кривично дело употребом рачунарског система*[501], подаци о саобраћају (и то само они у складу са

[498] C. Roxin, B. Schunemann, Strafverfahrensrecht, 27. Auflage, Munchen 2012, 291.

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

[500] Roxin, *op.cit.*, 292.

[501] Ова одредба се, дакле, може применити у свим случајевима када је кривично дело почињено употребом телекомуникационих средстава, без обзира на то да ли се ради о тешком кривичном

члановима 96. и 113а Закона о телекомуникацијама) могу се захтевати од пружаоца услуга и без знања и сагласности корисника услуга. 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 је то потребно за утврђивање чињеничног стања и боравишта осумњиченог, а резултати се нису могли остварити на другачији начин и ако су трошкови прикупљања сразмерни за значајем конкретног случаја. Осим наведеног, полиција може упутити захтев за утврђивање идентитета корисника динамичке *IP* адресе (у виду тзв. захтева за откривање података о претплатнику услуге), што је нарочито корисно у пракси[502]. Наиме, на основу члана 163. Закона о кривичном поступку 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 пружалаца услуга електронских комуникација 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 кривично гоњење учиниоца кривичног дела које се гони по службеној дужности[503].

Закон о кривичном поступку не садржи посебне одредбе о претресу рачунара, него се примењују опште одредбе о претресу просторија и покретних ствари садржане у Одељку VIII Закона[504]. 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 која се претреса може се проширити и на медије за похрањивање података који су од истог

делу или делу малог значаја, нпр. када су електронска пошта, телефонски позиви или интернет употребљени за извршење кривичног дела, нпр. за онлајн превару.

[502] Roxin, *op.cit*., 298.

[503] У Немачкој није могуће затражити задржавање података о саобраћају од оператора, 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 телекомуникацијама, и ти подаци се могу затражити у складу са поменутом одредбом ЗКП-а. Gercke, Brunst, *op.cit,* 115.

[504] Овај одељак се односи на регулисање одузимање предмета, надзор телекомуникација, компјутерско сравњење личних података, коришћење техничких средстава, коришћење прикривених истражитеља и претресање.

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 је 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 мерама која 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 исту 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, исте се не могу поново одредити у истом поступку. Обавеза предавања предмета не односи се на лица који имају право да не сведоче (члан 52[505] и 53[506]). Од појединих категорија лица није дозвољено ни одузимање предмета докле год се користе правом да не сведоче (члан 97. став 4), односно одређених врста

[505] У складу са чланом 52. право да одбију сведочење има: 1. лице са којом је окривљении верен, односно са којим је размењио 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.

[506] 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 своргзанимања; 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 сазнале у обављању свог занимања; чланови адвокатске коморе имају исти ранг као адвокати; 3а. чланови или овлашћени представници лиценцираног саветовалишта, у складу Законом о о конфликту трудноће, о ономе што им је поверено или су сазнали у обављању свог занимања; 3б. саветници за питања зависности од наркотицика у саветовалишту које је лиценцирано или основано од стране државног органа или правног лица, установе или фондације, о ономе
што им је повјерено или су сазнали у обављању свог занимања; 4. чланови Парламента, Савезне скупштине, Европског парламента или покрајинског парламента о лицима које суим 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 учествовале 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.

предмета[507], 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 окончања сравњивања, 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.

Осим тога, предвиђено је компјутерско сравњивање података као мера којом се лични подаци лица, чија се обележја поклапају са обележјима учиниоца, компјутерски сравњују са другим подацима, како би се искључила лица које нису осумњичена, односно утврдила лица које имају друга обележја значајна за истрагу. Мера се може одредити уколико постоји довољно чињеничних показатеља да је почињено неко од законом одређених тешких кривичних дела (члан 98) и то само ако би испитивање чињеничног стања или утврђивање пребивалишта учиниоца на другачији начин било мање успешно или значајно отежано. Сравњивање података може наредити само суд, а у случају опасности од одлагања и тужилаштво, у ком случају се одмах тражити потврда суда (ако наредбу тужилаштва у року од три радна дана не потврди суд, иста престаје да важи). Наредба се издаје у писаном облику, и садржи име задужене особе а ограничава се на податке и обележја потребна за конкретни случај. На захтев тужилаштва, орган који похрањује податке који су потребни за компјутерско сравњивање треба да пружи помоћ органу који врши сравњивање података, те да у ту сврху тражене податке издвоји из базе података и преда их органима за кривично гоњење[508].

[507] Није дозвољено одузимање носилаца аудио и видео снимака и носилаца података, слика и других илустрација која држе лица које професионално учествују или су учествовале 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

[508] Уколико се тражени подаци могу издвојити од других података само са несразмерно великим тешкоћама, онда се на основу наредбе морају проследити и остали подаци (при чему се изричито

У погледу *надзора и снимања телекомуникација без знања лица* чији разговор се надзире, немачки Закон о кривичном поступку у члану 100а[509]предвиђа да је одређивање ове радње дозвољено под следећим условима: 1) ако одређене чињенице оправдавају сумњу да је неко као учинилац или саучесник учинио неко од тешких кривичних дела (која су таксативно наведена у члану 100. ставу 2, а међу којим је од дела против безбедности рачунарских података изричито наведена само компјутерска превара), покушао да учини дело чији је покушај кажњив или је кривичним делом припремио такво дело, 2) ако дело и као појединачно дело има тежину, и 3) ако утврђивање чињеничног стања или боравишта осумњиченог на неки други начин нема изгледа за успех или је значајно отежано. Наредба се односи само на осумњиченог или лица за које се на основу одређених чињеница сумња да у име осумњиченог или од осумњиченог примају и прослеђују поруке или да осумњичени користи њихов прикључак. Меру може наредити само суд одлуком у писаном облику на захтев тужилаштва, а уколико постоји опасност од одлагања, наредбу може издати и тужилаштво (с тим да таква наредба престаје важити, ако је у року од три радна дана не потврди суд) и њено извршење може трајати најдуже три месеца (а дозвољено је продужење за још максимално три месеца, ако су испуњени услови из наредбе у смислу резултата добијених истрагом). На основу наредбе, сваки субјект чија је делатност пружање или учешће у пружању телекомуникацијских услуга мора омогућити суду, тужилаштву и њиховом истражном особљу у полицији спровођење мера и доставити потребне информације без одлагања. Питање да ли и у ком обиму треба предузети одговарајуће припреме решава се у складу са Законом о телекомуникацијама и Правилником о надзору телекомуникација. Ради заштите приватности лица, значајна је одредба која предвиђа да уколико постоје чињенице које упућују на закључак да би се путем мере стекло само сазнање из приватног

наводи да коришћење тих осталих података није дозвољено). Занимљива је и одредба на основу које се у циљу расветљавања кривичног дела или утврђивања боравишта лица која се тражи у сврху кривичног поступка, омогућава компјутерско сравњивање личних података из једног кривичног поступка са другим подацима који су аутоматски похрањени ради кривичног гоњења, извршења кривичне санкције или спречавања опасности.

[509] Осим тајног надзора и снимања телекомуникација, Закон предвиђа и друге тајне мере: тајно тонско надзирање стамбених просторија: прислушкивање и снимање техничким средствима разговора који нису намењени јавности а који се воде у дому (члан 100ц), тајно тонско надзирање на јавним местима: прислушкивање и снимање техничким средствима разговора који нису намењени јавности а који се воде изван стана (100ф), оптичко снимање (100х), али ове мере нису релевантне у смислу одредаба Конвенције.

живота тих лица, таква мера није дозвољена. Такође, сва сазнања о приватном животу која стекну путем мере не смеју се даље користити, снимци о таквим сазнањима морају се одмах избрисати, а стицање таквих сазнања и брисање записа о истима мора се документовати у списима. Немачки Закон у члану 100и регулише *употребу специфичног уређаја* који служи за утврђивање 1. броја прикључка мобилног апарата и броја картице која је у њему коришћена, као и 2. локације мобилног апарата. Ако на основу одређених чињеница постоји сумња да је неко као учинилац или саучесник учинио кривично дело које је и као појединачно дело од посебног значаја, а поготово неко од дела из 100а, односно да је покушао починити дело чији је покушај кажњив или је кривичним делом припремио такво дело, онда се за потребе утврђивања чињеничног стања и боравишта осумњиченог може одредити употреба тог техничког средства. Ову меру одређује суд писаном наредбом и њено извршење може трајати најдуже шест месеци (с тим да је дозвољено продужење за најдуже шест додатних месеци, ако су и даље испуњени услови за одређивање мере). Уколико се приликом извршења мере прикупе лични подаци о трећим лицимам јер је то из техничких разлога неизбежно за постизање циља, такви се подаци не смеју користити у друге сврхе осим сравњења података ради утврђивања траженог броја апарата и броја картице, а након окончања мере одмах се морају избрисати[510].

2.2. Шпанија

У Шпанији процесно законодавство до скоро није садржало одредбе о чувању рачунарских података на експедитиван начин[511], али у складу са прописима Законом о задржавању података[512] постојала 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

[510] Види, Roxin, *op.cit*., 299-300.
[511] *Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal*, http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf.
[512] *Ley 25/2007 de conservación de datos comunicaciones electrónicas*, http://www.boe.es/boe_gallego/dias/2007/10/23/pdfs/A03094-03100.pdf.

рачунарских система. Дакле, Шпанија раније није имплементирала одредбу члана 16. Конвенције на одговарајући 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 електронских комуникација да задржавају податке о саобраћају и о кориснику услуге, не омогућава се 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. Међутим, Законом о изменама Закона о кривичном поступку у погледу оснаживања процесних гаранција и уређења техничких истражних мера[513] из октобра 2015. године у шпанско законодавство уврштене су одредбе којима се прецизно регулише предузимање радњи и мера значајних за прикупљање електронских доказа. Поглавље десето односи се на *привремене мере обезбеђење рачунарских података* (588 octies). Наиме, јавни тужилац или судска полиција може сваком физичком и правном лицу издати наредбу за очување и заштите потребних података и информација до доношења потребне одлуке суда којом се одобрава извршење неке од претходно наведених радњи и мера. Наредбом се лица обавезују да обезбеде податке у трајању до 90 дана (уз могућност продужења до максимално 180 дана). На тај начин је одредба Конвенције имплементирана на одговрајући начин.

Закон о кривичном поступку није садржало одредбе о претресу рачунара, него су се сходно примењивале одредбе о претресу просторија, што је било неадекватно решење. Законом о изменама Закона о кривичном поступкуж из октобра 2015. године у шпанско законодавство уврштене су одредбе којима се прецизно регулише предузимање радњи и мера значајних за прикупљање

[513] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725. Закон је донет 5. окотбра а са применом се почињен 6. децембра 2015. године.

електронских доказа. Четврто поглавље садржи одредбе заједничке за три истражне радње: а) пресретање телефонских и разговора другим телекомуникационим средствима, б) приступ подацима потребним за идентификовање корисника, терминалних уређаја и уређаја за повезивање са рачунарском мрежом в) остваривање приступа садржају електронских уређаја; г) остваривање приступа садржају удаљених рачунара (чланови 588 bis a- 588 bis k). Да би се ове радње могле применити у истрази конкретне ствари, потребно је судско одобрење уз пуно поштовање принципа одређености, адекватности, јединствености, потребности и пропорционалности. Принцип одређености подразумева да је радњу могуће применити само у погледу истраге тачно одређеног кривичног дела, али не и у циљу спречавања или откривања кривичног дела нити уколико не постоји сумња поткрепљена чињеницама. Принцип адекватности подразумева да су објективни и субјективни обим и трајање радње одређени њеном корисношћу. Радње се могу одредити само изузетно уколико не постоје друге радње које би биле мање штетне по гарантовања људска права а више корисне за истрагу или уколико би утврђивање или потврда чињеница или одређивање њиховог извора било знатно отежано без примене радње. Приликом одређивања радње потребно је у сваком конкретном случаја утврдити да штета по људска права која се ограничавају није већа од добробити које би одређивање радње донело. Оцењујући супротстављене интересе (заштита права окривљеног и јавног интереса), суд је дужан да узме у обзир друштвени значај кривичне ствари, степен техничке интрузивности радње, постојеће доказе и очекивање доказне резултате до којих би се дошло применом радње.

Суд доноси одлуку по службеној дужности или на захтев јавног тужиоца или судске полиције, који садржи: чињенични опис кривичног дела, податке о идентитету окривљеног (уколико су познати), детаљно образложење потребе да се радња одреди у складу са наведеним принципима (уз навођење доказа који су прикупљени до тада), опис техничког уређаја који ће се користити, потребно време трајања радње, назив органа који ће извршавати радњу. Суд ће најкасније у року од 24 часа од подношења захтева, захтев одбити или одобрити, након позивања и усменог образложења подносиоца (уз могућност да тражи додатна објашњења). Судска одлука садржи чињенични опис и правну квалификацију

кривичног дела, образложење у погледу потребног степена сумње, податке о идентитету окривљеног (уколико су познати), образложење потребе да се радња одреди, трајање радње, одређење јединице судске полиције који ће радњу извршити, начин и учесталост у ком је подносилац захтева дужан да извештава суд о резултатима радње, циљ који се има остварити извршењем радње, обавезивање одређених субјеката у вези са извршењем радње да сарађују и чувају као тајну података да се радња извршава. Извршење радње не може трајати дуже од времена које је потребно да се постигне у одлуци суда одређени циљ, али постоји могућност да суд (по служеној дужности или на захтев подносиоца првобитног захтева) продужи трајање докле год постоје разлози због којих је радња одређена. Захтев за продужење садржи детаљан извештај о то тада постигнутим резултатима и образложење потребе да се одреди продужење радње, а суд доноси одлуку у року од два дана од подношења захтева.

Судска полиција као орган који извршава радњу дужна је да суд на начин и у интервалима одређеним у судској одлуци извештава о току и постигнутим резултатима. Осим тога, судска полиција је дужна да престане са извршавањем радње, чим престану разлози за њено извршавање. Суд може својом одлуком обуставити извршење радње у сваком моменту у току извршења уколико, на основу обавештења добијених од судске полиције, процени да су престале да постоје околности које су оправдавале одређивање радње или да постигнути резултати нису задовољавајући. Након доношења одлуке о окончању радње, бришу се и уклањају оригинални подаци прикупљени током извршавања радње а који су похрањени у рачунарском систему, док се претходно направљена копија података уништавају уколико буде донета ослобађајућа или одбијајућа пресуда (осим уколико суд не захтева другачије).

Одељак трећи односи се на *приступ подацима потребним за идентификовање корисника, терминалних уређаја и уређаја за повезивање са рачунарском мрежом* (588 ter k- ter m).Уколико током вршења задатака у вези са спречавањем и откривањем кривичних дела почињених употребом Интернета судска полиција уочи IP адресу која је употребљена у вези са извршењем кривичног дела или друге податке који могу послужити идентификацији и лоцирању опреме и уређаја коришћених за успостављање везе са рачунарском

мрежом или податке који могу указати на идентитет корисника, овај орган може захтевати од суда да обавеже (у претходном делу наведена) лица на сарадњу у смислу предаје података потребних за идентификовање и лоцирање осумњиченог, терминалних уређаја или уређаја за повезивање са рачунарском мрежом.
Уколико током истраге није могуће утврдити одређени претплатнички број а то је неопходно за потребе истраге, судска полиција је овлашћена да користи техничке уређаје који обезбеђују приступ кодовима за идентификацију уређаја и опреме које припадају кориснику телекомуникационе услуге (*IMSI* или *IMEI* бројеве). Након остваривања приступа кодовима који омогућавају идентификацију уређаја судска полиција може захтевати одређивање радње пресретања комуникација.

Уколико је јавном тужиоцу или судској полицији потребно да утврде ко је власник одређеног телефонског броја или броја другог средства комуникације, односно да добију одређене идентификујуће податке корисника, могу се директно обратити пружаоцима услуга, који су дужни да податке предају, под претњом да ће се сматрати да су извршили кривично дело онемогућавања вршења службене дужности.

У осмом одељку садржане су одредбе о *остваривању приступа садржају електронских уређаја* (чланови 588 е а-588к). Уколико је приликом претреса стана потребно да се одузму рачунари, телефони или други телекомуникациони уређаји или уређаји за складиштење података или за приступ електронским базама података, потребно је да одлука суда о претресу стана садржи о образложену одлуку којом се судска полиција овлашћује да оствари приступ садржају тих уређаја. Наиме, овлашћење судске полиције да одузме наведене уређаје приликом претреса стана не обухвата овлашћење да се оствари приступ садржају тих уређаја, него је потребно накнадно одобрење суда. Одредба која се односи на приступ подацима садржаним у наведеним електронским уређајима и опреми примењује се и у ситуацијама независно од претреса стана. У тим случајевима, судска полиција је дужна да обавести суд о одузетим уређајима, те ће суд, уколико процени да је приступ садржају уређаја неопходан, овластити за то судску полицију.

Одлука суда којом се дозвољава приступ садржају уређаја и опреме утврђује услов и обим остваривања увида у садржај (између осталог, може

садржати овлашћење за копирање података), а нарочито се утврђују услови потребни да се очува аутентичност и интегритет садржаја, а по потреби се одређује вештачење. Ови уређаји се одузимају са лица места (обавезно уколико се ради о објекту или средству напада), но уколико постоје околности које овакво поступање не чине оправданим (уколико би одузимање рачунара и других уређаја произвело знатну штету власнику или држаоцу) могуће је стварање копије уређаја под условима који гарантују аутентичност и интегритет садржаја.

Уколико се током извршавања ове радње постоје околности које указују да се тражени подаци налазе у другом рачунарском систему или делу система, суд може одобрити проширење обухвата те радње, под условом да се том другом рачунару, односно делу рачунара може законито приступити из уређаја који је предмет радње. Овакво овлашћење може бити садржано у иницијалној одлуци суда или садржано у накнадно донетој одлуци. У изузетно хитним случајевима, судска полиција може предузети ову радњу и без претходне одлуке суда али уз обавезу да о томе обавести суд најкасније у року од 24 часа, а суд у року од 72 часа може својом образложеном одлуком потврдити или поништити дејство овако предузете радње. Орган надлежан да извршава ову радњу може наредити лицима која имају сазнања о раду предметног уређаја да пруже информације потребне за обезбеђење садржаја (осим окривљеном, лицима која су ослобођена дужности сведочења услед постојања одређеност степена сродства или обавезе чувања професионалне тајне).

Девети одељак посвећен је *остваривању приступа садржају удаљених рачунара* (588 f a –588 f b). Улазак у удаљени рачунар суд може одобрити само у погледу одређених кривичних дела: кривичних дела извршених од стране криминалне групе; тероризма; кривичних дела учињених против малолетних лица или лица са ограниченом пословном способношћу; кривичних дела против уставног уређења и националне безбедности и кривичних дела која су извршена употребом рачунара или информационе технологије или телекомуникационих услуга. Ова радња подразумева употребу идентификационих података и кодова, те инсталацију одређених софтвера који омогућавају да се са даљине прегледа удаљени рачунар и т без знања власника или корисника уређаја, те да се оствари приступ садржају рачунара, телефона или других телекомуникационих уређаја

или уређаја за складиштење података или за приступ електронским базама података. Судска одлука одређује уређај који је предмет радње, обухват и начин остваривања приступа и одузимања похрањеног садржаја (релевантног за конкретан случај) применом одређеног софтвера, органе којима се поверава извршење радње, начин очувања интегритета одузетих података и евентуално овлашћење да се незаконити садржаји обришу или да им се онемогући приступ. У одлуци суда се одређује и трајање радње до највише месец дана, али постоји могућност проширења трајања до максимално три месеца.

Пружаоци услуга и лица наведена у општим одредбама, а нарочито власници и администратори рачунарске мреже, дужни су да сарађују у смислу да омогуће органу који извршава раду приступ рачунарској мрежи и систему, те да пруже све информације потребне за предузимање радње (осим окривљеног и лица која су ослобођена дужности сведочења услед постојања одређеност степена сродства или обавезе чувања професионалне тајне). На овај начин Шпаније је у потпуности на одговарајући начин прилагодила своје законодавство одредбама Конвенције.

Шпански Закон о кривичном поступку предвиђа могућност задржавања поштанске и телеграфске комуникације ако је та мера потребна за откривање или потврђивање одређене чињенице битне за кривични поступак (члан 579.став 1) а даљи чланови (580-588) уређују процедуру узапћења писама и телеграма. Осим тога суд може да нареди и надзор поштанске, телеграфске и телефонске комуникације за период до 3 месеца (уз могућност продужења за још три месеца) у погледу лица за које постоји сумња да је извршилац било ког кривичног дела (члан 579.став 3). Надзор и снимање комуникација које се остварују другим техничким средствима није се до скоро помињало[514], а овај недостатак исправљен је изменама из октобра 2015. године. Одељак четврти посвећен је регулисању *пресретању телефонских и разговора другим телекомуникациним средствим*а (588 ter a- ter j). Радња се може одредити само у погледу таксативно набројаних кривичних дела (у члану 579.1) или у погледу било ког другог кривичног дела

[514] О критици шпанског Законика због недостатка процесне могућности за тајни надзор комуникација за потребе кривичног поступка, J. Pradillo, „Fighting against cybercrime in Europe: the admissibility of remote searches in Spain“, *European journal of crime, criminal law and criminal justice*, 19/2011, 363–395.

уколико је извршено употребом рачунара или информационе технологије или средстава комуникације.

Суд одобрава приступ садржају и подацима о комуникационом саобраћају у погледу тачно одређен комуникације у којима окривљени учествује као пошиљалац или прималац порука. Радња се односи на уређаје и средства које користи или поседује окривљени или оштећени, у случају озбиљне угрожености његовог живота или физичког интегритета). Изузетно, може се одредити и према уређајима и средствима које користе или поседује трећа лица уколико постоји доказ да то лице прима или преноси поруке за окривљеног или уколико то лице има учешћа у незаконитим активностима са окривљеним, односно има користи од њих. Осим тога, могуће је одредити радњу и уколико окривљени користи уређај користи без знања власника/корисника.

Захтев за одобрење радње садржи: 1) идентификациони број (или другу техничку ознаку) уређаја или идентификационе податке о окривљеном или податке потребне за одређивање средства комуникације; 2) одређивање обима радње утврђивањем: врсте комуникације и очекиваног садржаја или извора и одредишта комуникације и временског периода у ком се остварује комуникација или географске локације извора и одредишта комуникације или других релевантних података о саобраћају комуникације (у ком случају захтев мора да определи одређене податке који ће се прикупити радњом).

Прописана је дужност сарадње за све пружаоце телекомуникационих услуга, те услуге приступа рачунарским мрежама и другим услугама заснованих на информационим технологијама, односно за сва лица која на било који начин доприносе или омогућавају комуникацију употребом телефона или другог телекомуникационог средства. Дужност сарадње обухвата и дужност да се као тајна чува чињеница спровођења радње.

У вези са контролом извршавања радње, судска полиција је дужна да у извештају који доставља суду достави транскрипте релевантних делова разговора, као и оригиналне записе целокупне комуникације у периоду извештавања. У извештају морају бити наведени извор и одредиште комуникације, а записи морају бити заштићен употребом напредног електронског потписа или неког другог система који обезбеђује поузданост, аутентичност и интегритет података

који се преносе са рачунара домаћина на дигитални медиј на ком се комуникација снима.

Иницијално се радња може одредити на период до 3 месеца, а који се рачуна од момента издавања судске одлуке, с тим да постоји могућност продужења до свеукупног трајања до 18 месеци. По окончању радње копија делова разговора и транскрипти се достављају јавном тужиоцу (уз искључење делова који се односе на интимну сферу живота лица погођених радњом). Такође, предвиђена је дужност суда да обавести лице против кога је радња одређена (осим уколико би то угрозило даљи ток истраге) те да му преда копију записа или транскрипт, под условом да се тиме не вређа право на приватност трећих лица и да није у супротности са интересима поступка. Осим тога, предвиђена је могућност да се електронски подаци, које пружаоци услуга чувају у складу са прописима о задржавању података на сопствену иницијативу или у комерцијалне сврхе, „инкорпорирају“ у кривични поступак на основу одлука суда. Дакле, уколико би такви подаци били од значаја за истрагу конкретног кривичног дела, суд може одлучити да се прикупе подаци садржани у електронским базама пружалаца услуга.

2.3. Португалија

На основу Закона о компјутерском криминалу[515] 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 постати 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

[515] *Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa*, https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf.

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 одмах 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) (члан 12.). 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 пружалаца услуга електронских комуникација чије услуге су коришћене у оствареној комуникацији.

Закон о компјутерском криминалу у члановима 15. и 16. регулише претрес ради претраге рачунарских података и одузимање 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. 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. Члан предвиђа ограничења у погледу одузимања одређених категорија података. Наиме, ако током претреса ради претраге рачунарских података полиција наиђе документе са личним или интимним 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 им се онемогућава приступ у систему.

У вези са вршењем претреса ради претраге рачунарских података 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 предавање 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 се на одређене професије).

У Португалији је пресретање комуникација у складу са Законом о компјутерском криминалу дозвољено само у фази истраге поводом кривичног дела које је извршено употребом рачунарског система у смислу поглавља 2. Закона као и других кривичних дела када је потребно прикупљање електронских доказа. У складу са чланом 18. *пресретање и снимање рачунарских података који се преносе путем рачунарског система* на основу предлога јавног тужиоца одређује истражни судија уколико постоје разлози који указују да је предузимање ове радње неопходно за утврђивање истине или да би то било немогуће или знатно отежано применом других радњи и мера. Ова радња се може односити како на прикупљање података о саобраћају комуникације, тако и на садржај комуникације, а у наредби се утврђује обухват података који се прикупљају, у складу са околностима конкретног случаја. Овај члан предвиђа сходну примену одговарајућих одредаба Законика о кривичном поступку[516] које се односе на пресретање телефонских разговора (у члановима чланове 187,188. и 189). Значајно је да радњу може и у изузетно хитним случајевима одредити и јавни тужилац, али је у року д 72 часа потребно да његову наредбу потврди истражни судија, у супротном се извршење радње обуставља. Пресретање може трајати најдуже три месеца, уз могућност продужења за још три месеца. Осим тога, члан 189. Законика проширивао је примену одредаба о надзору и снимању телефонских разговора на комуникације које се остварују другим техничким средствима (наводећи електронску пошту и друге видове преноса података у рачунарском систему) али само ако постоји сумња да је извршено неко од кривичних дела који су наведени у члану 187. Законика. Међутим, одлуком Врховног суда из јануара 2015. године је утврђено да се члан 189. Законика не

[516] http://www.gddc.pt/codigos/code_criminal_procedure.html.

примењује више на режим надзора електронских комуникација у вези са делима компјутерског криминала, него да се примењује само Закон 109/2009[517].

2.4. Холандија

У холандском Закону о кривичном поступку[518] постоји одредба која регулише меру хитног очувања података (члан 125). Наиме, 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 кривично гоњење учинилаца одређеног кривичног дела, да их сачува у неизмењеном облику, а уколико се подаци односе на електронску комуникацију, пружалац услуга је дужан да пружи довољно података потребних за утврђивање идентитета других пружалаца услуга електронских комуникација чије мреже или услуге су коришћене у релевантној комуникацији. Захтев се може упутити у писаном облику или усмено (али се у том случају у року од три дана саставља у писаном облику наредба са потписом јавног тужиоца) а садржи следеће елементе: тачно одређење података које је потребно сачувати, образложење, временски период за који се захтева чување података (до 90 дана), те да ли се захтев односи и на податке потребне за откривање идентитета других пружалаца услуга електронских комуникација 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.

Закон о кривичном поступку уређује претрес рачунара међу одредбама којима се регулише претрес просторија и 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

[517] Одлука Врховног суда од 20.01.2015. године, http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument.

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

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 тајне). 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 (наводе се 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

аутоматско 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 погођен овом мером, прикупљени подаци уништавају, чим се утврди да прикупљени подаци до који 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).

Законик о кривичном поступку међу специјалним истражним техникама које се могу применити у истрази одређених кривичних дела, која по својој природи или повезаности са другим кривичним делима представљају тешку повреду владавине права, регулише и спровођење *тајног надзора комуникација које се остварују путем система за аутоматску обраду, пренос и складиштење података*. Радња се може одредити првенствено у погледу кривичних дела за која је предвиђена казна затвора од најмање четири године, као и у погледу таксативно наведених кривичних дела из Кривичног закона, међу којима су и неовлашћен приступ рачунару (138а), неовлашћено ометање приступа рачунарској мрежи (138б), неовлашћено прислушкивање комуникација техничким средствима (139ц), неовлашћено ометање комуникација техничким средствима (139д) и угрожавање безбедности употребом техничких средстава (285б). Пружаоци услуга електронских комуникација (члан 126*l*) се обавезују на сарадњу тако да омогуће спровођење радње на основу наредбе истражног судије издате поводом предлога

јавног тужиоца. Осим тога, на сарадњу се могу обавезати и друга лица, осим осумњиченог, уколико се претпоставља да имају информације потребне за декрипцију енкриптованих комуникација (126*m*). У складу са чланом 126*n* јавни тужилац може, ако то налажу разлози истраге кривичних дела наведених у члану 67, да од пружалаца услуга електронских комуникација тражити да доставе податке о кориснику услуга и о томе које услуге електронске комуникације користи, у моменту подношења таквог захтева или у наредна три месеца од подношења таквог захтева. Осим тога, и полиција може од пружалаца услуга тражити достављање следећих података о кориснику: име и презиме, адресу, број и врсту услуга које користи (члан 126*na*). У складу са чланом 126т у случају сумње да је организована криминална група извршила или да припрема извршење кривичних дела из члана 67, јавни тужилац је овлашћен (није потребна наредба истражног судије) да изда наредбу полицији да предузме радњу тајног надзора комуникација које се остварују путем система за аутоматску обраду, пренос и складиштење података.

2.5. Италија

У Италији су изменама Законика о кривичном поступку из 2008. године[519] 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

[519] *Testo del decreto-legge 23 maggio 2008, n. 92 (in Gazzetta Ufficiale - serie generale - n. 122 del 26 maggio 2008), coordinato con la legge di conversione 24 luglio 2008, n. 125 (in questa stessa Gazzetta Ufficiale alla pag. 6), recante: «Misure urgenti in materia di sicurezza pubblica»*, http://www.altalex.com/index.php?idnot=41643.

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[520]. Наиме, на основу члана 132. Закона, телекомуникациони оператори 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 пружалаца услуга електронских комуникација 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 пружаоцима услуга електронских комуникација за предају рачунарских података потребних за откривање кривичног дела и учиниоца. Након што утврди да су испуњени законски услови, јавни тужилац издаје наредбу 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 (члан 256.ЗКП).

Изменама Законика из 2008. године унете су и одредбе које имају за циљ да омогуће вршење претреса рачунара[521]. Наиме, у члану 247, који одређује услове за предузимање радње претреса 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 предавање истих, а уколико одбије да учини, суд може издати наредбу за

[520] *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.

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

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 одговарајућем 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.

Законик о кривичном поступку регулише *пресретање разговора и других комуникација*, односно телефонских разговора и комуникација које се остварују другим телекомуникационим средствима. Радња се може одредити у погледу тешких кривичних дела у смислу члана 266[522], док члан 266 *bis* проширује могућност одређивања радње и у погледу других кривичних дела која су извршена употребом информационих система и телекомуникационе технологије и тиме дозвољавајући пресретање комуникација које се преносе преко рачунарских система. На предлог јавног тужиоца судија за претходни поступак одобрава извршење радње уколико постоје озбиљне индиције да је учињено неко од наведених кривичних дела а радња је неопходна за настављање истраге. Ако то налажу разлози изузетне хитности, јавни тужилац може одредити предузимање

[522] Ради о кривичним делима за која је запрећена доживотна казна затвора или казна затвора од најмање пет година, кривичним делима против јавне администрације за која је запрећена казна затвора од најмање пет година, кривичним делима у вези са дрогом и другим психотропним супстанцама, кријумчарењем и дечјом порнографијом, те кривичним делима изнуде, незаконите финансијске активности, манипулација на тржишту, узнемиравања употребом телефона.

ове радње, али је о томе дужан да у року од 24 часа обавести суд коју у року од 48 часова од одређивања радње одобрава наредбу тужиоца (уколико наредбу не потврди, радња се обуставља, а резултати се не могу користити као доказ). Извршење радње не може трајати дуже од 15 дана али по основу одобрења суда се може продужити до две недеље уколико и даље постоје разлози за одређивање радње.

Осим тога, на основу члана који уређује узапћење пошиљки, предвиђа се да суд може обавезати пружаоце телекомуникационих услуга да „заплене“ електронску комуникацију уколико се процени да је у комуникацији учествовао окривљени или је повезана са извршењем кривичног дела (члан 254). Полиција чак може у хитним случајевима наредити оператерима да зауставе прослеђивање електронске комуникације, али за то мора обезбедити сагласност јавног тужиоца у року од 48 часова, у супротном се мера обуставља (члан 353. став 3). Уколико је заплену наредила полиција, дужна је комуникацију у одговарајућем облику предати суду без одлагања, без измена и без сазнавања садржаја комуникације. Када се нареди заплена комуникација на овај начин, пружаоци услуга се обавезују да предају податке о кориснику, као и податке о саобраћају комуникације и о локацији учесника у комуникацији, а који подаци су похрањени у њиховим информационим системима, при чему је омогућено и предавање копија података (уколико је то нужно ради нормалног функционисања система) али су тада у обавези да примене одговарајуће мере да задрже аутентичност и интегритет података (члан 254-bis).

2.6. Финска

У Финској је у члану 24. Закона о мерама процесне принуде[523], а у вези са претресом рачунарских уређаја (чланови 20-23), изричито регулисано хитно чување података (као налог за задржавање 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

[523] *Pakkokeinolaki 806/2011,* http://www.finlex.fi/fi/laki/kaannokset/2011/en20110806.pdf.

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 поруци која се преноси у информационом систему (наредба 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, занимљиво је да се мера може односити и на податке за које се претпоставља да ће бити упућени рачунарском уређају, односно пренети 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 пружалаца услуга. Наредба се 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.

Претрес рачунарских уређаја је регулисан у оквиру поглавља 8. Закона о мерама процесне принуде (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 процедуре 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 су у складу са законом имају право, односно обавезу да одбију сведочење (у складу са поглављем 7, чланом 3, ставовима 1. и 2).

Закон о мерама процесне принуде десето поглавље посвећује прикривеним мерама принуде које се одређују када постоји вероватноћа да се њиховом применом може доћи до информација корисних за разјашњење кривичног дела, под условом да је њихова примена потребна и од изузетног значаја, тако да се са извршавањем престаје и пре истека временског периода за које су одређена уколико су испуњени циљеви или су престали разлози одређивања радње. У члану 3. поглавља уређује се *пресретање комуникација, односно надзор и снимање порука* које шаље осумњичено лице или су њему упућене, а које су послате или се преносе преко рачунарске комуникационе мреже како би се сазнао садржај порука и утврдили подаци о саобраћају комуникације. Пресретање комуникација може бити усмерено или ка одређеној адреси у рачунарској мрежи или ка терминалном уређају за који се претпоставља да користи лице осумњичено за тешка кривична дела таксативно набројана у ставовима 2-5. члана 3. Осим тога, уколико су наведене поруке и идентификујући подаци[524] у вези са њима недоступне за пресретање, полиција може тражити њихово одузимање, односно копирање из информационих система пружалаца услуга електронских комуникација, у складу

[524] У погледу идентификујућих података Закон упућује на члан 2. став 8. Закона о заштити приватности електронских комуникација, у ком су они одређени као подаци помоћу којих се може утврдити идентитет корисника а који се обрађују у телекомуникационим рачунарским мрежама ради преноса или складиштења порука.

са чланом 4. (*радња прикупљања порука на други начин у односу на пресретање комуникација*). Одлуку о предузимању ове две радње доноси суд на захтев јавног тужиоца, у ком се наводи кривично дело за које се лице сумњичи, име и презиме осумњиченог, околности из којих произлази да су испуњени услови за одређивање радње, адресу у рачунарској мрежи или терминални уређај који су предмет предузимања радње. Временски период на који се ове радње одређује не може бити дужи од месец дана. Осим радње пресретања комуникација и радње прикупљања порука на други начин у односу на пресретање комуникација, Закон у члану 6. предвиђа и *радњу надзор над подацима о саобраћају комуникације*. Ова радња се одређује ради прикупљања идентификујућих података повезаних са поруком која је послата или примљена употребом одређене адресе у рачунарској мрежи или терминалним уређајима, као и података о локацији адресе у рачунарској мрежи или терминалног уређаја, или ради привременог онемогућавања коришћења адресе/уређаја. Суд издаје наредбу за предузимање ове радње ако постоји основи сумње да је лице учинило кривично дело за које је запрећена казна затвора у трајању од најмање четири године или од најмање две године уколико је дело учињено употребом адресе у рачунарској мрежи или одређеног терминалног уређаја или је учињено неко од таксативно набројаних кривичних дела (међу којима су и дела против безбедности рачунарских података). Надзор података о саобраћају може се одредити и у складу са чланом 7, уколико постоји сагласност лица (оштећеног лица и сведока) које учествује у надзираној комуникацији, уколико постоје основи сумње да је учињено кривично дело за које је предвиђена казна затвара од најмање две године или је дело учињено употребом адресе у рачунарској мрежи или одређеног терминалног уређаја или је повређено ограничење комуницирања са одређеним лицима или се ради о злостављању жртве проституције. Осим тога, може се наредити прикупљање података о локацији адресе у рачунарској мрежи или терминалног уређаја за које се претпоставља да их користи осумњичени за наведена кривична дела у члану 6. који је у бекству, односно избегава кривични поступак. Одлуку о надзору података о саобраћају доноси суд на захтев јавног тужиоца, али уколико то захтевају разлози хитности, јавни тужилац може наредити предузимање ових радњи али је дужан да у року од 24 часа о томе обавести суд који може да потврди

или поништи одлуку јавног тужиоца, у ком случају се прикупљени подаци не могу користити. У одлуци суда се наводи кривично дело за које се лице сумњичи, име и презиме осумњиченог, околности из којих произлази да су испуњени услови за одређивање радње, евентуалну сагласност оштећеног/сведока, адресу у рачунарској мрежи или терминални уређај који су предмет предузимања радње. Члан 10. предвиђа могућност *прикупљања података од базних станица*. Наиме, на основу наредбе суда, а без ње у изузетно хитним случајевима (уз накнадно одобрење суда у року од 24 часа), јавни тужилац може тражити податке о адреси у рачунарској мрежи или терминалном уређају које је осумњичено лице (за дела наведена у члану 6) користило да преко одређених базних станица на одређеном месту и у одређено време приступи телекомуникационој рачунарској мрежи. Одлука суда садржи податке о кривичном делу, опис околности из којих произлази да су испуњени услови за одређивање радње, временски период за који се траже подаци и одређивање базне станице која је предмет радње. Осим наведених радњи, Закон у члану 23. уређује *радњу техничког надзора уређаја* која подразумева надзор и праћење операција у одређеном рачунару или другом техничком уређају или података похрањених у њима али не и сазнавање садржаја података. Радња се може одредити уколико је од изузетне важности за разјашњење одређених тешких кривичних дела (члан 16.став 3) и то у трајању до најдуже месец дана. Одлуку доноси суд, а она садржи осим података о кривичном делу и описа чињеница из којих проистиче оправданост примене мере и одређивање техничког уређаја или програма која је предмет надзора и праћења. У циљу предузимања свих наведених радњи, одлуком суда се одређује који орган је надлежан за извршавање радњи и овлашћује га у складу са чланом 26. Закона да инсталира или уклони уређај, процедуру или програм ради техничког надзора одређеног информационог система, као и да заобиђе, реинсталира или на други адекватан начин привремено онемогући мере заштите у информационом систему.

2.7. Летонија

Законик о кривичном поступку *Летоније*[525] уређује и питање експедитивног чувања рачунарских података (члан 191) и питање парцијалног откривања података о саобраћају остварених комуникација (члан 192). Истражитељ из посебне јединице полиције за борбу против компјутерског криминала и заштиту интелектуалне својине може наредити лицу (било ком физичком или правном лицу, укључујући и пружаоце услуга електронске комуникације), које има у поседу или врши контролу над рачунарским системом у ком су ускладиштени потребни подаци да их 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 истражитељ може по одобрењу истражног судије да тражи од пружаоца услуга електронских комуникација да открије и преда податке похрањене у електронском информационом систему који су сачувани.

У члану који регулише вршење увиђаја (члан 160) наведено је 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

[525] *Krimināl procesa likum*, http://www.knab.gov.lv/uploads/eng/criminal_procedure_law_2014.pdf.

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 период 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 података 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 обавезује 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 мање озбиљних, озбиљних и нарочито озбиљних кривичних дела[526], 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.

Међу посебним доказним радњама *летонски* Законик о кривичном поступкуу члану 215. предвиђа и *надзор комуникација које је остварују употребом*

[526] 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, озбиљна су она кривична дела за које је могуће изрећи казну затвора од 3 до 8 година, а нарочито озбиљних су кривичних дела за које је могуће изрећи казну затвора од најмање 8 година или доживотну казну. Члан 7. КЗ: http://www.knab.gov.lv/uploads/eng/the_criminal_law2014.pdf.

техничких средстава (тачка 2) и *контролу садржаја података који се преносе* (тачка 4). Ове посебне доказне радње може одредити истражни судија у погледу мање озбиљних, озбиљних и нарочито озбиљних кривичних дела, ради прикупљања само оних информација потребних за доказивање чињеница у кривичном поступку за конкретно кривично дело или за спречавање непосредне и значајне претње по јавну безбедност (члан 211). Надзор телефона и других средстава комуникације без знања учесника у комуникацији или пошиљаоца и примаоца информације може одредити истражни судија ако постоји вероватноћа да се из разговора или пренесених информација могу добити информације потребне за доказивање околности у кривичном поступку а то није могуће остварити на други начин. Осим тога, члан 220. предвиђа да се *пресретање, прикупљање и снимање података који се преносе у системима за аутоматску обраду података* употребом уређаја за комуникацију без знања власника или држаоца тог система, може одредити уколико постоји вероватноћа да се из прикупљених података могу добити информације потребне за доказивање околности у кривичном поступку.

2.8. Норвешка

У Норвешкој Закона о кривичном поступку[527] садржи немали број одредаба које су интересантне. На *претресање* рачунара примењују генералне одредбе о претресу (чланови 190-202). Претрес просторија, других просторија за становање и складишење може се извршити уколико су у власништву лица за које постоји сумња да је извршило кривично дело за које је могуће одредити казну затвора, а уколико су у власништву других лице, претресање је могуће у следећим ситуацијама: ако је кривично дело извршено у ти просторијама или је у њима ухапшен осумњичени или је ухваћен на делу или ако постоје нарочита вероварниоћа да це у тим просторијама може пронаћи осумњичени или трагови и докази потребни за покретање кривичног поступка. Претресање је могуће извршити или уз сагласност држаоца просторије или предмета дату у писаном облику или на основу одлуке суда (у изузетним случајевима уколико то налажу

[527] Консолидован текст *Lov om rettergangsmaten i straffesaker (Straffeprosessloven) 53/2006* доступан је на следећем линку: http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

разлози хитности, одлуку може донети и јавни тужилац, али је потребно да накнадно одобрење те одлуке да суд). Случајеви у којим је без одлуке могуће извршити претрес нису предвиђени. Претресање врши полиција, у присустује један сведок, који потписује записник. Једна одредба се изричито односи на претрес уређаја и система за аутоматску обраду података. Чланом 199а предвиђено је 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.

Предмети (и рачунарски подаци) који могу имати значај доказа *одузимају* привремено до доношења правноснажне судске одлуке. У случају добровољне предаје предмета, јавни тужилац доноси наредбу о узапћењу предмета (и полиција приликом вршења претреса, али је о отме дужна да обавести тужиоца). У погледу писаних докумената или других предмета који садрже изјаве лица која су ослобођена дужности сведочења или могу одбити да дају исказ због оабевез чувања професионалне или службене тајне, одузимање се може извршити само на основу одлуке суда. Лице од кога се одузмају предмети, у сваком случају може тражити преиспитивање одлуке тужиоца од стране суда о чему се обавештава приликом одузимања предмета, но постоји могућност да се таква обавештење одложе уколико се ради о кривичном делу за које је предвиђена казна затвора од најмање шест месеци.

Посебно је регулисано *одузимање писама, пошиљки и других средстава комуникације* (чланови 211-213). Пошта и оператери који пружају услуге приступа електронској комуникационој мрежи или друге услуге у вези са електронским комуникацијама дужни су на основу судске одлуке да предају пошиљке уколико могу имати значај доказа. Обавеза предаје пошиљки односи се на све врсте комункације уколико постоји сумња да је извршено кривично дела за које је предвиђена казна затвора од најмање шест месеци. Уколико то разлози хитности захтевају, јавни тужилац може наредити овим лицима да задрже пошиљке до доношења судске одлуке, али не дуже од недељу дана. Изричито је предвиђено да се ни једна пошиљка (било које врсте комунакције) не отвара без одлуке суда или сагласности пошиљоца или примаоца дату у писаном облику. Све

пошиљке које нису од значаја за конкретан предмет, прослеђују се лицу на које су адресиране, а потребне се предају тужиоцу ради даљег поступања.

Члан 215а регулише *хитно обезбеђивање рачунарских података* 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 пружаоцу услуге којој се налаже да сачува релевантне податке, а компанија 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.

Закон у 16. поглављу регулише надзор комуникација (односно, надзор комуникација и контролу уређаја за комуникацију). Суд може наредити *надзор комуникација* које се остварују употребом телефона, рачунара и других уређаја за електронску комуникацију за које се претпоставља да су у власништву или да их користи лице осумњичено да је учинило или да припрема извршење кривичних дела за која је запрећена казна затвора од најмање 10 година затвора или таксативно наведених кривичних дела[528]. У члану 216б се, пак, уређује *контрола уређаја* у смислу а) ометања или прекидања комуникације која се остварују употребом телефона, рачунара и других уређаја за електронску комуникацију за које се претпоставља да су у власништву или да их користи лице осумњичено да је учинило или да припрема извршење кривичних дела за која је запрећена казна затвора од најмање 5 година затвора или таксативно наведених кривичних дела, б) онемогућавања рада уређаја којим се остварује комуникација, в) идентификовања уређаја употребом техничке опреме, г) захтевања од власника или пружаоца

[528] Ради се о кривичним делима против независности државе и против устава и највиших представника државе и кривичном делу неовлашћена производња и стављање у промет опојних дрога (чланове 90, 91, 91а, 94, 104. и 162 КЗ Норвешке), http://www.ub.uio.no/ujur/ulovdata/lov-19020522-010-eng.pdf.

услуга приступа рачунарској мрежи/услуга електронских комуникација да преда полицији податке о томе који уређаји за комуникацију у одређеном временском периоду ће бити/су били повезани са уређајима којима се остварује комуникација, као и друге податке у вези са оствареном комуникацијом. Контролу, такође, наређује суд, али из разлога хитности, одлуку може донети и јавни тужилац, с тим што је потребно накнадно одобрење суда у року од 24 часа. Надзор комуникација и контрола уређаја за комуникацију суд одређује само ако ове радње могу бити од изузетног значаја за решавање кривичне ствари, а што би применом других мера било тешко (члан 216ц) а време трајања ових радњи је ограничено на 4 недеље.

2.9. Француска

У француском Законику о кривичном поступку[529] не постоји специфична одредба о хитном чувању рачунарских података али на основу овлашћења да по наредби јавног тужиоца изврши претрес рачунара и нареди предавање рачунарских података, судска полиција може захтевати од лица које у поседу има потребне податке о саобраћају остварене комуникације, не само да их на експедитиван начин сачува, него и да делимично полицији открију одређене податке (члан 56). На основу члана 60-2. 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 до најдуже годину дана. Лице које без оправданог разлога одбије да поступи по наредби може се казнити новчаном казном у износу од 3750 еура.

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 (чланови 97-98. Законика о кривичном поступку). Пре одузимања рачунарских података, врши се претрес

[529] Консолидован текст *Code de procédure pénale* доступан је на следећем линку: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&dateTexte=20051213.

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 предају 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 новчаног казном од 4500 еура. 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.

Законик о кривичном поступку садржи одредбе о *пресретању комуникација које се остварују употребом телекомуникационих средстава*, али се пресретање, снимање и транскрипција комуникација може одредити само у погледу кривичних дела за које је запрећена казна затвора од најмање две године, и то на основу одлуке истражног судије на период до 4 месеца (уз могућност продужења за још 4 месеца, уколико и даље постоје разлози због којих је мера и одређена).

3. ДОКАЗИВАЊЕ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У ПОЈЕДИНИМ ДРЖАВАМА БИВШЕ СФРЈ

3.1. Црна Гора

Радње доказивања уређене су одредбама у оквиру главе осме Законика о кривичном поступку[530].

У погледу одређивања разлога за *претресање* стана, других просторија, покретних ствари и лица, предвиђено је да се може предузети ако постоје основи сумње да ће се претресањем окривљени ухватити или да ће се пронаћи трагови кривичног дела или предмети важни за кривични поступак. Изричит је наведено да се претресање покретних ствари обухвата и претресање рачунара и сличних уређаја за аутоматску обраду података који су са рачунаром повезани.

У вези са тим, лице које се користи рачунаром дужно је на захтев суда да омогући приступ рачунару и преносивим медијима на којима се чувају подаци који се односе на предмет претресања (дискови, УСБ-флеш диск, УСБ-хард диск, дискете, траке и слично), као и да пружи потребна обавештења за употребу рачунара. Лице које то одбије, може бити кажњено (уколико за такво одбијање не постоје разлози из члана који се односи на могућност да сведок ускрати одговор на поједина питања уколико би давање одговора себе или себи блиско лице тешкој срамоти или кривичном гоњењу). Лице које одбије да поступи по наредби суда може се казнити новчаном казном до 1.000 €, а у случају даљег одбијања може се затворити. Затвор траје до поступања по наредби или до завршетка кривичног поступка, а најдуже два месеца. На исти начин поступиће се према службеном или одговорном лицу у државном органу, привредном друштву или другом правном лицу, али ове мере не могу се применити према осумњиченом, односно окривљеном или лицима која су ослобођена дужности сведочења.

Претресање се предузима по наредби суда, а на захтев државног тужиоца или на захтев овлашћеног службеног лица полиције које је добило одобрење

[530] "Службени лист ЦГ", бр. 57/2009, 49/2010, 47/2014 - Одлука УС ЦГ, 2/2015 - Одлука УС ЦГ и 35/2015. Консолидован текст Законика доступан је на линку: http://www.pravda.gov.me/ResourceManager/FileDownload.aspx?rid=214598&rType=2&file=Zakonik%20o%20krivi%C4%8Dnom%20postupku,%20pre%C4%8Di%C5%A1%C4%87eni%20tekst%20jul%202015.pdf.

државног тужиоца[531]. Изузетно, захтев се може поднети и усмено, кад постоји опасност од одлагања, тако што се саопштава судији за истрагу и телефоном, радио везом или другим средством електронске комуникације. У том случају, судија за истрагу ће даљи ток разговора забележити, а у случају кад се користи аудио или стенографски записник, у року од 24 сата, направиће се његов препис чија ће се истоветност оверити и чувати са оригиналним записником. Тиме се дозвољава поступање у хитним случајевима мимо основног правила, уколико би у хитним случајевима писмена би кореспонденција довела до опасности одлагања[532].

Кад судија за истрагу прими захтев за доношење наредбе, ако се са њим сагласи, доноси одмах наредбу за претресање[533], коју извршава је полиција. На основу наредбе о претресању могу се одузети не само предмети наведени у захтеву за доношење наредбе, него и други предмети[534]. Уколико претресању није присуствовао надлежни државни тужилац, он се одмах обавештава о проналаску предмета, ради покретања кривичног поступка, па ако државни тужилац нађе да нема основа за покретање кривичног поступка, а не постоји други законски основ по коме би се ти предмети могли одузети, привремено одузети предмети ће се одмах вратити. Уколико се код претресања рачунара и сличних уређаја за аутоматску обраду података одузму одређени предмети, они ће се одмах вратити својим корисницима, ако нису потребни за вођење поступка, а лични подаци прикупљени претресањем могу се користити само у сврху вођења кривичног поступка и бришу се чим та сврха престане.

---

[531] *Захтев за доношење наредбе* подноси се у писаној форми, а садржи: 1) назначење подносиоца захтева; 2) назив суда којем се захтев упућује; 3) чињенице из којих произилази вероватноћа постојања разлога за претресање; 4) име и презиме, а по потреби и опис лица које је потребно ухватити током претресања стана или других просторија, *односно очекиване трагове и опис предмета које је потребно претресањем пронаћи*; 5*) одређивање предмета на коме ће се обавити претресање* уз навођење адресе, података о власнику, односно држаоцу ствари или стана или других просторија и других података који су битни за утврђивање идентитета; 6) потпис подносиоца захтева.

[532] Д. Радуловић, *Коментар Законика о кривичном поступку Црне Горе*, Подгорица 2009, 122.

[533] Наредба садржи: 1) податке наведене у захтеву; 2) да ће претресање извршити полиција; 3) поуку да се претресање врши у складу са законником; 4) потпис судије и службени печат суда. Уколико се, пак, судија за истрагу не сагласи са захтевом за доношење наредбе за претресање, одмах ће затражити да о захтеву одлучи ванрасправно веће у року од 24 часа.

[534] Наиме, уколико се приликом претресања стана или лица нађу предмети који немају везе са кривичним делом због којег је претресање наређено, али који указују на друго кривично дело за које се гони по службеној дужности, они се описују у записнику и привремено одузимају, а о одузимању се одмах издаје потврда.

Привремено одузимање предмета који се по Кривичном законику имају одузети или могу послужити као доказ у кривичном поступку одређује решењем суд, а на предлог државног тужиоца (члан 85)[535]. Изричито је наведено да се наведена правила односе и на податке који се чувају у уређајима за аутоматску, односно електронску обраду података и медије у којима се ти подаци чувају, а који се на захтев суда морају предати у читљивом и разумљивом облику.

Лице које држи предмете дужно је да их преда, а уколико одбије то да учини, може се казнити новчаном казном до 1.000 €, а у случају даљег одбијања може се затворити (затвор траје до предаје предмета или до завршетка кривичног поступка, а најдуже два месеца). На исти начин поступиће се према службеном или одговорном лицу у државном органу, привредном друштву или другом правном лицу, али се ове мере не могу се применити према осумњиченом, односно окривљеном или лицима која су ослобођена дужности сведочења.

Законик предвиђа и неколико изузетака у смислу да привременом одузимању не подлежу: списи и друге исправе државних органа чије би објављивање повредило обавезу чувања тајних података у смислу прописа којима се уређује тајност података, док надлежни орган не одлучи другачије; писма окривљеног браниоцу или блиским лицима, осим ако их окривљени добровољно преда; записи, изводи из регистра и сличне исправе које се налазе код браниоца, а које су она сачинила о чињеницама које су сазнали од окривљеног у обављању свог занимања, чијим објављивањем би била повређена дужност чувања професионалне тајне. Ипак, овакво ограничење се односи на браниоца или лице ослобођено обавезе сведочења, ако постоји основана сумња да су помагали окривљеном у извршењу кривичног дела или су му пружили помоћ после извршеног кривичног дела или су поступили као прикривачи.

Приликом одузимања предмета назначиће се где су пронађени и описаће се, а по потреби ће се и на други начин обезбедити утврђивање њихове истовјетности, а за одузете предмете издаје се потврда. Предмети се привремено

[535] Решење о привременом одузимању предмета садржи: 1) назив суда који доноси решење; 2) правни основ за привремено одузимање предмета; 3) означење и опис предмета који ће се привремено одузети; 4) име и презиме лица од којег се предмет привремено одузима и место на којем, односно у којем треба привремено одузети одређени предмет.

одузимају и предају на чување суду или се на други начин обезбеђују њихово чување.

Законик у посебном члану уређују *привремено одузимање писама, телеграма и других пошиљки* (члан 88). Наиме, на захтев државног тужиоца судија за истрагу може наредити да поштанска, друга привредна друштва и правна лица регистрована за пренос информација задрже и да му уз потврду пријема, предају писма, телеграме и друге пошиљке које су упућене осумњиченом или окривљеном или које они шаљу, ако постоје околности због којих се основано може очекивати да ће ове пошиљке послужити као доказ у поступку. Пошиљке отвара судија за истрагу у присуству два сведока, а приликом отварања пази се да се не повреде печати, док ће се омоти и адресе сачувати, о чему се саставља записник. О садржају писама, телеграма и других пошиљки судија за истрагу обавештава државног тужиоца и на његов захтев му доставља њихову копију и примерак записника састављеног приликом отварања. Ако интереси поступка дозвољавају, садржај пошиљке може се саопштити у целини или делимично осумњиченом или окривљеном, односно лицу коме је упућена и може му се пошиљка и предати, а уколико је осумњичени или окривљени одсутан, пошиљка се може, уколико то не би штетило интересима кривичног поступка, вратити пошиљаоцу.

Законик у деветом поглављу уређују *мере тајног надзора*. Законодавац познаје десет мера које се могу одредити у погледу одређених кривичних дела, а које се разликују по материјалном (у погледу постојања вероватноће) и формалном (у погледу овлашћеног лица за одређивање мере) услову за одређивање. Мере се могу одредити ако постоје основи сумње да је неко лице само или у саучесништву са другим извршило, врши или се припрема за вршење таксативно наведених кривичних дела[536], међу којима су изричито наведена кривична дела против безбедности рачунарских података.

[536] Мере се могу наредити за кривична дела: 1) за која се може изрећи казна затвора у трајању од десет година или тежа казна; 2) са елементима организованог криминала; 3) проузроковање лажног стечаја, злоупотреба процене, примање мита, давање мита, противзаконити утицај, злоупотреба службеног положаја, као и злоупотреба овлашћења у привреди и превара у служби за која је прописана казна затвора од осам година или тежа казна; 4) отмица, изнуда, уцена, посредовање у вршењу проституције, приказивање порнографског материјала, зеленаштво, утаја пореза и доприноса, кријумчарење, недозвољено прерађивање, одлагање и складиштење опасних материја, напад на службено лице у вршењу службене дужности, спречавање доказивања,

Уколико се на други начин не могу прикупити докази или би њихово прикупљање захтевало несразмерни ризик или угрожавање живота људи, према лицима за који постоји потребан степен сумње се могу се одредити следеће мере: тајни надзор и снимање телефонских разговора и других комуникација на даљину; пресретање, прикупљање и снимање рачунарских података; улазак у просторије ради тајног фотографисања и видео и аудио снимања у просторијама; и тајно праћење и видео и аудио снимање лица и предмету. Прва мера се може наредити и према лицу за које постоје основи сумње да извршиоцу или од извршиоца кривичних дела преноси поруке у вези са кривичним делом, односно да се извршилац служи њиховим прикључцима на телефон или другим средствима за електронску комуникацију. Ове мере одређује судија за истрагу писаном наредбом на образложени предлог државног тужиоца.

Уколико, пак, околности случаја указују да ће се са најмање повреда права на приватност прикупити докази, према лицима за које постоји потребан степен сумње могу се одредити: симулована куповина предмета или лица и симуловано давање и примање мита; пружање симулованих пословних услуга или склапање симулованих правних послова; оснивање фиктивног привредног друштва; праћење превоза и испоруке предмета кривичног дела; снимање разговора уз претходно информисање и сагласност једног од учесника разговора; и ангажовање прикривеног иследника и сарадника. Ове мере писаном наредбом одређује државни тужилац на образложени предлог овлашћеног полицијског службеника или по службеној дужности[537]. Изузетно, ако се писана наредба не може издати на време, а постоји опасност од одлагања, предузимање мере може започети на основу усмене наредбе судије за истрагу, односно државног тужиоца. У том случају писана наредба мора да буде прибављена у року од 12 сати од издавања усмене наредбе.

криминално удруживање, одавање тајних података, повреда тајности поступка, прање новца, фалсификовање новца, фалсификовање исправе, фалсификовање службене исправе, прављење, набављање и давање другом средстава и материјала за фалсификовање, учествовање у страним оружаним формацијама, договарање исхода такмичења, недозвољено држање оружја и експлозивних материја, недозвољен прелаз државне границе и кријумчарење људи; 5) против безбедности рачунарских података.

[537] Предлог и наредба о издавању мера тајног надзора садрже: врсту мере, податке о лицу према коме се мера спроводи, ако је то лице познато, разлоге за основе сумње, начин извршења мере, њен циљ, обим и трајање.

Све мере (осим) могу трајати до четири месеца, али је могуће продужење из оправданих разлога, према истом лицу и за исто кривично дело најдуже до 18 месеци од доношења прве наредбе за одређивање мера тајног надзора. Извршење мера ће се наредбом прекинути кад престану разлози за њихову примјену, но, предвиђена је могућност да се мере чије је извршење прекинуто могу из оправданих разлога наставити према истом лицу и за исто кривично дело на основу наредбе, у ком случају се у максимални рок трајања мере рачуна се и време прекида извршења мере. Након протека рокова из овог става, не може се наставити извршење, нити се може одредити нова мера за исто кривично дело и према истом извршиоцу. Осим могућности прекида, законодавац предвиђа могућност замене мере. Наиме, уколико се у току извршења мере покаже да се том мером не може постићи сврха, она се може замијенити другом мером и тада се у максимални рок трајања новоодређене мере рачуна се и време трајања претходно одређене мере.

Када се издаје наредба за меру тајни надзор и снимање телефонских разговора и других комуникација на даљину, уз њу судија за истрагу ради извршења издаје посебан налог у којем ће навести само телефонски број или е-маил адресу или интернационални идентификациони број корисника, интернационални идентификациони број мобилног уређаја и адресу интернет протокола и трајање мере. Тај налог овлашћени полицијски службеник предаје одређеним привредним субјектима у поступку извршења мере. Наиме, законодавац је прописао да су поштанска, друга привредна друштва и правна лица регистрована за преношење информација дужна су да овлашћеном полицијском службенику омогуће извршење мера тајног надзора и снимање телефонских разговора и других комуникација на даљину.

Службена и одговорна лица која учествују у поступку доношења наредбе и извршењу мера тајног надзора дужна су да као тајне податке чувају све податке које су сазнали у овом поступку.

Ако се приликом примене мера тајног надзора забележе подаци и обавештења који упућују и на неко друго лице за које постоје основи сумње да је извршило кривично дело за које је одређена мера тајног надзора или неко друго кривично дело, тај део материјала издваја се и доставља државном тужиоцу, а

може се користити као доказ само за кривична дела у погледу којих је могуће одређивање мера тајног надзора.

Мере тајног надзора извршава овлашћени полицијски службеник који је дужан да води рачуна да се у што мањој мјери нарушава приватност лица на која се мера не односи. У том циљу дужан је да води евиденцију о свакој предузетој мери, о чему државном тужиоцу, односно судији за истрагу доставља периодичне извјештаје. Ако државни тужилац, односно судија за истрагу оцени да више не постоји потреба за предузимањем наређених мера, доноси наредбу о њиховом обустављању. По извршењу мера овлашћени полицијски службеник *доставља државном тужиоцу* коначан извештај и остали материјал прибављен предузимањем мере, па уколико одлучи да не покрене кривични поступак, односно ако подаци и информације прикупљени применом мјера тајног надзора нису потребни за кривични поступак, тужилац доставља материјал у затвореном омоту са посебном ознаком судији за истрагу, који ће наредити да се материјал уништи у присуству државног тужиоца и судије за истрагу, о сачињава записник. Судија за истрагу ће овако поступити и ако државни тужилац донесе наредбу о спровођењу истраге против осумњиченог према коме су предузете мјере тајног надзора, али добијени резултати или део њих нису потребни за вођење кривичног поступка.

У погледу обавештавања лица према коме је предузета мјера тајног надзора у случају кад не дође до покретања кривичног поступка, предвиђено је да је, пре него што се уништи материјал добијен извршењем мера тајног надзора, судија за истрагу дужан да обавести лице према коме је мера предузета, а то лице има право увида у прикупљени материјал. Уколико, међутим, основана бојазан да би обавештавање лица или увид у добијени материјал могло да представља озбиљну опасност по живот и здравље људи или би могло угрозити неку од истрага које су у току или из других оправданих разлога, судија за истрагу, по прибављеном мишљењу државног тужиоца, може одлучити да не обавештава лице према коме је предузета мјера и да му не дозволи увид у добијени материјал.

У погледу прикупљања података о електронској комуникацији од значаја је и одредба која уређује једно од овлашћења полиције у извиђају: достављање података о електронском комуникацијском саобраћају (члан 25). Наиме, уколико

постоје основи сумње да је регистровани власник или корисник телекомуникацијског средства извршио, врши или се припрема за вршење било ког кривичних дела за која се гони по службеној дужности, ради откривања учиниоца и прикупљања доказа или ради лоцирања или идентификације лица и трагања за лицем које се налази у бјекству или лица за којим је расписана међународна потерница, полиција може на основу наредбе судије за истрагу да од оператера комуникацијских услуга затражи проверу истоветности, трајања и учесталости комуникације са одређеним електронским комуникацијским адресама, утврђивање места на којима се налазе лица која успостављају електронскукомуникацију, као и идентификацијске ознаке уређаја; техничким уређајем извршити идентификацију интернационалног идентификационог броја корисника и интернационалног идентификационог броја мобилног уређаја и лоцирање телефона и других средстава за електронску комуникацију.

Уколико на предлог државног тужиоца у року од четири сата судија за истрагу изда наредбу, уз њу издаје и посебан налог у којем ће навести само телефонски број, е-маил адресу или интернационални идентификациони број корисника, интернационални идентификациони број мобилног уређаја и адресу интернет протокола лица у односу на које се прикупљају подаци о електронском комуникацијском саобраћају. Изузетно, ако се писана наредба не може издати на време, а постоји опасност од одлагања, предузимање мера се може започети на основу усмене наредбе судије за истрагу, у ком случају писана наредба мора да буде прибављена у року од 24 часа од издавања усмене наредбе.

Ако државни тужилац одлучи да не покрене кривични поступак, односно кад се лице за којим се трага пронађе, прикупљени материјал ће се у затвореном омоту доставити судији за истрагу, који ће наредити да се материјал уништи у присуству државног тужиоца и судије за истрагу, о чему ће судија за истрагу сачинити записник. Исто тако ће судија поступити и кад државни тужилац донесе наредбу о спровођењу истраге против осумњиченог, а прикупљени материјал или дио материјала није потребан за вођење кривичног поступка. Изричито је предвиђено да се подаци прибављени противно одредбама закона не могу се користити као доказ у кривичном поступку.

3.2. Република Српска

Међу радњама доказивања Закон о кривичном поступку Републике Српске[538] регулише претресање стана, просторија и лица (чланови 115-129), привремено одузимање предмета и имовине (чланови 129-140), а осим тога, Закон међу одредбама које уређују ток кривичног поступка садржи и одредбе посебним истражним радњама (чланови 234-241).

Предмет *претресања* могу бити стан, остале просторије и покретне ствари осумњиченог, односно оптуженог и других лица може се предузети уколико постоји довољно основа за сумњу да се код њих налазе учинилац, саучесник, трагови кривичног дела или предмети важни за поступак. Осим тога, могуће је извршити претресање покретних ствари наведених лица и ван стана, односно осталих просторија.

Изричито је предвиђено да претресање покретних ствари обухвата и претресање компјутерских система, уређаја за похрањивање компјутерских и електронских података, као и мобилних телефонских апарата. Установљена је обавеза лица која се користе ове уређаје да омогуће приступ, предају медиј на коме су похрањени подаци, и да пруже потребна обавештења за употребу тих уређаја. Уколико лице одбије њихову предају, предвиђена је санкција - лице се може казнити новчаном казном до 50.000 КМ, а у случају даљег одбијања - може се затворити (при чему је трајање затвора ограничено до предаје предмета или до завршетка кривичног поступка, а најдуже 90 дана). Закон садржи још једну важну одредбу у вези са претресањем компјутера и сличних уређаја, а то је да се ова радња обавља уз помоћ стручног лица. Све стале одредбе које се односе на претресање стана односе се на претресање ствари, а тиме и на компјутере и сличне уређаје, што је изузетно значајно.

Закон садржи прецизне одредбе о подношењу захтева за издавање наредбе за претресање[539]. Уколико судија за претходни поступак установи да је захтев за

[538] Закон о кривичном поступку Републике Српске (Сл. гласник РС 53/2012).

[539] Наиме, захтев се може поднети у писаној или усменој форми. Захтев се првенствено подноси у писаној форми и садржи: а) назив суда, као и име и функцију подносиоца захтева, б) чињенице које указују на вероватност да ће се лица, односно трагови и предмети н наћи на означеном или описаном месту или код одређеног лица и в) захтев да суд изда наредбу за претресање ради проналажења лица или одузимања предмета. Осим обавезних елемената, у захтеву се може се

издавање наредбе за претресање оправдан, може одобрава захтев и издаје наредбу за претрес. Уколико судија за претходни поступак одлучи да изда наредбу за претрес на основу усменог захтјева, подносилац захтева сам саставља наредбу и дужан је прочитати у целости судији за претходни поступак[540].

Закон прецизно уређује поступак извршења наредбе за претресање. Закон садржи одредбу којом се одређује време извршења наредбе за претресање[541]. Пре почетка претресања овлашћено службено лице обавештава о својој функцији и разлогу доласка и предати наредбу за претресање лицу код којег ће се извршити претресање. Ако је након тога овлашћеном службеном лицу приступ ускраћен, може употребити силу у складу са законом[542]. Кориснику стана и других просторија омогућава се да буде присутан претресању, а ако је он одсутан - позваће се његов заступник или неко од одраслих чланова домаћинства или

предложити: а) да се наредба за претресање изврши у било које време зато што постоји оправдан разлог да претресање неће моћи бити извршено у периоду од 6.00 часова до 21.00 час, да ће се тражени предмети склонити или уништити ако се наредба не изврши одмах, као и да ће лице које се тражи побећи или починити друго кривично дело или да може угрозити безбедност овлашћеног службеног лица или другог лица ако се наредба не изврши одмах или у периоду од 21.00 час до 6.00 часова и б) да овлашћено службено лице изврши наредбу без претходне предаје наредбе ако постоји основана сумња да се тражени предмети могу лако и брзо уништити ако се одмах не одузму, да предаја наредбе може угрозити безбедност овлашћеног службеног или другог лица као и да ће лице које се тражи учинити друго кривично дело. Изузетно, захтев за издавање наредбе за претресање се може поднети усмено када постоји опасност од одгађања. У том случају, судија за претходни поступак је дужан да даљи ток разговора забележи. У случају када се користи звучни или стенографски записник, судија за претходни поступак је дужан да записник преда на препис, те да овери истоветност преписа и преда оригинални записник и препис суду у року од 24 часа од издавања наредбе. У случају дословног бележења разговора, судија за претходни поступак потписује копију записника и предаје је суду у року од 24 часа од издавања наредбе.

[540] У погледу садржаја наредбе за претресање, предвиђено је да садржи: а) назив суда који издаје наредбу, осим када се наредба за претресање одобрава на основу усменог захтева и потпис судије за претходни поступак који издаје наредбу, б) ако се наредба за претресање одобрава на основу усменог захтева, то се наводи уз назначење имена судије за претходни поступак који издаје наредбу и времена и места издавања, в) сврху претресања, г) име и функцију овлашћеног лица на које се наредба односи, д) опис лица које треба пронаћи или опис ствари које су предмет претресања, ђ) одређивање или опис места, просторија или лица која се траже, са навођењем адресе, власништва, имена или сличног за сигурно утврђивање идентитета, е) упутство да се наредба треба извршити у времену између 6.00 и 21.00 или овлашћење да се наредба може извршити у било које време, ж) овлашћење, када то суд изричито одреди, извршиоцу наредбе да може ући у просторије које треба да се претресу без претходне најаве, з) упутство да се наредба и одузете ствари донесу у суд без одгађања и и) поуку да осумњичени има право да обавести браниоца и да се претресање може извршити и без присуства браниоца ако то захтевају изузетне околности.

[541] Тако је предвиђено да се наредба мора се извршити најкасније 15 дана од издавања наредбе, а у супротном се, без одгађања, враћа суду. Наредба се извршава било којег дана у недељи, и то у периоду од 6.00 часова до 21.00 час (осим ако у наредби није изричито дато овлашћење да се може извршити у било које доба дана или ноћи).

[542] Обавеза обавештавања о функцији и разлозима претресања, не постоји ако су стан или друге просторије празне или ако овлашћено службено лице оправдано сматра да су празне или је наредбом изричито овлашћено да уђе без претходне најаве

комшија[543]. О сваком претресању стана, просторије или лица (не стоји изричито и за претресање ствари) саставиће се записник који потписује лице код којег се врши претресање или на којем се врши претресање и лица чије је присуство обавезно.

Приликом вршења претресања одузимају се привремено само они предмети и исправе који су у вези са сврхом претресања. У записник се уносе и тачно описују предмети и исправе који се одузимају, што се назначава и у потврди о одузимању предмета која се одмах издати лицу којем су предмети, односно исправе одузете. Након привременог одузимања предмета на основу наредбе за претресање, овлашћено службено лице издаје потврду у којој наводи одузете предмете и назив суда који је издао наредбу. Ако је предмет привремено одузет од одређеног лица, таква потврда мора се уручити том лицу. Ако је предмет привремено одузет из стана или просторије, таква потврда мора се уручити власнику, станару или кориснику. Након одузимања предмета на основу наредбе за претресање, овлашћено службено лице мора, без одгађања, вратити суду наредбу и предати предмете и списак одузетих предмета, а суд након пријема ствари одузетих на основу наредбе за претресање, суд задржава предмете под својим надзором до коначне одлуке. Ако се, међутим, приликом претресања стана, просторије, односно лица (не стоји изричито и приликом претресање ствари) нађу предмети који нису у вези са кривичним делом због којег је издата наредба за претресање, али упућује на друго кривично дело, они се описују у записнику и привремено одузимају, о чему се одмах издати потврда и обавештава се тужилац. Наиме, ако тужилац установи да нема основа за покретање кривичног поступка, а не постоји неки други законски основ по којем би се ти предмети могли одузети, предмети се враћају.

Закон садржи одредбу која се изричито односи на претресање компјутера. Наиме, предмети употребљени (можда би требало: пронађени?) приликом претресања компјутера и сличних уређаја за аутоматску обраду података враћају

[543] Уколико лице код кога се претресање треба извршити није присутно, наредба се оставља у просторији где се врши претресање, а претресање извршава и без његовог присуства. Претресању присуствују два пунолетна грађанина као сведоци који се пре почетка претресања упозоравају да пазе како се претресање врши, као и да имају право да пре потписивања записника о претресању ставе своје приговоре, ако сматрају да садржај записника није тачан.

се након претресања њиховим корисницима, ако нису потребни за вођење кривичног поступка.

Осим приликом претресање, предмети који по Кривичном закону треба да се одузму или који могу послужити као доказ у кривичном поступку привремено се могу одузети и на основу судске одлуке се обезбеђује њихово чување. Наредбу за одузимање предмета издаје судија на предлог тужиоца или овлашћеног службеног лица које је добило одобрење од тужиоца[544].

Привремено одузимање предмета могуће је и без наредбе, уколико постоји опасност од одгађања. Уколико се лице које се претреса изричито успротиви одузимању предмета, тужилац ће у року од 72 часа од извршеног претреса поднијети захтјев судији за претходни поступак за накнадно одобрење одузимања предмета, но уколико судија за претходни поступак одбије захтев тужиоца, одузети предмети се не могу користити као доказ у кривичном поступку, а привремено одузети предмети ће се одмах вратити лицу од којег су одузети.

Закон у посебном члану регулише привремено одузимање писама, телеграма и других пошиљки упућених осумњиченом, односно оптуженом или које он одашиље, а које се налазе код предузећа и лица која врше послове поште и телекомуникација. Пошиљке се привремено могу одузети ако постоје околности због којих се са основом може очекивати да ће ове пошиљке послужити као доказ у поступку, али само на основу наредбе судије за претходни поступак а на предлог тужиоца. Наредба обавезно садржи: податке о осумњиченом, односно оптуженом на којег се наредба односи, начин извршења наредбе и време трајања мере, као и предузеће које ће извршити наложену меру. Изузетно, наредбу може издати и тужилац, ако постоји опасност од одгађања, с тим да о њеном потврђивању одлучује судија за претходни поступак у року од 48 часова од

[544] Прецизно је утврђен садржај наредбе, тако да садржи: назив суда, правни основ за привремено одузимање предмета, назнаку предмета за одузимање, име лица од којег се одузимају предмети, место одузимања предмета и рок за одузимање предмета. Лица која држе такве предмете дужан је да их преда по наредби суда. Уколико, пак, одбије да то учини може се казнити до 50.000 КМ, а у случају даљег одбијања - може се затворити, при чему затвор траје до предаје предмета или до завршетка кривичног поступка, а најдуже 90 дана (ове санкције се не могу применити према осумњиченом, односно оптуженом нити лицима која су ослобођена дужности сведочења). Изричит је предвиђено да се одредбе о одузимању предмета односе се и на податке похрањене у компјутеру или сличним уређајима за аутоматску обраду података, као и да се при њиховом прибављању посебно води рачуна о прописима који се односе на чување тајности одређених података.

привременог одузимања пошиљки. У случају да наредба тужиоца не буде потврђена, те пошиљке се не могу користити као доказ у кривичном поступку. Преду- зете мере су временски ограничене, јер је предвиђено да могу трајати најдуже три месеца, а из важних разлога судија за претходни поступак може продужити трајање ових мјера за још три месеца, али их укида чим престану разлози за њихово даље предузимање.

Осим ове мере која се предузима према пошиљкама, Закон садржи одредбу којом се уређује предаја података о комуникацијама. Наиме, уколико постоје основи сумње да је лице извршило било које кривично дело, суд може (на основу предлога тужиоца или на предлог овлашћених службених лица која су добила одобрење од тужиоца) да наредит оператеру телекомуникација или другом правном лицу које врши пружање телекомуникационих услуга да достави податке о коришћењу телекомуникационих услуга тог лица, под условом да би такви подаци могли да буду доказ у кривичном поступку или да послуже за прикупљање информација које могу да буду од користи у кривичном поступку. Наредбу у хитним случајевима може да изда и тужилац, али се рада добијени подаци док не буде издата судска наредба морају запечатити. Наиме, о предузетим мерама тужилац одмах обавештава судију за претходни поступак, који може у року од 72 часа издати наредбу, па у случају да судија за претходни поступак не изда наредбу, тужилац је дужан да податке врати оператеру без претходног отварања. Прописана је дужност оператера телекомуникација или других правних лица која пружају телекомуникационе услуге да тужиоцу и полицијским органима омогуће спровођење ове мере. Осим према осумњиченом, радња се може одредити и према лицу за које постоје основи сумње да учиниоцу, односно од учиниоца преноси информације у вези са кривичним делом, односно да учинилац користи његово средство телекомуникације.

У погледу посебних истражних радњи, закон прописује да се могу одредити против лица за које постоје основи сумње да је само или заједно са другим лицима учествовало или учествује у извршењу одређених кривичног дела, ако се на други начин не могу прибавити докази или би њихово прибављање било повезано са несразмерним тешкоћама. Круг лица према којима се могу одредити ове радње је проширен, јер је предвиђено да се исте могу одредити и према лицу

за које постоје основи сумње да учиниоцу, односно од учиниоца кривичног дела преноси информације у вези са кривичним делом, односно да учинилац користи његово средство телекомуникације.

У погледу кривичних дела, изричито су наведена кривична дела против Републике Српске, кривична дела против човечности и међународног права и тероризам, но, с обзиром да је предвиђено да се могу одредити за кривична која се према Кривичном закону може изрећи казна затвора од три године или тежа казна, круг кривичних дела је релативно широк. Закон међу посебним изричитим радњама предвиђа и надзор и техничко снимање телекомуникација и приступ компјутерским системима и компјутерско сравњење података.

Истражне радње одређује наредбом судија за претходни поступак, на образложен предлог тужиоца, који садржи: податке о лицу против кога се радња предузима, основе сумње, разлоге за њено предузимање и остале битне околности које захтевају предузимање радњи, навођење радње која се захтева и начин њеног извођења, обим и трајање радње. Осим података које садржи предлог тужиоца, наредба садржи и утврђивање трајања наређене радње. Изузетно, са извршавањем истражне радње може се започети и на основу усмене наредбе судије за претходни поступак, уколико се писана наредба не може добити на време и ако постоји опасност од одгађања. У том случају, писани налог судије за претходни поступак мора се прибавити у року од 24 часа од издавања усмене наредбе. Наредбу извршава полицијски орган, а предузећа која врше пренос информација дужна су да тужиоцу и полицијским органима омогуће спровођење радњи.

Надзор и техничко снимање телекомуникација и приступ компјутерским системима и компјутерско сравњење података могу трајати најдуже до месец дана, а из посебно важних разлога могу се, на образложени предлог тужиоца, продужавати за по месец дана, али не могу трајати укупно дуже шест месеци од првобитно издате наредбе. У сваком случају, судија за претходни поступак је дужан да писаним налогом, без одгађања, обустави извршење предузетих радњи ако су престали разлози због којих су радње биле одређене. Након престанка примене радњи полицијски органи све информације, податке и предмете добијене предузетим радњама, као и извештај о томе предају тужиоцу, који доставља судији за претходни поступак писани извештај о предузетим радњама, на основу

ког судија за претходни поступак проверава да ли је поступљено по његовој наредби. Уколико тужилац одустане од кривичног гоњења, односно ако информације и подаци прибављени применом наређених радњи нису потребни за кривични поступак, уништиће се под надзором судије за претходни поступак, који ће о томе саставља посебни записник. Само у том случају, о предузимању радњи, разлозима за њихово предузимање, информацији да добијени материјал није био основ за кривично гоњење и да је уништен писано се обавештава лице против којег је радња предузета. Лице против којег је радња била предузета може од суда затражити испитивање законитости наредбе и начина на који је спроведена радња.

Подаци и информације добијени предузимањем радњи се чувају док се чува судски спис. Техничке снимке, исправе и предмети прибављени под условима и на начин прописан овим законом могу се користити као докази у кривичном поступку, али, ако су радње предузете без налога судије за претходни поступак или у супротности са њом, суд на прибављеним подацима или доказима не може заснивати своју одлуку.

3.3. Хрватска

Закон о кривичном поступку предвиђа могућност провере успостављања телекомуникацијског контакта (339а)[545]. Наиме, уколико постоји сумња да је регистровани власник или корисник телекомуникацијског средства учинио кривично дело за која се кривични поступак покреће по службеној дужности (као и за лице које је повезано са осумњиченим) полиција може да, на основу налога судије истраге, а ради прикупљања доказа, од оператора јавних комуникацијских услуга затражи проверу истоветности, трајања и учесталости комуникације с одређеним електронским комуникацијским адресама, утврђивање положаја комуникацијског уређаја, као и утврђивање места на којима се налазе особе које успостављају електронску комуникацију, те идентификацијске ознаке уређаја. Судија истраге је дужан да о образложеном предлогу јавног тужиоца донесе одлуку у року од 4 сата од пријема предлога. Међутим, постоји и изузетна

[545] Zakon o kaznenom postupku Republike Hrvatske (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13), http://www.zakon.hr/z/174/Zakon-o-kaznenom-postupku.

могућност, да у случају опасности од одгоде, јавни тужилац изда налог за проверу, ако верује да на време неће моћи прибавити налог судије, али је тада дужан да у року од 24 сата од издавања налога, упути судији допис у ком образлаже разлоге за такво поступање и тада судија решењем одлучује о законитости налога у року од 48 сати од пријема налога и дописа, против ког решења јавни тужилац нема права жалбе. Уколико су подаци прибављени без налога судије истраге односно ако јавни тужилац није у року доставио судије истраге налог или ако је одбијен захтев државног тужиоца за потврду налога за проверу успостављања телекомуникацијских контаката, тако прикупљени подаци не могу се употребити као доказ у поступку.

Закон о кривичном поступку прописују да се претрес предузима ако је вероватно да ће се пронаћи трагови и предмети потребни за кривични поступак (у члановима 240-250), 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 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 телекомуникацијских услуга, 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 након 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. Вредна помена је одредба члан 331. која предвиђа да се применом одредаба члана 257. (којим се уређује претрес покретне ствари), 262. и 263. (којима се уређује привремено одузимање предмета) прибавља електронски (дигитални) доказ (одређен у смислу члана 202. става 2. тачке 303. као податак који је као доказ у електроничком (дигиталном) облику.

У Хрватској се посебне доказне радње могу одредити уколико се извиди кривичних дела не би могли спровести на други начин или би то било могуће само уз несразмерне тешкоће. На писани образложени захтев јавног тужиоца, судија истраге може против лица за коју постоје основе сумње да је починило неко од кривичних дела наведених у члану 334. Закона о кривичном поступку[546], писаним, образложеним налогом одредити посебне доказне радње којима се привремено ограничавају одређена уставна права грађана, а међу којима су релевантне две: 1) надзор и техничко снимање телефонских разговора и других комуникација на даљину, и 2) пресретање, прикупљање и снимање рачунарских података (у члановима 332-334). Изузетно, налог може издати и јавни тужилац, ако постоји опасност од одгоде и ако јавни тужилац верује да на време неће моћи прибавити налог судије истраге, али само на време од двадесет четири сата. При томе је јавни тужилац дужан да налог, с ознаком времена издавања, и допис, у ком образлаже разлоге за његово издавање, у року од осам сати од издавања достави судији истраге. Истовремено, уколико сматра да треба наставити са спровођењем посебне доказне радње, подноси судији истраге писани образложени захтев за даљње спровођење[547]. Међутим, јавни тужилац није овлашћен да изда налог за предузимање радње пресретање, прикупљање и снимање рачунарских података, ако начин извршења те радње захтева улазак у дом или удаљени улазак

[546] Посебне доказне радње могу се одредити за таксативн наведена кривична дела међу којима су и искоришћавања деце за порнографију), кривична дела против интелектуалног власништва (Глава XXVII) ако су почињена упорабом рачунарсих система или мрежа, као и за сва кривична дела против рачунарских система, програма и података (Глава XXV).

[547] Судија истраге одмах по пријему налога и дописа испитује да ли су постојали услови за издавање налога и опасност од одгоде, па решењем одлучује о законитости налога. Ако судија истраге одобри налог, а јавни тужилац је поднео захтев за даљње спровођење доказне радње, доноси налог о спровођењу посебне доказне радње. Ако се не сложи с налогом јавног тужиоца, о томе одлучује ванрасправно веће у року од дванаест сати од пријема захтева. Ако веће потврди налог, а јавни тужилац је захтевао даљње спровођење доказне радње, веће издаје налог о спровођењу радње. Уколико, пак, веће не одобри налог, у решењу налаже да се одмах обуставе радње, а подаци прикупљени на основу налога јавног тужиоца се предају судији истраге који их уништава и о томе саставља записник.

у рачунар осумњиченог који се налази у његовом дому. Дакле, пресретање, прикупљање и снимање рачунарских података је могуће одредити тако да се врши удаљени улазак у рачунар осумњиченог који се налази у његовом дому, али само на основу налога судија истраге.

Надзор и техничко снимање телефонских разговора и других комуникација на даљину може се одредити и према лицима за које постоје основе сумње да учиниоцу или од њега преносе саопштења и поруке у вези са делом, односно да се учинилац служи њиховим прикључцима на телефон или другим телекомуникацијским уређајем, које крију учиниоца кривичног дела или му прикривањем средстава којима је кривично дело учињено, трагова кривичног дела или предмета насталих или прибављених кривичним делом или на други начин помажу да не буде откривен. Осим тога, обе посебне доказне радње могу се уз писани пристанак лица које је учесник у комуникацији, применити на средства, просторије и предмете те особе. Ове посебне доказне радње извршава полиција, а оперативно-технички центар за надзор телекомуникација, који обавља техничку координацију с пружаоцима телекомуникацијских услуга, као и пружаоци телекомуникацијских услуга, дужни су да полицији осигурају потребну техничку помоћ[548].

[548] За непоступање по овој обавези, судија истраге на образложени предлог јавног тужиоца, може пружаоца телекомуникацијске услуге казнити новчаном казном до 1.000.000,00 куна, а одговорно лице у Оперативно-техничком центру за надзор телекомуникација који обавља техничку координацију и у пружаоцу телекомуникацијских услуга, може казнити новчаном казном у износу до 50.000,00 куна. Ако и након тога не изврши решење, одговорно лице се може казнити затвором до извршења, али најдуже месец дана.

Шести део

МЕЂУНАРОДНА САРАДЊА У СУПРОТСТАВЉАЊУ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Високотехнолошки криминал је феномен са израженом транснационалном, глобалном димензијом која органима гоњења намеће потребу за прикупљањем доказа и хватањем учиниоца који се налазе *на територији других држава*, уколико се извршилац радње кривичног дела налази на територији једне државе, а последице радње и оштећена лица на територији једне или више других држава. Овај проблем није јединствен само за високотехнолошки криминал, јер су учиниоци кроз историју прелазили у другу државу у односу на територију у којој су извршили радњу кривичног дела како би избегли кривично гоњење и осуду. Оно што је специфично за високотехнолошки криминал јесте да су такви сценарији учестали до те мере да се може говорити о правилу. Експанзија информационих технологија, нарочито Интернета, као средства и предмета извршења кривичног дела, односно окружења у ком се радња извршења предузима, довела је до тога *да надлежни органи једне државе не могу без сарадње са надлежним органима друге државе да се ефикасно супротставе овом облику криминала*. Примера ради, 2006. године британски пружалац услуга електронских комуникација је пријавио полицији да је створена мрежа ботнетова од око 19.000 рачунара чији власници су корисници те копманије. Иако је рачунар који је компромитовао ботнетове првобитно био лоциран у Лондону, даљи оперативни рад је показао да је осумњичени из Канаде убрзо „пребацио“ контролу на сервер лоциран у Немачкој, потом у Кореју и САД, па је у истрази нужно учествовала полиција свих наведених држава[549]. У операцији *Rescue* на разбијању мреже од 70.000 лица осумњичених да су размењивали приказе порнографског материјала преко форума *boylover.net* учествовала је полиција из 13 држава[550]. Током 2008. и 2009. године на територији Републике Србије оштећена лица пријавила су десет случајева са елементима „Нигеријских превара или „419

[549] R. Bryant, P. Stephenson, „Policing Digital Crime: the International and Organisational Context“, Bryant, Bryan, *op.cit*, 111.

[550] http://ceop.police.uk/Media-Centre/Press-releases/2011/HUNDREDS-OF-SUSPECTS-TRACKED-IN-INTERNATIONAL-CHILD-ABUSE-INVESTIGATION/.

превара“ против непознатих учинилаца у којима су радње кривичних дела предузете на подручју Нигерије, Сенегала и Бенина, међутим, међународна полицијска сарадња са наведеним државама до данас није довела до значајнијих резултата истраге ових случајева[551].

Традиционално поимање информационе безбедности које у центар пажње поставља изоловани рачунарски систем није адекватно у околностима дигиталне и бежичне повезаности. Концепт по ком су рачунарски подаци похрањени у одређеном рачунарском систему на одређеном месту и у оквиру једне државе постаје све мање релевантан из разлога што је локација на којој се рачунарски подаци нестабилна. Наиме, подаци се „крећу“ између сервера и јурисдикција или могу бити из разлога сигурности и доступности „пресликани“ на више локација и тиме се налазити у територијама различитих држава у исто време, као што садржај веб страница може бити састављен од динамички повезаних извора информација лоцираних на различитим серверима[552]. Тако *умрежени свет постао је велико „игралиште“ за извршиоце кривичних дела* против поверљивости, целовитости и доступности рачунарских система и података, односно дела високотехнолошког криминала уопште. *Изазови технолошког напретка* пред органима гоњења се огледају у *повећаном обиму података* који се чувају, обрађују или преносе кроз рачунарске мреже, употреби *више различитих уређаја* за приступ подацима, могућности извршиоца да *сакривају трагове активности и очувају анонимност* (коришћењем енкрипције, *proxy* сервера, *TOR* рутера, услуга иностраних пружалаца услуга електронских комуникација, *Voice-over-IP* технологија и друго), *искоришћавању рачунара невиних лица или удаљених информационих структура* за извршење дела високотехнолошког криминала

[551] У овим кривичним делима оштећени су примили електронску пошту у ком се моли да помогне у пребацивању веће суме новца из Сенегала у Африци. Пошиљаоци оваквих мејлова углавном се представљају као рођаци неких од званичника или државника страних земаља, који увек желе да пребаце велике своте новца, за шта им је потребан банковни рачун из друге земље, а за узврат обећавају одређену провизију. Описане преваре су углавном вршене помоћу *Spam* порука преко бесплатних налога за електронску пошту отвараних на Интернет сервисима *Yahoo, Hotmail* и др, а употребљаване су и лажне Интернет адресе на којима су се налазиле Интернет презентације постављене од стране извршилаца кривичних дела, са намером да обману наивне кориснике Интернета. У реализацији превара коришћена је и фалсификована документација државних органа и предузећа Нигерије, Гане, Сенегала, Камеруна и других држава са територије Западне Африке.

[552] S. Gareth, *Website Location: Cyberspace vs. Geographic Space*, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/Gareth%20Samson%20Website%20Location.pdf

(нпр. у виду *botnet* напада), *коришћењу услуга cloud computing*-а којим се електронски докази похрањују у серверима *на различитим локацијама* (у серверима на територији једне или више држава) или *веб страница чије се IP адресе непрекидно мењају*[553]. Све ове технолошке промене означавају се термином „губитак локације“ (“*loss of location*”[554]), што има директне последице на рад органа надлежних за откривање и доказвање кривичних дела.

Дакле, поменути фактори доприносе томе да је откривање дела и учинилаца отежано, а у одређеним случајевима и немогуће без сарадње са надлежним органима друге државе, па је стога потребно пронаћи *механизам* употребом ког би се могли *обезбедити електронски докази који су непостојани, нестабилни и расути у различитим надлежностима*. Примена мера и радњи за приступ електронским доказима подразумева препознавање одређене локације на којој су рачунарски подаци похрањени. Уколико се тражени подаци налазе ван територијалне надлежности државе, надлежни органи те државе не могу предузимати доказне радње на територији друге државе у складу са принципом територијалног суверенитета. Осим тога, приступ доказима о транснационалним облицима високотехнолошког криминала треба да буде остварен у складу са законом како би се они могли користи пред судом у кривичном поступку.

Стандардна процедура у овој ситуацији подразумева активирање механизама прекограничне сарадње надлежних органа (како полиције, тако и јавних тужилаштава) и међународне правне помоћи у кривичним стварима[555]. Прибављање доказа путем међународне правне помоћи игра важну улогу у раду полиције и тужилаштва за гоњење учинилаца свих кривичних дела са прекограничним елементима, али за гоњење и истрагу дела високотехнолошког криминала, потреба за сарадњом се не може никада превише нагласити. Како

---

[553] G. Laykock, “New Challenges for Law Enforcement”, *European Journal on Criminal Policy and Research* 1/2004, 42.

[554] *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf , 5.

[555] Међународна кривична помоћ се дели на велику кривичноправну помоћ (правну помоћ у ширем смислу - која се односи на извршење стране кривичне пресуде, уступање кривичног гоњења страној држави, те издавање окривљених и осуђених) и малу кривичноправну помоћ (правну помоћ у ужем смислу) која се односи на одређене облике процесне и доказне асистенције. Види, М. Шкулић *et al*, *Усаглашеност домаћих прописа са институтима Европске уније у области међународне правне помоћи у кривичним стварима и препоруке за хармонизацију*, Удружење јавних тужилаца и заменика јавних тужилаца, Београд 2011, 9-10.

„дигитални криминал не познаје границе између држава[556]“ неспорно је да „борба против високотехнолошког криминала треба буде или глобална или нема смисла“[557] јер „без обзира колико је ефикасан правни оквир једне државе (локални прописи), глобална природа високотехнолошког криминала чини међународну сарадњу неизбежном“[558]. Дакле, међународна сарадња је императив за ефикасно супротстављање глобалној транснационалној природи злоупотреби информационих технологија у кибер простору.

Како су механизми пружања међународне правне помоћи спори а у појединим случајевима и непостојећи, актуелно је питање да ли и под којим околностима надлежни органи једне државе могу легално да предузимају радње изван граница сопствене земље (укључујући ситуацију да се докази чувају у "облаку", који би могао да буде било где), односно да директно приступе рачунарским подацима који су похрањени у рачунарским системима/мрежама у иностранству преко рачунара на територији државе, посебно у случају када постоји потреба за хитним реаговањем.

У овом поглављу ћемо настојати да дамо одговор на следећа питања:

1) Применом којих мера и радњи надлежни органи могу да обезбеде и приступе електронским доказима уколико су рачунарски подаци и рачунарски системи налазе у надлежности једне или више других држава или уколико је њихова локација непозната или се мења? Ради проналажења одговора на то питање, приказаћемо најпре *опште оквире* за пружање међународне правне помоћи у кривичним стварима.

2) Да ли је оправдано инсистирати на редовним механизмима за пружање правне помоћи у кривичним стварима, а који су дуготрајни, док је природа података који могу бити електронски докази таква да се они лако и брзе мењају, односно прикривају и губе. У том смислу ће бити сагледани *специфични механизми* који су неопходни за убрзавање прекограничне сарадње надлежних органа у откривању, истраживању и гоњењу односно супротстављању криминалу коју почива на злоупотреби дигиталне технологије и рачунарских система (уз

[556] Grabosky, *op.cit*, 15.
[557] R. Broadhurst, „Developments in the global law enforcement of cyber-crime“, *Policing: An International Journal of Police Strategies and Management* 2/2006, 414.
[558] Clough, *op.cit*, 4.

указивање на потребу стварања експедитивних процедура за хитно чување података како би се спречио њихов губитак или измена пре окончања редовне процедуре слања и поступања по замолницама);

3) Под којим условима и у којој процедури државе једна другој могу дозволити спровођење прекограничног мрежног претраживања, а уз поштовање права осумњиченог, као и права и интереса трећих лица. У случају да се надлежним органима стране државе прекогранично мрежно претраживање не дозволи, да ли би било могуће на одређени начин обезбедити податке који се обрађују, складиште и преносе у оквиру рачунарске мреже или система на територији те државе и у каквој процедури (прекограничан приступ рачунарима).

У циљу остваривања сарадње неопходне за вођење кривичног поступка за дела високотехнолошког криминала са прекограничним елементима, надлежни државни органи имају две могућности: једна се односи на *спонтану размену информација и оперативну сарадњу*, а друга на *формалне механизме пружања узајамне правне помоћи*. У том смислу, могу се разликовати три нивоа сарадње[559]: макро-ниво (сарадња која се остварује између држава и међународних организација на основу мултилатералних и билатералних уговора које предвиђају механизме за пружање међународне правне помоћи у кривичним стварима), мезо-ниво (сарадња која се остварује између надлежних државних органа појединих држава за *ad hoc* потребе, нпр. стварањем заједничких истражних тимова), и микро-ниво (директна неформална сарадња надлежних органа која је неопходна ради активирања формалних механизама сарадње). У остваривању поменутих видова сарадње на наведеним нивоима, државе и њихови надлежни органи могу користити како општи оквир за пружање међународне правне помоћи у кривичним стварима, тако и специфичне могућности за унапређење сарадње на супротстављању високотехнолошком криминалу предвиђене у Конвенцији о високотехнолошком криминалу.

[559] Bryant, Stephenson, *op.cit*, 112-113.

1. ОПШТИ ОКВИР ЗА ПРУЖАЊЕ МЕЂУНАРОДНЕ ПРАВНЕ ПОМОЋИ У КРИВИЧНИМ СТВАРИМА

То што извршиоци кривичног дела не познају границе у кибер простору, не значи да надлежни државни органи не морају да поштују територијалне границе суверенитета друге државе. Без обзира на „безграничност“ кибер простора, сарадња са надлежним органима друге државе је императив. Суверене државе једна другој упућују молбу у ситуацији када је ради прикупљања доказа за кривични поступак потребно предузети мере и радње у другој држави, у оквиру узајамне правне помоћи или других облика међународне сарадње. Међународна сарадња држава чланица у кривичним стварима је прилично комплексно питање на које утичу бројни фактори, при чему је стварање правног оквира само један од њих. Примера ради, проблем коришћења ботнета у криминалне сврхе и немогућност реаговања правног система на спречавање, откривање и доказивање овог облика високотехнолошког криминала постао је алармантан након напада у Естонији током априла и маја 2007. године, када важни делови јавних критичних информационих инфраструктура и велики део информационих система приватног сектора данима нису функционисали услед напада великих размера на њих (дистрибуираног напада ускраћивања услуга посредством преко милион зомби рачунара). Као резултат опсежних напада Парламент је донео одлуку о блокирању система електронске поште, две велике банке присутне у Естонији су потпуно обуставиле *on-line* пословање и блокирале своје контакте са иностранством, а како је нападнут естонски телефонски систем, ометан је рад сваке друге јавне телефонске централе, естонске Инетенет странице нису биле доступне данима и слично. Више *IP* адреса које су користили осумњичени су биле лоциране, али резултат истраге је био да је само једно лице идентификовано као осумњичени, и то држављанин Естоније, који је кривично гоњен и осуђен, док су остали осумњичени користили *IP* адресе лоциране у држави која није потписница Конвенције о високотехнолошком криминалу (Русија) па у конкретним случајевима нису могле бити примењене одредбе Конвенције о облицима међународне сарадње а Русија је одбила поступање по молби естонских надлежних органа јер постојећи механизми за пружање узајамне правне помоћи

нису били одговарајући[560]. У принципу, постојање правног оквира је неопходан предуслов за успостављање, односно унапређење сарадње, али и други фактори играју важну улогу. Чињеница да правни инструмент постоји није никаква гаранција да се правила постављена у њему примењују у пракси на предвиђен начин нити да се постижу очекивани резултати. Као пример да постојање правног основа за међународну сарадњу није резултирало гоњењем учиниоца може се навести случај у ком аутор *Love Bug* вируса, иако је постојала сарадња између надлежних органа Филипина и других држава, није био гоњен[561]. Вирус је у року од 2 часа заразио више од 45 милиона корисника у преко 20 држава и проузроковао штету која се процењује између 2 и 10 милијарди долара. Истражним радњама је утврђено да вирус потиче са територије Филипина, а на основу сарадње *FBI*, истражних органа Филипина и пружалаца услуга, утврђен је идентитет креатора вируса. Како прављење вируса и уношење у рачунарску мрежу није било предвиђено као кривично дело у тој држави, било је потребно неколико дана да судски органи одлуче да ли ће дозволити претрес стана осумњичених, за које време су прикрили велики део електронских доказа у вези са поменутим активностима. Налог за претрес стана је издат и пронађени су докази против једног лица (*Onel de Guzman).* Како у Филипинима није било инкриминисано нити ометање рачунарског система нити диструбуирање вируса, лице је оптужено за превару у вези са кредитним картицама, али је оптужба одбијена из разлога недостатка доказа за та кривична дела. С друге стране, ни екстрадиција није била могућа у САД из разлога што није био испуњен услов двоструке инкриминације[562].

Међународна правна помоћ у кривичним стварима у Републици Србији указује се првенствено по основу потврђених међународних уговора којима се уређује сарадња надлежних државних органа у вези са гоњењем и кривичним поступком, а ако такав уговор не постоји или одређена питања њиме нису регулисана, помоћ се указује сходно одредбама Закона о међународној правној помоћи у кривичним

[560] Више о проблемима непостојања одговарајућег механизма за међународну сарадњу, E. Tikk, K. Kaska, „Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons", *Proceedings of the 9th European Conference of Information Warfare and Security – Thessaloniki*, 2010, 290.
[561] Singh, *op.cit*, 62.
[562] Goodman, Brenner, *op.cit*, 141.

ствaрима (у даљем тексту: ЗМПП)[563]. Република Србија је потписница великог броја међународних уговора у области сарадње у кривичним стварима, и то како конвенција, тако и билатералних уговора, који представљају основ за пружање међународне правне помоћи[564], а од нарочите важности је *Конвенција Савета Европе о узајамној правној помоћи у кривичним стварима* из 1959. године (са пратећим Протоколом из 1978. године[565]. Конвенција је изузетно значајна, јер је концепт, по ком је за пружање међународне правне помоћи неопходно покретање одговарајућег поступка упућивањем формалне молбе преко надлежних органа једне државе надлежним органима замољене државе, представљао модел како за касније усвојене конвенције које садрже одредбе о пружању међународне правне помоћи (па и за одредбе у КВК), тако и за решења у ЗМПП, па и за прописе ЕУ у овој области.

Како је Република Србија држава кандидат за чланство у Европској унији, на уму треба имати и акте усвојене у циљу остваривања сарадње држава чланица у кривичним стварима. Први корак у правцу стварања оквира за пружање узајамне правне помоћи између надлежних органа држава чланица Европске уније представљало је усвајавање *Конвенције Европске уније о узајамној правној помоћи у кривичним стварима* 2000. године[566]. Како је у пракси поступања надлежних

[563] "Сл.гласник РС", бр.20/2009.

[564] Међу потврђеним мултилатерланим уговорима најзначајнији су следећи: Конвенција Уједињених нација против транснационалног организованог криминала, Конвенција Савета Европе о међусобном пружању правне помоћи у кривичним стварима са додатним протоколима, Европска конвенција о екстрадицији са додатним протоколима, Европска конвенција о трансферу осуђених лица, Европска конвенција о међународном важењу кривичних пресуда, Европска конвенција о преносу поступка у кривичним стварима. Попис мултилатералних и билатералних уговора о правној помоћи у кривичним стварима може се видети на следећем линку: http://arhiva.mpravde.gov.rs/cr/articles/medjunarodne-aktivnosti-eu-integracije-i-projekti/medjunarodna-pravna-pomoc/medjunarodni-ugovori-o-pravnoj-pomoci-u-krivicnim-stvarima.html.

[565] Закон о потврђивању Европске Конвенције о узајамној правној помоћи у кривичним стварима, са додатним протоколом („Сл. лист СРЈ-Међународни уговори", бр.10/2001).

[566] *Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01): http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF*. Када је потребно да се предузму одређене радње у вези са кривичним поступком у једној земљи, надлежни органи те земље имају могућност да затраже помоћ од надлежних органа друге државе чланице у смислу да предузму те радње у оквиру своје надлежности а чији резултати се потом могу користити у кривичном поступку који се води у држави чланици која је помоћ у конкретном случају затражила. Према одредбама Конвенције пружање узајамне правне помоћи се заснива на механизму писаних замолница: држава молиља подноси другој држави преко надлежних органа замолницу, уз одговарајућу документацију, а замољена држава у одређеном поступку одговара на захтев за пружањем помоћи садржан у замолници ако су испуњене одређене претпоставке и

органа уочено да постављени услови и поступак пружања узајамне правне помоћи чине овај „традиционални“ облик сарадње спорим и компликованим, а тиме и неефикасним, осмишљена је „напреднија“ форма сарадње која се заснива на принципу *међусобног признавања одлука.* Овај облик сарадње у кривичним стварима је постао могућ након усклађивања релевантних националних прописа кроз примену заједничких минималних правила прописаних на нивоу ЕУ, која се углавном односе на услове за прихватљивост доказа и права процесних субјеката у кривичним поступцима. Постоји неколико правних инструмената чији је циљ да се обезбеди међусобно признавање одлука у кривичним стварима[567]. Са циљем олакшавања и убрзавања сарадње између држава чланица у погледу прикупљања и преноса доказа за потребе кривичног поступка, 3. априла 2014. године донета је *Директива 2014/41/ЕУ о европском налогу за истрагу у кривичним стварима*[568]. Поред поменутог, циљ Директиве је и хармонизација прописа који уређују овај облик међународне сарадње између држава чланица. Замисао је да Директива замени постојећа правила о прекограничном прикупљању доказа ради превазилажења фрагментације правне регулативе у овој области на нивоу Европске уније. Ипак, тенденцији да се систем узајамне правне помоћи замени механизмом заснованим на принципу узајамног признавња одлука у кривичном поступку, могу се упутити одређени приговори[569]. Ради подстицања сарадње правосудних и полицијских органа у кривичним стварима на нивоу ЕУ су *формирана и одређена тела и агенције,* од којих најзначајнију улогу имају

услови. Помоћ се пружа у складу са националним прописима и од стране надлежних органа замољене државе. Осим тога, предвиђена је могућност спонтане размене информација о истрагама у току (без слања замолница и дуге процедуре), као и посебни облици сарадње: контролисана испорука, заједнички истражни тимови, прикривене истраге итд.

[567] За преглед правних инструмената о међусобном признавању одлука у кривичним стварима види http://ec.europa.eu/justice/criminal/recognition-decision/index_en.htm. Релевантна правила у погледу признавања одлука, а у вези са сарадњом у супртотстављању високотехнолошком криминалу налазе се у следећим инструментима: Оквирна одлука о привременом одузимању имовине и доказа, усвојена 2003. године, Оквирна одлука о прикупљању доказа у смислу одузимања предмета, исправа и података за употребу у кривичним стварима, усвојена 2008. године, Оквирна одлука о спречавању и решавању сукоба надлежности у кривичном поступку, усвојена 2009. године.

[568] *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters* (*Official Journal of the European Union L*130/1).

[569] Више о томе вид. L. Bachmaier, „European Investigation Order for obtaining evidence in the criminal proceedings: study of the Proposal for a European Directive“, *Zeitschrift für Internationale Strafrechtsdogmatik* 9/2010, 581.

Јединица Европске уније за правосудну сарадњу (*EUROJUST: The European Union's Judicial Cooperation Unit*[570]) и Европска полиција (*EUROPOL*[571]).

Прекогранични захтеви за пружање помоћи су од нарочитог значаја за обезбеђење електронских доказа јер постоји велика вероватноћа измене или губитка и велики изазов за органе је да им се *омогући ургентно реаговање,* односно да се радње предузму што је пре могуће. Да би прекогранична сарадња надлежних органа била ефикасна, од суштинског је значаја да се *потребне и прецизне информације могу размењивати спонтано, брзо и ефикасно* у оквиру одговарајућих процедура и механизама, и због тога је сврсисходно и корисно умрежавање базе података надлежних државних органа више држава у једну информациону структуру. У том смислу је недвојбено значајна улога *Interpol*-а као међународног оквира за размену информација и сарадњу на оперативном нивоу између полиција држава чланица. У оквиру *Interpol*-а функционише *информациона инфраструктура* коју чине базе података чланица и захваљујући том заштићеном комуникационом систему државе чланице могу константно свакодневно да размењују податаке безбедно и брзо, што доприноси квалитетном решавању криминалистичких случајева како на локалном плану, тако и у регионалном и међународном нивоу и тиме се омогућава промптно реаговање криминалистичке полиције[572]. Национални централни биро *Interpol*-а у Београду

[570] *EUROJUST* је стална агенција Европске уније са правним субкетивитетом основана Одлуком Савета 2002. године (која је измењена и допуњена Одлукама Савета из 2003. и 2009. године) са циљем да подржи и координира сарадњу надлежних правосудних органа држава чланица у истрагама и гоњењу кривичних дела организованог прекограничног криминала. У чл.4.ст.1.Одлуке из 2009.године наводи се да се ради о кривичним делима за које је успостављена надлежност *EUROPOL*-а и са њим а повезаним кривичним делима.

[571] *EUROPOL* је основан 1998. године, а од 2010. године је стална агенција Европске уније са правним субјективитетом која има за циљ да олакша сарадњу полиције држава чланица у борби против организованог прекограничног криминала. Ради се о следећим кривичним делима: недозвољена трговина дрогом, илегалне миграције, тероризам, фалсификовање новца и других средстава плаћања, трговина људским бићима, *укључујући дечју порнографију,* недозвољена трговина моторним возилима и прање новца. Дакле, *EUROPOL* има мандат само у односу на поједина дела високотехнолошког криминала и то уколико су последица деловања организованог криминала.

[572] Колико је потребна добра заштита информационог система за управљање базама података показује следећи пример. Током 2012. године (у периоду од 28.02. до 01.03.2012. године) хакерска група *Anonymous* извршила је тзв. *DDoS* напад на сајт *Interpol*-а. Наиме, са 698.274 Интернет адресе са свих континената било је симултано упућено и до 400.000 напада у минути (2.300.000 у првих 25 минута) због чега је био „оборен" сајт али није остварен ниједан случај неовлашћеног приступа базама података, нити је угрожен заштићени комуникациони систем. Генерални секретаријат водио је операцију *Unmask*, којом приликом је лишено слободе 25 лица из Шпаније, Колумбије, Чилеа и Аргентине.

налази се у саставу МУП-а Републике Србије (у оквиру Управе за међународну оперативну полицијску сарадњу) и преко њега се одвија међународна полицијска сарадња, у смислу размене информација од оперативног и тактичког, а у извесним случајевима и стратешког значаја. Својим системом евиденције и вођењем документације Национални централни биро чини доступним оперативним организационим јединицама Управе криминалистичке полиције, али и других управа Министарства унутрашњих послова Републике Србије, у кратком временском року, криминалистички значајне податке из око пола милиона досијеа[573]. Осим система за размену података, у оквиру Генералног секретаријата *Interpol*-а образован је *Поддиректорат за борбу против финансијског и високотехнолошког криминала* који је своју пажњу усмерио на следеће криминалне активности: фалсификовање новца, прање новца, злоупотребу интелектуалне својине, преваре платним картицама, нападе компјутерским вирусима и кибер тероризам. У оквиру Поддиректората се формирају радне групе које се баве конкретним случајевима из праксе криминалистичких полиција држава чланица, односно обезбеђује се подршка чланицама у свим фазама истраге дела високотехнолошког криминала и координисање заједничких истрага[574]. Тако је, на пример, у склопу међународне полицијске акције у сузбијању дечије порнографије на Интернету, полиција Републике Србије у сарадњи са немачком савезном полицијом, посредством *Interpol*-а, прикупила податке о већем броју лица са територије Србије који су путем Интернета вршили дистрибуцију видео материјала порнографске садржине, настале искоришћавањем малолетних лица,

[573] Урошевић, Ивановић, Уљанов, *op.cit,* 85. и 110.

[574] Радне групе чине представници националних криминалистичких служби, који ради размене оперативних података долазе на месечне, шестомесечне, годишње и *ad hoc* састанке, који се могу организовати у Генералном секретаријату *Interpol* -а или у седишту криминалистичке полиције његове државе чланице. Поред овога *Interpol* је активан и на пољу сузбијања и спречавања криминалитета Интернет технологија, у оковиру којег су формиране регионалне радне групе у Европи, Африци, Азији и јужном Пацифику, те Латинској Америци. Њихова надлежност је у области злоупотреба: бежичних технологија, *3G* мобилних телефона, мултимедијалних порука *MMS* и виртуелног новца. Посебан значај ове радне групе имале су на плану едукације припадника националних бироа у погледу борбе против високотехнолошког криминала. У оквирима европске радне групе значајни су пројекти: Пројекат полицијског надзора виртуелног Интернета, Пројекат првих полицијских службеника на месту извршења дела, Пројекат праћења ботнетова, Пројекат форензике података у реалном времену уживо или пројекат супростављање антифорензичким мерама. Више о томе, Урошевић, Ивановић, Уљанов, *op.cit,* 117-122.

лицима са територије Немачке[575]. Осим тога, постојање тзв. *Cyber Fusion Center* омогућава надзор и анализу малициозних активности на Интернету у реалном времену, те пружање информација и стручне подршке потребне за ефикасну истрагу[576], а током 2014.године у Сингапуру је почео са радом *форензички центар* под називом „Глобални комплекс за иновације[577]“ у ком се налази најсавременија форензичка лабораторија за подршку истрагама дигиталног криминала полицији држава чланица.

Европска полиција у циљу олакшавања сарадње полиције држава чланица ЕУ у борби против организованог прекограничног криминала прикупља, обрађује и размењује податке и информације, обавештава државе чланице преко националних чланова о информацијама релевентним за истраге у тим државама, захтева од држава да покрену, воде или координирају истраге и предлаже формирање тимова за заједничку истрагу, обезбеђује оперативну анализу, израђује стратешке извештаје и обезбеђује експертизу и техничку подршку за истраге које се воде на територији држава чланица[578]. С тим у вези је значајна *Одлука 2008/615/ЈНА о унапређењу прекограничне сарадње, посебно у борби против тероризма и прекограничног криминала* из 2008. године[579] заснована на тзв. Прумском споразуму. Смисао Одлуке није успостављање јединствене наднационалне базе података, него су правила заснована на „умрежавању“ националних база података држава чланица ради аутоматске размене личних

[575] У наставку акције, српска и немачка полиција су прибавиле део доказног материјала који је дистрибуиран путем Интернета, као и податке који су послужили за идентификацију и проналажење извршилаца на територији Србије. Након размене и увида у прибављени материјал, утврђено је да се ради о видео и другим материјалима у електронском формату, који приказују вулгарно сексуално злостављање деце. На основу прикупљених података, у одвојеним акцијама, идентификовани су осумњичени. Крајем марта 2010. год. у Србији је дошло до лишења слободе више лица на подручју Кикинде и Београда због због постојања основа сумње да су извршила кривично дело приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију. Урошевић, Ивановић, Уљанов, *op.cit,*115-116.

[576] http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[577] *INTERPOL Global Complex for Innovation (IGCI),* http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.

[578] Више о задацима и овлашћењима, организацији и начину рада, *https://www.europol.europa.eu/sites/default/files/council_decision.pdf.*

[579] *Council Decision 2008/616/JHA f 23 June 2008 n the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,* www.europarl.europa.eu.

података у циљу спречавања кривичних дела и одржавање јавног реда и безбедности у вези са масовним догађајима са прекограничном димензијом[580].

Ове две најзначајније међународне полицијске организације су 2011. године постигле *договор о заједничкој иницијативи* за јачање међусобне сарадње и унапређење глобалног одговора на проблем међународних криминалних активности, са закључком да њихов однос није ривалски, већ комплементаран и усмерен ка борби против истих облика криминалних активности са елементима организованости и транснационалности (међу којима је и високотехнолошки криминал)[581]. Међутим, проблем у сарадњи представљају различити заштићени комуникациони системи за размену података њихових држава чланица. На бројним састанцима ових међународних полицијских организација разрађивана су могућа решења за превазилажење ове техничке и методолошке препреке и као решење је пронађен *поступак интероперабилности* (повезивање комуниционих система ради стварање безбедне везе за размену података) а са циљем омогућивања и поједностављивања међусобне размене података ових међународних полицијских организација, како на оперативном, тако и на стратешком нивоу.

Спонтана размена информација је основа за експедитивну сарадњу у односу на дуготрајне и споре формалне механизме пружања узајамне помоћи, који су, међутим, још увек неопходан и незаменљив пут за остваривање сарадње. Приказани формални механизми узајамне правне помоћи јесу дуготрајни, али спонтана размена информација не обезбеђује прикупљање доказа који се могу користити у кривичном поступку, него увек претходи формалној процедури за

[580] Полазећи од тога да би ближа полицијска и правосудна сарадња у кривичним стварима трабало да се спроводи у складу са поштовањем основних права и слобода, посебно права на поштовање приватности и права на заштиту личних података, било је неопходно установити посебан режим заштите података, који би био прилагођен специфичној природи различитих облика размене података, а нарочито одређене специфичности прекограничног *online* приступа базама података. У том смислу значајне су одредбе Одлуке које прописују правила заштите података приликом аутоматског претраживања и упоређивања релевантних података. Више о значају Оквирне одлуке, Писарић М.: „Унапређење размене података у оквиру прекограничне полицијске и правосудне сарадње у кривичним стварима на нивоу Европске уније - "Прумски процес", Зборник радова Правног факултета у Новом Саду 3/ 2010, 560.

[581] https://www.europol.europa.eu/sites/default/files/flags/interpol .pdf. Циљ Споразума јесте унапређење размене стратешких и тактичких информација и координација активности, кроз развој заједничких стандарда и акционих планова, обуку и научна итраживања, те размену официра за везу.

пружање узајамне правне помоћи[582]. Ефикасна борба против транснационалних облика злоупотреба информационих технологија, а нарочито прикупљање електронских доказа, захтева хитно и брзо реаговање, из ког разлога је *постојеће опште оквире сарадње надлежних органа потребно прилагодити специфичним изазовима* које пред њих поставља посебна природа дела високотехнолошког криминала. Стога смо мишљења да би најделотворнији начин за постизање екефтивне и ефикасне сарадње надлежних државних органа у супротстављању високотехнолошком криминалу био *кроз потпуно искоришћавање могућности које предвиђа Конвенција СЕ*.

2. СПЕЦИФИЧНИ ПРАВНИ МЕХАНИЗМИ САРАДЊЕ У СУПРОТСТАВЉАЊУ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ

Конвенција о високотехнолошком криминалу у Поглављу III садржи одредбе (у члановима 23-35) које се односе на међународну сарадњу надлежних државних органа страна потписница у вези са истрагом дела високотехнолошког криминала и прикупљањем електронских доказа о било ком кривичном делу. Конвенција садржи опште и специфичне одредбе које се односе на међународну сарадњу, а приступ усвојен у тексту Конвенције представља *комбинацију привремених мера у циљу обезбеђења електронских доказа на експедитиван начин* (релевантне су одредбе чланова 29, 30. и 35. које предвиђају оперативне механизме) *са традиционалним облицима узајамне правне помоћи у погледу предузимања*

[582] Тако су у случају нигеријских превара, након подношења кривичних пријава оштећених држављана Републике Србије, полицијски службеници прикупили доказе и трагове у виду електронских података о оствареној комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама, које је оштећени извршио према инструкцијама које је добио од извршилаца. Након описаног обављене су провере лог фајлова сервера у потрази за IP адресом, у циљу лоцирања сервиса преко којих су извршиоци кривичног дела слали електронске поруке оштећенима, као и преглед целокупне електронске поште коју је оштећени примио (уз упоређивање података са сервера и рачунара оштећеног), како би се уочили пропусти направљени од стране извршиоца а који су могли указати на постојање кривичног дела и места одакле је извршена превара. Након изоловања ИП адресе и времена слања електронских порука из лог фајлова преко Интерпола су, у зависности од државе са чије је територије извршено кривично дело, вршене провере у вези корисника коме је она била додељена у тренутку вршења кривичног дела. Ове провере су вршене према расположивим подацима уз захтеве према државама порекла нежељених или преварних порука на начин слања неког вида замолнице о предузимању појединих оперативно-тактичких радњи. Урошевић, В. Уљанов, С. Вуковић, Р.: „Полиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије“, ZITEH 2006, 345-346.

појединих доказних радњи. У одељцима који следе, анализиране су одредбе Конвенције које садрже општа правила у вези са пружањем узајамне правне помоћи (међу њима и правила о екстрадицији), а потом одредбе које регулишу обавезе држава потписница на пружање узајамне помоћи у односу на привремене мере и доказне радње. Посебан одељак посвећен је разматрању могућности за прекогранични приступ подацима похрањеним у рачунарским системима у другој држави.

2.1. Општа правила Конвенције у вези са пружањем узајамне правне помоћи

Као опште начело у вези са међународном сарадњом у члану 23. Конвенције предвиђено је да стране уговорнице међусобно сарађују у најширем могућем обиму, што подразумева да се од држава *очекује спремност да поступају по одговарајућим основама за пружање међународне правне помоћи, уз што рестриктивније позивање на сметње у сарадњи* са другим државама потписницама у вези са истрагом и кривичним поступком за кривична дела у вези са рачунарским системима и прикупљањем доказа у електронском облику за било које кривично дело.

У погледу основа за пружање међународне правне помоћи, примењен је *принцип субсидијаритета*. Наиме, Конвенција предвиђа да државе потписнице сарађују у складу са одредбама поглавља III Ковенције *а кроз примену одговарајућих међународних инструмената о међународној сарадњи у кривичним стварима, договора усаглашених на основу једнообразних или реципрочних прописа, као и домаћих прописа о међународној правној помоћи у кривичним стварима*. То значи да одредбе Конвенције нису замена за постојеће основе за сарадњу у кривичним стварима (потврђене мултилатералне и билатералне међународне уговоре), него *представљају својеврсну допуну тим инструментима сарадње.* У том смислу, у члану 39. изричито је прописано да је сврха Конвенције је да допуни важеће мултилатералне или билатералне уговоре или договоре између држава уговорница, укључујући одредбе: Европске конвенције о екстрадицији; Европске конвенције о узајамној помоћи у кривичним стварима и

Додатног протокола уз Европску конвенцију о узајамној помоћи у кривичним стварима. Одредбе ових конвенција су прецизиране одговарајућим одредбама у Одељку 3. Конвенције које се односе на специфичности пружања помоћи у смислу предузимања оперативних и процесних радњи откривања и доказивања кривичних дела на које се Конвенција односи. Како би, дакле, држава уговорница испоштовала обавезу да другим странама уговорницама пружи узајамну помоћ у најширем могућем обиму у поступцима који се односе на кривична дела у вези са рачунарским системима и подацима или прикупљању доказа у електронском облику о кривичном делу, *потребно је да у националним прописима постоји адекватан правни основ неопходан да држава изврши обавезе установљене члановима 27. до 35. Конвенције*. Уколико су две или више држава уговорница имају закључен споразум који се односи на материју регулисану Конвенцијом или су на други начин успоставиле своје односе или уколико то у будућностиураде, оне могу да примењују тај споразум или уговор или да на други начин, сходно томе, успоставе своје односе. Међутим, ако државе уговорнице успоставе своје односе у вези са материјом на коју се односи Конвенција, другачије него што је њоме предвиђено, оне то могу даураде само на начин који није у супротности са циљевима и начелима Конвенције.

Према томе, државе сарађују на основу билатералних и мултилатералних споразума, а Конвенција треба да служи као допуна, односно спецификација одредаба у потврђеним међународним уговорима у поступку пружања правне помоћи у кривичним стварима у погледу дела високотехнолошког криминала али може да представља основ за сарадњу, уколико између држава други основ не постоји.

У погледу *прописа који се примењују* у поступцима за пружање узајамне помоћи, предвиђено је да се примењују *услови предвиђени законима замољене државе* или важећим уговорима о узајамној помоћи, укључујући и разлоге на основу којих замољена држава може да одбије сарадњу (члан 25. став 4). Захтеви за узајамну помоћ се *извршавају у складу са поступцима које одреди држава молиља*, изузев уколико су у супротности са законима замољене државе[583]. Овакво решење је потребно из разлога како би се обезбедило да докази који

[583] Такво решење је садржано и у ЗПМПП у члану 90.

настану као резултат предузимања радњи од стране органа замољене државе буду прихватљиви у кривичном поступку пред судом у држави молиљи. Тако се у складу са чланом 12. ЗПМП у поступку пружања међународне правне помоћи сходно примењују одредбе Законика о кривичном поступку и закона којима се уређује организација и надлежност судова и јавних тужилаштава, *а на захтев надлежног органа државе молиље предузимање радњи осталих облика међународне правне помоћи* (међу којима су....., увиђај, претресање просторија и лица, привремено одузимање предмета; примену мера, као што су надзор и снимање телефонских и других разговора или комуникација и оптичка снимања лица, ...рачунарско претраживање и обрада података; размену обавештења и достављање писмена и предмета који су у вези са кривичним поступком у држави молиљи, достављање података без замолнице; .....;) *врши се на начин који предвиђа законодавство државе молиље,* ако то није у супротности са основним начелима правног поретка Републике Србије. Ипак, да би се уопште поступало по молби за предузимање осталих облика међународне правне помоћи *морају бити испуњене претпоставке из члана 7. ЗПМПП, као и услови предвиђени Законником о кривичном поступку* за предузимање тих радњи.

У вези са *условом двоструке инкриминације,* сматра се да је тај услов испуњен, без обзира на то да ли закони замољене државе не прописију то дело у истој групи кривичних дела или га не означавају истим терминима као и држава молиља, докле год је радња која је у основи кривичног дела у вези за које се узајамна помоћ захтева, одређена као кривично дело и по њеним законима (члан 25. став 5).

За *спонтану размену информација* је важна одредба по којој држава уговорница може, у границама домаћег права и без претходног захтева, да другој страни уговорници проследи информације до којих је дошла у оквиру сопствених истрага, уколико сматра да би откривање таквих информација могло да помогне дражави уговорници која их прима, у покретању или вођењу истрага или поступака у вези са кривичним делима прописаним у складу са Конвенцијом, или када би те информације могле да доведу до упућивања захтева те стране уговорнице за узајамну сарадњу, на основу овог поглавља (члан 36). Пре него што достави такве информације, држава уговорница која их доставља може захтевати

да оне буду чуване у тајности или да се могу користити само под одређеним условима. Уколико држава уговорница која прима информације не може да прихвати такав захтев, о томе је дужна да обавести страну уговорницу која доставља информације, која након тога одлучује да ли ће ипак да проследи те информације, а уколико држава уговорница прихвати информацију под одређеним условима, ти услови су за њу обавезујући.

Свака страна уговорница треба да *одреди орган за комуникацију на принципу 24 сата 7 дана у недељи* на који начин би се омогућило пружање тренутне помоћи у истрагама или кривичним поступцима у вези са кривичним делима која се односе на рачунарске системе и податке или ради прикупљања доказа у електронском облику о кривичном делу. Таква помоћ треба да обухвати олакшавање или, уколико то домаће законодавство дозвољава, непосредно спровођење следећих мера: а) давање техничких савета; б) заштиту података у складу са чл. 29. и 30. Конвенције, и в) прикупљање доказа, давање информација правне природе и лоцирање осумњичених. Орган одређен као контакт треба да располаже могућностима довољним да може брзо да размењује поруке са лицима и органима задуженим као контакт од стране друге дражаве уговорнице. Уколико лице/ орган које је одредила држава уговорница није део њених државних органа или органа надлежних за међународну узајамну помоћ или екстрадицију, потребно је обезбедити могућност да то лице/ орган може да брзо да сарађује са тим органима. Како је пружање узајамне помоћи у кривичним стварима предмет процедуре која може дуго да траје, прописано је да свака држава уговорница може, у хитним случајевима, да поднесе захтев за узајамну помоћ или пружање информација, користећи се брзим средствима комуникације (а не уобичајеним каналима комуникације[584]), укључујући факс или електронску пошту, у мери у којој ова средства могу да обезбеде одговарајући степен безбедности и аутентичности (укључујући коришћење шифри, када је потребно) уз накнадно формално упућивање молбе за помоћ, ако замољена држава то захтева, док је замољена држава дужна у том случају да прихвати и одговори на захтев брзим средством комуникације (члан 25. став3).

[584] Као што је, примера ради, предвиђено у члану 5. и 6. ЗМПП.

Од изузетне важности су одредбе садржане у 4. Одељку III поглавља Конвенције којима се уређује пружање међународне правне помоћи у ситуацијама у којима између државе молиље и замољене државе *не постоји важећи уговор или договор* о узајамној помоћи на основу једнообразног или реципрочног права, односно када не постоји основ за пружање правне помоћи, и у том смислу ове одредбе уређују одговарајуће основе, услове и процедуре. Постоји више начина за упућивање захтева за пружање правне помоћи. Најпре, Конвенција предвиђа обавезу државе потписнице да приликом потписивања или депоновања инструмената о потврђивању, прихватању, одобравању или приступању Конвенцији, *именује централни орган или органе* одговорне за слање и одговарање на захтеве за узајамну помоћ, извршавање или прослеђивање органима надлежним за њихово извршење (који органи директно међусобно комуницирају упућивањем захтева за узајамну помоћ), те да достави Генералном секретару Савета Европе имена и адресе тих именованих органа, који о томе формира и одржава регистар[585]. Осим наведеног, у хитним случајевима, *захтев* за узајамну помоћ или обавештења у вези са њим (али који не садрже елементе принуде), правосудни органи државе молиље *могу директно да пошаљу одговарајућим надлежним органима замољене државе* (у таквим случајевима преко централног органа државе молиље треба истовремено послати копију захтева централном органу замољене државе). Ако је захтев поднет органу који није надлежан да поступи по захтеву, он захтев прослеђује надлежном домаћем органу и о томе директно обавештава државу молиљу. Такође, сваки захтев или обавештење може да се спроведе непосредно преко Међународне организације криминалистичке полиције (Интерпол).

Не постоји обавеза замољене државе да поступи по захтеву државе молиље у сваком случају. Наиме, замољена држава може да *одбије да пружи помоћ*, поред случајева који су предвиђени у њеном законодавству и ако се захтев односи на дело које сматра политичким деликтом или делом које је повезано са политичким деликтом, или ако сматра да извршење захтева вероватно може да угрози њен суверенитет, безбедност, јавни поредак или друге битне интересе (при чему разлог „други битни интереси“ не би требало превише екстензивно тумачити у

[585] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp.

конкретном случају, у складу са општим начелом да се помоћ пружа у најширем могућем обиму). Осим могућности да одбије да пружи затражену помоћ, замољена држава може да *одложи поступање* по захтеву уколико би оно угрозило кривичне истраге или поступке које спроводе њени надлежни органи. У сваком случају, пре одбијања или одлагања пружања помоћи, замољена држава разматра да ли захтеву може да удовољи делимично или ће извршење захтева везати за испуњење одређених услова, које сматра неопходним, а након консултације са државом молиљом када је то целисходно.

Замољена држава одмах обавештава државу молиљу *о исходу извршења захтева* за помоћ, при чему је дужна навести разлоге за одбијање или одлагање, као и о разлогу који онемогућава извршење захтева или вероватно, у значајној мери, одлаже извршење. Осим тога, држава молиља може да тражи да замољена држава чува у тајности постојање захтева као и садржај захтева, у мери која је неопходна да би захтев могао да се изврши, но уколико замољена држава не може да испуни захтев у вези са тајношћу, о томе одмах обавештава државу молиљу, која затим одлучује да ли ће, упркос томе, да упути захтев на извршење. Такође, свака држава уговорница која доставља податке, може да захтева од друге државе уговорнице да јој, у вези са тим условом, образложи у коју ће сврху те податке да употреби. У том смислу, замољена држава може достављање тражених података да услови: а) чувањем тајности захтева, када захтеву за узајамну правну помоћ не може да се удовољи без тог услова; б) забраном коришћења за потребе других истрага или поступака, осим оних који су наведени у захтеву. Уколико држава молиља не може да испуни неки од ових услова, о томе одмах обавештава другу страну уговорницу, која затим одлучује да ли ће, упркос томе, да достави информације, а уколико прихвати услов, обавезна је да га испуни.

У складу са позитивноправним прописима, у погледу *поступка изручења* окривљеног или осуђеног првенствено се примењују одредбе Конвенције Савета Европе о екстрадицији са додатним протоколима које је Република Србија потписала и ратификовала[586], односно билатерлани уговор између Србије и друге

[586] Закон о потврђивању Европске конвенције о екстрадицији са додатним протоколима („Сл.лист СРЈ – Међународни уговори“, бр. 10/2001). Стране уговорнице се обавезују да ће, према прописима и условима који су наведени у Конвенцији, издавати једне другима лица која се гоне због почињеног кривичног дела или се траже ради извршења казне или мере безбедности од стране правосудних органа стране молиље. Издавање ће се вршити за дела за која је, према

државе. У случају да друга држава није потписница Конвенције о екстрадицији нити између ње и Србије постоји билатерални уговор или када одређена питања потврђеним међународним уговорима нису уређена, примењују се одредбе ЗПММП[587]. У том смислу значај КВК огледа се у томе што потписнице обавезују да *Конвенцију сматрају за основ за екстрадицију* између држава уговорница чак и ако оне нису потписнице неке конвенције која предвиђа обевезу прописивања екстрадиције или када између њих не постоји билатерални уговор на основу ког би се могло захтевати изручење учинилаца дела високотехнолошког криминала. Наиме, на основу члана 24. Конвенције, за учиноице кривичних дела која су прописана у складу са чл. 2. до 11. у случају да је испуњен услов двоструке инкриминације, односно под условом да су она по законима обе стране уговорнице предвиђена као кривична дела за која је прописана казна затвора од најмање годину дана, државе потписнице могу тражити једна од друге екстрадицију, чак и ако не постоји ниједан други основ за то[588]. У погледу основа за екстрадицију, предвиђено је да у случају да држава уговорница, која екстрадицију условљава постојањем уговора, прими захтев за екстрадицију од друге дражава уговорнице са којом нема уговор о екстрадицији, она може да сматра ову Конвенцију правним основом за екстрадицију у погледу кривичних дела прописаних у складу са чл. 2. до 11. ове Конвенције. С друге стране, стране уговорнице које екстрадицију не условљавају постојањем уговора, сматраће та кривична дела делима која подлежу међусобној екстрадицији. У погледу услова и поступака за екстрадицију, примењују се прописи замољене државе уговорнице или важећи уговори о екстрадицији, укључујући и разлоге на основу којих замољена дражава може да одбије екстрадицију. Даље је предвиђено да у случају да замољена држава одбије екстрадицију само на основу држављанства лица које

законима стране молиље и замољене стране, као највећа казна прописана казна лишења слободе или мере безбедности, лишења слободе од најмање годину дана или строжа казна. Када се ради о казни или мери безбедности изреченој на територији стране молиље, трајање изречене казне мора да буде најмање четири месеца.

[587] У Републици Србији су питања изручења окривљеног/ осуђеног регулисана у члановима 13-40. Закона о пружању међународне правне помоћи у кривичним стварима.

[588] Такође, изричито је наведено да се сматра да ова кривична дела спадају у групу кривичних дела која подлежу екстрадицији у сваком уговору о екстрадицији који постоји између две или више држава уговорница, при чему се исте обавезују да у сваки уговор о екстрадицији који убудуће закључују са две или више држава уговорница та дела укључе у групу дела која подлежу екстрадицији.

се тражи или зато што сматра да има надлежност за то дело, а у складу са принципом *aut dedere aut judicare,* на захтев државе молиље је дужна да достави предмет својим надлежним органима ради гоњења а потом страни уговорници која тражи екстрадицију благовремено саопшти крајњи исход, при чему надлежни органи доносе одлуку, спроводе истраге и поступке, као у случају било ког другог дела сличне природе, у складу са својим законима[589].

2.2. Пружање узајамне правни помоћи у односу на привремене мере

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 државе молиље да приступе тим подацима у складу са прописима о узајамној правној помоћи, потребно је предвидети могућност надлежних органа једне државе да од надлежних орагана друге државе траже да предузму одређене мере у циљу да се спречи губитак или измена тих рачунарских података, и то у складу са одредбама којима се уређују мера *Хитно чување ускладиштених рачунарских података* из члана 29. Конвенције и мера *Хитно откривање ускладиштених рачунарских о саобраћају* из члана 30. Конвенције.

Рачунарским подацима који су укладиштени у рачунарским системима који се налазе у другим држава се иначе приступа у складу са процесним радњама из члана 31-34. 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 из *члана 29. Конвенције* које има карактер хитне мере јер се њеним предузимањем обезбеђује тренутно чување

[589]У овом одељку је садржана и одредба по којој свака држава уговорница, приликом потписивања или приликом депоновања инструмената о потврђивању, прихватању, одобравању или приступању, доставља Генералном секретару Савета Европе име и адресе свих органа који су, у случају непостојања уговора, одговорни за подношење или пријем захтева за екстрадицију или притвор, који формира и одржава ажурност регистра надлежних органа које одређују државе уговорнице.
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp.

података који се већ налазе ускладиштени у рачунарском систему (као својеврсно „замрзавање“ у неизмењеном облику), и то како података о саобраћају, тако и садржаја остварене комуникације, који су 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[590].

Држава уговорница може другој држави уговорнице упутити захтев у смислу да њени надлежни органи наређе или на други начин обезбеде хитну заштиту података сачуваних преко рачунарског система који се налази на територији замољене државе и у вези са којим држава молиља намерава да тражи узајамну помоћ у сврху претраге или сличног приступа, заплене или сличног обезбеђења или откривања података[591].
Када надлежни органи замољене државе приме овакав захтев, дужне су да предузму све одговарајуће мере да би се хитно, у складу са националним прописима, хитно сачувају тражени подаци.

У погледу могућности државе да одбије поступање по оваквом захтеву, наведено је да држава не може да се захтева постојање двоструке кажњивости као услов за обезбеђење заштите података. Уколико држава захтева двоструку кажњивост као услов за одговор на захтев за узајамну помоћ у сврху претраге или сличног приступа, заплене или сличног обезбеђења или откривања сачуваних података она може да, у вези са другим делима, осим оних на које се Конвенција односи, задржи право да одбије захтев за хитно чување, у случајевима у којима има основа да верује да у време откривања, услов двостране кажњивости не може

[590] Више о томе, М. Писарић, „*Мера хитног чувања ускладиштених рачунарских података*“, Зборник радова Правног факултета у Новом Саду 1/2014, 230-231.
[591] Уколико подноси овакав захтев, надлежни орган државе молиље је дужан да наведе следеће податке: а) назив органа који захтева хитно чување података; б) дело које је предмет кривичне истраге или поступака и сажет опис чињеница у вези са тим; в) који рачунарски подаци треба да се сачувају и њихову повезаност са делом; г) све расположиве информације које идентификују лице које поседује или под контролом има потребне рачунарске податке или податке о месту где се налази рачунарски систем; д) разлог због којег је неопходно да се подаци хитно сачувају; и ђ) наводе да држава уговорница намерава да поднесе захтев за узајамну помоћ у сврху претраге или сличног приступа, заплене или сличног обезбеђења или откривања сачуваних рачунарских података.

да се испуни[592]. Приликом одлучивања да ли ће по захтеву поступити или ће позивајући на наведене основе такво поступање одбити, надлежни органи замољене државе такође могу да, уколико процене да хитно чување неће да обезбеди будућу доступност података или, пак, да угрожава тајност или на други начин угрожава истрагу, о томе одмах обавесте државу молиљу, која затим одлучује да ли ће, упркос томе, да упути захтев на извршење[593]. У вези са предузимањем мере хитног чувања ускладиштених рачунарских података на захтев државе молиље је и одредба *члана 30. Конвенције* којом се уређује хитно откривање сачуваних података о саобраћају. Наиме, уколико током извршења захтева, који се односи на хитно чување података о саобраћају који се односе на одређену комуникацију, замољена држава открије да је пружалац услуга електронских комуникација у другој држави умешан у пренос такве комуникације, замољена држава треба хитно да открије другој држави уговорници количину података о саобраћају која је довољна за идентификацију пружаоца услуге и путање којом је комуникација остварена. Откривање података о саобраћају је могуће одбити само уколико се захтев односи на дело које замољена држава сматра политичким деликтом или делом које је повезано са политичким деликтом, или уколико замољена држава сматра да извршење захтева вероватно може да угрози њен суверенитет, безбедност, јавни поредак или друге битне интересе.

Што се тиче имплементације ових одредаба у прописима појединих држава, потребно је навести да већина не садржи специфичне одредбе о овим радњама, него се користе механизми пружања узајамне помоћи у вези са одредабама које уређују ове привремене мере када их предузимају домаћи надлежни органи[594]. Изричите одредбе у циљу имплементације члана 29. Конвенције садржи, примера

[592] Ипак, поступање по захтеву за заштиту података замољена држава може да се одбије само: а) ако се захтев односи на дело које сматра политичким деликтом или делом које је повезано са политичким деликтом, или б) ако сматра да извршење захтева вероватно може да угрози њен суверенитет, безбедност, јавни поредак или друге битне интересе.

[593] Уколико поступа по захтеву који упућује држава молиља, хитно чување ускладиштених рачунарских података је потребно обезбедити у року до 60 дана, да би се држави молиљи омогућило да поднесе захтев за претрагу или сличан приступ, заплену или слично обезбеђење или откривање података, а хитно чување података података ће се осигурати и након пријема таквог захтева, у до доношења одлуке да ли ће се по њему поступити.

[594] Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf.

ради, португалски Закон компјутерском криминалу. Овај Закон садржи одредбу која се непосредно односи на хитно чување и откривање рачунарских података у оквиру међународне сарадње. Надлежни орган стране државе може тражити експедитивно чување података који су похрањени у рачунарском систему на територији Португалије, а такав захтев треба да садржи назив кривичног дела и чињеничне околности случаја из којих проистче потреба за овом привременом мером, означавање рачунарских података које треба обезбедити и њихову повезаност са кривичним делом, доступне информације које идентификује држаоца потребних рачунарских података или локацију рачунарског система у ком су похрањени подаци, као и намеру органа да упути формалан захтев за узајамну правну помоћ у погледу приступа тако обезбеђених подацима. На основу таквог захтева суд може наредити држаоцу или лицу које има контролу над подацима (првенствено пружаоцима услуга електронских комуникација) да предузму потребне мере за обезбеђење потребних података, а уколико постоје разлози хитности или опасност од одлагања, меру може наредити и судска полиција (уз накнадну ауторизацију од стране суда). У наредби за хитно чување података се означава природа података, извор и одредиште комуникације, временски период за који је потребно податке обезбедити (до три месеца, уз могућност продужења до највише годину дана од момента одређивања мере). Суд може одбити да изда наредбу уколико се захтев иностраних орган односи на дело које је политичке природе или би издавање наредбе угрозило суверенитет државе, јавну безбедност или друге важне интересе, уколико држава чији орган је упутио захтев не пружа довољно гаранција у погледу заштитите података о личности или ако је вероватно да ће се захтев за пружање узајамне правне помоћи одбити из разлога што није испуњен захтев двоструке инкриминације. Сходна примена ових правила предвиђена је и у ситуацији да португалски надлежни органи упуте захтев за експедитивно чување података надлежном органу друге државе.

У погледу члана 30. Конвенције у већини држава је за делимично откривање података о саобраћају надлежним органима друге државе потребно активирање механизама међународне правне помоћи, чиме се не остварује сврха одредбе у смислу експедитивности ове привремене мере. Тако се у Немачкој у складу са

Законом о међународној правосудној сарадњи[595] (члан 61. и 92.) спонтана размена информација остварује на основу формалног захтева за међународну праву помоћ. Једино поменути члан 22. португалског Закона предвиђа да полиција након што јој пружаоци услуга, поступајући по наредби за хитно обезбеђење података, доставе податке о саобраћају (који идентификују све пружаоце укључене у остваривање комуникације и путању којој се она преноси) те податке без одлагања прослеђује надлежном иностраном органу како би се омогућило упућивање формалног захтева за остваривање приступа тим подацима.

2.3. Пружање узајамне правни помоћи односу на доказне радње

Уколико током истраге дела високотехнолошког криминала појави за прикупљањем електронских доказа који се налазе у иностранству, правила међународног јавног права налажу да се у таквим случајевима користе механизми пружања узајамне правне помоћи у кривичним стварима, на основу којих надлежни органи једне државе упућују молбу да надлежни органи друге државе предузму поједине доказне радње како би се докази до којих се дође њиховом применом употребили у кривичном поступку. На овом правилу се заснивају и решења у члановима 31, 33. и 34. Конвенције.

Тако на основу *члана 31*. Конвенције (*Узајамна помоћ у вези са приступом ускладиштеним рачунарским подацима*) надлежни органи једне државе могу да упуте захтев да надлежним органима замољене државе да претраже или на други сличан начин приступе, заплене или на други сличан начин обезбеде и открију податке ускладиштене у рачунарском систему који се налази на територији замољене државе, укључујући и податке у односу на које су примењене мере из чл. 29. Конвенције. Замољена држава треба да одговори на захтев на нарочито експедитиван начин применом међународних инструмената, договора и закона, уколико: а) постоји основи сумње да су одговарајући подаци нарочито подложни губитку или измени, или б) инструменти, договори и закони и иначе налажу експедитивну сарадњу.

[595] Gesetz über die internationale Rechtshilfe in Strafsachen, http://www.gesetze-im-internet.de/englisch_irg/englisch_irg.html.

С обзиром на то да су за кривични поступак од значаја не само подаци који су већ ускладиштени у једном рачунарском систему/мрежи, него и подаци који се генеришу у реалном времену док сигнал кроз рачунарску мрежу пролази од извора до одредишта комуникације, потребно је у процесном законодавству предвидети могућност прикупљања тих података, и то како података о саобраћају тако и података који се односи на сам садржај комуникације. У погледу предузимања радњи прикупљања наведених података а у оквиру узајамне правне помоћи, релевантне су одредбе чланова 33. (*Узајамна помоћ у вези са прикупањем у реалном времену података о саобраћају комуникација*) и 34. (*Узајамна помоћ у вези са пресретањем садржаја комуникација*) Конвенције. Тако, у складу са *чланом 33. Конвенције*, државе треба да обезбеде узајамну помоћ у циљу прикупљања у реалном времену података о саобраћају, који се односе на одређене комуникације које се остварују у оквиру рачунарских мрежа и система на њиховој територији. У погледу узајамне помоћи у пресретању података из садржаја комуникација, у складу са *чланом 34. Конвенције* државе треба да обезбеде узајамну помоћ у циљу прикупљања или снимања у реалном времену података из садржаја одређених комуникација, пренетих преко рачунарског система, до границе коју дозвољавају међусобно важећи уговори и домаће право.

На основу анализе прописа појединих држава, дошли смо до недвосмисленог закључка да се доказне радње за потребе кривичног поступка који се води у другој држави предузимају у складу са националним прописима о пружању међународне правне помоћи у кривичним стварима, а извршавају их домаћи органи по правилима које уређују кривичну процедуру. Дакле, надлежни органи једне државе нису овлашћени да прикупљају у реалном времену податке о саобраћају комуникација нити да пресрећу комуникације, него у случају потребе за тим упућују захтев за пружањем помоћи другој држави, па уколико су испуњени услови за пружање помоћи, предузимањем одговарајућих радњи и мера у складу са прописима замољене државе, надлежни органи те државе предузимају радње и о резултатима обавештавају органе државе молиље. Пружање помоћи предузимањем ових радњи се, дакле, остварује у складу са условима и поступцима прописаним правом замољене државе и то најмање у погледу оних кривичних дела за које би прикупљање података о саобраћају у реалном времену,

односно пресретање комуникација било могуће у сличном домаћем предмету. Из тог разлога је изузетно важно да прописи који садрже овлашћења надлежних органа за предузимање радњи и мера у циљу прикупљања електронских доказа буду у што већој мери усаглашени, како би се докази применом процесних одредаба у једној држави могли користити као доказ у кривичном поступку у другој држави[596]. У том смислу Конвенција о високотехнолошком криминалу је од непроцењивог значаја.

Јасно је да државе нису спремне да се одрекну свог суверенитета у овом делу. Међутим, у научној и стручној јавности је актулено питање да ли је и под којим условима могуће да органи једне државе применом техничких средстава предузимају радње у циљу прикупљања података за потребе кривичног поступка за дела високотехнолошког криминала, односно да ли приступ рачунару и рачунарским системима који се налазе на територији друге државе а коришћењем међународне комуникационе инфраструктуре, какав је Интернет, представља кршење принципа територијалног суверенитета или превазилажењу овог проблема треба приступити прагматично прописивањем могућности екстратериторијалног деловања државних органа под одређеним условима.

2.4. Прекогранични приступ рачунарским системима

Држава је заинтересована не само да инкриминише екстратериторијална понашања која производе значајне последице у оквиру њене територије, него и да њени надлежни органи истражују та понашања предузимањем прекограничног приступа и претраге удаљеног рачунарског система/мреже који се налази ван граница њене територије. Надлежни органи су у појединим државама овлашћени *да даљински претраже*, тј. на одговарајући начин приступе рачунарском систему, односно делу рачунарског система као и уређајима за складиштење података који се *налазе на територији државе, уколико је вероватно* да су подаци потребни за доказивање дела високотехнолошког криминала похрањени у том другом рачунарском систему или делу рачунарског система а њима се може приступити, односно на одређени начин могу постати доступни преко рачунарског система

[596] О овој проблематици, Rashbaum K. et al., „Admissibility of non-U.S. Electronic Evidence“, *The Richmond Journal of Law and Technology* 5/2011, 1-76.

који се предмет првобитне претраге. Тако се у САД на основу *Pen register* користи *remote forensic software* - програм за електронски мониторинг на бази тројанаца који се даљински инсталира на рачунар који је предмет претраге, ради снимања и преношења свих рачунарских података на рачунар надлежних државних органа, те праћење активности рачунара на Интернету[597] (тзв. *Magic Lantern* , односно *Computer and Internet Protocol Address Verifier: CIPAV*[598]). У Европи је Немачка била прва земља која је законом предвидела могућност удаљеног прекограниченог приступа и претраге рачунара у вези са превенцијом и откривањем кривичних дела повезаних са међународним тероризмом[599] али је тај пропис проглашен неуставним[600]. Питање је *да ли би надлежни органи били овлашћени да иницијалну претрагу прошире и на тај други систем уколико се он налази на територији друге државе*. Уколико би услед транснационалне природе високотехнолошког криминала и могућности просторне удаљености између учиниоца и оштећеног, након дуготрајне истраге са пуно техничких детаља органи гоњења утврдили да се рачунар учиниоца налази у иностранству, с обзиром да надлежни органи предузимају радње само у оквиру територије своје државе, једини начин да се прикупе потребни докази и лице лиши слободе односио би се на коришћење механизама међународне правне помоћи у кривичним стварима, што налажу правила међународног јавног права. Међутим, с обзиром на неефикасност таквих механизама у смислу дуготрајности процедура, с једне стране, и природу података који се обрађују, складиште и преносе путем Интернета и потребу хитног реаговања у кибер простору, с друге стране, да ли би било оправдано, чак и уколико не постоји међународни уговор који би омогућио међународну сарадњу у предузимању радњи прикупљања доказа, *надлежним органима дати овлашћење да под одређеним условима и у одређеним случајевима приступе и претраже рачунарске системе и мреже која се налази на територији друге државе*, односно да предузимају одређене радње ради прикупљања података за потребе кривичног поступка за дела високотехнолошког криминала

[597] W. Abel, „Agents, Trojans and tags: The next generation of investigators“, *International Review of Law, Computers & Technology* 1-2/2009, 107.
[598] J. Nogueira, „Mobile Intelligent Agents to Fight Cyber Intrusions“, *International Journal of Forensic Computer Science* 1/2006, 30.
[599] Тзв. *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*.
[600] Gercke, Brunst, *op.cit,* 56-57.

чак и ван граница њихове територије. Овакав радикалан приступ није широко прихваћен јер већина држава није спремна да се одрекне свог суверенитета и прихвати да надлежни органи друге државе предузимају одређене истражне радње на њиховој територији[601]. Након што надлежни орган утврди да се потребни подаци налазе похрањени у рачунарском систему/мрежи која се налази у иностранству и након што се утврди на територије које државе је лоциран систем/мрежа, орган провера да ли са односном државом постоји одговарајући основ за пружање узајамне правне помоћи и покрећу се механизми међународне сарадње[602].

Међутим, потреба регулисања приступа рачунару, рачунарским системима и рачунарским мрежама у другој држави и претраживања података који су ускладиштени, обрађују се или преносе у њима произилази из чињенице да је у Интернет окружењу, услед природе ове глобалне рачунарске мреже и повезаности рачунарских система који се налазе у различитим државама, сасвим могућа ситуација да надлежни органи једне државе, предузимајући одређене доказне радње не буду свесни да су претрагом обухваћени подаци у оквиру рачунарских система који се налазе у другим државама, чиме може доћи до повреде територијалног суверенитета држава уколико би претраге биле предузете без претходног обавештења, односно сагласности друге државе[603]. Како у кибер простору границе националних држава и надлежности државних органа могу имати нејасне оквире, може се десити да органи приступају похрањеним подацима преко електронских мрежа а да при томе нису у могућности да процене да ли се одређени рачунарски подаци ускладиштени у рачунару који се физички налази на њиховој територији или на територији друге државе. *Овај проблем додатно усложњава повећано коришћење hosting услуга иностраних пружалаца услуга електронских комуникација и примена уређаја и услуга заснованих на cloud computing-у.* Једнострани приступ рачунарским подацима похрањеним у рачунарском систему на страној територији без потребе упућивања захтева за узајамну правну помоћ је сложено питање које захтева преиспитивање правила

[601] Goodman, Brenner, *op.cit,* 178.
[602] S. Brenner, J. Schwerha, "Transnational evidence gathering and local prosecution of international cybercrime", *John Marshall Journal of Computer and International Law* 3/2002, 356-358.
[603] P. Bellia, „Chasing bits across borders", *University of Chicago Legal Forum*, 2/2001, 39-40.

међународног јавног права о суверенитету државе, с једне стране, а повезано је за заштитом права појединаца у смислу гаранција у складу са националним прописима, с друге стране[604]. Из тог разлога неопходно би било да постоје експлицитна међународноправна правила која би уређивала могућност прекограничног приступа и претраге рачунарских система и мрежа, односно споразуми који дефинишу услове под којима се претрага може вршити, уместо праксе по принципу *laisee faire*[605].

Ово питање је било актуелно од краја 1980-тих година, а у форми „директне пенетрације" надлежних органа на територију друге државе помиње се у Препоруци о кривичним делима повезаним са рачунарима[606] из 1989. године и у завршном извештају Европског комитета о проблемима кривичних дела[607] из 1990. године. Комитет министара Савета Европе је у Препоруци која се односи на проблеме које информационе технологије постављају пред кривично процесно право[608] из 1995. године указао на хитност потребе за преговарањем у циљу стварања међународног споразума који би регулисало питање када, како и до ког обима би било могуће проширивање претреса рачунарског система који је у територијалној надлежности друге државе. На основу две поменуте препоруке, у нацрту Конвенције о високотехнолошком криминалу је указано на потребу стварања механизма за регулисање прекограничног претреса рачунара и одузимање похрањених рачунарских података. Разматрање потребе за омогућавањем прекограничног приступа подацима може се уочити и у документима Групе 8, у оквиру које су 1999. године усвојени Принципи о прекограничном приступу похрањеним рачунарским подацима[609], по којима се од

[604] Осим правних захтева, не треба занемарити непостојање утврђене и научно проверене методологије за прикупљање података на овај начин. О томе више, E. Kenneally, „Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection", UCLA Journal of Law and technology 5/2005,17.

[605] Kaspersen, *op.cit*, 26.

[606] R*(89)9 on Computer-related Crime, http://www.oas.org/juridico/english/89-9&final%20Report.pdf.*

[607] *European Committee on Crime Problems,* Final Report, http://www.oas.org/juridico/english/89-9&final%20Report.pdf

[608] *Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology*, http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp

[609] Принципи су усвојени на састанку министара у Москви. *Principles on Transborder Access to Stored ComputerData*,http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf.

држава очекује да омогуће експедитивно чување података и експедитивну узајамну правну помоћ, уз истовремено предвиђање могућности да органи једне државе без претходно добијеног овлашћења од стране друге државе приступе јавно доступним подацима без обзира где су географски лоцирани.

Поменути принципи су уграђени Конвенцију о високотехнолошком криминалу, али не у смислу да је дозвољено надлежним органима једне државе да прошире претрагу рачунара на рачунарски систем који се налази на територији друге државе а ком је преко претраживаног рачунарског система у оквиру њихових граница могуће приступити путем Интернета или друге рачунарске мреже, него је у случају потребе за тим, обавезно ангажовање одговарајућих механизама узајамне правне помоћи у кривичним стварима (у смислу члана 31. Конвенције). Међутим, *у складу са чланом 32*. Конвенције, који регулише прекогранични приступ као изузетак од територијалног принципа, надлежни органи једне државе могу, без упућивања захтева за пружање узајамне помоћи другој држави уговорници, под *одређеним условима* једнострано приступити *одређеним подацима* који су ускладиштени у рачунарским системима на територији друге државе. Наиме, на основу поменутог члана у ком је предвиђена радња *Прекогранични приступ похрањеним рачунарским подацима уз сагласност или када су доступни јавности*, надлежни органи једне државе уговорнице могу без претходног добијања дозволе и обавештавања друге државе уговорнице да:

а) приступе рачунарским *подацима који су иначе доступни јавности* (*open source*), без обзира где се подаци географски налазе (нпр. надлежни органи могу приступити и преузети податке који су похрањени на Интернет страници без обавезе да о томе обавештавају државу у којој се налази рачунарски систем који је хост те станице), или

б) приступе или да приме рачунарске податке похрањене у иностранству преко рачунарског система на својој територији, уколико прибаве *законит и добровољан пристанак лица које има законско овлашћење да учини доступним податке преко тог рачунарског система* (нпр. уколико би лице, чија је електронска пошта од стране пружаоца услуга ускладиштена у другој држави или које намерно чува податке у рачунарском систему у другој држави, добровољно омогућило надлежним органима приступ тим подацима).

Законит и добровољан пристанак значи да према лицу није упућен обавезујући захтев који садржи принуду и предочавање последица непоступања по захтеву нити да је лице обмануто, а *пристанак лица* се цени према прописима државе према чијим органима је дат, односно који остварују прекогранични приступ. Као први познати случај у ком је остварен прекогранични приступ рачунарима у иностранству помиње се предмету *United States v. Gorshkov. FBI* је 2001. године истражујући кривична дела која су два лица користећи рачунаре у Русији извршила против америчких компанија, на превару прибавио лозинке за приступ рачунарима осумњичених и на тај начин дошао до инкриминишућег материјала који је искоришћен за оптужбу[610]. Међутим, управо овакво поступање наводи се као негативан пример у литератури, јер је прекогранични приступ дозвољен само уколико постоји добровољан пристанак лица. Да ли је *лице законски овлашћено да преда податке*, цени се према прописима државе на чијој територији се налази рачунар ком се прекогранично приступа. Битно је и питање места на ком се налази лице када даје пристанак, односно омогућава приступ подацима. Постоје две ситуације, лице се налази на територији државе чији надлежни органи траже прекогранични приступ или се налази у иностранству[611], у ком случају је потребно водити рачуна о томе, да ли је кажњиво прикупљање и одавање података иностраним државним органима без посредства домаћих органа, чак и ради потребе вођења кривичног поступка[612]. Битно је напоменути да се на овај начин може приступити *само тачно одређеним рачунарским подацима* који су *јасно лоцирани*, а да то није дозвољено у погледу неодређених података за које није утврђено где се налазе. Такође, једнострани приступ подацима *не подразумева обавезу државе да обавести другу државу* о предузетим радњама у складу са овим чланом али таква могућност није ни искључена.

Осим у ситуацијама предвиђеним у ставовима члана 32. Конвенције, надлежним органима једне државе није дозвољено да приступају рачунарским подацима који су ускладиштени у рачунарском систему на територији друге државе, него имају само могућност да упуте захтев у смислу члана 31.

[610] N. Seitz, „Transborder search: a new perspective in law enforcement?“, *Yale journal of law and technology* 7/ 2005, 24-25.
[611] Kaspersen, *op.cit*, 27.
[612] J. Goldsmith, „The Internet and the Legitimacy of Remote Cross-Border Searches“, *The University of Chicago Legal Forum* 103/2001, 12.

Конвенције. На овом месту бисмо указали да је Комитет Конвенције 2011. године формирао радну групу[613] са циљем да се преиспитају могућности унапређења регулисања и примене једностраног прекограничног приступа рачунарским подацима похрањеним у иностранству. Група има за задатак да креира инструмент (у виду амандмана на Конвенцију, додатног протокола или препоруке) регулисања прекограничног приступа и других доказних радњи које се предузимају на Интернету, уважавајући принципе међународног јавног права, суверенитета држава и принципе заштите људских права, јер је постојање међународног правног основа неопходан услов за превазилажење неадекватности процедура пружања узајамне правне помоћи у циљу прикупљања електронских доказа који су похрањени у иностранству, у смислу занемаривања природе рачунарских података као потенцијалних доказа.

Постоје две ситуације у којима су потребни електронски докази похрањени у рачунарским системима у иностранству, а чије околности условљавају различито поступање надлежних државних органа: А. Надлежни орган је преузео контролу над рачунаром који је повезан са Интернетом и има овлашћење да приступи сајтовима или рачунару који се налази у територијалној надлежности друге државе на основу домаћег закона или комбинације домаћег закона и одредаба члана 32. Конвенције о високотехнолошком криминалу[614]; или Б. Електронски докази се налазе у "облаку" - на пример, поруке електронске поште осумњиченог се не чувају у његовом кућном рачунару који је одузет, него су ускладиштени на другом месту, на удаљеном серверу, на пример, у САД[615]. У том смислу можемо разликовати директан прекогранични приступ и прекогранични приступ посредством пружалаца услуга електронских комуникација.

[613] Тзв. *Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows"*.
[614] Huey L., Rosenberg R., „Watching the Web: Thoughts on expanding police surveillance opportunities under the Cyber-crime Convention", *Canadian Journal of Criminology and Criminal Justice* 10/2004, 600.
[615] M. Wittow, D. Buller, „Cloud Computing: emerging legal issues for access to data, anywhere, anytime", *Journal of Internet Law* 1/2010, 3.

2.4.1. Директан прекогранични приступ рачунарским системима

Невезано за решења садржана у Конвенцији, државе су превазилажењу поменутих потешкоћа у истрази дела високотехнолошког криминала приступиле различите начине. Поједине полазе од тога да њихови надлежни имају могућност да предузимају удаљене прекограничне претраге рачунара, односно да употребом рачунара на њиховој територији приступе и прегледају рачунарске податке који су похрањени у иностранству, уколико је то оправдано потребом конкретног кривичног предмета. У основи полазишта да је дозвољена прекогранична претрага рачунара и да су надлежни органи овлашћени да остваре директан прекогранични приступ је „виртуелна присутност" података на територији државе, односно преко рачунара у границама њихове надлежности. На овај начин поступају и надлежни органи у Србији, иако не постоји непосредан законски основ за то[616], што сматрамо би било оправдано уколико би Законик о кривичном поступку предвидео такву могућност. У *Белгији* је 2000. године усвојен Закон о информатичком криминалу, у вези са којим је у белгијски Законик о кривичном поступку[617] унет члан 88*ter* на основу ког истражни судија може наредбу за претрагу рачунарског система проширити тако да су органи унутрашњих послова овлашћени да приступе другом рачунарском систему где год се налазио. Истражни судија проширује наредбу обухватајући и удаљени рачунарски систем уколико је то неопходно за утврђивање истине а друге истражне радње нису адекватне за постизање тог циља или постоји јасан ризик да докази могу бити изгубљени (услов који је испуњен увек када се ради о непостојаним подацима у рачунарској мрежи). Давањем овог овлашћења полиција нема потпуну дискрецију у погледу обухвата рачунарског система, јер истражни судија у наредби ограничава проширену претрагу на тачно одређене делове рачунарског система ком се може приступити преко првобитно претраживаног рачунара. Уколико околности указују да се потребни електронски докази налазе у рачунару који је на територији друге државе, подаци којима се приступило се копирају. О том

[616] Што произлази из разговора са Тужиоцем и Шефом одсека.
[617] COE, *Transborder access and jurisdiction: What are the options?*, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf, 32.

истражни судија обавештава Министарство правде преко канцеларије Јавног тужилаштва, а Министарство обавештава државу на чијој територији се налази рачунарски систем на који је проширена претрага.

Међутим, једнострано регулисање могућности прекограничног приступа рачунару не решава проблем екстратериторијалног деловања и може се сматрати не само противно принципима територијалног суверенитета, него и некорисним и контрапродуктивним за остваривање легитимних циљева кривичног поступка, јер иако прекогранична претрага рачунара може бити легална у једној, у другој држави би представљала кривично дело у смислу неовлашћеног приступа рачунарском систему. Тако је у *Шпанији* остваривање удаљеног приступа рачунару могуће само на основу претходног одобрења суда на образложен предлог јавног тужиоца у погледу тешких кривичних дела, уколико се другим радњама потребни докази не би могли прикупити (карактер посебне доказне радње) али је ова могућност изричито забрањена у погледу рачунара који се налазе у иностранству[618].

Законодавац појединих држава је на становишту да је прекогранични приступ рачунару који је лоциран у иностранству а коме се може приступити са њихове територије, питање које се може решити само у складу са међународним уговорима између држава. Тако *норвешки* Законик о кривичном поступку[619] не предвиђа могућност приступа рачунарском систему који се налази на територоји друге државе преко рачунара на домаћој територији, него се полази од тога да мера експедитивног чувања података (из члана 29. и 30. Конвенције) има за циљ обезбеђење електронских доказа до упућивања молбе за помоћ надлежним органима друге државе. Слично решење садржи и *холандски* Закон о кривичном поступку[620] предвиђајући да постоји могућност проширења претреса на други рачунар уколико се њему може приступити преко рачунара који је предмет претреса и уколико се налази унутар граница државе, док приступ рачунарима ван територије Холандије није дозвољен у смислу ових одредаба Законика о кривичном поступку, него само применом правила међународног јавног права,

[618] Pradillo, *op.cit*, 382-383.

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

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

односно коришћењем редовних механизама за узајамну правну помоћ (члан 552x). Ипак, у случају „*Bredolab*“ током 2010. године је створена мрежа ботнетова (употребом 143 сервера чији хост је био пружалац услуга електронских комуникација у Холандији али је напад иницран из иностранства) којим је било заражено преко 30 милиона рачунара из више држава, а холандска полиција је након преузимања ботнета и угасила сервере, те је послата аутоматска порука свим зараженим рачунарима. Слично томе, у случају *Descartes*, полиција је приступила серверима (*TOR: The Onion Router*) који се не налази у Холандији, а на ком су биле похрањени прикази дечје порнографије – ти подаци су копирани, а потом уклоњени са сервера[621]. Иако је суд о овим акцијама претходно био обавештен, такво поступање полиције би се могло сматрати недозвољеним приступом рачунару у смислу поменутих одредаба Закона.

Занимљиво решење садржано је у *португалском* Закону о компјутерском криминалу[622] који се односи на међународну сарадњу надлежнх органа у циљу истраживања кривичних дела повезаних за рачунарским системима и рачунарским подацима, као и у циљу прикупљања електронских доказа невезано за врсту кривичног дела. Изричито је предвиђено да се сви видови сарадње остварују уз поштовање Закона бр. 67/98 о трансферу податка о личности (члан 20). Поводом молбе надлежних органа друге државе да им се омогући приступ подацима похрањеним у рачунарским системима који се налазе на територије државе, предвиђено је да португалски надлежни органи предузимају претрес рачунара и одузимања података на молбу органа друге државе, и то само у ситуацијима у којима је то могуће извршити у складу са националним прописима, а уколико постоје околности које указују на то да би тражени подаци могли бити уништени или измењени, органи су дужни да поступају са нарочитом хитношћу. Ипак, члан 25. предвиђа да надлежни органи друге државе могу без претходног одобрења од стране португалских органа: 1. приступити подацима који су

[621] *The effectiveness of international cooperation against cybercrime: examples of good practice*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp;

[622] *Lei do Cibercrime*, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf;

похрањени у рачунарском систему који се налази у Португалији уколико су ти подаци јавно доступни, и 2. примити или приступити преко рачунарског система на њиховој територији податке који су похрањени у Португалији, под условом да постоји законит и доборовољан пристанак лица које је овлашћено у складу са законом да те податке учини доступним (члан 25). У погледу прекограничног приступа рачунарским подацима који су ускладиштени у рачунарском систему ван граница Португалије значајан је чланом 16. Закона, а који се односи на прекогранично одузимање рачунарских података којима се приступило у складу са чланом 15. Наиме, претрес рачунара се врши на основу наредбе суда ради проналаска одређених рачунарских података у одређеном систему, а уколико се током претреса утврди да се тражени података налази у другом рачунарском систему, па и ван територије државе, а ком се може на законит начин приступити преко претресаног рачунара, наредбом органа поступка се може проширити овлашћење надлежних органа и на тај други удаљени рачунарски систем. Ову процесну радњу наређује јавни тужилац, а овлашћење издато од стране истражног судије је потребно уколико се одузимају рачунарски подаци или датотеке чији садржај би могао да укаже на личне или интимне информације о лицима и тиме угрозе њихово право приватности. Одузимање података може бити у различитим облицима: физички (одузимањем физичког уређаја који је носилац података), копирањем података, очувањем интегритета (без копирања или уклањања), трајним бесповратним уклањањем података или блокирањем приступа подацима.

Након анализе законских текстова појединих држава, може се закључити да се директан прекогранични приступ практично остварује на неколико начина:

А. Приликом извршавања претреса просторија полиција наиђе на рачунар који је укључен и након што добије на законит начин од лица потребне лозинке, остварује приступ рачунарским подацима који су похрањени у удаљеном рачунарском систему. У погледу могућности претраживања удаљеног рачунарског система, разликују се две ситуације: у појединим државама полиција може остварити удаљени приступ чак и уколико је очигледно да је рачунар лоциран у јурисдикцији друге државе (нпр. у Финској, Литванији, Португалији, САД), док је у другим државама даља претрага дозвољена само уколико је обезбеђен пристанак лица у смислу члана 32 б Конвенције (нпр. Немачка,

Шведска, Холандија) при чему пристанак лица не може као услов законитости радње бити замењен чак ни разлозима изузетне хитности (тако прикупљени електронски докази не би се могли користити у кривичном поступку).

Б. Полиција је на законит начин прибавила лозинке потребне за приступ рачунарским подацима похрањеним у удаљеним рачунарским системима којима остварује приступ преко свог рачунарског система. Оваква могућност постоји у појединим националним законодавтсвима чак и у ситуацији да је очигледно да се удаљени рачунар налази ван територије државе и тако прикупљени електронски докази могу се користити на суду (нпр. Финска, Норвешка, Шведска, Португалија).

В. Прекогранични приступ удаљеном рачунару се остварује коришћењем посебног софтвера (*key loggers, sniffers*) или других техничких средстава уколико није очигледно у јурисдикцији које државе је рачунар лоциран. Уколико је, пак, недвосмислено утврђено да се рачунар у ком се тражени подаци налазе ван територије државе, оваква могућност није дозвољена (са изузетком Јапана).

Г. У току истраге полиција добије законит и добровољан пристанак лица на основу ког остварује приступ рачунарским подацима који могу представљати електронски доказ а који су похрањени у рачунарима у јурисдикцији друге државе. Полиција може у појединим државама приступити и обезбедити (преузети) потребне рачунарске податке, без обзира на то где се налази лице које даје пристанак - да ли на на територији државе са које се остварује прекогранична претрага или на територији на којој се удаљени рачунар налази (нпр. Финска, Португалија, Шведска). Да ли лице има законско овлашћење да омогући приступ подацима, међутим, процењује се на основу прописа државе на чијој територији су подаци похрањени (нпр. Финска, Португалија, САД).

Уколико државе дозвољавају прекогранични приступ подацима похрањеним на страној територији, добро решење би било да се предвиди обавеза надлежних органа да по сазнању да се ради о таквим подацима о томе обевесте другу државу и захтевају помоћ у смислу одредаба Конвенције (преко мреже 24/7), евентуално уз могућност да направе копију података. Интрузивне технике, попут хаковања налога или рачунарског система, инсталирање *key logger*-а за континуирани надзор активности корисника, уклањање података или онемогућавање приступа

систему у смислу једностраног предузимања не би требало ни у ком случају да буду дозвољене.

2.4.2. Прекогранични приступ посредством пружалаца услуга електронксим комуникација

Осим директног приступа јавно доступним рачунарским подацима похрањених у рачунарима ван граница територије или коришћењем средстава узајамне правне помоћи, надлежни државни органи подацима који су физички ускладиштени у иностранству могу приступити и преко пружалаца Интернет услуга и других ентитета приватног сектора који су пружаоци других услуга електронских комуникација (и то преко правних заступника тих ентитета у држави или непосредним обраћањем ентитету који се налази у иностранству). Поставља се питање, под којим условима и на који начин се овакав приступ може остварити? Наиме, надлежни органи могу у том погледу искористити могућност у смислу члана 32б Конвенције или захтевати предају потребних података на основу судског налога друге државе (а преко инструмената међународне сарадње).

Уколико, примера ради, осумњичени користити услуге *Google Docs*, потребни подаци би могли бити похрањени на серверу који се налази у САД (држава седишта *Google*-а) или у било којој другој држави у којој *Google* има представника. Да би остварила приступ потребним подацима, полиција најпре треба да утврди локацију на којој се налази сервер у ком су подаци похрањени, што је такође вид прекограничне претраге. Може се десити да полиција не утврди локацију на којој су подаци похрањени, о чему податке имају само пружаоци услуга, па се може обратити или надлежним органима САД који би обавезали пружаоце услуга електронских комуникација на предају тих података или директно *Google*-у. Уколико утврди локацију, полиција се за остваривање приступа подацима може обратити или надлежним органима државе на чијој територији се налазе подаци (преко механазама узајамне правне помоћи тражи се да надлежни судски органи те државе обавежу пружаоце услуга електронских комуникација на предају података) или директно *Google*-у. При томе, треба имати у виду Правила о приватности овог пружаоца услуга електронских комуникација

и могућност предавања података о кориснику услуга само уз његову сагласност[623].

Уколико се анализира члан 32б Конвенције који предвиђа „законит и добровољан пристанак“ као основ за предузимање прекограничног приступа подацима у иностранству, могли бисмо поћи од тога да не постоји сметња да пристанак на откривање података потиче и од правног лица који контролише податке, у овом случају пружаоца услуга[624]. Међутим, лице које даје пристанак треба да има законско овлашћење да те податке преда, а пружаоци услуга су дужни да чувају приватност својих корисника и да без њиховог пристанка не предају податке о њима никоме, па ни државним органима - могли би евентуално предати податке о саобраћају и о кориснику али не и садржај комуникације (за шта би била потребна одлука суда[625]). Из тог разлога, члан 32б не представља адекватан основ за прекограничну претрагу у смислу пристанка пружалаца услуга, мимо механизама узајамне правне помоћи. Од пружалаца услуга се може формално захтевати да поступају у складу са националним прописима који уређују претрес рачунара ради проналаска одређених рачунарских података и омогућавања приступа тим подацима, али ова ситуација не подразумева постојање добровољног пристанка у смислу члана 32.б Конвенције (ради се о имплементацији одредаба 18. и 19. Конвенције) него поступање по захтеву надлежних органа. У националним прописима поједине државе предвиђају под којим условима се од пружалаца *cloud* услуга који се налазе на њиховој територији може захтевати да омогуће приступ подацима који су похрањени на њиховим серверима у иностранству, Међутим, погрешно би било закључити да постоји могућност неограниченог приступа тим подацима, јер се прописују бројни услови које се морају испунити да би надлежни органи могли од пружалаца услуга захтевати приступ тим подацима (нпр. да је *IP* адреса повезана са територијом те државе или да се осумњичени налази на територији или да је

[623] *Google's Privacy Policy*, http://www.google.com/privacypolicy.html

[624] J. Schwerha, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers,* 2010, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf, 14.

[625] K. Kurek, "How to achieve balance between effective crime preventing and protecting privacy of citizens, Online search as a new challenge for e-justice", *Masaryk University Journal of Law and Technology* 3/2009, 384.

захтев предмет судске контроле и слично). Тако су у Француској надлежни органи овлашћени да захтевају од пружалаца услуга електронских комуникација да омогуће приступ подацима који су похрањени на серверима и у земљи и у иностранству. У Немачкој оваква могућност не постоји у погледу података који су чувају на рачунарима ван територије државе, док је у Данској полиција овлашћена да таквим подацима приступи уколико постоји налог за претрес просторија пружалаца услуга и да се из тих просторија може приступити серверима у иностранству (у супротном, неопходно је упућивање молбе за узајамну правну помоћ надлежним органима државе на чијој територији се сервери налазе). У случају да надлежни органи у Великој Британији имају налог за прикупљање електронких доказа, овлашћени су да захтевају претрагу било које информације која је садржана у рачунару или јој се може приступити из просторије која се претреса, што значи да полиција може од пружалаца услуга захтевати предају података који су похрањени на серверима у иностранству уколико се серверу може приступити из просторија које се претреса ма где се сервер налазио. У САД је прихваћено становиште да се коришћењем законских механизама може од пружаоца *cloud* услуга захтевати да преда податке без обзира на то где се налази сервер на ком су похрањени, уколико је пружалац услуге под јурисдикцијом државе, што је случај када је привредни субјект основан и има седиште, следбеника или огранак или континуирано и систематско послује на територији САД. Слично томе, и пружаоци услуга електронских комуникација који су под јурисдикцијом Канаде дужни су да доставе све релевантне податке над којима имају контролу, у смислу да могу приступити тим подацима директно или посредством огранка компаније. У Аустралији се захтеви за приступ подацима који се налазе у серверима у иностранству може остварити упућивањем захтева пружаоцима *cloud* услуга само уколико је радња кривичног дела које се истражује извршена на територији државе или се односи на лица који су њени држављани[626].

У научној литератури је пресуда белгијског Касационог суда у *Yahoo!* предмету препозната као случај од велике важности у погледу прикупљања доказа од

[626] Више о томе, W. Maxwell, C.Wolf, *Lovells White Paper: A Global Reality: Governmental Access to Data in the Cloud*, 2012, http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf

пружалаца електронских услуга са седиштем у иностранству[627]. Наиме, белгијски прописи обавезују све пружаоце улуга електронских комуникација, без обзира на седиште, да предају на захтев надлежних органа потребне податке. Током 2007. године покренут кривични поступак за дело комппјутерске преваре употребом електронске поште преко *Yahoo* налога, па је јавни тужилац на основу члана 46. Законика о кривичном поступку упутио захтев овом пружаоцу услуга електронских комуникација да достави податке о кориснику (укључујући *IP* адресу која је коришћена приликом регистрације, датуме и време регистрације), адресе електронске поште повезане за налогом корисника и друге податке који би могли да послуже за идентификацију корисника. Захтев је прослеђен преко адресе електронске пошту, коју је *Yahoo!* отворио за белгијску територију, али је у одговору јавни тужилац упућен да се обрати седишту пружаоца услуга електронских комуникација у САД, што је тужилац и учинио почетком 2008. године. Међутим, *Yahoo!* је одговорио да се на њега не односи белгијски прописи, па је потребно упутити захтев за добијање података на основу америчког Закона о електронским комуникацијама, а посредством америчког Министарства правде. Званичан допис је упућен јула 2008. године у ком се захтева поступање по белгијском пропису, на шта *Yahoo!* није одговорио. Због тога се тужилац обратио првостепеном кривичном суду, који је марта 2009. године новчано казнио *Yahoo!* казном од 55.000 еура и одредио да ће се за сваки следећи дан одбијања по захтеву тужиоца одредити казна од 10.000 еура. *Yahoo!* се жалио апелационом суду марта 2010. године, јер је суд закључио да је, с обзиром на виртуелну присутност овог пружаоца услуга електронских комуникација на територији Белгије, установљена територијална надлежност белгијских органа и отуда *Yahoo!* има обавезу да поступа у складу са захтевима органа за издавање тражених података, тим пре, што се исти односе само на податке о саобраћају, а да се осим тога, амерички прописи не могу примењивати на услуге које пружалац услуга електронских комуникација пружа држављанима Белгије. Одбијање поступања по захтеву белгијског суда заступник компаније је заснивао на неколико тврдњи: да

[627] P. Berman, „The globalization of jurisdiction“, *University of Pennsylvania Law Review* 12/2002, 502. О покушају државе да обавеже својим прописима пружаоца услуга ван њених територија занимљива је одлука Врховног суда Велике Британије у случају *Football Dataco Limited and others v. Sportradar GmbH and Sportradar AG* (C. O'Reilly, "Finding jurisdiction to regulate Google and the Internet", *European Journal of Law and Technology* 1/2011, 9)

кривично дело није учињено на територији Белгије, да јавни тужилац није поступао у складу са механизмима за пружања узајамне правне помоћи у кривичним стварима јер нема никакву (ни материјалну ни процесну) надлежност у односу на *Yahoo!,* да та фирма не може предати податке јер би то било у супротности са прописима о приватности који важе у САД где се налази седиште фирме. Поводом жалбе заступника, Апелациони суд је заузео став да је *Yahoo!* америчка компанија која се с обзиром на то да предствља *web-mail* платформу, не може сматрати мрежним оператером нити пружаоцем услуга електронских комуникације у смислу белгијских прописа, па сходно томе захтев јавног тужиоца у смислу члана 46. Законика о кривичном поступку не обавезује ову фирму за сарадњу. Ипак, Касациони суд је у пресуди од 11. јануара 2011. године заузео став да је *Yahoo!* „комерцијално" пристутан на територији Белгије у смислу Закона о електронским комуникацијама, јер пружа услуге држављанима на територији Белгије посредством Интернета, и да се сходно томе и на њега примењује одредба члана 46. Законика која се односи на обавезу предавања података за све фирме које пружају услуге електронских комуникација на територији Белгије[628].

Из наведених разлога је постало јасно колико је сарадња са пружаоцима услуга од изузетног значаја. Поједини пружаоци услуга са седиштем у САД-у су преко својих огранака у појединим европским државама постигле споразум о сарадњи са органима гоњења (тзв. *criminal compliance programmes*) којима се регулише могућност предавања одређених података за потребе кривичног поступка, уместо слања захтева америчком Министарству правде у оквиру процедуре пружања међународне правне помоћи. Захтев пружаоцу услуге треба да буде упућен у складу са законом и од стране овлашћеног органа надлежног за истрагу кривичног дела, односно за прикупљање електронских доказа, из ког разлога је неопходно да постоје јасне законске процедуре, а од надлежних органа се очекује да поштују принципе заштите људских права а нарочито право приватности. Подаци који се траже би требало да су повезани са територијом државе чији надлежни органи упућују захтев (као што су *IP* адреса комуникације или домен налога за електронску пошту). Кривично дело поводом ког се подаци траже би требало да

[628] За детаљнији приказ случаја, P. De Hert, M. Kopcheva, „International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! Case", *Computer Law and security Review* 27/11, 291.

буде инкриминисано и у законодавству САД (а да се не ради о политичком делу нити о истраживању случајева који су у вези са слободом говора)[629]. Пружаоци су спремни да предају податке који су у њиховом поседу и под њиховом контролом, као што су подаци о саобраћају или о кориснику услуга, док за добијање приступа садржају које креирају корисници (а тиме и садржају остварене комуникације) није довољна одлука домаћег суда, него је неопходно упућивање захтева у оквиру међународне правне помоћи[630].

Мишљења смо да би став Касационог суда, теоретски посматрано, могао да послужи као инспирација за заснивање надлежности сваке државе са чије територије се може приступити пружаоцима *cloud* услуга и сличним платформама, без обзира што се ради о страним компанијама и што се подаци похрањују на серверима у иностранству, а што је од изузетне важности за прикупљање електронских доказа за дела високотехнолошког криминала.

[629]Kaspersen, *op.cit*, 44.

[630] S.Brenner, „Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model", *Journal of International Commercial Law and* Technology 2/2007, 63. Више о томе, *Guidelines for the coopeation between law enforcement and Internet servise providers against cybercrime*, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

Седми део
ДИГИТАЛНА ФОРЕНЗИКА

Од појаве рачунара у 1940-им годинама прошлог века јављају се и први случајеви њихове злоупотребе, а како од 1970-их година персонални рачунари постају све доступнији ширем кругу лица, повећава се и број злоупотреба у криминалне сврхе, чега и надлежни државни органи постају свесни. Током 1970-их рачунари су били у употеби у великим организацијама и предузећима, као што су банке и осигуравајућа друштва, па су се први забележени случајеви злоупотреба рачунара углавном односили на финансијске преваре[631] и повреду права интелектуалне својине[632], а ретки су случајеви у којима су рачунари били објект напада. Као последица потребе да се прикупе докази за гоњење и суђење у случајевима злоупотребе информационих технологија настала је дигитална форензика. Наиме, током 1980-их група привредника указује на потребу обуке полиције у циљу препознавања и реаговања на проблеме (не)безбедности информационих технологија, а су развијени и први софтверски алати у форензичке сврхе[633]. У САД се федерални агенти обучавају за обављање задатака који спадају у рачунарску форензику - у оквиру *FBI*-а је 1984. године започет Програм за магнетне уређаје (*FBI Magnetic Media Program*) који је 1992. прерастао у Тим за рачунарску анализу и реаговање (*Computer Analysis and Response Team*: *CART*[634]). Такође, основано је Удружење јавних тужилаштава за

[631] Један од првих забележених напада на рачунарске системе током овог периода заснивао се на «заокруживању камата» (*interest rounding*). J. Kizza , *Guide to Computer Network Security*, Springer Science & Business Media, Berlin 2013, 299.

[632] Први случај гоњења у кривичном поступку забележен је 1966. у Тексасу. Ради се о случају *Hancock v. Texas, 402 S.W. 2d 906 (Tex. Crim. 1966)*, у ком је лице осуђено за крађу компјутерског програма. M. Rasch, „Criminal Law and The Internet“ , Ruh, J (ур) *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, Computer Law Association, Stanford 1996, 23.

[633] Као што су *X-Tree Gold* и *Norton Disk Editor* помоћу којих су истражитељи могли да препознавају типове датотека и да екстрахују податке из оперативног система. Kizza, *op.cit*, 299.

[634] Од доношења Закона о рачунарским преварама и злоупотребама 1986. године у САД све више захтева је упућивано канцеларији *FBI* -а ради прикупљања доказа за потребе вођења кривичног поступка за кривична дела предвиђена овим законом. Током 1989. године *FBI* је заједно са Агенцијом за заштиту животне средине у САД истраживао случајеве корупције у фабрици за нуклеарно оружје у Денверу, САД. Резултати претреса просторија у фабрици показали су да се кључни докази налазе похрањени у рачунарском систему због чега је оформљен *ad hoc* тим састављен од стручњака за рачунарске претраге и анализе. Током 1991. радни тим, који је разматрао проблеме у вези са истрагом кривичних дела почињених злоупотребом рачунара, усвојио је препоруку за стварање сталне јединице која би била састављена од стручњака за

технолошку крађу[635] које је 1986. прерасло у Удружење за истрагу високотехнолошког криминала (*High Technology Crime Investigation Association: HTCIA*)[636]. Ово удржење је данас водеће међународно асоцијацијама стручњака са циљем обуке и размене знања и искустава у области спречавања и истраживања дела високотехнолошког криминала, заједно са Међународним удружењем стручњака за рачунарску истрагу (*Association of Computer Investigative Specialists: IACIS*)[637] основаним 1989. године, а које издаје најпризнатије сертификате за стручњаке дигиталне форензике. У оквиру лабораторије Службе за преглед поштанских пошиљки (*Postal Inspection Service*) формирана је 1997. Јединица за рачунарску форензику (*Computer Forensic Unit*). На састанку са представницима *FBI* -а током 1998. је од групе стручњака који су се неформално окупљали с циљем проналажења најбоље праксе поступања са електронским доказима (*Technical Working Groups: TWG*), створена је Научна радна група за дигиталне доказе (*Scientific Working Group on Digital Evidence: SWGDE*)[638] са задатком да се у оквиру ње креирају стандарди поступања са доказима похрањеним у рачунарима[639].

Током 1990-их одржано је неколико значајних међународних конференција посвећених рачунарским доказима у организацији *FBI* -а[640] на којој су запослени у полицији и тужилаштву у државама представницама указали на потребу стварања стандарда рачунарске форензике. Ти напори су резултирали стварањем Међународне организације за рачунарске доказе (*International Organization on Computer Evidence: IOCE*)[641] којој су 1998. године државе из Групе 8 поверile задатак да изради међународне принципе и водиче за поступање са дигиталним

релевантне области и 1992. је званично формиран Тим за рачунарску анализу и реаговање. http://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence.

[635] *District Attorney's Technology Theft Association: DATTA.*

[636] http://www.htcia.org/history/.

[637] http://www.iacis.com/.

[638] https://www.swgde.org/.

[639] Са развојем ових стандарда, уочава се потреба и за стварањем програма за обуку форензичара. SWGDE је 2002. објавила смернице за обуку службених лица у надлежним органима, а Америчко друштво управника криминалистичких лабораторија (*American Society of Crime Laboratory Directors*) је предложило смернице за поступање форензичара који обрађују дигиталне доказе. Наведено према: C.M. Whitcomb, „An Historical Perspective of Digital Evidence", I*nternational Journal of Digital Evidence* 1/2002, 2.

[640] 1993. године у Калифорнији, а потом потом 1995. у САД, 1996. у Аустралији и 1997. у Холандији.

[641] http://www.ioce.org/.

доказима[642]. У овом периоду се побољшавају софтверски алати[643] који су омогућавали форензичарима да прикупљају податке у систему без измене битних детаља тих података (у почетку су форензичари просто копирали појединачне датотеке са диска, што је резултирало неприхватљивошћу таквих доказа на суду услед непоштовања принципа аутентичности и интегритета доказа), а временом се јављају и напреднији алати који су додатно олакшали задатак истражитеља[644] јер су садржали функцију аутоматизоване претраге[645].

Период од 1999. до 2007. сматра се „златним добом дигиталне форензике“[646] у ком се ова дисциплина посматрала као свемогућа за опоравак података и реконструкцију догађаја из прошлости у дигиталном окружењу и поклањало јој се толико поверења у стручној и општој јавност, да је створен тзв. “*CSI Effect*”[647], па су налази и искази стручњака рачунарске форензике готово у већини случајева прихватани без оспоравања и било какве задршке у поступцима пред судовима[648]. Међутим, много тога се променило од тада и пред дигиталном форензиком су бројни изазови условљени рапидним технолошким развојем, па је оправдано и потребно преиспитати да ли дигитална форензика данас задовољава одређене критеријуме да би се сматрала научном дисциплином и да би резултати њене примене имали снагу научног доказа.

---

[642] О томе више, M. Politt, “The very brief history of digital evidence standards”, M. Gertz, Integrity and internal control in information systems V, Springer, Bonn, 2003, 137-142.
[643] Као што су *SafeBack* и *DIBS*. P. Stephenson, *Investigating computer-related crime*, CRC Press, Boca Raton 2000. 254.
[644] Као што су *Encase* и *FTK*.
[645] Casey, *op.cit*, 483.
[646] Овај период карактерише: широка употреба *Microsoft Windows* оперативног система, релативно мали број формата које је обрађивала дигитална форензика (документи *Microsoft Office-a,* .jpeg за дигиталне фотографије, *.avi* и *.wmv* за видео записе); дигитална истрага се врши на једном изолованом рачунару који је у власништву одређеног лица; уређаји за складиштење података су у стандардном облику спојени са рачунаром преко покретним каблова и конекотора, у употреби су прилично добри алати за опоравак избрисаних података; није била раширена примена технологије енкрипције; истраживања у области дигиталне форензике су била у повоју и јављају се први акредитовани програми за обуку дигиталних форензичара. S. Garfinkel, “Digital forensics research: The next 10 years”, *Digital Investigation* 7/2010, 66.
[647] S. Donald E, The ‘CSI Effect’: does it really exist? NIJ J March 2008; 259, http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm
[648] T. Talleur, „Digital evidence: moral challenge“, *International Journal of Digital Evidence* 1/2002,2.

1. ПОЈАМ ДИГИТАЛНЕ ФОРЕНЗИКЕ

Постоји више дефиниција дигиталне форензике, а у литератури је најчешће цитирана (уз незнатне модификације) дефиниција коју је 2001. године створила Радна група за истраживање дигиталне форензике[649], по којој „*дигитална форензика"* подразумева „употребу научноизведених и потврђених метода ради очувања, прикупљања, валидације, идентификовања, анализе, тумачења, документовања и представљања дигиталних доказа изведених из дигиталних извора за потребе омогућавања или побољшања реконструкције кривичног догађаја"[650]. Осим термина дигитална форензика, поједини аутори користе термин *„форензичко рачунарство",* којим означавају исте оне активности које су обухваћене претходно поменутом дефиницијом дигиталне форензике[651] (али са додатном функцијом анализе безбедносних напада на информационе системе[652]).

Дигитална форензика се се може поделити на рачунарску форензику (*Computer Forensics*)[653], форензику аудио-записа (*Forensic Audio Analysis),* форензику

---

[649] *The Digital Forensics Research Workshop*: *DFRWS* , http://www.dfrws.org/.

[650] DFRWS technical report: *A Road Map for Digital Forensic Research*, New York 2001, http://www.dfrws.org/2001/dfrws-rm-final.pdf, 15. Дигиталну форензику дефинишу и следећи аутори: C. Garrison, T. Lillard, C. Schiller, J. Steele, *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*, Elsevier Science & Technology, Boston 2010, 279; A. Marshall, *Digital Forensic*, Wiley, Chichester 2008, 10.

[651] „Форензичко рачунарство" (*Forensic computing*) означава „употребу научно изведених и доказаних метода са циљем очувања, прикупљања, валидације, уочавања, анализе, тумачења, документовања и представљања дигиталних доказа изведених из дигиталних извора у сврху омогућавања или олакшавања реконструкције догађаја који представљају радњу кривичног дела, као и у сврху предвиђања неовлашћених активности које би могле бити сметња за планиране операције у информационом систему", (B.Carrier, „Defining digital forensic examination and analysis tools using abstraction layers", *International Journal of Digital Evidence* 1/2003, 2). Аутори *McCombie* и *Warren* указују на фундаменталне карактеристике форензичког рачунарства у односу на остале форензичке дисциплине и отуда на потребу укључивања тих карактеристика у дефиницију овог појма (S. McCombie, M. Warren, „Computer forensic: An issue of definition", *Proceedings of the First Australian Computer, Network and Information Forensics Conference*, 2003, http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2003/forensics/.) На основу анализе постојећих дефиниција, *Hannan* закључује да „ниједна дефиниција није адекватна у смислу да обухвати значај форензичког рачунарства" (M. Hannan, „To revisit: What is forensic computing?", P*roceedings of the Second Australian Computer, Network and Information Forensics Conference*, 2004, 108).

[652] Слично томе, D. Barrett, G. Kipper, *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments*, Elsevier Science & Technology, Heidelberg 2010, 22.

[653] Иако је данас рачунарска форензика само део дигиталне форензике, термин је историјски означавао оквире садашње дигиталне форензику у периоду када су предмет форензичке обраде били само рачунари, а не и други дигитални уређаји. Упор. W. Kruse, Heiser, *Computer Forensics: Incident Response Essentials*, Addison Wesley, London 2001, 4; W. Harrison et al, "A Lessons Learned Repository for Computer Forensics", *International Journal of Digital Evidence* 3/2002, 8; Meyers,

сликовних записа (*Forensic Image Analysis*) и форензику видео-записа (*Forensic Video Analysis*)[654], као уже област у оквиру дигиталне форензике које се баве форензичком обрадом појединих врста дигиталних уређаја. Поједини аутори употребљавају и термин кибер форензика (*Cyber Forensics*) који, поред поменутог, обухвата и форензику рачунарских мрежа (*Network Forensics*) и Интернет форензику (*Internet Forensics*), као још ужу област у односу на форензику рачунарских мрежа, па тиме представља генусни појам за наведене области истраживања дигиталних уређаја и кибер простора уопште, ради проналажења релевантних дигиталних доказа[655]. Такође, постоји мишљење да су форензичко рачунарство, рачунарска форензика и дигитална форензика синоними, јер сви термини означавају методолошки, научно-заснован и правом ограничен процес обраде рачунарских система и мрежа ради проналажења доказа који се могу користити пред судом[656].

Упркос минорним разликама у постојећим дефиницијама, за све њих се као заједнички именитељ може уочити циљ, а који се огледа у потреби да се обезбеди доказана снага резултата дигиталне форензике. Тај елемент се означава као: „правна прихватљивост“[657], „усклађеност са правилима о доказивању“[658] и „квалитет научног доказа“ [659].

Из овога се може извести закључак да је ***смисао дигиталне форензике изналажење процедура, метода и техника које резултирају дигиталним доказом*** који треба да има снагу научног доказа. Према томе, циљ ове форензичке дисциплине је ***изналажење научно изведених и потврђених метода идентификовања, очувања, прикупљања и анализе рачунарских података и представљања резултата те анализе за потребе кривичног поступка***. Процес

Rogers, *op.cit*, 8; Vacca, *Computer forensics: Computer Crime Scene Investigation*, Charles River Media, Boston 2005, 17.

[654] Barbara, *op.cit*, 8.

[655] A. Brinson et al., „A cyber forensics ontology: Creating a new approach to studying cyber forensics“, *Digital Investigation* 3/2006, 39. Упор. A. Marcella, D. Menendez, *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Second edition, Auerbach Publications, New York 2008, 15; J. Bayuk, *Cyber Forensics: Understanding Information Security Investigations*, Springer, New York-Dordrecht 2010, 3.

[656] Britz, *op.cit*, 6.

[657] R. McKemmish, „What is forensic computing?“, *Trends and Issues in Crime and Criminal Justice* 118/2002, www.aic.gov.au/publications/tandi/ti118.pdf.

[658] D. Bem et al, „Computer Forensics: Past, Present and Future“, Journal of information science and Technology 3/2008, 46.

[659] Casey, *op.cit*, 60 и Carrier, *op.cit*, 17.

у ком се од „сирових“ рачунарских података, као дигиталних трагова, применом метода и техника дигиталне форензике добијају електронски докази означићемо ***дигиталном истрагом***.

1.1. Дигитална форензика као научна дисциплина

Циљ и сврха форензичких дисциплина је да се кроз примену *научно проверених и објашњених метода* природних и техничких наука *обезбеди разумевање чињеница* које су *предмет доказивања у кривичном поступку*. Данас се докази који настају као резултат ДНК анализе узимају као неспорни и непобитни у кривичном поступку. Ипак, тако није било на самом почетку. Први пут се овај доказ појавио у кривичном поступку у САД свега два године након што је 1987. Џефрис открио да се помоћу ДНК изузетног из крви може извршити неспорна идентификација лица[660], а што је уследило 32 године након што су Вотсон и Крик указали на постојање ове супстанце[661]. Као што се може уочити из овог података, процес од фактичког открића метода до употребе у доказне сврхе у кривичном поступку је временски дуго трајао. Наиме, након открића је било је потребно да се провери валидност употребљеног метода од стране других научника, односно да применом исте методологије дође до истих резултата и тиме докаже тачност научног открића. Без тог процеса, суд није био спреман да се ослони и поклони веру одређеном научном резултату и употреби га као доказ у поступку. Посматрајући развој форензичких наука које су данас прихваћене као посебне научне дисциплине, недвосмислено се долази до закључка да *за успостављање и валидацију једног научног метода потребно време,* а да би резултат примене тог метода био *прихваћен као доказ* у кривичном поступку, исти треба да се *заснива на провереним научним сазнањима,* а *сви алати и процедуре* који су коришћени да би се до доказа дошло, требало би да буду *предмет независног тестирања*. Међутим, шта се дешава у ситуацији када се материјал на ком се одређени метод примењивао мења током одређеног времена потребног за валидацију тог метода? Од када су утврђени јединствени маркери у ДНК, методи за анализу ДНК су се мењали: развијали су се а поједини су били одбацивани као

[660] Фејеш, *op.cit*, 121.
[661] K. Ramsland,*The DNA Revolution*, http://www.crimelibrary.com/forensics/dna/6.htm.

недовољно прецизни, али је ДНК као материјал остао исти. Исто тако, методи за анализу боје су се током година мењали, али су ретке нове технологије за израду боје које се не могу анализирати неком од постојећих и прихваћених метода за анализу, што никако није случај са информационим технологијама[662].

Да би се дигитална форензика могла сматрати научном дисциплином, потребно је да задовољава неколико *критеријума*: да постоји развијена теорија (систем изјава и принципа којима се настоје објаснити како ствари функционишу) и у оквиру теорије одређене апстракције и модели (разматрања поврх очигледног, фактичког и уоченог); да теорије полази од одређених практичних елемената (повезане технологије, алати и методи); да постоји корпус литературе и професионалне праксе као и поверење у теоријом потврђене резултате у пракси (корисност и сврсисходност) [663]. У вези са наведеним, може се поставити питање, да ли је дигитална форензика научна дисциплина? Тренутно би се могло рећи да дигитална форензика задовољава само неке од ових критеријума, да је још у повоју и да постоји потреба за даљим усмеравањем њеног развоја. Наиме, не постоји сагласност у погледу садржаја и значења појединих појмова - поједине дефиниције су неадекватне а бројни појмови нису ни дефинисани. Практични елементи се огледају у уобичајеној употреби одређеног броја алата и техника којима се указује одређен степен поверења, иако нису развијени у складу са специфичним научним стандардима нити су тестирани у довољној мери. Такође, не постоје стандардна правила која би омогућила једнообразно поступање, нити су одређене специфичне области знања и вештина у правцу којих је потребно обучити лице да би се оно могло сматрати стручњаком за дигиталну форензику.

Дигитална форензика је изворно настала како би се применом одређених техника и метода прикупили рачунарски подаци који се могу употребити докази потребни у кривичном поступку против учинилаца кривичних дела код којих је рачунар био средство извршења или објект напада. Надлежни органи поступка већ неколико десетина година одузимају рачунаре и са њима повезане уређаје првенствено због тога што могу да послуже као извор доказа у кривичном поступку, а већи део истраживања у оквиру дигиталне форензике је био

[662] P. Sommer, „Forensic science standards in fast-changing environments“, *Science and Justice* 1/2010, 12.
[663] Brinson, *op.cit*, 38.

фокусиран на екстракцију рачунарских података ради презентовања пред судовима. Иако се до скоро област дигиталне форензике стихијски развијала[664], уложени су велики напори у правцу формализације поступања са електронским доказима кроз издавање одређених водича[665], а дигитална форензика постала је призната академска дисциплина која се изучава на високошколским установама[666]. Међутим, *данас се дигитална форензика суочава са бројним изазовима*.

Један од највећих изазова јесте *комплексност проблема прикупљања и анализе података* услед све веће *разноликости дигиталних уређаја* који су извори електронских доказа и *обима материјала* (рачунарских података/дигиталних доказа)[667]. Сваки нови хардвер и софтвер намеће разне изазове стручњацима који настоје да екстрахују доказе: непознате апликације, нови формати датотека, карактеристике оперативног система, до тада непознате проблеме у функционисању хардвера и слично[668]. Осим тога, поједине конфигурације или уређаји са собом носе неке неспецифичне проблеме, па раније утврђено решење за сличан проблем, а које је у претходним случајевима било ефикасно, у конкретној ситуацији не функционише и потребно је пронаћи ново решење, за шта је потребно време (некада дани и недеље[669]).

Како се разноврсност предмета форензичке истраге повећава, форензичким стручњацима су потребни *алати* који врше *више функција* од просте претраге и презентовања датотека, примера ради функције реконструкције, анализе, екстраховања и груписања података, те аутономног доношења одлука о даљим

---

[664] B. Lathoud, "Formalization of the Processing of Electronic traces*", International journal of Law, Computers and Technology* 2/2004,188.

[665] *Association of Chief Police Officers: Good Practice Guide for Computer-Based electronic Evidence*, 2012, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf (у даљем тексту: *ACPO*).

[666] Тако нпр. *University of Glamorgan* има акредитоване студијске програме свих нивоа за форензичаре рачунарске форензике, http://courses.southwales.ac.uk/courses.

[667] На следећем примеру можемо приказати како се једном утврђена правила поступања мењају услед технолошког развоја. Један од првобитних правила прикупљања електронског доказа јесте да се помоћу одговарајућег хардверског или софтверског алата креира физичка копија рачунарске меморије (*disk-to-disk copy*). Међутим, овакав приступ постаје практично све теже примењив, улед повећања величине хард диска - уобичајена величина до скоро је износила до 2 *TB* (*terabyte*) у стандардом персоналном рачунару, а током 2014. на тржишту се појавио хард диск меморијског капацитета од 8 *TB.* http://9to5mac.com/2014/08/26/seagate-announces-massive-8tb-hard-drive-for-bulk-data-storage/.

[668] A. Geschonneck, *Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklaren*, Springer, Heidelberg 2012, 53.

[669] Harrison, *op.cit,* 1.

корацима. Проблем представља и то што се *олако прихватају као валидни резултати анализе до којих се дошло применом комерцијалних алата* за дигиталну истрагу, а ти алати нису проверени у складу са захтевима који су постављени пред методима и техникама једне научне дисциплине. Да би се обезбедила поновљивост и проверљивост резултата, а тиме и валидност одређеног алата, потребно је да буде прихваћен од стране шире научне заједнице, али то није могуће пошто произвођачи комерцијалних алата не чине изворни код доступан јавности[670]. Обезбедити поновљивост резултата једног метода је много компликованије него омогућити проверљивост резултата дигиталне истраге у конкретном случају у кривичном поступку. Осим тога, с обзиром на рапидан темпо развоја информационих технологија, *веома је тешко верификовати методе* који се користе у обради рачунарских података за потребе кривичног поступка. Може се поставити питање: *да ли је отуда оправдано поклонити веру дигиталном доказу који је настао као резултат примене неприхваћеног метода и непроверених техника*?

Како би се потврдила „научност“ дигиталне форензике, која црпи инструментаријум из практичних дисциплина, и испратиле поменуте тенденције, потребно је прилагођавање постојећих оквира за поступање форензичара, али и стварање нових метода и техника, нарочито из разлога: а) не постоје стандардизоване процедуре и протоколе поступања, нити је терминологија стандардизована; б) употребљавају се аналитички алати који нису у довољној мери испитани од стране лица у погледу којих постоји недостатак искуства и обуке; в) прикупљање и анализа рачунарских података за потребе кривичног поступка може бити у сукобу са приватношћу појединца услед несигурности у погледу тачности и ефикасности техника, дужине чувања података итд, па најнапреднија рачунарска технологија за потребе дигиталне форензике може бити бескорисна ако није употребљена у складу са захтевима правног система[671]. У вези са поменутим изазовима, потребно је дати одговор на неколико битних питања:

[670] S. Garfinkel et al., „Bringing science to digital forensics with standardized forensic corpora“, *Digital Investigation* 6/2009, 4.
[671] Geschonneck, *op.cit*, 13-15.

- Нису сви рачунарски подаци трагови, а још мање су дигитални докази[672], па се поставља питање за чим форензичар трага?
- Полазећи од карактеристика рачунарских података, како се обезбеђује интегритет електронских доказа?
- Ако се интегритет доказа обезбеђује стандардизованим поступањем, у складу са правилима, ко утврђује, на који начин и у ком облику те стандарде и правила поступања?
- Ко утврђује стандарде квалитета (поузданост, прецизност, тачност, безбедност, флексибилност, економичност) за технике и алате који се користе у форензичкој обради?
- Која знања и вештине треба да поседују лица која користе технике и методе, да ли их је потребно сертификовати и ко доноси одлуку о томе?

Иако на први поглед може изгледати да су ова питања само од практичног значаја, одговор на њих захтева научно истраживање и пврду. У томе треба да се огледа смисао дигиталне форензике као научне дисциплине јер је њен циљ превазилажење *апстрактне и лако измењиве природе рачунарских података ради обезбеђења интегритета и поузданости електронских доказа на начин да се обезбеди квалитет научног доказа* (*форензички исправног доказа*[673]), односно другим речима, *изналажење метода и техника чијом применом се може обезбедити да структура рачунарског податка остане неизмењена од тренутка када је исти уочен и прикупљен до представљања на суду*.

Интегритет електронског доказа се може *довести у питање из више разлога:* а) податке у дигиталном облику је једноставније изменити и фалсификовати неко податке у физичком облику; б) током анализе се на одређени начин мења облик дигиталног податка, (оно што се презентује као електронски доказ било у електронском било у физичком (*hardcopy*) облику пролази кроз неколико слојева трансформације и пребацивања из једног облика у други) при чему не постоје коректни механизми трансформације и превођења из једног облика (који се обрађује) у други (који се презентује); в) већина анализа се обавља на дигиталној

[672] J.M. Dinant, „The Long Way from Electronic Traces to Electronic Evidence“, *International Review of Law Computers & Technology* 2/2004, 174.
[673] Користи се и термин: “*forensically sound*” . R. McKemmish, „When is Digital Evidence Forensically Sound?“, у: Ray I, Shenoi S., *Advances in Digital Forensics IV*, Springer, New York 2008, 6; Casey, *op.cit*, 3.

копији или клону уређаја; г) објашњења аналитичких метода могу бити конфузна и погрешно се разумети; д) недостају стандарди поступања са дигиталним подацима, па стога постоји проблем аналитичке субјективности; ђ) при томе постоји велики број алата и метода помоћу којих било ко без превише знања и вештина може изменити скоро све атрибуте додељење податку у дигиталном облику. И поред поменутих тешкоћа, интегритет је потребно обезбедити и очувати, како се не би оставило простора за сумњу у поузданост и поверење у доказ који је настао као резултат анализе применом одређених метода и техника, јер ако је очуван интегритет а тиме и поузданост доказа, обезбеђена је и доказна вредност.

Да би се обезбедио интегритет и поузданост дигиталног доказа, процедура обраде доказе мора да задовољи два основа циља: 1. Прикупљање и анализа електронских записа се врши тако што се претходно предузму сви кораци како би се обезбедило да подаци остану у стању у ком су откривени, и 2. Форензички процес не сме ни на који начин да умањи доказну вредност електронских записа кроз техничке, процедуралне или интерпретативне грешке. Да би дигитални доказ био „форензички исправан“, односно имао карактер „научног“ доказа, потребно је предвидети и пратити кораке у поступању од открића електронских записа (дигиталних трагова) до њихове интерпретације као дигиталних доказа на суду. Свакако да је овај концепт логичан и сврсисходан, али да би остварио пуну вредност, потребно је *постићи униформност у поступању са електронским записима*. Међутим, мишљења које кораке треба предузети на путу од електронских записа до дигиталних доказа, односно шта чини процес дигиталне истраге разликује се од аутора до аутора. Стога сматрамо да није довољно само разматрати техничке методе и алате које је најбоље користити, него је, како би се гарантовао интегритет и поузданост електронских доказа и умањила аналитичка субјективност у дигиталној форензици, од кључног значаја пажњу посветити стандардизацији.

Суд јесте тај који оцењује доказе, али суд у оцени дигиталног доказа оправдано очекује *помоћ лица које поседује стручна знања потребна за утврђивање чињеница и које примењује проверене технике у оквиру стандардизованих правила*

поступања заснованих на научном методу, и тиме пружа гаранцију да су резултати његовог рада поуздани.

2. СТАНДАРДИЗАЦИЈА ДИГИТАЛНЕ ФОРЕНЗИКЕ

У области форензичких наука актуелна је расправа о коришћењу стандарда квалитета као средства за демонстрацију подобности научних метода чијом применом се долази до материјала који се може користити као доказ у оквиру система кривичног правосуђа[674], јер је „успостављање валидности нових научних техника или теорија и основа за њихово тумачење неопходно, пре него што се докази до који се дође њиховом применом могу користи на суду", а „...одсуство договореног протокола за валидацију научних техника да пре њиховог коришћења на суду је потпуно неприхватљиво"[675].

Дигитална форензика је толико широка област да је могуће говорити о специјализацијама дигиталних форензичара. Иако су утврђене дефиниције одређених појмова, принципи и стандарди, исте је потребно прилагодити постојећем стању технолошког окружења. Међутим, и поред тога, као највећи изазови који стоје форензичким наукама, истиче се да постоје случајеви у којима је доказ до кога се дошло непровереном форензичком анализом довео до погрешних осуђујућих пресуда[676]; „да не постоји униформност у издавању сертификата форензичарима као ни у акредитацији форензичких лабораторија[677]";

[674] У више радова се указује на потребу стварања одређених стандарда у циљу валидације дигиталне форензике као научне дисципине. О томе, примера ради, види M. Meyers, M. Rogers, "Computer Forensics: The Need for Standardization and Certification", *International Journal of Digital Evidence* 2/2004, 7; J. Schwerha, „Cybercrime: Legal Standards Governing the Collection of Digital Evidence", *Information Systems Frontiers* 2/2004, 133; G. Hall, „Toward Defining the Intersection of Forensics and Information Technology", *International Journal of Digital Evidence* l/2005, 13; S. Garfinkel et al., *op.cit*, 7; A. Marshal, "Standards, regulation & quality in digital investigations: The state we are in", *Digital Investigation* 8/2011, 142; P. Sommer, „Certification, registration and assessment of digital forensic experts: The UK experience", *Digital Investigation* 8/2011, 99; S. Ballou.„Emerging paper standards in computer forensics", *Digital Investigation* 8/2012, 96.

[675] *Forensic Science on Trial*, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf, 75.

[676] *Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, „Strengthening Forensic Science in the United States: A Path Forward*", 2009, http://www.nap.edu/catalog/12589.html, 4.

[677] *„Strengthening Forensic Science in the United States: A Path Forward*", 6.

„да се неретко примењују неуједначена правила поступања[678]“, односно да не постоји консензус о основним аспектима дигиталне форензике.

Током година је формирано више удружења и организација које за циљ имају професионализацију и стандардизацију дигиталне форензике, што се настоји постићи развијањем стандарда за поступање, предвиђањем основних компетенције за форензичаре и повећањем „научне заснованости“ метода дигиталне форензике[679]. Међутим, проблем је што све ове групе раде независно једна од друге на остварењу истог циља, што може бити контрапродуктивно. Стога, и поред напора поменутих актера, *постоји потреба да се у оквиру научне заједнице постигне договор о одређеним фундаменталним принципима дигиталне форензике, као и о томе која основна знања, вештине и способности би требало да поседује дигитални форензичар и на који начин се потврђује поседовање тих компетенција*.

Из свега наведеног произлази да је, како би се дигитална форензика сматрала валидном форензичком науком, чије технике и методе резултирају дигиталним доказом, веома важно да се сертификују форензичари, акредитују форензичке лабораторије, верификују методи и технике и стандардизују правила поступања.

2.1. Сертификовање форензичара и акредитација лабораторија

Ови процеси имају за циљ да обезбеде квалитет услуга које појединци, односно установе пружају, при чему се сертификују појединци а установе се акредитују. Сертификовање појединаца у случају стручњака дигиталне форензике треба да гарантује да је лице компетентно за одређену област дигиталне форензике, док је акредитовање механизам који треба да пружи гаранцију да форензичка

[678] *„Strengthening Forensic Science in the United States: A Path Forward*“, 133.

[679] Напори за валидацију дигиталне форензике као дисциплине форензичких науке могу се препознати у деловању следећих удружења и организација: Међународна организација за стандардизацију (*International Organization for Standardization (IOS)*, http://www.iso.org/iso/home.html), Европска мрежа института за форензичке науке (*European Network of Forensic Science Institutes* (*ENFSI*), http://www.enfsi.eu/), Одбор за сертификовање дигиталне форензике (*Digital Forensic Certification Board* (*DFCB*), http://www.dfcb.org/), Међународна електротехничка комисија (*International Electrotechnical Commission* (*IEC*), http://www.iec.ch/), Научна радна група за дигиталне доказе (*Scientific Working Group on Digital Evidence* (*SWGDE*), https://www.swgde.org/), Конзорцијум стручњака за дигиталну форензику (*Consortium of Digital Forensic Specialists* (*CDFS*), http://www.cdfs.org/), Америчка академија за форензичке науке (*American Academy of Forensic Sciences* (*AAFS*), http://www.aafs.org/) и друге.

лабораторија има систем за обезбеђење квалитета и да примењује научне методе чији резултати примене сутехнички валидни[680]. С тим у вези се поставља питање, која то знања и вештине квалификују лице да буде стручњак дигиталне форензике, односно који капацитети лабораторије чине чине резултате истраживања у њој научно валидним?

Технолошки аспект је тај који одређује област образовања (наставни план и програм студијских програма чији образовни профил јесте дигитални форензичар одређеног степена звања), специјализацију (постдипломски и стручни курсеви, те додатно образовање и обука у одређеним ужим областима) и сертификовање (од стране овлашћених институција и издавање дозволе за рад/ упис у регистар судских вештака). Дакле, осим академског образовања, сматрамо да је потребно да лица стекну и додатну обуку и да то буде потврђено од стране одређене националне, односно међународне организације за сертификовање форензичара[681]. Тренутно постоји више међународних удружења основних са циљем сертификовања дигиталних форензичара[682]. Међутим, услед постојања великог броја оперативних система, хардверских уређаја и концепата у рачунарству, не може се очекивати да једно лице буде стручњак за све, односно да поседује знања и вештине потребна за различите околности случаја[683].

Иако овакав механизам није гаранција да се грешке у обради доказа неће појавити, примена система за обезбеђење квалитета дигиталне форензике обезбеђује валидност крајњих резултата, односно дигиталних доказа као научног доказа[684]. Државе на различите начине приступају превазилажењу овог проблема[685], јер су препознале предности сертификовања форензичара и акредитације лабораторија у којима се врше форензичка обрада дигиталних

---

[680] Више о акредитацији форензичких лабораторија, D. Watson, A. Jones, *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*, Syngress, Waltham 2013, 795-825.

[681] О потреби сертификовања форензичара, више о томе, Brown, *op.cit*, 55.

[682] На овом месту поменућемо тренутно најзначајније: *Cyber Security Institute's Cyber Security Forensic Analyst: CSFA* (http://www.cybersecurityforensicanalyst.com/), *SANS Institute GIAC Certified Forensics Analyst* (http://www.giac.org/certification/certified-forensic-analyst-gcfa); *International Society of Forensic Examiners Certified Computer Examiner* (https://www.isfce.com/certification.htm); *Computer Hacking Forensic Investigator* (http://www.eccouncil.org/certification/computer-hacking-forensics-investigator).

[683] Више о томе, D. Kahvedzic, T. Kechadi, „Dialog: A framework for modeling, analysis and reuse of digital forensic knowledge", *Digital Investigation* 6/2009, 23-25.

[684] Barbara, *op.cit*, 25.

[685] О прегледу постојећих сертификата за стручњаке дигиталне форензике, Barbara, *op.cit*, 27-42.

доказа за потребе кривичног поступка. Оба процеса је потребно уредити националним прописима у складу са међународно установљеним стандардима и прихваћним критеријумима. У том смислу су вредна помена упутства које је Међународно удружење за акредитацију лабораторија[686] утврдило у „Смерницама за лабораторије форензичких наука“ (*ILAC-G19*)[687]. Ове смернице су релевантне за примену стандарда Међународне организације за стандардизацију постављених у оквиру „Општх услова за компетентност лабораторија за тестирање и калибрацију» (ISO/IEC 17025[688]), којим су утврђени општи услови које треба да испуни лабораторија да би добила одобрење да врши испитивања у области форензичких наука. Поменути стандарди би остварили пун смисао уколико би државе у одговарајућим прописима утврдиле као обавезне услове које би лабораторија као и поједини форензичари требало да испуне да би добили одобрење за практиковање дигиталне форензике. Тако у Великој Британији постоји документ „Правила праксе и поступања“[689] која је 2011. године, полазећи од поменутих међународних стандарда, усвојило помоћно тело *Home Office*-а ради регулисања форензичких наука, кроз утврђивање правила за примену научних техника како би резултат њихове примене могао да буде доказ прихватљив на суду у кривичном поступку. Све сертификоване лабораторије биле су дужне да ускладе своје поступање са Правилима до 2013. године и само оне лабораторије и форензичари који су испунили прописане услове добили су дозволу за рад од стране надлежног тела[690], са изузетком лабораторија у којима се практијује

[686] *International Laboratory Accreditation Cooperation (ILAC)*, http://ilac.org/.
[687] *ILAC-G19 "Guidelines for Forensic Science Laboratories", http://ilac.org/news/ilac-g19082014-published/.*
[688] *ISO/IEC* 17025 :2005, https://www.iso.org/obp/ui/#!iso:std:39883:en.
[689] *Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System,* 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf. Овим документом се уређује поступање форензичара да би резултат обраде могао да буде доказ прихватљив у систему кривичног правосуђа, те постављају услови које форензичари и форензичке лабораторије морају да задовоље да би добили одобрење, односно да би били акредитвани да обављају следеће активности: иницајалну форензичку активност на лицу места; стварање стратегије за преглед лица места; опоравак, обезбеђење, превоз и складиштење трагова и предмета изузетих са лица места; процена, одабир, преглед, стварање узорака и анализу трагова и предмета; тестирање употребом лабораторијски потврђених метода; регистровање свих предузетих активности; процену резултата прегледа и тестирања; писање извештаја и презентовање резултата, са пратећим тумачењем и мишљењем.
[690] *United Kingdom Accreditation Service (UKAS)*, http://www.ukas.com/.

дигитална форензика којима је остављен рок до октобра 2015. да испуне услове предвиђене *ILAC-G19, ISO/IEC 17025* као и са Правилима праксе и поступања[691].

У Србији суд у кривичном поступку може поверити вештачење физичком и правном лицу које је уписано у Регистар судских вештака код Министарства правде, а услови за обављање вештачења, поступак именовања и разрешења судских вештака, поступак уписа и брисања правних лица која обављају послове вештачења, као и права и обавезе лица која обављају вештачење уређени су Законом о судским вештацима[692]. Вештачење[693] обављају физичка и правна лица која испуњавају услове предвиђене Законом (члановима 6-8. за физичка лица, чланом 9. за правна лица) која су након поступка спроведеног у складу са члановима 11-21. Закона уписани у регистар судских вештака, као и државни органи у оквиру којих се може обавити вештачење, и научне и стручне установе[694] (уколико су испуњени услови предвиђени у члану 10). За вештачење у области информационих технологија у Регистар судских вештака код Министарства је уписано 77 физичких лица и 3 правна лица[695].

Међутим, питање је да су ли физичка лица сертификована на одговарајући начин и да ли су правна лица акредитована у складу са међународним стандардима, када ови услови нису ни постављени као обавезни за упис у Регистар. Наиме, физичко лице може бити именовано за вештака ако, између осталог, поседује *стручно знање и практична искуства* у одређеној области вештачења, што доказује објављеним стручним или научним радовима, потврдом о учешћу на саветовањима у организацији стручних удружења, као и мишљењима или препорукама судова или других државних органа, стручних удружења, научних и других институција или правних лица у којима је кандидат за вештака

[691] *Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System*, 5.
[692] „Сл.гласник РС“, бр. 44/2010.
[693] Послови вештачења одређени су као стручне активности чијим се обављањем, уз коришћење научних, техничких и других достигнућа, пружају суду или другом органу који води поступак, потребна стручна знања која се користе приликом утврђивања, оцене или разјашњења правно релевантних чињеница (члан 2).
[694] Вештачење могу обављати и државни органи у оквиру којих се може обавити вештачење, као и научне и стручне установе (факултети, институти, заводи и сл.), који одређују једног или више стручњака одговарајуће специјалности, који обављавештачење или образују комисије састављене од научних или стручних радника који су код њих запослени. Међутим, да би државни органи и научне и стручне установе обављали послове вештачења, није потребно да буду уписани у регистар вештака.
[695] http://www.mpravde.gov.rs/court-experts.php. Увид у регистар априла остварен је 2015. године

радио, односно за које је обављао стручне послове (члан 7). У складу са поменутом потребом за сертификовањем стручњака дигиталне форензике, сматрамо да објављивање радова или присуствовање саветовањима није довољан гарант нечије стручности и да би у погледу тог услова, *Закон требало да захтева и обавезно поседовање одређених сертификата издатих од стране међународно признатих удружења и организација.* У погледу могућности правног лица да обавља вештачења, Закон прописује као услов да је правно лице уписано у регистар надлежног органа за делатност вештачења у одговарајућој области и да су у том правном лицу запослена лица која су уписана у Регистар вештака, док се не постављају никакви додатни услови услови које лабораторије морају да задовоље да би добили одобрење. Стога сматрамо да *би међу обавезним условима за упис правног лица у Регистар било потребно предвидети усклађеност са ILAC-G19 и ISO/IEC 17025 стандардима*.

2.2. Валидација и верификација форензичких алата

Стручњак дигиталне форензике у процесу од дигиталних трагова до дигиталних доказа користи разне софтверске и хардверске алате. Што се тиче *софтверских алата*, могу се класификовати на следећи начин: алати за преглед (за стварање извештаја о стању система датотека и типовима датотека на свим дисковима рачунарског система); алати за стварање форензичке слике диска (што се разликује од обичног копирања датотека јер се ствара потпуни клон диска са свим скривеним датотекама и просторима у меморији); алати за потпуно брисање садржаја диска (свега што остане након уобичајеног брисања датотека у меморији диска); те алати за детаљну претрагу диска.

Алати могу бити намењени за детаљан дуготрајан преглед (у контролисаном техничком окружењу), за брзи преглед на лицу места (нпр. за тријажу података), за преглед уређаја прикључених на напајање и спојених са мрежом као и уређаја који су угашени и нису спојени са мрежом[696]. Велики број алата се користи у форензичке сврхе, од којих су неки креирани непосредно за ту намену, а други

[696] P. Hunton, „The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation“, *Computer Law and security Review* 27/2011, 65.

имају изворно другу намену[697]. Постоји више софтверских алата који се слободно, односно бесплатно могу преузимати са Интернета (тзв. *free/open source*[698]), а постоје и комерцијални производи које су направили и продају поједини произвођачи[699]. Иако су већина форензичких алата посебно креирани софтвери, постоје и алати засновани на употреби хардвера. *Хардверски* уређаји су најчешће у облику преносивих радних станица, а одабир уређаја зависи од околности конкретног случаја и окружења у ком се напад десио. Постоје уређаји посебно конструисани за ову сврху у комерцијалној понуди, а форензичар може и сам креирати свој[700].

---

[697] Нпр. *JkDefrag* за дефрагментизацију диска за *Windows 2000/2003/XP/Vista/2008/X64.*

[698] Међи најчешће коришћеним бесплатним софтверским форензичкин алатима су: *Sleuth Kit* – библиотека и колекција командно-линијских алата који омогућавају претраживање диска и система датотека (http://www.sleuthkit.org/); *Helix* – скуп форензичих алата који укључује *Sleuth Kit* и многе друге апликације (http://www.efense.com/helix/); *Foremost* – алат за претраживање, као што су: *Linux ext2/ext3, Linux swap, UFS, JFS, NTFS, FAT12, FAT16, FAT32* (http://sourceforge.net/projects/foremost); *F.I.R.E.* (*Forensic and Incident Response Environment*) – самостални скуп алата који се покреће када се рачунар упали (http://fire.dmzs.com/); *Forensic Toolkit, BinText, Galleta, NTLast, Pasco, Patchit, Rifiuti* и *ShoWin* – алати посебно намењени *Windows* систему (http://www.foundstone.com/); *WinHex* – алат за управљање датотекама, дисковима и радном меморијом у хексадекадском формату (http://www.x-ways.net/winhex/); *SMART Linux* – *Linux* дистрибуција посебно осмишљена за форензичку анализу доказа, а садржи алате за анализу података, претраживање и одговор на сигурносни инцидент (http://www.asrdata2.com/); *Wireshark* – алат за анализу мрежног саобраћаја (http://www.wireshark.org/); *NTFSWalker* – алат за анализу *NTFS* система датотека (http://www.brothersoft.com/ntfswalker-262095.html).

[699] Комерцијални софтверски алати који се најчешће користе су: *EnCase* који омогућава стварање форензичке слике и прелгед хард драјва, диска и *PDA* уређаја (https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx); *Password RecoveryToolkit (PRTK*) који пресреће и проналази шифре и декодира у *Office, WinZip, Internet Explorer* и *Netscape* (http://accessdata.com/product-download/digital-forensics/password-recovery-toolkit-prtk-version-7.6.0); *Forensic Toolkit* (*FTK*) има неколико функција: претраживање и опоравак датотека различитих формата (*NTFS, FAT*, компресоване *NTFS Linux Ext2fs* и *Ext3fs),* опоравак порука електронске поште, екстракцију датотека из архиве (из *PKZIP, WinZip, GZip, TAR*), филтрирање датотека итд *(*http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk*); CaptureIT* омогућава анализе у физички оштећеном диску (http://www.captureitota.com/). За детаљнији преглед и критичка анализи форензичких алата, Marcella, Menendez, *op.cit*, 31-47; Li, *op.cit*, 234-257; Д. Ранђеловић, Т. Богдановић, „Алати за дигиталну форензику“, *Наука, безбедност, полиција* 2/2010, 26, 33, 37.

[700] У ову групу алата спадају уређаји који омогућавају форензичару да, након што се споји са рачунаром (уз помоћ *Firewire, USB* или *SCSI* конектора) уклони и издвоји хард диск из предметног уређаја без потребе да се систем искључи - тзв. *write-blocker* уређај (http://www.digitalintelligence.com/forensicwriteblockers.php). Постоје уређаји за опоравак избрисаних датотека, као што су нпр. комерцијални уређаји *NormaTech Recover* (http://www.normatecrecovery.com/) и *DeepSpar File Recovery (*http://www.deepspar.com/*)*. У употреби су и вишенаменски уређаји. Тако *WinHex* прегледа и опоравља датотеке на диску, клонира диск, креира форензичку слику сектора у хард диску без да их компресује; *Disk sector*, погодан је за енкрипцију, као и претраживање по кључним речима. *Data Lifter* представља колекцију алата за екстракцију датотека, разврставање датотека, враћање избрисаних порука електронске поште и историје претраживања на Интернету, као и брисаних датотека у *Recycle Bin-у* (http://www.x-ways.net/winhex/).

Током касних 1990-их развоју области компјутерске форензике допринела је појава и развој прве генерације алата намењених за форензичку анализу, односно креираних за приступ и преглед рачунарских података на форензички безбедан начин. Алати као *EnCase* и *FTK* постали су стандардни алати за дигиталну истрагу. Ови алати опште намене почивају на уобичајеном и кориснику прилагођеном окружењу за вршење форензичке анализе и представљали су велики напредак у односу на ранији „ручни" преглед и интерпретацију структура у систему датотека, јер омогућавају преглед података, претрагу по кључним речима и спровођење бројних других техника анализе података.

Прва генерација алата опште намене има заједничку архитектуру - апликације које извршавају задатке на једном десктоп рачунарима који се заснивају на *Microsoft Windows* оперативном систему. У деценијама од појаве прве генерације алата ограничења њихове архитектуре су постала очигледна јер постојећи алати нису успевали да држе корак са повећаном комплексношћу рачунарских уређаја и великом количином података који се обрађују у оквиру модерне форензичке истраге рачунара. Зато су креатори тих алата настојали да их побољшају повећањем рачунарских капацитета а тиме и брзине форензичке анализе која се обавља употребом тих алата[701], а нарочито повећањем капацитета за обраду података кроз увођење паралелне обраде (ствара се више „чворова" за обраду података који су спојени са централном базом података и радном станицом за анализу, као нпр. код професионалне верзије *FTK 2* алата). Неколико недостатака алата се може навести: велики меморијски капацитет рачунарских уређаја који су предмет прегледа и анализе представља проблем, па иако се користе скупе радне станице са више процесора, великом меморијом и великом брзином чувања

[701] Неколико параметара се може користити за мерење ефикасности и перформанси форензичких алата: апсолутна брзина (време потребно за комплетну анализу) и релативна брзина (просечно време у ком алат обрађује рачунарске податке у поређењу са временом за које се податак очитава у оригиналном извору података), поузданост (проценат у ком алат извршава задатаке успешно и даје резултат у документованом облику), тачност резултата (проценат у ком алат даје исправне резултате анализе), потпуност резултата (проценат у ком алат уочава и приказује тражене рачунарске податке), проверљивост резултата (проценат резултата који се могу повезати са изворним рачунарским податком на основу документовања свих рачунарских радњи и наредби које су извршене да би се до резултата дошло) и поновљивост резултата (проценат у ком се до истих резултат може доћи поновном обрадом и анализом, нпр. помоћу детаљних записа о извршеним наредбама које алат ствара). D. Ayers, „A second generation computer forensic analysis system", *Digital Investigation* 6/2009, 35.

података, анализа понекад може потрајати сатима, па и данима; нису ретке ни грешке у раду софтверских алата, па и оних комерцијалних.

Осим тога, управо ови комерцијални алати не дозвољавају кориснику увид у начин функционисања (не стварају се детаљни записи о извршеним наредбама а тиме ни како се дошло до резултата) па је на тај начин ограничена поузданост и тачност тих резултата. Наиме, ради се о тзв. *closed source* алатима јер продавац алата не даје увид у изворни код софтвера, за ралику од *open-source* алата код којих је код доступан и на основу њега се могу пратити све активности којима се дошло до резултата. Да би се обезбедила проверљивост и поновљивост резултата, неопходно је да алат има могућност да ствара детаљан запис о свим активностима које су предузете да би се до приказаних резултата дошло а тиме и да би се обезбедио интегритет електронских доказа. Управо ово последње, без обзира на техничка побољшања алата, представља проблем. Наиме, да би се алати могли користити, потребно је, осим ефикасности обраде и чувања података, обезбедити поузданост и могућност поновљеног добијања истих резултата, јер се у супротном може истакнути приговор испитаности функционисања алата и поверења у резултате њихове примене!

Поузданост софтверских алата и њихова правилна употреба је од кључног значаја за обезбеђење интегритета електронских доказа, а да би алат осигурао интегритет електронских доказа, потребно је да буде валидан и верификован. Наиме, методе и технике које имају за циљ да обезбеде поузданост софтвера називају се валидација и верификација софтвера, при чему постоје два приступа: инспекција софтвера (која се одвија у свим фазама циклуса развоја једног софтвера) и тестирање софтвера (проверава се да ли функционише у складу са наменом). У погледу форензичких софтверских алата, а у складу са стандардом *ISO 17025*, валидација подразумева потврду да алат, техника или процедура функционише исправно и како је предвиђено, а верификација је потврда валидације у лабораторијски контролисаним условима.[702] Стога сматрамо да примена алата треба да буде у складу са прихваћеном методологијом, а да алат буде тестиран да би се резултати добијени његовом применом могли третирати

[702] Више о томе, Y. Guo, J. Slay, J. Beckett, „Validation and verification of computer forensic software tool - searching Function“, *Digital investigation* 6/2009, 12–13.

као тачни и поуздани[703]. При томе, није довољна валидација и верификација коју врше продавци комерцијалних софтверских алата[704], јер није у довољној мери документована и не полази од њихове функционалности, него је приоритет на комерцијалним интересима. Стога сматрамо да је потребно да то врши тело за стандардизацију, као што је учињено за методе које се користе у балистици или за вештачење ДНК, кроз преиспитивање усклађености са одговарајућим ISO стандардима квалитета[705]. Како се све више за прикупљање и анализу рачунарских података користе аутоматизовани алати, да би се обезбедила поузданост резултата примене тих алата, потребно је изабрати и користити оне који су валидни, исправни и одговарајући у конкретном случају[706]. Иако постоји тенденција за аутоматизацијом дигиталне истраге (аутоматским извршавањем задатака применом одређених рачунарских техника[707]) што је свакако добро, јер се тиме умањује могућност манипулације и грешке начињене људском активношћу (под условом да претходни параметри за мерење ефикасности алата буду задовољени[708]), сматрамо да је алат, то што и треба да буде, само помоћно средство у рукама обученог и искусног стручног лица[709] и да се форензичар не би требао ослањати просто на аутоматизоване функције алата, него је нужно да разуме информационе технологије и основе криминалистике[710] и увек да

[703] О потреби стварања оквира за тестирање форензичких софтверских алата, Li, *op.cit*, 258.
[704] Као што је *Guidance Software* за *Encase* алат или *Access data* за *FTK* алат.
[705] J. Beckett, J. Slay „Digital forensics: validation and verification in a dynamic work environment“, у: 40th Annual Hawaii International Conference on 2007. System Sciences, 2007, 266.
[706] Marcella, Menendez, *op,cit*, 78.
[707] Примера ради, применом тзв. *data mining* техника за преглед и претрагу одређених датотека и директоријума. О примеру аутоматизације алата у претрази и прикупљању рачунарских података, B.Carrier, E. Spafford, „Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence“, Digital Forensic Research Workshop, 2005, 7.
[708] J. Nogueira, „Ontology for Complex Mission Scenarios in Forensic Computing“, *The International Journal of Forensic Computer Science* 1/2008, 44.
[709] Поверавање свих задатака које обавља стручно лице у вези са обрадом дигиталног лица места, једном рачунару, са у ту сврху конструисаним софтвером и хардвером, чак и када би се створио савршени и непогрешиви рачунар, још увек представља научну фантастику, али не у погледу техничких решења (истраживања и примена вештачке интелигенције је постала стварност), него незасмисливости замене човека машином и поверења у резултате такве анализе на суду. Поједини аутори, пак, превазилажење проблема недовољног броја стручних лица, недовољне брзине анализе и обраде прикупљених података а превеликих трошкова, виде у поверавању задатака аутоматизованом рачунарском систему који аутономно и аутоматизовано извршава задатке у вези са прикупљањем и обрадом рачунарског система. J. Nogueira, J. Celestino, „Autonomic Forensics a New Frontier to Computer Crime Investigation Management“, *International Journal of Forensic Computer Science* 1/2009, 29-41.
[710] Да би се у пракси форензичарима омогућило да знају које процедуре да се прате у одређеној фази дигиталне истраге како би резултати поступања били доказ који задовољава правне захтеве и

инсистира на двострукој валидацији техника (да користи више од једне технике за проверу резултата).

2.3. Стандардизација правила поступања

Што се тиче стандардизације правила поступања, бројни теоретичари и практичари из области дигиталне форензике настојали су да осмисле најпогодније *моделе за поступање* са рачунарским подацима (моделе дигиталне истраге). Такође, поједине организације и удружења, као и надлежни органи појединих држава посветили су пажњу стварању најадекватнијих смерница у *виду стандарда поступања* који резултира прихватљивим доказима за систем кривичног правосуђа, а нарочито су значајна настојања у оквиру Међународне организације за стандардизацију. Осим поменутог општег стандарда који се односи на услове за рад форензичара и лабораторија, формирана је радна група за израду стандарда који су релевантни за дигиталну форензику а као резултат рада овог тела настало је неколико релевантних стандарда[711]. Приликом формулисања

да би се могао користити на суду, Европска комисија је финансирала пројекат под називом „*Cyber-tools Online Search for Evidence*“ током 2003. године, али Пројекат, нажалост, није резултирао остварењем циља који је био постављен. http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=0FA936B6-3A43-4D66-86F5-7281A6030C00.

[711] Релевантни су следећи стандарди: стандард *ISO/IEC 27035* „Управљање нападима на информациону безбедност“ (усвојен 2011. године) који утврђује кораке које треба предузети приликом реаговања на напад на информациону безбедност (*ISO/IEC* 27035 “*Information security incident management*”, http://www.iso27001security.com/html/27035.html - у време писања овог рада јавности су доступни нацрти три специјална стандарда који произлазе из ISO/IEC 27035, а ради се о станадардима којима се настоје предвидети принципи управљања инцидентима на информациону безбедност (*ISO/IEC 27035-1: principles of incident management*), смернице за планирање и припрему одговара на инциденте против информационе безебедности (*ISO/IEC 27035-2: guidelines to plan and prepare for incident response*) и смернице за реаговање на инциденте против информационе безебедности (*ISO/IEC 27035-3: guidelines for incident response operations*); стандард *ISO/IEC 27037* “Смернице за уочавање, прикупљање и очување дигиталних доказа” (усвојен 2012. године) који утврђује кораке које треба предузети како би се прикупили и обезбедили дигитални докази о нападу на информациону безбедност (*ISO/IEC 27037* “*Guidelines for identification, collection, acquisition, and preservation of digital evidence*“, http://www.iso.org/iso/catalogue_detail?csnumber=44381); стандард *ISO/IEC 27041* „Смернице за обезбеђење погодности и примерености метода који се примењују у истраживању напада на информациону безбедност“ (нацрт) који би требало да утврди механизам којим се обезбеђује да примењени методи и алати задовољавају захтеве постављене пред методе форензичке науке (*ISO/IEC 27041* „*Guidelines on assuring suitability and adequacy of incident investigative methods*“, http://www.iso27001security.com/html/27041.html); стандард *ISO/IEC 27042* „Смернице за анализу и тумачење дигиталних доказа“ (нацрт) који би требало да утврди основна правила којих се треба форензичар придржавати како би обезбедио интегритет дигиталних доказа (ISO/IEC 27042 „*Guidelines for the analysis and interpretation of digital evidence*“,

ових стандарда циљ није био стварање хомогенизованих, стандардизованих поступака који су у складу са националним прописима, с обзиром да је тако нешто уз помоћ ових инструмената немогуће, него истицање основних принципа у виду смерницама за поступање у уобичајеним сценаријима. Сматрамо да је приликом регулисања дигиталне истраге ове стандарде корисно узети у обзир, јер иако нису правно обавезујући за поједине националне државе, исти могу допринети уједначавању поступања са дигиталним доказима[712], с обзиром на то да су и настали полазећи од метода који су препознати као примери добре праксе.

Постојање стандарда поступања има истовремено и добру и лошу страну. Одређујући минимални ниво прихватљивог начина за предузимање неке радње, стандарди имају за циљ осигурање квалитета, јер пружају гаранцију да су резултати радње предузете у складу са стандардима поуздани. Из тог разлога, логично је да судови више вере поклањају доказима за које постоје стандарди поступања утврђени од стране научне заједнице. Са друге стране, постојање стандарда може успорити прогрес и ограничити креативност. С појавом нових техничких алата и проблема, потребно је прилагодити постојеће и стварати нове методе за рад са електронским доказима. За разлику од фундаменталних природних наука, код којих су темељни постулати трајни и непроменљиви, не би се могло рећи да је то карактеристика рачунарских наука. Штавише, променљивост и флексибилност су окоснице савременог технолошког развоја. Из тог разлога правила поступања са електронским доказима која нису прилагодљива променама нису добро решење, па је стандардне оперативине процедуре потребно

---

http://www.iso27001security.com/html/27042.html); стандард *ISO/IEC 27043* „Принципи и процес истраге напада на информациону безбедност“ (нацрт) који би требало да утврди идеални модел дигиталне истраге примењив на све могуће сценарије (*ISO/IEC 27043* „*Incident investigation principles and processes*“, http://www.iso27001security.com/html/27043.html); стандард *ISO/IEC 27050* „Информације похрањене у електронском облику“ (нацрт) који би требало да утврди принципе за уочавање, обезбеђење, прикупљање и обраду информације похрањене у електронском облику (*ISO/IEC* 27050 „*Electronic discovery*“, http://www.iso27001security.com/html/27050.html). Усвајање наведених нацрта је предвиђено за 2016. годину,

[712] Тако је у Великој Британији, Британска институција за стандарде 2008. године усвојила стандард „Доказна снага и прихватљивост информација у електронском облику“ којим се утврђују формални захтеви за системе управљања електронским документима а са циљем да се стриктним придржавањем прописаних техничких услова обезбеди аутентичност података у електронском облику који се у оквиру одређене организације складиште, обрађују и преносе. *BS 10008:2008* “ *Evidential weight & legal admissibility of electronic information*“, http://shop.bsigroup.com/Browse-By-Subject/ICT/Legal-Admissibility/. Последње измене стандарда су објављене 2014.године.

креирати тако да буду технички неутралне, а корисно их је периодично процењивати, те по потреби иновирати у складу са технолошким развојем[713].

Када говоримо о стандардизацији поступања, сматрамо да *стандард треба посматрати као трослојну структуру, у којој су слојеви хијерархијски усторојени спрам различитог степена општости и обавезности.* Тако, стандард подразумева постојање одређених: 1. Принципа (највишег нивоа општости, обавезно применљиви у свим случајевима); 2. Модела (који конкретизују принципе, а конкретозовани су кроз процедуре), и 3. Процедура (најмањег степена општости, прилагођене конкретним случајевима).

Наиме, *неопходно* је да постоје **одређени принципи** који се морају поштовати када се поступа са електронским доказима. Основним правилима која имају циљ максимизирање прихватљивости процеса дигиталне форензике први пут је посвећена пажња 1999. године у делу „What is Forensic Computing" чији је аутор *McKemmish.* Препозната су четири правила: 1. Процес форензичке обраде оригиналног материјала треба свести на минимум; 2. Промене проузроковане на оригиналу треба детаљно документовати (карактер, обим и разлог зашто је до промене дошло); 3. Примена и развој форензичких техника и алата треба да буде у складу са релевантним правилима о доказима[714]. Ова правила су послужила као основа за стварање општих приницпа у поступању са дигиталним доказима[715]:

Принцип 1: Интегритет података - радње које се предузимају, да би се обезбедили и прикупили докази, не смеју да утичу на интегритет доказа, односно ниједна радња која се предузима не би требало да произведе промене на електронским уређајима или медијима, како би се рачунарски подаци могли употребити као доказ на суду. Приликом руковања електронским уређајима и подацима, они се не смеју мењати, било у вези са хардвером или било у вези са

[713] ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf, 30.

[714] R. McKemmish, „What is forensic computing?", *Trends and Issues in Crime and Criminal Justice* 118/2002, (www.aic.gov.au/publications/tandi/ti118.pdf).

[715] Општи принципи поступања са дигиталним доказима на сличан начин постављени су у следећим насловима: International Organization on Computer Evidence: Digital Evidence Standards Working Group, *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, 2002; U.S. Department of Justice: Computer Crime and Intellectual Property Section, S*earching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Washington, 2002, (www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm), National High Tech Crime Unit: Association of Chief Police Officers, *Good Practice Guide for Computer Based Electronic Evidence*, London 2003 (www.acpo.police.uk/asp/policies/Data/gpg computer based evidence.pdf);

софтвером. Лице испред органа поступка је одговорно за интегритет материјала изузетог са лица места и на тај начин и за почетак „форензичког ланца доказа“ (*forensic chain of custody*). У одређеним околностима је неопходно донети одлуку да се приступи подацима на „живом“ рачунарском систему или уређају за електронску обраду и/или складиштење података како би се избегао губитак потенцијалног доказа (*live forensic).* Ово се мора предузети на такав начин да се изазове најмањи утицај на податкеа и само од стране лица квалификованог да то учини (које је довољно стручно да предузме те радње и да пружи доказ тј. објашњења у погледу релевантности и последица предузетих радњи)[716]. Кроз све то, стручно лице које рукује доказима треба да буде свесно неопходности да се преглед електронских доказа спроведе на тачан и непристрасан начин.

Принцип 2: Снимање радњи - радње које се односе на одузимање, складиштење, пренос или преглед електронских доказа морају бити документоване, фиксиране и доступне за прегледање. Треба створити и чувати аудио или други запис о свим предузетим радњама приликом руковања електронским доказима. Независна трећа страна би требало да буде у стању да испита те акције и постигне исти резултат. Зато је неопходно прецизно евидентирати све активности које се односе на на заплену, приступ, складиштење и пренос електронских доказа, како би се омогућило да треће лице реконструише радње предузете на лицу места како би се осигурала доказна вредност на суду.

Принцип 3: Стручна подршка - лица које врше преглед електронских доказа морају за то бити посебно обучена. Када се претпоставља да се могу наћи електронски докази у току предузимања радњи на лицу места, лице које руководи радњом треба да обавести специјалисту/ спољне саветнике на време да би исти присуствовали. У истрагама у којима постоји потреба за претрес и одузимање електронских доказа, може бити неопходно да се консултују стручна лица (као спољни експерти или лица у саставу јединице, у зависности од начина организације специјалног одељења), која треба да буду упозната са одређеним принципима/правилима у вези руковања електронским доказима, и да поседује: потребну стручност и искуство за рад на терену, потребна знања о предузимању истражних и оперативних радњи, неопходно познавање материје, неопходно

[716] Ово је из принципа 2 ACPO водича: http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

познавање прописа, одговарајуће вештине комуникације (за усмена и писмена објашњења) и неопходну одговарајућу терминологију.

Принцип 4: Одговарајућа обука - лица која прва излазе на лице места на ком постоји могућност постојања електронских доказа морају бити адекватно обучена да би могли да траже и искористе електронске доказе, ако нема стручњака који су доступни на лицу места. У изузетним ситуацијама када је неопходно да та лица прикупе и/или да приступе изворним подацима ускладиштеним на електронском уређају или медијуму за дигитално складитење података, она морају бити обучена да тоураде правилно и да умеју да објасне релевантност и импликације својих поступака.

Принцип 5: Законитост - наведена лица и орган поступка су дужни да обезбеде да се у вези са поседовањем и приступом електронским доказима поштује закон, општи форензички и процедурални принципи.

Државе треба да у својим општим актима предвиде операционализацију ових принципа у свим фазама суочавања са потенцијалним изворима електронских доказа. Ове принципи треба да универзално важе као начела без обзира на промене у хардверу и софтверу. Осим тога, *потребно је* да буду утврђена одређена *правила* примене одређених радњи и мера која се предузимају у вези са електронским доказима. Та правила би требало да буду *„омеђена“ општеважећим принципима*. При томе, иако је примена одговарајућих алата и техника прилагођена околностима конкретног случаја, правила у погледу фаза у оквиру којих се предузимају поједине радње треба да су у довољној мери генерализована у виду **модела поступања са електронским доказима, односно модела дигиталне истраге**. Осим што је нужно да постоје општеважећи принципи и што је потребно да се створи модел за поступање са електронским доказима, *корисно* би било и да се креирају **процедуре** *које би уважавале принципе а биле у складу и са постваљеним моделом поступања*. Те процедуре би заправо корак по корак предвиђале тактику поступања, односно како се поједини алати и технике користе спрам околности конкретног случаја. Заправо, процедуре би предствљале конкретизације модела на различите случајеве. Из тога разлога било би контрапродуктивно стандардизовати процедуре, већ их оправдано третирати као прилагодљиве форме поступања.

Значај оваквог раслојавања се нарочито огледа у нормирању правила поступања. Наиме, *сматрамо да принципе треба као обавезујућа правила унети у кривично процесно законодавство* која се морају поштовати у сваком случају када се поступа са електронским доказима, без обзира на кривично дело поводом ког се радње предузимају, а непоштовање принципа имало би за последицу незаконитост електронског доказа. *Опредељење за одређени модел дигиталне истраге је од значаја за опредељење како регулисати поједине радње* које се предузимају а тиме има импликације на одредбе кривичног процесног законодавства. Непоступање по тако уређеним одредбама би могло резултирати правном неваљаношћу доказа. *Саме процедуре поступања* не би требало због њихове конкретне и индивидуалистичке природе прописивати у оквиру кривичног процесног законодавства, него у правилницима, као подзаконским актима, или инструкцијама у оквиру надлежних органа[717]. Ипак, знатније одступање од утврђене процедуре могло би у конкретним случајевима да доведе до незаконитости доказа.

3. ДИГИТАЛНА ИСТРАГА

Рачунарски ситем је материјални доказ, али не може се третирати на исти начин као други предмети који су пронађени приликом вршења увиђаја или претресања, јер садржи велики број рачунарских података који могу имати значај електронских доказа и зато сам по себи представља „лице места“ које треба применом специфичних тактичких и техничких радњи и мера обрадити на систематичан и формализован начин у складу са законом. Тако се у литератури се користе термини „дигитално лице места“ (*digital crime scene*) за означавање сваког лица места на ком је пронађен рачунар[718] или, пак, са ужим значењем као окружење које ствара јединство хардвера и софтвера[719].

Коришћењем знања и техника које се примењују приликом вршења увиђаја у физичком свету може се установити модел поступања приликом вршења увиђаја у

[717] Као што постоји у оквиру Министарства унутрашњих послова.
[718] ICAPO, Computer Usage For Child Abuse Investigators, http://www.vrhome.com/icapo/pedo/webax/index.htm.
[719] Kruse, Heiser, *op.cit,* 4; Vacca, *op.cit,* 17.

виртуелном окружењу, односно приликом обраде дигиталног лица места. Полазећи од принципа и метода који се примењују традиционално у „физичком“ свету и њиховог прилагођавања виртуелном окружењу, научна и стручна јавност се у последњих двадесетак година бавила развијањем одговарајућег модела поступање са електронским доказима. У теорији и пракси је предложено више модела поступања који претендују да постану општеприхваћени стандарди за радње чијим предузимањем се долази до валидних електронских доказа. За означавање одговарајућег модела за поступање са електронским доказима користи се термин дигитална истрага,. Ради се о инструментаријуму дигиталне форензике, као научне дисциплине настале из потребе да се пронађу техничка решења за правне проблеме који су се јавили са последицама које је распрострањена употреба информационих технологија у свакодневном животу произвела и у судским поступцима.

Дигиталну истрагу можемо схватати *као процес у ком од рачунарских података* који су прикупљени из рачунарског система (и других електронских уређаја за обраду и пренос података) и рачунарске мреже *долази до електронских доказа* који се могу користити у кривичном поступку[720]. Дакле, спровођење дигиталне истраге има за циљ проналазак поузданих и релевантних електронских доказа. У том смислу, може се уочити да ефикасност дигиталне истраге има две компоненте: квалитативну компоненту (да резултатира поузданим електронским доказима, уз поштовање свих законских ограничења и очување интегритета доказа) и квантитативну компоненту (да резултатира релевантним електронским доказима, уз што мање времена и са што мање трошкова)[721].

[720] Процес означен као дигитални истрага је предмет истраживања и обраде у радовима не малог броја аутора у литератури с краја 20. и почетка 21. века: F. Clark, K. Diliberto, *Investigating Computer Crime*, CRC Press, New York 1996, 51; T. Johnson, *Forensic Computer Crime Investigation(International Forensic Science and Investigation)*, CRC Press, Chicago 2005, 14; C. Franklin, *The Investigator's Guide to Computer Crime*, Charles C. Thomas Pub. Ltd, Springfield 2006, 147; Knetzger, Muraski, *op.cit*, 75; I. Walden, *Computer Crimes and Digital Investigations*, Oxford University Press, Oxford 2007; R. Bryant, S. Bryan (eds.), *Investigating Digital Crime*, John Wiley&Sons, Chichester 2008, 55; Marshall, *op.cit*; Clifford R., Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime, Carolina Academic Press, Durham 2011, 63; G. Curtis, *The Law of Cybercrime and their Investigation*, Taylor&Francis, Boca Raton 2012, 45.

[721] M. Losavio, J. Adams, “Gap Analysis: Judicial Experience and Perception of Electronic Evidence”, *Journal of Digital Forensic Practice* 1/2006, 15.

3.1. Модел дигиталне истраге

Стварање и примена доброг модела дигиталне истраге је важно, јер се тиме може обезбедити апстрактан референтни оквир поступања, примењив независно од степена развијености и врсте технологије или организационог окружења у конкретном случају, што доприноси ефикасности дигиталне истраге. На тај начин модел представља полазни основ за одређивање одговарајуће техничке подршке раду форензичара, као и за стварање заједничке уобичајене терминологије, што даље доприноси дискусијама и размени знања и искуства између стручњака. Модел се, осим тога, може искористити за развој и примену метода прилагођених новим технологијама које се временом могу појавити. Модел има и проактивну димензију, јер може да се користи на начин да сагледају могућности за развој и распоређивање технологије за подршку раду форензичара, као и да пружи оквир за анализу потребних захтева које треба да задовоље форензички алати (посебно напредни аутоматизовани аналитички алати). Уколико, пак, процедуре по којој се врши обрада дигиталног лица места не постоје или су неконзистентне или нестандардизоване, то може да има директне последице на резултате обраде дигиталног лица места. Одабир неодговарајуће процедуре може резултирати непоптуним доказима или чак неприкупљањем истих. „Прескакање“ једног корака или замена у редоследу корака који су фазе у процедури, може довести до резулатата из којих се не могу извести одговарајући закључци, а докази прикупљени применом *ad hoc* методе или на неструктуиран начин може довести до ризика неприхватања на суду. Стога је од круцијалног значаја да се све радње које се предузимају приликом обраде дигиталног лица места и даљи рад у лабораторији са изузетим доказима одвија по унапред утврђеном редоследу, јер се на тај начин ствара одговарајући механизам који резултира поузданим електронским доказима који се пред судом презентују.

Почевши од 1984. године, када је предложен први модел дигиталне истраге[722], више аутора је у научној и стручној литератури износило своје предлоге. У првом

[722] Методологија руковања са дигиталним доказима први пут је предложена на састанку Федералног бироа за истрагу у САД, како би резултати поступања били научно поуздани и правно прихватљиви. Тај модел поступања састојао се од 4 фазе: *фаза прикупљања* доказа на прихватљив начин уз постојање потребних одобрења надлежних органа; у *фази идентификације* се уочавају дигиталне компоненте у прикупљеним доказима и конвертују се у „разумљив“ облик па се у *фази*

периоду развоја дигиталне форензике, предмет обраде су били рачунари релативно малог меморијског капацитета а тиме и мале количине похрањених података за преглед и обраду, што је омогућавало да се цео хард диск копира на други диск и да се на копији анализира садржај и траже докази. У већини наслова написаних током 2000-тих развијане су методи дигиталне форензике за једноставне, типичне случајеве. На основу њихове анализе, може се уочити да неки од модела имају тенденцију да се примењују на врло специфичне сценарије, док се други могу применити у ширем обиму; неки од модела садрже изузетно пуно детаља, а други су сувише уопштени, па може бити тешко или чак збуњујуће определити се за исправан и одговарајући модел. Интенција аутора је била да кроз анализу различитих модела, уочи заједничке битне фазе и предложи модел опште намене, који би представљао полазни модел примењив, без обзира на околности конкретног случаја. У току обраде литературе, уочено је да различити аутори користе разне термине за означавање модела поступања са електронским доказима, и то: модел, поступак, процес, процедура, фаза, задаци, итд. Аутор се определио за термин „дигитална истрага“ као модел поступања, термин „фаза“ подразумева делове модела, док се термином „задаци“ означавају поједини кораци, односно радње које се предузимају у оквиру фазе.

Пионирски модел за обраду и преглед дигиталних доказа представио је 2000. године *Eoghan Casey*, један од најутицајнијих аутора у области дигиталне форензике[723]. Значај оваквог модела је што посматра процес обраде електронских доказа као циклус, тако да реконсктрукција као завршна фаза може резултирати потребом враћања на прву фазу прикупања доказа, и тако у круг, до добијања резултата који потврђују првобитне поставке. Модел је најпре осмишљен за појединачни рачунарски систем, али се показало да је примењив и за рачунарске

евалуације процењује да ли су уочене и конвертоване дигиталне компоненте релевентне за конкретан случај, те да ли се могу сматрати доказом; у завршној *фази излагања* се прикупљени и екстраховани докази презентују на суду. M. Pollitt,“Computer Forensics: An Approach to Evidence in Cyberspace”, *Proceeding of the National Information Systems Security Conference*, Baltimore, MD, Vol. II, 1995, 487-491; M. Pollitt,“An Ad Hoc Review of Digital Forensic Models”, in Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE’07), Washington 2007.

[723] Модел предвиђа постојање четири фазе: 1. Уочавање електронских доказа, 2. Обезбеђење, прикупљање и документовање електронских доказа; 3. Класификовање, упоређивање и индивидуализација електронских доказа; 4. Реконструкција догађаја. E. Casey, *Digital evidence and computer crime: forensic science, computers and the Internet*, Academic Press, Amsterdam-Boston 2011.

мреже, што указује да је добра страна оваквог модела његова уопштеност, а тиме и невезаност за технологију.

Следећи модел вредан помена је **модел научне обраде лица места,** који је 2001. предложила група аутора[724]. Недостатак овог модела је што се односи само на обраду лица места, али не и на даље фазе у поступању са доказима, и што се бави само материјалним доказима (може се применити само на физичке предмете који су носиоци, односно извори електронских доказа), па услед неуважавања специфичности електронских доказа, нису дати никакви предлози у вези са поступањем са њима. Поред овог уопштеног и недовољно специфичног модела, исте године је друга група аутора креирала **модел реговања на напад на одређени информациони систем**[725]. Ова методологија је усмерена првенствено ка поступању са „живим" системом, односно покренутим информационим системом који је објект напада. Преглед система је временски најобимнији и најзахтевнији задатак, али представља само једну од фаза, па он није одговарајући за поступање полиције, већ може да буде буде од користи само за реаговање информтичког сектора у оквиру корпорације чији информациони систем је нападнут.

Као резултат рада техничке групе у полицији Њујорка 2000. године је настао је тзв. ***DFRWS*** **истражни модел**[726]**.** Модел је осмишљен тако да има широко

[724] Разликују су четири фазе у овом моделу. У оквиру прве фазе се уочавају трагови и предмети који могу послужити као доказ, који се потом документују, прикупљају и обезбеђују. Следећа фаза се своди на идентификовање доказа уз помоћ класификовања и поређења прикупљених доказа. У трећој фази се врши индивидуализација доказа, односно тумачење њиховог значаја ради довођења у конкретну везу са одређеним лицем и догађајем. У оквиру последње фазе се резулати претходних фаза и друге релевантне информације уклапају како би се утврдио редослед догађаја и радњи на лицу места у време извршења радње кривичног дела, а за потребе израде извештаја који се презентује на суду. H. Lee et al., *Crime Scene Handbook*, Academic Press, San Diego 2001, 15-45.

[725] Модел предвиђа поступање кроз једанаест фаза: 1. Припрема за реаговање на напад (подразумева одговарајућу обуку лица и потребну инфраструктуру); 2. Уочавање инцидента; 3. Инцијални одговор (утврђивање да је до напада дошло и прикупљање непостојаних података); 4. Формулисање стратегије за реаговање на напад (на основу познатих чињеница); 5. Стварање дупликата (бекапа) система; 6. Преглед система (да би се дошло до одговара на питање: Ко? Шта? и Како?); 7. Примена безбедносних мера (изоловање система и сигурносно паковање); 8. Надгледање мреже (како би се уочили евентуални нови напади); 9. Опоравак система у изворно стање (пре напада) уз уградњу нових безбедносних мера; 10. Извешатај о предузетим корацима у оквиру реаговања на напад; 11. Процена целог процеса реаговања. C. Prosise, K. Mandia, *Incident Response: Investigating Computer Crime*, McGraw Hill Osborne Media, 2001, 153.

[726] Прва фаза јесте идентификација у оквиру које се предузимају следећи задаци: уочавање, надгледање и анализа система. Овој фази следи фаза обезбеђења, како би се осигурао прихватљив *chain of custody,* а који је одређен као битна фаза, како се прикупљени рачунарски подаци не би накнадно прогласили као незаконити докази. Затим следи фаза прикупљања релевантних рачунарских података употребом одговарајућих делотворних техника, након које следе две

употребу, као и а**пстрактни модел** који се на њега ослања[727]. Овај модел пружа конзистентан и стандардизован начин поступања, који тиме што је у довољној мери уопштен није везан за степен развијености технологије, а истовремено се истиче нужност коришћења специфичних алата и техника за потребе конкретног случаја. Ипак, проблем у вези са овим моделом је што предвиђа да би фаза припреме требало да претходи уочавању инцидента како би увиђајна екипа могла да буде спремна са опремом и људством пре изласка на лице места (што није део процедуре поступања). Такође, недовољно се наглашава разлика између прегледа система и анализе дигиталних доказа.

Претходно поменути модели имају своје недостатке и потребно их је било допунити традиционалним правилима која се односе на обезбеђење физичког лица места и поступање кроз фазе (вербално-информативна, статичка, динамичка), уз поштовање захтева темељног документовања лица места, предузетих радњи и предмета који се након обраде изузимају са лица места и преносе у лабораорију ради даље анализе. Ова правила су узета у обзир у оквиру **интегрисаног модела** за процедуру на лицу места. Полазећи од тога да је рачунар доказ сам по себи, али истовремено дигитално лице места секунадрно у односу на физичко лице места, предвиђа се примена традиционалних правила прилагођених потребама и специфичностима виртуелног окружења[728]. На поставкама

кључне фазе, а то су фаза прегледа и фаза анализе прикупљених података. У оквиру ове две фазе се предузимају следећи задаци: уочавање електронских доказа, њихова валидација, опоровак сакривених/избрисаних података, *data mining* итд. Последња је фаза представљања резулатата претходних фаза: састављање налаза и мишљења, те исказ вештака и сл. G. Palmer, (2001) "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research", Digital Forensics Workshop (DFRWS), Utica, New York. Овај модел је значајан, јер га је Министарство правде САД употребило као основ за припрему водича за поступање са електронским доказима (U.S. Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf).

[727] Овај модел предвиђа следеће фазе: 1. Уочавање инцидента; 2. Припрема (опреме, техника, добијање потребних сагласности); 3. Развијање стратегије приступа чија примена омогућава максимизирање прикупљања доказа и минимизира утицај оштећења; 4. Изоловање и обезбеђење материјалних и дигиталних доказа; 5. Прикупљање материјалних доказа и прављење копије дигиталних доказа; 6. Преглед ради проналаска релевантних доказа; 7. Анализа релевантних дигиталних доказа и потврђивање иницијално постављених верзија догађаја; 8. Састављање извештаја о резултатима анализе; 9. Враћање одузетих предмета. M. Reith, C. Carr, G. Gunsch, „An Examination of Digital Forensic Models“, *International Journal of Digital Evidence* 3/2002, 6.

[728] B. Carrier, „Spafford E., Getting Physical with the Digital Investigation Process“, *International Journal of Digital Evidence*, 2/2003, стр.6-12. Предвиђено је 17 радњи које су груписане у 5 фаза: 1. Припремна фаза; 2. Фаза обавештења; 3. Фаза обраде физичког лица места; 4. Фаза обраде виртуелног лица места; 5. Фаза извештаја. Припремна фаза је основна специфичност овог модела и има за циљ да се створе предуслови оперативне и инфраструктурне спремности органа за суочавање са проблемима прикупљања дигиталних доказа, а у оквиру ње се издвајају две фазе: 1.

интегрисаног модела створен је тзв. **ојачани модел** поступања на дигиталном лицу места, који у односу на претходно анализиране моделе уводи нову фазу: улажење у траг ради проналаска везе са уређајем помоћу ког је радња дела предузета[729]. Поменути модели као недостатак имају то што се концентришу само на поступање са електронским доказима (са акцентом на прикупљање или анализу), а недовољно пажње је посвећено питању *chain of custody,* односно утврђивању и описивању токова информација, чиме се обезбеђује аутентичност прикупљених доказа. У том смислу значајан је **проширени модел**[730] који

Обезбеђење оперативне спремности (подразумева обуку и опремање особља надлежног органа тако да се обезбеди њихова способност правовременог и одговарајућег реаговања по сазнању да је учињено кривично дело); 2. Обезбеђење инфраструктурне спремности (подразумева постојање потребних података у окружењу које може бити објект напада кривичног дела - то може бити постављање видео камера или читача картица који могу регистровати догађаје у време извршења дела или слање логова са сервера на обезбеђени сервер или подешавање интерних сатова и слично). Оперативна и инфраструктурна спремност се може означити као форензичка спремност, а подразумева способност надлежних органа да је што више могуће повећају свој потенцијал за прикупљање и коришћење електронских доказа, уз што мање трошкова предузимања радњи прикпљања и анализе истих. Уз критеријум што мање трошкова требало би додати критеријум и „за што мање времена", јер време и трошкови јесу детерминанте ефикасности неког поступка. О томе како се обезбеђује форензичка спремност, R. Rowlingson, „A Ten Step Process for Forensic Readiness", *International Journal of Digital Evidence* 3/2004, 1-28.

[729] Тзв. *Enhanced Digital Investigation Process Model: EDIP.* Наиме, након припремне фазе (која је на исти начин обрађена као у претходно приказаном моделу) следи фаза која представља механизам за потврђивање да ли је дошло до напада на систем, и састоји се из следећих задатака: откривање и пријављивање инцидента; посматрање физичког лица места; посматрање дигиталног лица места; потврда да се ради о кривичном делу и предствљање резултата предузетих радњи надлежним органима. Следи фаза у којој се предузимају радње како би се ушло у траг и пронашла директна веза са уређајем и локацијом уређаја којим је извршења радња кривичног дела. У оквиру ове фазе се предузимају два задатака: преглед уређаја који је објект напада и ауторизација (односно, добијање одобрења/овлашћења) ради обраде података. Следи динамичка фаза, у оквиру које се спроводи преглед физичког и дигиталног лица места (активни приступ за ралику од пасивног приступа лицу места у оквиру друге фазе) те реконструкција догађаја. Завршна је фаза заправо и почетна фаза, јер је цео модел замишљен као циклус задатака који се понављају иуз могућност уласка у наредну и враћања у претходну фазуV. Baryamereeba & F. Tushabe, (2004) "The Enhanced Digital Investigation Process Model", in Proceeding of Digital Forensic Research Workshop, Baltimore, MD.

[730] Тзв. *Extended Model of Cybercrime Investigation* предвиђа тринаест фаза у обради случаја: 1. Сазнање да је извршено дело и утврђивање потребе за предузимањем радњи и мера; 2. Ауторизација (добијање потребног формалног одобрења за предузимање радњи и мера); 3. Планирање (на основу постојећих података, а у границама општег правног оквира); 4. Обавештавање одређених лица о намери предузимања радњи мера (са изузетком осумњиченог лица); 5. Претрага ради уочавања електронских доказа; 6. Прикупљање електронских доказа ради чувања и анализе; 7. Превоз доказа; 8. Складиштење електронских доказа; 9. Преглед прикупљених електронских доказа употребом одговарајућих техника; 10. Постављање хипотезе у записнику о спроведним активностима; 11. Представљање хипотезе ради провере; 12. Потврђивање/оповргавање хипотезе; 13. Чување и управљање информацијама о резултатима активности (стварање базе података ради праћења примера добре праксе). Овај модел постављен је у форми „водопада" (каскадно организован), па иако предвиђене фазе следе једна другу, уколико резултати наредне фазе захтевају преиспитивање резултата претходне фазе или поновно предузимање радњи у тој фази, овај модел то омогућава и подстиче (нарочито у вези са

идентификује активности које се предузимају у оквиру истражног процеса, али и токове информација у вези са предузимањем тих активности.

Већина приказаних модела подразумева да се врши најпре форензичка обрада рачунарских података на лицу места (планирање, идентификација, обезбеђење и прикупљање). Но, како активности које се предузимају на лицу места захтевају доста времена с обзиром на велики обим података које треба прегледати, уобичајено поступање је да се ствара се клон рачунарског система или форензичка копија укладиштених података и да се тако изузети подаци се потом преносе ради даље обраду у одговарајуће лабораторије (ради подробнијег прегледа и анализе и састављања одговарајућих извештаја о резултатима анализе). Овакав метод је прихватљив када се не ради о критичним ситуацијама (изузетно хитним случајевима) у којима је потребно промптно реаговање ради добијања релевантних информација (не доказа!), па је предложен модел који се заснива на одабиру података који се обрађују на лицу места - тзв. **модел тријаже података на лицу места**[731]. Применом технике тријаже на лицу места одступа се од основих принципа поступања са електронским доказима и не пружа се довољно гаранције да се у конкретним случајевима на адекватан начин обезбеђује обрада свих релевантих података, па би се евентуално овај модел оправдано могао применити у изузетно хитним случајевима, но остаје отворено питање на основу чега се одређује које су то околности.

Интересантан приступ дат је у виду **трослојног модела**[732], али који је прилично апстрактан и у оквиру фаза не предвиђа конкретније активности, па је

постављањем хипотеза и њеним потврђивањем или оповргавањем). Значајна карактеристика овог моделе је инсистирање на протоку информација кроз предузимање активности у оквиру појединих фаза. Као недостатак се може навести то што се фазе које се односе на хипотезе беспотребно раздвојене, јер се у суштини предузимају у оквиру анализе доказа и изношења закључака. S. Ciardhuáin, „An Extended Model of Cybercrime Investigations“, *International Journal of Digital Evidence* 1/2004/, 6.

[731] Тзв. *Computer Forensics Field Triage Process Model: CFFTPM*. Модел се заснива се на *in situ* приступу идентификацији, анализи и интерпретацији дигиталних доказа у релативно кратком временском оквиру без потребе стварања форензичке копије уређаја или упућивања уређаја у лабораторију на подробнију анализу. M. K. Rogers Et al,“Computer Forensic Field Triage Process Model”, *Conference on Digital Forensics, Security and Law*, 2006, 31.

[732] Три су фазе у оквиру овог модела: 1. Проактивна фаза (подразумева спремност која треба да обезбеди промптно прикупљање доказа уз што мање трошкова, у што краћим временским оквирима); 2. Активна фаза (подразумева прикупљање непостојаних података у „живом“ систему – тзв. "*live forensics*"); 3. Реактивна фаза (подразумева идентификацију, екстраховање, анализу и тумачење доказа ускладиштених у уређају у лабораторијским условима - тзв. "*dead forensics*"). G.

непримењив у пракси без потребне операционализације. Вредан помена је и **тзв. генерични модел** који предвиђа постојање пет фаза у оквиру којих су категоризовани задаци заједнички за све претходно анализиране моделе[733]. За разлику од већине приказаних модела у којима фазе линерано следе једна другу, **модел анализе извршења кривичног дела** обухвата осам фаза које се циклично понављају, при чему је модел усредсређен на активности планирања дигиталне истраге[734]. На основу упоређивања постојећих модела и анализе жељених резулата фаза у оквиру тих модела, настао је и тзв. **компаративни модел**[735], који представља солидну синтезу добрих решења.

Louwrens, S. H.Von Solms, "A Multi-component View of Digital Forensics," in: Availability, Reliability, and Security, ARES '10 International Conference on, 2010, 647.

[733] Тзв. *Generic Computer Forensic Investigation Model: GCFIM*. Предвиђене су следеће фазе: 1. Претходна фаза, у оквиру које се предузимају све активности које претходе отпочињању рада на обради рачунарских података на лицу места (прибављање потребних одобрења, припрема алата који ће се користити и сл.); 2. Фаза прикупљања и обезбеђења доказа, у оквиру које се идентификују релевантни извори података, изузимају, сигурно складиште и превозе до лабораторије; 3. Фаза анализе, која је средиште рада са рачунарским подацима да би се дошло до електронских доказа потребних за идентификовање учиниоца кривичног дела; 4. Фаза презентације, у оквиру које се документују налази из претходно предузете фазе за потребе кривичног поступка; 5. Накнадна фаза, као својеврсна евалуација предузетих активности у вези са обрадом конкретног случаја. Y. Yusoff, R. Ismail, Z. Hassan, „Common phases of computer forensics investigation models“, *International Journal of Computer Science & Information Technology* 3/2011, 29.

[734] Тзв. *Cybercrime Execution Stack* модел. Ради се о следећим фазама: покретање истраге, која има циљ да се идентификују почетна сазнања; логичко моделовање, довођење у везу кључних фактора понашања учиниоца, коришћене технологије и техничких последица дела; процена утврђених фактора; уочавање и процена утицаја и ризика од поновног вршења дела; планирање истражних активности; прелиминарни технички преглед ради утврђивања потребне опреме и алата; предузимање радњи и мера надлежних органа; састављање извештаја о резултатима истраге. P. Hunton, “A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment”, *Digital Investigation* 7/2011, 106; P. Hunton, „The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model“, *Computer Law & Security Report* 25/2009, 530.

[735] Тзв. *Comparative Digital Forensic Model*. Превиђа постојање пет фаза: 1. Фаза постављања основа: након добијања потребних одобрења од надлежних органа за предузимање радњи на лицу места, прикупљају се релевантни подаци о рачунарској инфраструктури, како би се припремила потребна опрема и алати и направила стратегија поступања на лицу места; 2. Прикупљање доказа: након идентификовања уређаја који су потенцијални извори дигиталних доказа, предузимају се радње које имају за циљ обезбеђење интегритета доказа и њихову аутентичност и стварање форензичке копије уређаја; 3. Преглед и анализа уређаја (физичког предмета) ради одабира одговарајуће технике за екстраховања релевантних електронских доказа, након чега се ствара потребна документација о извршеном прегледу и анализама; 4. Презентовање документације (која је настала окончањем претходне фазе) на суду; 5. Фаза у којој се анализира рад на случају како би се дошло до закључка о правилно предузетим корацима и унапредио постојећи корпус знања за потребе рада на будућим случајевима. D. Kalbande, N. Jain,” Comparative digital forensic model”, *International Journal of Innovative Research in Science, Engineering and Technology* 8/ 2013, 3415.

3.2. Фазе дигиталне истраге

Узимајући у обзир све напред наведено, долазимо до закључка да је за стварање доброг модела дигиталне истраге који би био примењив у пракси и који би резултирао поузданим и релевантним електрнским доказима, потребно водити водити рачуна о следећем: 1. Предвидети *поступање кроз фазе* (као код увиђаја); 2. Поставити модел тако да буде *довољно уопштен и технички неутралан*, да би се могао примењивати без обзира на промене у стању техничких производа и процедура; 3. Истовремено, модел треба да буде у *довољној мери одређен*, како би се развили општи технички предуслови за сваку фазу; 4. Модел треба да допринесе решавању недоумица техничке терминологије, дефинисању захтева и подржавању развоја нових техника и алата за форензичаре [736]. Водећи рачуна о свему наведеном, и комбинујући добра решења у постојећим моделима, предлажемо стварање једног свеобухватног, али уопштеног модела. **Предложени модел дигиталне истраге** обухватао би следеће **фазе**:

I. Припремна фаза;

II. Обрада физичког лица места;

III. Обрада дигиталног лица места;

IV. Фаза анализе;

V. Представљање електронских доказа на суду.

Овакав модел је у довољној мери уопштен, и употребљен је као основа за приказ појединачних радњи које се предузимају у оквиру фаза поступања са рачунарским подацима који се у кривичном поступку могу појавити као електронски доказ[737].

[736] Више о условима које би требало да задовољи механизам који би регулисао дигиталну истрагу, P. Hunton, „Cybercrime and security: A new model of Law enforcement“, *Investigation* 4/2010, 388-389.

[737] За приказ и објашњење појединих задатака који се предузимају у оквиру фаза коришћени су стандарди добре праксе садржани у следећим публикацијама (Council of Europe, *Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges*, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp; Association of Chief Police Officers, *Good Practice Guide for Computer-Based electronic Evidence* , 2012, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf; ITU, *Understanding cybercrime: phenomena , challenges and legal response*, 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf; Good Practice Guide for Computer-Based Electronic Evidence, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf; U.S. Department of Justice, Office of Justice Programs National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf; ACPO,

3.2.1. Припремна фаза

Припремна фаза има за циљ да се, од момента сазнања да је учињено кривично дело, прикупи довољно информација за планирање и припрему активности (односно, мера и радњи), што подразумева стварање потребних техничких предуслова и добијање потребних сагласности за приступ лицу места, односно обезбеђење правног основа за предузимање потребних радњи које доводе до одузимања опреме или изузимање података (у оквиру увиђаја или претресања). Пажљиво спроведена припремна фаза је од великог значаја јер се на тај начин могу избећи потешкоће на лицу места[738].

По сазнању за конкретан случај, након почетне процене на основу расположивих података и информација[739], требало би размотрити следећа питања:

Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.npcc.police.uk/*;* ITU, *Toolkit For Cybercrime Legislation*, 2011, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf; Network Working Group, *Guidelines for Evidence Collection and Archiving*, 2002, http://www.faqs.org/rfcs/rfc3227.html; *Packaging, Transportation, and Storage of Digital Evidence*, 2010, *http://www.dfinews.com/article/packaging-transportation-and-storage-digital-evidence; Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs*, 2005, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf; *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community*, 2006, http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf, CERT Training and Education Handbook, *First Responders Guide to Computer Forensics*, 2005, http://www.sei.cmu.edu/reports/05hb001.pdf). Наведене публикације мање-више предвиђају иста, односно слична решења, а одступања и специфичности су на одговарајућим местима поткрепљени коментарима у посебно наведеним научним и стручним радовима.

[738] Припремна фаза одговара оријентационо-информативној фази увиђаја, која обухвата активности које претходе увиђају и које служе да се прибаве информације, односно створе услови за вршење увиђаја. Радње које се предузимају имају информативни, организационо-припремни или оријентациони карактер. Тако се прикупљају релевантне информације од екипе које је обезбеђивала лице места и од очевидаца (информативни), предузимају се припремне радње и организује се спровођење увиђаја (организационо-припремни), те се установљава положај лица места које ће бити обухваћено увиђајем (оријентациони). Б. Симоновић, Криминалистика, Крагујевац 2004, 674.

[739] Корисно је прикупити следеће податке: 1. Уобичајени подаци о случају (ко су осумњичени, која кривична дела се истражују, *modus operandi* итд.); 2. На који начин су рачунари и други електронски уређаји коришћени; 3. Техничка софистицираност извршиоца; 4. Како се уочени дигитални трагови доводе у везу са осумњиченим; 5. Врста (стамбене или пословне просторије и сл.), величина и друге карактеристике физичког окружења које је лице места; 6. Потенцијални физички и електронски уређаји за складиштење дигиталних доказа и њихова локација (физичка или мрежна); 7. Тип и величина електронских уређаја који се одузимају; 8. Оперативни систем, примењени софтвери и мрежно окружење; 9. Ризик од уништења дигиталних уређаја, и сл. Наведено према: Barbara, *op.cit*, 67.

Шта је основ за предузимање радњи, односно да ли постоји одговарајуће овлашћење?

Прво што треба узети у обзир јесте да ли су органи овлашћени за предузимање радње. Ниједна радња која се односи на одузимање уређаја и података не би се смела предузети без одговарајуће ауторизације, а овлашћење може бити у различитим формама. Најједноставнији од њих је када сагласност да лице које има у поседу/под контролом уређаје, опрему и/или податке којима треба приступити. Ту сагласност би требало увек обезбедити у писаној форми, а да при томе лице, које даје сагласност, разуме последице давања такве сагласности, иако се свакако решења у националним законодавствима морају узети у обзир. За орган поступка који предузима ове радње потребно је одобрење у виду наредбе суда или јавног тужиоца[740]. Међутим, поставља се питање који ниво ауторизације је потребан у случају да су процесним законодавством за предузимање одређене радње овлашћени и адвокати као браниоци, односно оштећени и приватни тужилац (и адвокати као пуномоћмици ових лица), као и које активности је потребно предузети када се планира одузимање потенцијалних извора електронских доказа из просторија које су у поседу осумњиченог.

Где су ускладиштени потребни подаци?

Није неуобичајено да се потребни подаци налазе на другом месту у односу на локацију на којој се налази опрема, па је то потребно узети у обзир из два разлога: прво, приступ подацима може захтевати додатну ауторизацију, посебно у случају ако су похрањени у систему који је у надлежности других органа (па и другој држави), и друго, могу бити потребни и додатни технички услови да би се одржао интегритет тих података.

Колико је софистициран осумњичени?

Потребно је прикупити што више информација о осумњиченом лицу и његовим способностима, односно да ли је применио одређене техничке процедуре које могу да утичу на одузимање опреме или података, како би се предупредили негативни утицаји тих техника на лицу места уколико се сумња, на пример, да је

[740] То је, примера ради, следеће питање: да ли је потребна наредба за претрес или је могуће извршити радње без икакве ауторизације од стране овлашћених надлежних органа, при чему је мало вероватно да је основ за вршење претреса позив у помоћ или непосредна опасност по живот. Међутим, претресу се може приступити уколико би постојало одобрење лица које је корисник система. Easttom, Taylor, *op.cit*, 228-229.

уређаје за складиштење података енкриптовао или инсталирао наредбу за брисање свих података са рачунара или похранио податке у *online* сервисима за складиштење података, тако да уопште нема података који се чувају на уређајима и опреми који се могу наћи на лицу места.

Да ли постоје алтернативни извори за прикупљање тих потребних рачунарских података?

Пре предузимања активности које подразумевају директан контакт са осумњиченим и заплену његове опреме и похрањених рачунарских података, у фази планирања треба размотрити могућност постојања и других извора из којих се подаци могу добити, на пример, од друге стране у одређеној *online* трансакцији, као што је лице са којим је остварена комуникација електронском поштом или пружалац услуга електронских комуникација.

Да ли податке одузети од осумњиченог или прибавити из алтернативних извора, односно од треће стране?

У појединим законодавствима је пружалац, у овом случају трећа страна, дужан да обавести корисника услуге о свим захтевима за приступ подацима који се на њега односе, што може представљати упозорење за осумњиченог. Такође, треба узети у обзир и то да ли законска процедура за добијање података од треће стране, нарочито ако се налазе у иностранству, може и у којој мери утицати на ефикасност истраге. Осим тога, потребно је поставити питање, да ли одлагање директног контакта са осумњиченим може негативно утицати на истрагу.

По разматрању наведених питања, може се *приступити стварању плана за поступање*, што подразумева доношење одлуке кога повести и шта понети на лице места, односно утврдити која знања и вештине (људски ресурси) и која опрема (технички ресурси) су потребни за предузимање радњи првог захвата.

Људски ресурси: добра припрема и планирање имају за циљ одређивања потребног степена подршке на лицу места, уколико се претпоставља да се могу пронаћи електронски докази, у ком случају је потребно обезбедити присуство лица специјализованог за руковање електронским доказима[741]. Да ли је то лице у

[741] *Association of Chief Police Officers: Good Practice Guide for Computer-Based electronic Evidence* , 2012, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf , 22. Исто, Good Practice Guide for Computer-Based Electronic Evidence, *http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf*, 44.

локалној полицијској јединици или централној специјализованој јединици или помоћном форензичком центру, зависи од организације полиције у одређеној држави. Полазећи од улога које остварују при обради лица места, може се уочити неколико категорија лица: а) вођа случаја, који надгледа активности на лицу места; б) тим за лишење слободе; в) тим за обезбеђење лица места; г) тим за вођење информативног разговора; д) тим за скицирање и фотографисање лица места; ђ) тим за физички преглед лица места; е) тим за изузимање трагова и одузимање предмета са лица места[742]. У ситуацијима када постоје сазнања да се на лицу места налазе рачунари, односно када се наиђе на њих, сматрамо да је потребно да извшриоци наведених задатака поседују минимална знања дигиталне форензике, док су за обављање послова изузимања трагова и одузимање предмета са лица места неопходна посебна знања и вештине, па ове задатке треба да обављавају лица која су посебно обучена у области дигиталне форензике (форензичари) или пак лица криминалистичке полиције која макар у основи познају правила поступања са рачунарским подацима и уређајима за електронску обраду података.

Проблеми са којима се сусреће полиција приликом поступања у вези са електронским доказима захтевају ангажовање лица са специјализованим техничким знањем и вештинама и одговарајући процедурални оквир. Комплексност прикупљања и презентовања електронских доказа на суду учиниће у великом броју случајева нужним присуство вештака, чији задатак се састоји у томе да суду пружи објашњења, с обзиром на то да је готово све у вези са електронским доказима тешко схватљиво за лаика. У том смислу, вештак се овде јавља у улози интерпретатора података који су прикупљени, објашљавајући поставке електронског уређаја из ког су подаци прикупљени, дајући осим приказа чињеница (налаз) и мишљење и тумачења из материје за коју је стручњак. Ко је лице које се пред судом јавља у улози вештака? По логици ствари, то ће бити стручно лице које је у раним фазама поступка било позвано да полицији и тужилаштву пружи помоћ у прикупљању и анализи података. Један од проблема у вези са стручњацима у пољу рачунарства и информационих технологија је широк дијапазон уређаја, система и апликација који могу бити релевентни за конкретан

[742] Britz, *op. cit*, 309-310.

предмет, а који захтевају понаособ специфична знања и вештине[743]. Може се стога десити да је на једном компликованом случају потребно ангажовати више стручњака. Технолошки развој у области рачунарства је толико убрзан да знања, уколико се константно не унапређују, врло брзо постају застарела и некорисна. Када полиција или јавни тужилац процене да је у току истраге потребно присуство специјалисте дигиталне форензике, јер је, примера ради, неопходно посебно знање за одређени оперативни систем или Интернет апликацију, кључно питање у избору тог лица је да ли поседује потребна знање или искуства да да своје мишљење о одређеним питањима, а уз ово треба указати на то да непоседовање минималних знања у области дигиталне форензике, лицу који одређује ког стручњака је потребно ангажовати у конкретном случају, може отежати процену да ли су знања одговарајућа и довољна за конкретан случај[744]. Стога су правовремене консултације између полиције, јавног тужиоца и форензичара од суштинског значаја за успешну истрагу и кривично гоњење, како у погледу тога да полиција и тужиоци треба да дају јасне инструкције, тако и да упознају стручно лице са потребним детаљима.

Технички ресурси: с обзиром на то да се веома велики број техника и метода може применити за извршење кривичног дела, ни откривање дела и прикупљање доказа није могуће применом само једног алата. Стога је у припремној фази корисно, на основу расположивих података о околностима случаја, припремити одговарајући форензички алат, потребна одобрења и формуларе за састављање записника о предузетим радњама, средства за безбедно паковање предмета

[743] Примера ради, стручњак за *Unix* систем можда неће бити подобан да пружи одговарајућу професионалну подршку у погледу *IP* протокола и мрежа.

[744] Приликом избора „спољног консултанта“ - форензичара, нарочито у компликованим случајевима када је потребно уже специјализовано техничко знање, потребно је водити рачуна да ли лице поседује одговарајуће: *техничко знање* (вештине, односно компетентност да обавља одређене послове, а обухвата следеће: релевантну квалификованост, вештине за обављање одређеног посла, специфична знања које лице поседује, да ли се вештина заснива на техничким квалификацијама или на временском искуству (или комбинацији оба); *искуство* (врста послова у којима је стечено искуство, број и врста случајева у којим је био ангажован, временски период у ком се лице бави овим активностима, да ли постоји доказ о поседовању искуства); *познавање прописа* (нарочито них који уређују предистражни поступак и истрагу, нарочито да би био свестан потребе поверљивости истраге и разликовање између информација, индиција и доказа, те поступак пред судом, улози и одговорностима у кривичном поступку); *одговарајуће комуникационе вештине* (да уме да објасни јасним и разумљивим терминима природу специјалности, методе тумачења, слабости и предности одређених доказа и да да алтернативно објашњење).

(материјалних доказа) и уређаје за тонско и видео снимање тока активности на лицу места[745].

Одговарајући форензички алат за прикупљање и анализу рачунарских података подразумева разне софтверске апликације, хардверски уређаје и уређаје за складиштење података. Основна опрема стручњака дигиталне форензике подразумева: уређај са оперативним системом (за потребе стварања бекапа, манипулисање хард диском и слично), односно лаптоп рачунар са стандардним форензичким алатима (а то су најчешће: софтвер за опоравак података (*data recovery*), који се користи уколико су подаци избрисани), софтвер за преглед датотека и комерцијалне заштитне зидове (*firewall*, који се користи за *network sniffing* и *port scanning*), мрежни каблови, као и хард диск довољног капацитета за складиштење података (на пример, екстерни хард диск са више терабајта меморије).

При томе увек пажњу треба посветити и правним оквирима за предузимање радње, па је потребно припремити одговарајуће исправе, којим се потврђује постојање ауторизације за предузимање радње (одговарајуће наредбе/налоге). Употребом алата се може постићи много тога у техничком смислу, али уколико то не буде у складу са прописима, резултат су незаконити докази, односно резултати који се не могу прихватити као доказ. Стога би приликом одабира алата, требало да водити рачуна о следећем: да ли постоје ограничења, односно сметње у прописима да се алат користи, да ли се применом алата може обезбедити интегритет података који се обрађују и да ли се употребом алата може у поновљеној (контролној) обради доћи до истих резултата.

[745] Ради документовања предмета и трагова, паковање и транспорт одузетих предмета, потребно је понети етикете и траке (за означавање и идентификацију саставних делова система), траке за одвајање каблова и друге потребне образце потребне за поступање на лицу места, као и камеру и/или видео камеру (за фотографисање лица места), антистатичке кесе за заштиту опреме, везице (за обезбеђивање каблова), вреће за доказе и траке, кутије за паковање спољних уређаја за складиштење података (као што су *USB* уређаји, DVD или CD), материјал за паковање (материјале који могу да произведу статички електрицитет, као што је стиропор треба избегавати), картонске кутије за пренос опреме различитих величина (требало би користити оригинално паковање кад год је доступно).

3.2.2. Обрада физичког лица места

Обрада физичког лица места има за циљ прикупљање и анализу предмета и трагова који могу бити материјални докази и реконструкцију следа догађаја приликом извршења радње кривичног дела[746]. Ради остварења тог циља, потребно је предузети следеће мере и радње: 1. Обезбеђење лица места; 2. Регистровање затеченог стања лица места, предмета и трагова; 3. Преглед лица места ради уочавања предмета и трагова; 4. Обезбеђење предмета и трагова[747]; и 5. Изузимање предмета и трагова са лица места, паковање и транспорт у лабораторију ради анализе.

У вези са предузимањем свих ових радњи, пажњу је нужно посветити прикупљању података и информација од појединих лица**,** те записнички или у белешци фиксирати изјаве присутних лица, а нарочито је корисно обавити информативни разговор са корисницима[748] и администратором система[749] (*вербално-информативна фаза*).

На лицу места је потребно осигурати безбедност свих присутних лица и интегритет доказа, како традиционалних, тако и електронских. При томе је од

---

[746] Више о општим криминалистичко-тактичким правилима за спровођење увиђаја, Ж. Алексић, М. Шкулић, *Криминалистика*, Досије, Београд 2002,68-75.

[747] Прва четира корака одговарају сттаичкој фази увиђаја. У статичкој фази не уносе се никакве промене на лицу места, него се оно посматра у непромењеном стању - трагови и предмети се не додирују, не померају и не мења се њихов изглед и међусобни положај. Наиме, у оквиру ове фазе врши се преглед и описивање лица места и сачињавање белешки или тонског записа, анализа чињеничног стања и мисаона реконструкција кривичног дела, обележавање трагова и предмета кривичног дела применом бројчаних ознака, утврђивање међусобног односа трагова и предмета, скицирање и фотографисање лица чињеничног стања. Симоновић, *op.cit,* 301.

[748]Из информативног разговора са корисницима се могу сазнати, примера ради, следеће информације: у које сврхе се користи одређени уређај/систем; ко је власник/држалац/корисник уређаја/система; које су лозинке за приступ систему, софтверу или подацима, које су лозинке и корисничка имена за приступ налозима (при чему се поставља питање да ли је лице који је осумњичено може принудити да открије лозинку с обзиром на постојање привилегије од самооинкриминације); где се налазе спољни уређаји за складиштење података, приручници за рад уређаја/опреме као и друге релевантне информације.

[749] Из информативног разговора са администртаором се могу сазнати, примера ради, следеће информације: која лица су била регистрована у систему у последња 24 часа; које лице је последње приступило систему; да ли наведена лица уобичајено раде ноћу и прековремено; које су радни шаблони тих лица; када се инцидент десио; шта се појавило на монитору рачунара; када је последњи пут урађен *back up* система; да ли су уочена неуобичајена дешавања у мрежи у последње време; које програме је користио компромитовани рачунар; који ниво приступа мрежи имају поједини корисници; који је ниво познавања рачунарског система и мреже код појединих корисника; ко, на који начин и када је пријавио инцидент; како изгледа архитектура рачунарске мреже и слично. Наведено према: B. Middleton, *Cybercrime investigator's field guide,* Auerbach Publications, Boca Raton 2005, 6-7.

суштинске важности имати на уму да су рачунарски подаци, потенцијални електронски докази, у рачунарском систему и другим електронским уређајима веома подложни изменама, брисању или губитку.

Из наведених разлога, посебну пажњу треба посветити *обезбеђењу лица места*, што поред уобичајених радњи, подразумева и следеће: одредити границе лица места, при чему је логичко обезбеђење лица места специфичност дигиталне истраге. На пример, у ситуацији када је потребно прикупити податке из „живог" система, потребна је његова изолација од локалне рачунарске мреже, што захтева разумевање комплексних питања архитектуре рачунарске мреже[750]; простору на ком се налазе уређаји и опрема који ће се одузети, односно на коме се претпоставља да се налазе потенцијални докази, потребно је онемогућити приступ свим неовлашћеним лицима (претходно утврдити сва лица затечена на лицу места и документовати њихов положај у тренутку уласка на лице места), при томе, посебну пажњу треба посветити онемогућавању даљинског приступа рачунару, односно мрежи; уклонити осумњиченог уколико је присутан на лицу места, с обзиром на то да постоји ризик да је у систему инсталиран програм за аутоматско брисање похрањених података (тзв. *data-removal/destruction program*)[751].

Након обезбеђења, приступа се *прегледу лица места* којим се утврђује и документује: број и тип рачунара; присуство рачунарске мреже[752]; број и тип преносивих уређаја и опреме за складиштење података који су потенцијални извори електронских доказа, као и коришћење удаљених сервиса за складиштење података (*remote computing*)[753]. С обзиром на то да се чак и најискуснији истражитељи могу сусрети за одређеним типом рачунарског система, мреже или уређаја који је непознаница за њих, у тим ситуацијима корисно тражити помоћ стручњака који су обучени за поступање са таквим системима и мрежама[754]. Исто

[750] Brown, *op.cit*, 6.

[751] Ради се о програмима који су подешени тако да се притиском на један тастер (тзв. *hot key*) покреће процес својеврсног самоуништења система. Наведено према: Moore, *Cybercrime: Investigating High-Technology Computer Crime*, 206. Постоји више таквих програма, а поједини се могу бесплатно преузети са Интернета, а критички преглед постојећих доступан је на: http://pcsupport.about.com/od/toolsofthetrade/tp/free-data-destruction-software.htm.

[752] Cross, Shinder, *op.cit*, 211.

[753] У рачунарској мрежи један рачунарски систем може да контролише датотеке и програме на другом са њим повезаном рачунару преко те мреже. Постоји више техника та контролу приступа, а да би се спречило могуће брисање или оштећење потенцијалних доказа, потребно је уклонити мрежне каблове из рачунара.

[754] Easttom, Taylor, *op.cit*, 235.

тако није препоручљиво прихватати савете нити техничку подршку од било ког лица, које није овлашћено да предузима радње, а које је евентуално присутно на ширем простору[755].

Прегледом лица места се уочавају предмети који не садрже електронске доказе, али могу садржати корисне информације о активностима корисника и функционисању рачунара или бити релевантни за испитивање електронских доказа, и стога имати значај доказа у кривичном поступку. Из тог разлога, од велике важности је пажљиво поступање (уочавање, обезбеђење и чување)[756] са одређеним предметима, као што су: белешке на којима су записане лозинке за приступ одређеним налозима у рачунарском систему и друге писане белешке, приручници за употребу хардвера/софтвера, календари и роковници, одштампани документи, фотографије и слично[757].

Рачунар и други електронски уређаји, пратећа опрема и наведени предмети се обележавају и фиксирају у оквиру *статичке фазе обраде*. При томе, не треба заборавити на традиционалне технике обраде лица места, јер управо проналазак одређених контактних трагова или трагова биолошког порекла може помоћи да се осумњичени повеже са лицем места[758]. Након што је лице места физички и електронски обезбеђено, и што су уочени и фиксирани трагови и предмети, следи изузимање тих трагова, одузимање предмета, односно паковање и транспорт у лабораторију ради анализе, а ове радње се врше у оквиру *динамичке фазе обраде*[759].

---

[755] Britz, *op.cit*, 316.
[756] *COE* водич, 27.
[757] Britz, *op.cit*, 319.
[758] Статичка фаза је успешно обављена уколико се након њеног спровођења добију одговори на, између осталог, следећа питања: који пут је користио извршилац да би дошао до лица места, куда се све кретао по лицу места, време бављења извршиоца на лицу места, само време извршење кривичног дела, средства и начин извршења, тачно место извршења и положај окривљеног, мере припремања дела, обезбеђење од изненађења и препознавања, да ли је на лицу места извшилац оставио трагове који указују на његов идентите, постоје ли остале индиције на лицу места, величина нанете штете, мотив, пут којим се извршилац удаљио са лица места. Види: В. Водинелић, Криминалистика, Београд 1996, 393-395.
[759] Након што се утврди да је потребно неку другу врсту трага изузети са електронског уређаја који ће бити одузети (нпр. трагове папиларних линија) исти се изузимају на одговарајући начин, при чему је пожељно да се избегавају оне технике и процедуре које би могле угрозити итегритет електронских трагова. Тако се препоручује да се латентни трагови папиларних линија на тастаури или мишу изазову и фиксирају након што рачунарски подаци из тих уређаја буду на одговарајући начин изузети (наведено према: *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 31.). Осим тога, треба избегавати алуминијумски прах за изазивање латентних трагова папиларних линија јер може оштетити

Након уочавања рачунарских система, мрежа и других уређаја, приступа се њиховом обезбеђењу[760] и овај моменат заправо означава *почетак обраде дигиталног лица места.* Обрада дигиталног лица места се, дакле, предузима у оквиру динамичке фазе обраде физичког лица места[761].

Сваки корак у току обраде физичког лица места је потребно документовати (редослед, ток и резултате свих радњи које се предузимају) како се не би довела у питање примењена тактика и резултирала недозвољеном употребом тако прикупљених доказа, а што је корисно и у случају да службена лица која су била присутна на лицу места буду позвана у својству сведока да дају исказ на околности примењених процедура. Записник би требало да садржи најмање следеће податке: датум, време и место предузимања радњи и хронолошки приказ корака који су предузети; идентитет лица присутних на лицу места по доласку; идентитет службених лица која су учествовали у обради лица места; опис и локацију свих рачунара и уређаја који су уочени током прегледа, те физички опис уочене опреме (укључујући и евентуална оштећења); присуство и статус мрежних конекција; опис свих других одузетих предмета; детаљан опис лица места као и сваке компоненте рачунараског система поноаособ (стање, те функције које је компонента обављала у тренутку доласка на лице места); хронолошки приказ свих уочених трагова и индиција; датум, време и опис коришћених софтверских и хардверских алата[762]. Уз записник се прилаже и одговарајућа пратећа документација, а нарочито је корисно сачинити скицу листа места и посебно

опрему и проузроковати губитак електронских доказа (наведено према: *ACPO Good Practice Guide for Computer-Based Electronic Evidence*, 2011, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, 12). Док статичка фаза увиђаја има за циљ да се на лицу места трајно фиксира затечено чињенично стање настало извршењем кривичног дела, у динамичкој фазисе могу уносити промене на лицу места: померају се предмети и трагови, врши се њихов детаљан преглед и анализа, па се поједини трагови и предмети се изузимају са лица места. У оквиру ове фазе врше се следеће активности: изузимање предмета и њихово детаљно анализирање, откривање видљивих трагова, те изазивање латентних трагова, фиксирање и паковање трагова и предмета са лица места, обезбеђење материјала за компарацију (узорака и предмета) за додатне анализе и вештачења, обављање ситуационих и других вештачења, реконструкције, криминалистичког експеримента и осталих потребних оперативних и доказних радњи. Више о томе види: Симоновић, *op.cit*, 309- 311.

[760] Обезбеђење се врши нарочито у односу на „електронске“ претње, као што су нпр. *booby-trapped* дрјвови и *remote access*. Britz *op.cit*, 316. Осим тога, могуће се да је функционисање система неопходно за пословање фирме. Тако се у случају нпр. напада на сервер на ком су базе података, обезбеђује систем тако што се привремено сервер дисконектује са мреже, ствара се његов дупликат, који се повезује у мрежу а оригинални уређај се обезбеђује као доказ. Наведено према: Easttom, Taylor, *op.cit*, 235.

[761] Више о томе, следеће поглавље.

[762] Britz, *op.cit*, 317.

скицу рачунарског система да би се уочиле његове компоненте и њихов међусобни полажај. Осим скице, потребно је направити фотографије и/или видео запис лица места као и рачунарског система/уређаја/опреме. Уз фотографије рачунарског система корисно је навести детаље о пронађеној опреми (врста, модел, серијски број), стање и локацију рачунарског система који садржи електронске доказе (укључујући и податак да ли је уређај био укључен или искључен или у *sleep mode*-у). Потребно је документовати фотографски и све конекције са рачунаром и другим уређајима (жичане или бежичне) са пратећом опремом; обележити све портове и каблове (укључујући и конекције са периферним уређајима) да би се омогућило касније поновно спајање (неискоришћене портове означити као такве); документовати детаље који се виде на монитору у тренутку уласка на лице места: фотографисати предњу страну рачунара, монитора и осталих уређаја; описати у записнику и направити видео запис о активним програмима који се приказују на монитору[763].

3.2.3. Обрада дигиталног лица места

Обрада дигиталног лица места је фаза која претходи изузимању предмета који представљају потенцијалне изворе дигиталних доказа са физичког лица места (и заправо представља *обезбеђење ових предмета)* јер иако представљају материјалне доказе, њих треба посматрати *као дигитално, односно виртулено лице места* које се претражује ради проналаска дигиталних доказа. При томе, сваки уређај се посматра као посебно лице места и резултати обраде сваког од њих представљају допуну материјала на основу ког се врши реконструкција у фази обраде физичког лица места.

Одабир које уређаје одузети и које податке из тих уређаја изузети није једноставно, као што се може у први мах чинити. Постоји одређени број фактора који утичу на одлуку да ли треба одузети са лица места све уређаје и транспортовати их у форензичку лабораторију где ће се из њих прикупљати подаци, или те податке изузимати из уређаја на лицу места. У литератури се препознају два приступа: "*tag and bag* " приступ („означи и пакуј"), по ком се

[763] Easttom, Taylor, *op.cit*, 238-240.

физички предмети просто пакују без икаквог прегледа уређаја на лицу места, и „*in situ"* приступ, по ком се применом одређених форензичких техника прегледају уређаји и мреже и изузимају одређени подаци[764].

Стандардна методологија у вези са електронским доказима је током 90-их година подразумевала да се на лицу места рачунар, за који се претпоставља да садржи релевантне податке, искључи из извора напајања, спакује и шаље у лабораторију у којој форензичар прави копију и на њој врши претраге и анализе, о чему саставља записник. С обзиром на т да су рачунарски подаци по својој природи веома склони изменама, оштећењу или губитку, а да би се заштитио и очувао интегритет и поузданост електронског доказа, уређај се безбедно пакује и транспортује ради анализе у лабораторији где се ствара клон уређаја, односно копија бит по бит (*dead box*) на ком се врши даља форензичка обрада.

Како оперативни систем и други програми често аутоматски мењају и додају податке у садржај меморије електронских уређаја (без свести и намере корисника уређаја), да би се захтев аутентичности испоштовао, потребно је направити тзв. клон *целог* уређаја употребом поузданог алата, а *делимично или селективно* копирање би било алтернатива у одређеним околностима, када је, на пример, количина података које је потребно копирати чини копрање практично немогућим (али тада је посебну пажњу посветити настојању да се сви релевантни и потребни подаци обухвате). Ови кораци се предузимају имајући у виду природу електронских доказа и принципе и стандарде у вези са прикупљањем и чувањем рачунарских података, све радње које могу проузроковати измену, оштећење или губитак података могу довести до неприхватања доказа на суду[765]. Традиционална методологија прикупљања електронских доказа се и даље широко примењује у поступању надлежних органа, јер се изузимањем рачунарског система и других уређаја, паковањем и спровођењем форензичког прегледа у каснијој фази, односно у лабораторији обезбеђује интегритет доказа и може се претпоставити да ће ово бити стандард и у наредним годинама.

---

[764] Barbara, *op.cit*, 68.

[765] *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2001, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf. Овај водич је саставио и одобрила Техничка радна група за увиђај лица места за електронски криминал (*Technical Working Group for Electronic Crime Scene Investigation*).

Међутим, временом се појавила потреба за установљањем одређених изузетака од овог правила. У специфичним околностима је понекад неопходно да се одређене радње (преглед уређаја и опреме и екстраховање података) предузму на лицу места, односно у рачунарском систему пре искључивања са мреже или из електронског напајања и транспорта у лабораторију. Дакле, у одређеним случајевима није могуће створити клон уређаја, него је на лицу места нужно приступити оригиналном уређају, да би се из „живог“ рачунарског система прикупљали подаци, јер постоје одређене околности које захтевају испитивање текућих система, и то у све већем броју случајева и из више разлога. Једна од околности се односи на све већу заступљеност малих жичаних или бежичних рачунарских мрежа у стану или пословном простору у ком се налази рачунар који је предмет прегледања. Осим тога, ово правило је у потпуности застерело и с обзиром на све већу заступљеност 1. непостојаних података (*volatile data*) у меморији, 2. даљинског повезивања (*remote connections*) и 3. коришћења софтвера за шифровање, тј. енкрипцију[766] . Како је прикупљање и анализа непостојаних података од битног значаја, јер ти подаци могу имати велику доказну вредност, а њихово прикупљање се не може обезбедити применом традиционалних правила која се односе на паковање и слање уређаја у лабораторију на анализу, потребно је стручно и пажљиво руковање подацима у „живим системима“, па све значајнију улогу добија и тзв. *Live Data Forensics*. Ради се о својеврсном ситуационом вештачењу које захтева виши степен специјализације, па то могу обавити само посебно обучена лица.

Из свега наведеног произлази да се приликом обраде виртуелног лица места предузимају следећи кораци:

1. Обезбеђење виртуелног лица места на самом физичком лицу места, изоловањем рачунарског система од рачунарске мреже;
2. Преглед виртуелног лица места ради уочавања рачунарских података (потенцијалних електронских доказа) који нестају са искључењем рачунара (непостојани подаци) као и сумњивих процеса који су покренути у рачунарском систему;

[766] Више о врстама енкрипције, M. Caloyannides, *Privacy protection and computer forensics*, Artech House, Boston 2004, 193-201.

3. Доношење одлуке да ли се прикупљају подаци на лицу места или се уређај пакује и шаље у лабораторију на даљу обраду:

- Претрага виртуелног лица места ради прикупљања непостојаних података;
- Паковање, транспорт у лабораторију и даља форензичка обрада.

Да бисмо уочене кораке што подробније анализирали, приказаћемо најпре поступање у оквиру традиционалног приступа, а потом указати на специфичности прикупљања података из живог система.

3.2.3.1. Поступање у оквиру традиционалног приступа

Кроз историју дигиталне форензике истраживане су и развијене одговарајуће технике, алати и методи за прикупљање, складиштење и чување података изузетих из рачунарског система, предвиђене у оквиру стандардних оперативних процедура у циљу чувања и обраде електронских доказа, које традиционално подразумевају два корака у обради дигиталног лица места:

- Прикупљање потенцијалних извора електронских доказа, и
- Паковање и транспорт потенцијалних извора електронских доказа у лабораторију ради анализе.

Потенцијалним изворима електронских доказа је потребно руковати пажљиво, као и са другим доказима, на начин да се обезбеди, односно не доведе у питање законитост прикупљања и могућност употребе на суду, што се обезбеђује уколико се води рачуна, не само о физичком интегритету компонената рачунарског система или другог уређаја, него и о интегритету електронских доказа који су у њима садржани. Зато изворе електронских доказа треба прикупити, односно изузети са лица места у складу са одређеним правилима која уважавају специфичности похрањених рачунарских података. Тако, на пример, рачунарски подаци могу бити подложни изменама или оштећењу услед деловања електромагнетног поља (које ствара статички електрицитет, магнети, радио трансмитери и слично) па морају бити заштићени на адекватан начин.

Најпре је потребно утврдити који подаци су доступни и где се они налазе, односно утврдити извор електронских доказа (а то могу бити рачунарски систем,

рачунарске мреже или други електронски уређаји за обраду, пренос и складиштење података), што се чини на темељан начин и уз поштовање околности конкретног случаја, чиме се одређује даљи редослед радњи које треба предузети. Приликом пртраживања простора ради *уочавања* свих компоненти рачунарског система и пратећих уређаја који могу садржати потенцијалне доказе, треба имати на уму да постоји више типова рачунарских система а потенцијални докази се могу пронаћи у датотекама које су ускладиштене у интерној или екстерној меморији (уређајима за спољашње складиштење података). Рачунарски систем не треба одузети с претпоставком да ће у њему бити пронађени електронски докази просто зато што се нашао на лицу места. Одузимању се приступа кад је то оправдано и сразмерно учињеном кривичном делу, односно када овлашћени орган донесе одлуку да се претрес изврши уколико постоји разумни степен сумње или довољно доказа да оправдава отварање истраге.

Након уочавања потенцијалних извора дигиталних доказа, потребно је регистровати положај и повезаност уочених компоненти система, мрежних конекција и других присутних уређаја[767]. По уочавању, *документују се*, односно фотографишу се и скицирају жице, каблови и други уређаји повезани са рачунаром; обележавају се сви извори напајања, каблови и конекције[768], а затим се фотографишу[769]. Прва одлука која се доноси по уочавању и документовању потенцијалног извора електронских доказа јесте на који начин у конкретном случају обезбедити тај извор и потом изузети са физичког лица места.

Један од принципа дигиталне форензике је да се никаква промена не проузрокује на оригиналном уређају који је носилац дигиталних доказа приликом прикупљања са лица места. Међутим, овај захтев, иако оправдан, био је примењив у старијим типовима уређаја за складиштење рачунарских података, док нове технологије онемогућавају задовољење тако стриктног захтева[770]. Повећање броја

[767] Brown, *op.cit*, 59.
[768] *ACPO*, 22.
[769] Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 24.
[770] Када се, примера ради, рукује са *solid-state hard* дисковима, може бити активирана команда „*TRIM*“ моментом када диск буде спојен на напајање, што може проузроковати трајно брисање података. Исто тако, да би се прикупили непостојани подаци, рецимо кључ за енкрипцију, у меморији рачунара потребно је алат за прикупљање података инсталирати у меморији, чиме се неминовно преснимавају неки, до тада, похрањени подаци. Повећана употреба енкрипције целог хард диска (*full disk encryption:FDE*) у модерним рачунарским системима утиче на проналажења

и врста уређаја (и количине података похрањених у њима) које треба обрадити у форензичким лабораторијама довело је до осмишљавања ефикасног приступа који се заснива на стварању приоритета у прегледу уређаја на лицу места уз помоћ формализованог процеса процене и екстраховања циљаних информација - тзв. *техника за тријажни преглед електронског уређаја*[771]. Тријажни преглед уређаја као новија техника дигиталне форензике, дакле, служи да се процени да ли је даља форензичка обрада потребна и по ком редоледу се врши обрада појединих уређаја пронађених на лицу места. Утврђивање приоритета у поступању врши се на основу следећих критеријума: врста/озбиљност конкретног кривичног дела, чињеничне околности случаја, врсте доказа за којим се трага, значај дигиталних доказа за конкретан случај, ризик од непрегледања/ одлагања временског момента почетка прегледања уређаја, и трошкови прегледања уређаја[772]. Ипак, ова техника још увек није шире прихваћена нити у стручној литератури нити у смерницама добре праксе[773], јер није у довољној мери испитано дејство њене примене на аутентичност и интегритет дигиталних доказа.

Прикупљање рачунарског система. Пре предуизмања било које радње на рачунару, проверава се да ли је рачунар укључен или искључен[774]. Уколико се утврди да је рачунар *искључен*, не укључује се, јер покретање система узрокује

техника за омогућавање приступа том рачунару, али има и одређене реперкусије на утврђене стандарде и принципе дигиталне форензике. E. Casey et al, "The growing impact of full disk encryption on digital forensics", *Digital Investigation* 2/2011, 131.

[771] Примена ове технике би била корисна нарочито у форензичкој обради паметних мобилних телефона, R. Mislan, E. Casey, G. Kessler, "The growing need for on-scene triage of mobile devices", *Digital Investigation* 6/2010, 115.

[772] E. Casey, M. Ferraro, L. Nguyen „Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence", *Journal of Forensic Sciences* 6/2009,1359.

[773] Тријажа је предложена у смерницама добре праксе у Великој Британији. Међутим, да ли је ова техника заиста поуздана и прихватљива још увек се процењује од стране националног Програма за електронски криминал. (ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf, 51).

[774] Чињеница да светле лампице или се чују звукови указују да је уређај вероватно укључен, а уколико је на додир топао, уређај је или укључен или недавно искључен. Посматрањем преносивих рачунара и других уређаја се понекад не може са сигурношћу утврдити да ли је укључен, јер не производе никакве звукове, а то што лампице не светле, не значи да је уређај искључен, него је могуће и да је у *standby* или *sleep mode*-у, у ком стању постоји могућност да му корисник приступи са даљине и измени или избрише податке. Такође, постављање одређених *screen saver*-а може навести на погрешан закључак да је уређај искључен. Посматрањем монитора, могуће је на следећи начин утврдити у ком је стању рачунар. Уколико је монитор укључен, препоручљиво је фотографисати и описати шта се на њему може видети. Уколико је монитор укључен а на екрану се не види ништа (рачунар је у *sleep mode*-у) или се види *screen saver,* благим покретима миша на екрану се могу уочити промене па се виде покренуте апликације или се појављује поље које захтева аутентификацију ради дозволе приступа, након чега је корисно фотографисати и описати шта се на њему може видети. Наведено према: *COE,* 50-51.

промене у рачунарским подацима што може резултирати оштећењем или губитком потенцијалних електронских доказа. Укључити угашени рачунар и претраживати хард диск је лоше решење, јер иако ова интеракција делује безопасно, увек проузрокује промене дигиталних доказа (нпр. мења се датум последњег приступа датотеци, што може бити од кључног значаја за конкретан случај)[775]. Из угашеног рачунара се уклањају каблови за напајање (не из утичнице), а из преносивих рачунара и других уређаја уклања се батерија, и региструје се време када је то учињено. Уколико се, пак, *не може утврдити стање рачунара*, претпоставља се да је искључен и поступа се на претходно описани начин. Уколико је рачунар *укључен*, не искључује се, јер одвајање од извора напајања рачунарског система утиче на све покренуте апликације и податке који се тренутно налазе у *RAM* меморији[776]. Доноси се одлука да ли да се врши прикупљање података у „живом" систему или се систем пакује[777]. Доношење одлуке да ли се у конкретном случају приступити одузимању уређаја и опреме, да ли ће се прегледати на лицу места или ће се применити комбинација оба приступа, зависи од околности самог случаја[778]. Уколико се донесе одлука да се врши прикупљање у „живом" систему, предузимају се мере физичке и електронске заштите у погледу непостојаних података (даљи кораци биће приказани у поглављу које следи). По прикупљању непостојаних података, рачунарски систем се гаси[779]. У погледу *начина гашења* рачунара, уобичајени аргумент да се систем гаси извлачењем кабла (*pulling the plug)* је указивање да

[775] Brown, *op.cit*, 57.
[776] Више о врстама меморије, Хајдуковић, Живанов, *op.cit*, 117-121.
[777] *ACPO*, 9.
[778] Међутим, још у фази планирања потребно је прикупити што је више информација могуће у погледу информационог система и потенцијалних извора електронских доказа, и то о: рачунарском хардверу, оперативном систему, софтверу, апликацијама, мрежама и повезаним подацима који се односе на комуникацију; које лице је одговорно за рачунарски систем и/или мрежу (на пример, да ли мрежом управља локални администратор или нека спољни компанија); колико опреме се очекује да буде присутно на лицу места и колико података ће се одузети и слично. Пажљиво планирање и припремање активности које доводе до одузимања опреме могу бити од помоћи да се избегне потешкоће у доношењу одлуке на самом лицу места, јер је за то потребно је проценити најмање следеће: колико времена је потребно да се на лицу места оствари прикупљање потребних података; да ли постоји адекватна логистичка и кадровска подршка у вези са дуготрајнијим боравком на лицу места; на који начин се дуготрајним увиђајем утиче на пословање/нормално одвијање активност; да ли су опрема, средства, обученост и искуство лица погодни за испитивање на лицу места.
[779] Који ће се од приступа применити у конкретном случају зависи, наравно, од околности и ризика које форензичар процењује, јер од његовог избора зависи и на који начин и у којој мери ће бити измењени подаци похрањени у систему пре гашења. Brown, *op.cit*, 54.

постоји могућност да се током уобичајеног *shutdown* процеса покрену деструктивни процеси, уколико је корисник створио и инсталирао код за уклањање података, односно поптуно брисање свега што је на рачунару похрањено, а лице које покуша да угаси рачунар редовним путем не заобиђе „замке“ познате само творцу тог кода[780]. Осим могућности инсталирања апликације која аутоматски уништава све доказе када се систем угаси, постоји могућност да се креира апликација са том наменом али у ситуацији када се изгубе мрежне конекције (тзв. *dead man's switch* апликација). Са друге стране, у прилог уобичајеном *shutdown* процесу је да се на тај начин са већом извесношћу може очувати интегритет система датотека и појединачних датотека[781]. Међутим, поступањем по правилу извлачења кабла избегава се стварање нових података, брисање постојећих и других промена које се дешавају у току уобичајеног *startup* и *shutdown* процеса[782]. Након што се уређај искључи, оставља се да се охлади и затим се *пакује* и шаље на даљу форензичку обраду, односно ради прикупљања података из постојане меморије[783].

Прикупљање компоненти рачунарске мреже. На постојање рачунарске мреже може указати присуство више рачунарских система, те присуство компоненти рачунарске мреже. Приликом разматрања да ли у оквиру мреже постоје информације које могу имати значај доказа и на који начин руковати њима, треба имати у виду да је потребно поступати на потпуно другачији начин у односу на ситуацију када постоји само један рачунарски систем, односно поједини уређаји за пренос, складиштење и обраду података. Наиме, уколико су рачунари умрежени, није једноставно уочити на ком рачунару су похрањене датотеке које се траже, посебно из разлога што ови рачунари деле изворе (као што су штампачи, скенери и конекције са Интернетом). Осим тога, мора се имати на уму да постоји могућност удаљеног приступа рачунару и манипулације подацима

[780] Иако је овакав приступ концептуално валидан, тешко да је остварљив у пракси, јер трајно уништење велике количине података похрањених на магнетном диску захетева одређени временски период услед процеса који већина апликација користе ради трајног и безбедног брисања података. Наиме, када оперативни систем прими наредбу за брисање датотеке, онда се просто уклони назив датотеке из директоријума који је видљив кориснику, док су сектори података још увек присутни на диску. За безбедно уклањање података из хард диска, апликације су написане да записују податке у област диска у ком је претхдони података постојао (да га пребришу).
[781] Moore, *Search and seizure of digital evidence*, 91.
[782] Brown, *op.cit*, 56.
[783] N. Clarke, *Computer forensic*, IT Governance Publishing, London 2010, 28.

који су похрањени у мрежи (*remote access*), што неизоставно треба спречити. Са друге стране, треба имати на уму могућност коришћења услуга за складиштење података у удаљеним серверима (који могу бити и ван територије државе), па се јавља проблем приступа тим садржајима (*cloud computing*[784]).

Најпре се проверавају мрежни уређаји да би се уочило да ли постоје активности мрежног саобраћаја (могуће је користити, нпр. *wireless network detector* да би се утврдило да ли постоји мрежа и да би се детектовали уређаји[785]). Могућа су два сценарија: постоји активни мрежни саобраћај (тада се приступа прикупљању података уз помоћ техника *Live forensics*) или не постоји опасност од губитка података (тада се рачунар дисконектује са мреже). Потом је препоручљиво фотографисати све каблове, конекције и мрежне уређаје, а потом их дисконектовати и паковати[786].

Прикупљање других електронских уређаја. Приликом одузимања рачунарског ситема треба имати на уму да поред основних јединца, систем обично обухавата и додатне компоненте. Наиме, постоје бројни периферни уређаји и сваки од њих је специфичан у погледу функционисања, па то захтева његовим карактеристикама прилагођено руковање на лицу места о чему је потребно водити рачуна[787]. Пажњу је потребно посветити кабловима и портовима (за конекције рачунара са додатним компонентама) али и чињеници да се уређаји са рачунаром могу повезати и бежично[788]. Све конекције (портови и каблови ка и од рачунара) се означавају, фотографски бележе и прави се дијаграм конекција. Све компоненте се означавају и документује се, како затечено стање (фотографише се дисплеј уређаја и бележи шта приказује), тако и све уочене промене на уређајима настале као резултат радњи које су предузете на лицу места. Уколико је уређај укључен, не треба га искључити јер то може активирати

[784] B. Martini, K. Choo, "An integrated conceptual digital forensic framework for cloud computing", *Digital Investigation* 9/2012, 78.

[786] *ACPO*, 15-16.

[787] О специфичностима прикупљања података из појединих периферних уређаја, више о томе, *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*, Syngress, Waltham 2013, 326-343; ACPO Good Practice Guide for Computer-Based Electronic Evidence, 2011, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf, 45-52.

[788] Односно, преко *Bluetooth-a* (нпр. *headsets, PDAs, notebooks, phones, GPS receivers)* или *infrared*-а (*wireless LANs, links between notebooks and PCs, cordless modems, intrusion detectors*). Више о томе, *COE* водич, 55.

механизме за закључавање и немогућност накнадног приступа. Приликом прикупљања уређаја који се напајају на батерију, треба имати на уму лимитирано време трајања те батерије (у неким случајевима мање од 24 часа), а с обзиром на то да се непостојани подаци похрањени у њима губе моментом када се батерија истроши, постоје специфичности обраде ових уређаја, односно након одузимања уређаја је потребно промтно предавање форензичару ради хитне форензичке обраде[789]. Уколико је, пак, уређај искључен, није препоручљиво да се покушава да се укључи, јер и то може проузроковати измену/ уништење доказа[790].

Како се функционисање рачунара и са њим повезаних уређаја и опреме засновано на електронским импулсима, они су осетљиви на промене у температури, влажност, механичко деловање, статички електрицитет, магнетно поље и др[791], и стога је веома важно да се приликом **паковања, транспорта и чувања** потенцијалних извора електронских доказа предузму све потребне мере опреза како би се избегло њихово оштећење или уништење, односно осигурао интегритет електронских доказа садржаних у њима, јер се на тај начин обезбеђује и валидност тих доказа. У англосаксонској литератури се за означавање овог низа радњи (паковање, транспорт и чување*)* користи термин *chain-of-custody* у погледу ког је веома битно да се за сваку од радњи остави документовани траг о поступању са доказима (да би се могло утврдити ко је паковао доказе, ко их је транспортовао, ко их је, на који начин и на ком месту чувао)[792].

Пре *паковања* сви прикупљени уређаји се морају на адекватан начин означити и документовати[793], у складу са његовом природом и околностима конкретног случаја. Кад год је то могуће, уређаји се транспортују у њиховом оригиналном паковању, а у случају да је оно недоступно, уређаји се раздвајају[794] и пакују у

[789] Brown, *op.cit*, 56-57.
[790] *ACPO*, 8.
[791] Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 31.
[792] Инсистира се да за доказе постоји тзв. *Chain of evidence* формулар, који садржи најмање следеће податке о случају (број случаја, додељен као његова идентификациона ознака; име службеног лица које је предузело радњу; природа случаја: кратак чињенични опис), коришћеној опреми (произвођач, продавац, модел и серијски број) и доказима (место на ком је пронађен, датум и време када је у односу на њега примењена одређена радња и име службеног лица који је предузео радњу). Kizza, *op.cit*,354.
[793] *COE*, 2013, 46.
[794] Све конекције и повезани уређаји се означавају на начин који обезбеђује поновну реконструкцију система у лабораторију (наведено према: *Electronic Crime Scene Investigation: A Guide for First Responders*, 31.)

сигурне и чврсте кесе за паковање доказа (одговарајуће спрам типа и величине уређаја) како би се осигурало да уређаји буду заштићени од хладноће, толопте и влаге (зато се користе антистатичка паковања нпр. папирне или антистатичке пластичне кесе[795]), а на начин да се спречи њихово савијање, оштећење или било каква друга деформација[796]. Ако се прикупља више рачунарских система, сваки је потребно посебно упаковати и означити како би се могао у лабораторији поново саставити на исти начин како је пронађен на лицу места. Тако се *wireless* уређаји на батерију (као што су мобилни телефони и *PDA* уређаји) остављају у стању (*on* или *off*) у ком су пронађени[797] и пакују у кесе од материјала који онемогућава дејство радио-фреквентних сигнала рачунарских мрежа (као што су Фарадејове изолационе кесе направљене од материјала који одбија радио-фреквенцију или алуминијумске фолије) како би се спречио пријем/слање података ка/од уређаја и тиме чувао интегритет података у одузетим уређајима, док је на кесама потребно означити који уређај је одузет, датум, време и место одузимања уређаја, као и лице које је одузело уређај[798].

Неколико смерница добре праксе се могу применити на *превоз* изузетих предмета са лица места до лабораторије у којој се прегледају и обрађују, како би се очувао интегритет доказа: приликом транспорта потребно је држати безбедно упаковане електронске уређаје подаље од извора магнетног зрачења, топлоте и влаге, као и од механичких удара (нпр. даље од радиофреквентних уређаја или избегавати држање испод загрејаног седишта и других извора топлоте[799]); изабрати безбедан, поуздан и проверен начин транспорта и лица укључена у транспорт (и све то документовати, нарочито потписом лица која су била укључена у превоз); како се приликом транспорта може довести у питање интегритет садржаја уређаја који се преносе, потребно је применити одговарајуће технике за скривање података (као што су енкрипција, стеганографија, заштита

[795] Обичне пластичне кесе треба избегавати јер производе статички електрицитет или омогућавају стварање влаге или кондензације, што може оштетити или уништити електронске доказе (*Electronic Crime Scene Investigation: A Guide for First Responders*, 32).
[796] *Ibidem*.
[797] *ACPO*, 12.
[798] Watson, Jones, *op.cit*, 344.
[799] *COE*, 47.

употребом лозинки и слично) како би се онемогућило да трећа лица пресретну, измене или модификују податке похрањене на одузетим уређајима[800].

Паковање физичких предмета (електронских уређаја и других материјалних доказа) и рачунарских података који се изузимају са лица места (а који се такође изузимају на одређеном носиоцу података) није довољно да би се сачувао интегритет доказа, него се морају предузети додатне мере за складиштење како би се сачували докази колико год је то времена потребно. У форензичкој лабораторији је транспортоване уређаје потребно *ускладиштити* у безбедном простору, подаље од извора електромагнетног зрачења, топлоте и влажности, прашине, у ком је ограничено и контролисано право приступа само лицима која су овлашћена да обрађују податке (стварањем одговарајућег система за контролу приступа)[801].

Осим поменутих мера физичке заштите, неопходно је посебну пажњу посветити облику у ком се дигитални докази чувају. Повећање меморијског капацитета електронских уређаја и потреба да се подаци чувају дужи временски период представља још један изазов за форензичке лабораторије, у погледу решења на ком *медијуму* чувати дигиталне доказе[802]. Приликом избора медијума у ком се похрањују подаци, узимају се у обзир количина података, трошкови складиштења и временски период за који је потребно податке чувати, али која год опција да се изабере, медијум треба да буде доброг квалитета и поуздан. Осим медијума у ком се подаци складиште, пажњу је потребно посветити и *формату* у ком се подаци чувају. Постоји неколико формата у којим се чувају дигитални докази (јер је сваки произвођач форензичких алата створио посебан формат), а услед недостатка стандардне форме за чување копираних података јавља се ризик од измене или губитке дигиталних доказа[803]. Из тог разлога уочена је потреба за

[800] Осим енкрипције, постоје и друге технике које се користе за заштиту приватности корисника уређаја и означавају се заједничким називом *PET* технологије*(Privacy Enhancing Technologies)*. Више томе, R. Weber, "Internet of Things – New security and privacy challenges", *Computer Law and security Review* 26/2010, 26.

[801] *COE,* 47.

[802] Капацитет хард диска непрестано повећава. Ради илустрације, 1*GB* хард диска садржи 218,000 страница текста и уколико би се одштампао тај текст и странице папира послагале једна на другу достигли би висину од око 25 метара, а за штампање података садржаног на диску капацитета од 1*TB,* 50000 стабала дрвета би било искоришћено за производњу потребне количине папира. *ACPO,* 16.). Штампање материјала није једина опција, него се користе одређени уређаји за складиштење података.

[803] A. Flaglien, „Storage and exchange formats for digital evidence", *Digital Investigation* 8/2011, 124.

стварањем стандардног формата у ком би се чували дигитални докази[804], независно од врсте дигиталног доказа и примењеног форензичког алата[805]. Најисправније би било информације и податке које полиција прикупи тужилаштву упућивати у оригиналном облику, јер чување и приказивање у другом формату или на другом медијуму за складиштење података у односу на оригинални формат не ствара тачне копије и губитак изворног квалитета се смањује у знатној мери, а тиме и аутентичност доказа. Такође, корисно је користити стандардизоване форме за прикупљање и складиштење доказа, а које се у истом облику приказују и на суду.

3.2.3.2. Специфичности прикупљања података из „живог" система

Прикупљање и анализа статичних података који су постојани (као што су ускладиштени подаци у хард диску) врши по правилу у форензичкој лабораторији, што представља уобичајен приступ у оквру дигиталне форензике, док се на физичком лицу места из уређаја као „живог система" (пре него што буду искључени или дисконектовани са мреже или извора напајања) прикупљају подаци само у одређеним ситуацијама. Ради се првенствено о прикупљању непостојаних података. Непостојани подаци (*volatile data*) су подаци који се дигитално ускладиштени на начин да постоји веома велика вероватноћа да њихов садржај буде избрисан, пребрисан или измењен у кратком временском периоду и то или активношћу корисника или као резултат аутоматизоване радње у

[804] Најчешће коришћен начин за стварање форензичке копије диска или уређаја за складиштење податак јесте стварање „сировог" формата (*sector-by-sector copy*) који не копира метаподатке датотека који могу бити од кључног значаја за истрагу (као што су серијски број диска, датуме и место клонирања диска и дигитални потпис који треба да поврди аутентучност података) нити се може на одговарајући начин направити разлика између празног простора у меморији диска и простора ком је приступ недоступан због неке грешке у хардверу. Још један недостатак оваквог формата јесте њихова величина (с обзиром на то да нису компресовани), па је тако за форензичку копију хард диска од 200 *GB* потребно исто толико меморије за складиштење иако су у драјву датотека које заузимају свега 100*MB*. Међутим, највећи проблем који се може јавити је то што произвођачи форензичких алата нису спремни да учине доступним кодове који су коришћени за писање софтвера па није могуће резултате обраде проверити употребом другог форензичког алата, и тиме обезбедити аутентификацију дигиталних доказа.

[805] Утврђивање тзв. *Common Digital Evidence Storage Format* један је од циљева Истраживачке радне групе за дигиталну форензику (http://www.dfrws.org/CDESF/), но, у време писања рада, још увек није постигнут концензус око овог техничког стандарда.

рачунару[806]. Разликује се више врста непостојаних података: *непостојани подаци у рачунару* (као што су подаци о отвореним мрежним конекцијама и покренутим апликацијама) и *привемено непостојани подаци,* који нису непостојани по својој природи али су доступни, односно може им се приступити само на лицу места (на пример енкриптовани подаци или подаци који се складиште на удаљеним изворима) па њихов садржај може постати недоступан, измењен или изгубљен ако их форензичар не прикупи у правом тренутку, јер то накнадно неће бити могуће.

Непостојани подаци су похрањени у *RAM* меморији (која представља основну меморију у рачунару - користе је оперативни систем и покренуте апликације док је рачунар укључен, па садржи информације о свим активним процесима у рачунару), губе се моментом искључивања рачунара и не могу се више повратити[807]. У *RAM* меморији су садржани веома корисни подаци, као што су, примера ради: подаци о процесима (тренутно покренутим, сакривеним и недавно окончаним процесима[808]), о отвореним датотекама и регистрима које је процес користио[809], информације о оперативном систему, дешифровани подаци или апликације (што је корисно уколико уређај има инсталиран софтвер за енкрипцију података/апликација), лозинке и криптографски кључеви за дешифровање енкриптованих садржаја и подаци о другим сигурносним механизмима у рачунару инсталираним од стране корисника[810], подаци о пријављеним корисницима, подаци о мрежним конекцијама[811], информације о начину покретања система, отворене инстант поруке, скривени подаци[812] и слично. Како меморијски

[806] У домаћој литератури користи се и термин „нестални подаци". В. Урошевић, И. Којадиновић, „Правни аспекти несталних података као доказа прикупљених приликом он лине анализе активног рачунара", *Криминалистичко форензичка истраживања* 1/ 2011, 521.
[807] Хајдуковић, Живанов, *op.cit*, 118-119.
[808] Иако су процеси окончани, део у меморији у ком се чувају још увек није пребрисан па се може поново покренути процес и анализирати.
[809] Подаци о томе које датотеке је покренути процес користио могу бит веома корисни. На пример, уколико је процес део малициозног софтвера, отворене датотеке које процес користи могу бити траг за откривање места где је малвер лоциран, где исписује своје аутпуте, као и које претходно чисте датотеке је малвер заразио.
[810] Лозинке и криптографски кључеви су похрањени у *RAM* меморији и њихов проналазак може послужити да се приступи садржајима који су заштићени лозинком или енкриптовани. Такође, проналаском лозинке може се остварити приступ *online* налозима корисника (нпр. за електронску пошту) или подацима ускладиштеним у облаку.
[811] Као што су листинзи рачунарских мрежа и отворени портови, *IP* адресе, *ARP (address resolution protocol*) *cache, DNS cache* и сл.
[812] Лице може свесно и намерно похранити инкриминишуће или осетљиве податке у *RAM* меморији, а не на хард-диску, полазећи од тога да се ова меморија најчешће не прегледа од стране

капацитет све више расте, није неуобичајено да *RAM* меморија садржи по неколико гигабајта података, па органи поступка не би требало да „приуште“ да изгубе 12 или 16 GB података (што је око 55.000 слика са просечном величином од 300 KB). Сви ти подаци би били бесповратно изгубљени уколико би се поштовала традиционална процедура по којој се уређај искључује из напајања, па је зато боље решење најпре прикупити те непостојане податке, а затим искључути уређај.

Анализа *RAM* меморије може да допринесе циљу истраге, а то је прикупљање релевантних података, јер превазилази неколико ограничења традиционалних корака дигиталне истраге (као и проблема које нове технологије, као што је енкрипција проузрокују), а ради се о следећим ограничењима: А. Форензичар не може приступити енкриптованим садржајима, уколико не открије лозинку корисника или кључ помоћу ког су подаци енкриптовани, а они су веома ретко сачувани на харддиску, па претреага харддсика неће дати резултате у том погледу. Међутим, када корисник на тастатури искуцава лозинке или када су подаци дешифровани, лозинке и кључ су похрањени у том моменту у *RAM* меморији и до њих се може доћи анализом *RAM* меморији у „живом“ систему; Б. Осим тога, физички диск не приказује податке о процесима који су били покренути у меморији рачунара, па се анализом хард диска не може сазнати на који начин су апликације биле коришћене у систему у време извршења радње; В. Постоји могућност да осумњичени сакрије податке у меморији, а не да их чува на харддиску; Г. Све је више уобичајено да се производе вируси, тројанци и црви који бораве у меморији, а не чувају се на хард диску рачунара који нападају, па се анализом диска не открива малициозни код нити начин на који је напад извршен[813]. Из овога се може недвосмислено закључити да непостојани подаци могу бити корисни за случај. Међутим, како су веома „крхки“, тј. могу се лако изгубити или изменити, ако се њима не поступа на одговарајући начин, потребно је пажњу посветити начину на који им приступа, тј. сачувати их брзо и коректно.

У погледу *начина прикупљања рачунарских података из „живих“ система*, постоје два метода прикупљања непостојаних података: 1. Метод заснован на

надлежних органа, а и да се веома лако унишити, простим искључивањем рачунара или издавањем наредбе са даљине.

[813] Као пример се може навести црв *SQL Slammer worm*.

употреби хардвера; и 2. Метод заснован на употреби сотфвера. Први начин прикупљања непостојаних података спроводи се употребом специјалног хардвера, који суспендује процесор и користи директан приступ меморији како би се створила копија меморије, која се потом анализира[814]. Овакво поступање сматра се поузданијим, јер чак и да су оперативни систем и софтвер компромитовани од стане корисника, на овај начин се добија идентична копија меморије а њено креирање не ослања се на поменуте компоненте рачунарског система. Ипак, недостатак овог приступа је цена специјалног хардвера. Зато се много чешће користи метод заснован на употреби софтвера. Постоји неколико специјалних форензичких алата који служе прикупљању непостојаних рачунарских података, међутим, имајући у виду брзину технолошког развоја, тренутно примењиве технике и алати могу постати некорисни у блиској будућности. Из тог разлога потребно је посветити пажњу осмишљавању и поштовању одређене *методологије* која би била технолошки неутрална, а у складу са утврђеним принципима поступања са електронским доказима.

Прикупљање и анализа непостојаних података је мање прецизна вештина у односу на анализу хард диска који има унапред утврђену структуру, и зна се где се елементи те структуре и одређене врсте података налазе. Меморија може бити лоцирана, дислоцирана и мењана, у зависности од тога која меморија се користи и у које намене, па није могуће унапред предвидети који подаци се могу пронаћи у меморији. Услед непостојања чврсте структуре у *RAM* меморији рачунара, брзине мењања те меморије и чињенице да свака радња која се предузме производи промене у њој, лице које приступа овим подацима мора предузети све *мере предострожности* да би заштитило непостојане податаке, а препоручују се следеће: а) идентификовање, обезбеђење и документовање сваког уређаја који садрже непостојане податке; б) надгледање понашања осумњиченог и других лица и спречавање у предузимању радњи које имају за циљ мењање или уништавање доказа; в) надгледање компоненти рачунарског система, како би се спречила промена или уништавање доказа.

Након што је омогућен приступ рачунару (рачунар није био заштићен *screensaver*-ом нити пољем за пријаву на систем, или је прибављена шифра за

[814] На пример, *Tribble card* што је је *PCI* картица која се инсталира у систем.

приступ), приступа се прегледу и прикупљању непостојаних података употребом посебних форензичких алата, тако што се предузимају одређени кораци. Иако постоје одређени конфигурисани *Live Forensics DVD* са широким спектром алата, препоручљиво је да истражитељ сам састави компилацију алата за сопствене потребе[815]. Пре предузимања било које радње, потребно је регистровати датум, време и историју команди у моменту извршења радње кривичног дела, а приликом давања наредби форензичком алату за прикупљање непостојаних података, потребно је генерисати датум и време. Затим се покреће опција регистровања историје наредби којом ће се бележити све радње које се предузимају ради прикупљања података[816]. Након што се прегледа приказ монитора, да би се утврдило да ли постоје трагови уништења електронских доказа[817], проверава се да ли се користи цео хард дик или постоје трагови енкрипције[818], даљинског

[815] Приликом избора форензичких алата за прикупљање непостојаних податак, форензичар треба да предност да алату који има најмањи могући утицај на систем. На пример, за прикупљање података у *RAM*, боље решење је да се користи једноставан алат (као што је *dumpit)* у односу на захтевани графички алат (као што је *FTK Imager)*. Алат би требало да има могућности аутоматског извршавања наредби, тако да се може покренути без употребе непроверених бинарних наредби из система из ког се подаци прикупљају, односно да не захтева пуно интеракције корисника с обзиром на то да форензичар неће запамтити опције за све команде нити ће бити у стању да све време посматра обраду података у ситуацији када постоји више уређаја које обрађује. Осим тога, алат би требало да буде конфигурисан тако да прикупља само непостојане податке, а не и податке који су иначе доступни на хард-диску рачунара (а који се накнадно свакако могу прикупути уобичајеним процедурама). Вид: B. Carrier, J. Grand, „A hardware-based memory acquisition procedure for digital investigations“, *Digital Investigation* 1/2004, 55.

[816] Да би се оставио траг о свим активностима предузетим приликом прикупљања непостојаних података у живом систему од изузетног значаја је стварање одговарајуће документације, односно *audit trail*, а да би се то створили потребно је: водити евиденцију о свим предузетим радњама; фотографисати екран рачунара; идентификовати оперативни систем; пребацити све из *RAM* меморије као и друге непостојане податке који се односе на оперативни систем у уређај за складиштење података. При томе треба имати на уму да прикључивање било ког уређаја за складиштење података на рачунарски систем производи одређене промене у систему. Нпр. прикључивање *USB* се приказује у *Microsoft Registry,* али то не утиче на потенцијалне доказе, односно на непостојане података који се складиште у *RAM* меморији.

[817] Што би, примера ради, биле речи: *delete (*избриши*), format (форматирај), remove* (уклони) *, copy* (прекопирај), *move* (премести), *cut (исеци)* или *wipe* (пребриши).

[818] Енкрипција, а посебно енкирпција целог диска је све више у примени а користе је не само лица која настоје да прикрију трагове својих криминалних активности, него и компаније и појединци у циљу безбедности и заштите података. Често политика компанија захтева да сви подаци буду заштићени одговарајућом шифром за приступ њима помоћу софтвера за енкрипцију, као што су *Microsoft Bitlocker, Truecrypt, Steganos, PGP* итд. Осим тога, савремени уређаји (лаптопови, мобилни телефони...) су све чешће заштићени помоћу енкрипције. Када се одузме шифром заштићени хард диск и накнадно се анализира, често је прекасно и веома тешко превазићи проблем енкриптованог садржаја. Да би се „разбила“ јака енкрипција, потребни су специјализовани алати и доста времена да се дешифрује комплетан шифровани диск, ако је то уопште и могуће, а у најгорем случају се никако не може приступити подацима и одузети хард дискови са више терабајта могу бити потпуно безвредни. Из тог разлога, не би требало пропустити прилику да се прикупе иначе енкриптовани подаци у фази када су они дешифровани. Да би

приступа са другог рачунара или другог уређаја[819] или коришћења *cloud* услуга, као и знаци активне комуникације са другим рачунарима или корисницима[820]. Након што се на описани начин оствари директни приступ *RAM* меморији и подацима који су у њој похрањени, ствара се се статична форензичка слика меморије која у поптуности одговара њеном стању у моменту прикупљања или се у реалном времену примењује екстерна форензичка анализа меморије. За анализу тако добијене слике меморије рачунара се користе разни софтверски алати помоћу којих је могуће добити информације о стању, конфигурацији и аномалијама рачунарског система[821]. Прикупљени подаци се снимају на уређају за складиштење података[822] и након прикупљања, бележи се датум и време и историја издатих команди[823]. Редослед прикупљања података такође може да буде од кључног значаја за истрагу, па форензичар и о томе треба да води рачуна. Иако се сваком конкретном случају треба приступити водећи рачуна о околностима тог случаја, пожељно је поступати у складу са претходоно утврђеном методологијом у погледу прикупљања непостојаних података према одређеном редоследу формираном на основу критеријума релативне непостојаности[824].

уопште знао да је у систему присутна енкрипција, форензичар би требало да потражи трагове њене примене. Добра полазна тачка је да се потраже трагови инсталираног софтвера за шифровање у покренутим процесима у *Windows Explorer*-у. О прикупљању енкриптованог материјала, више о томе, N. McGrath et al, „Investigating Encrypted Material", In: Sorell M, *Forensics in Telecommunications, Information and Multimedia*, Springer-Verlag, Berlin - Heidelberg 2009, 29-36.

[819] S. Brenner, „Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force", *Mississippi Law Journal* 1/2011, 1240.

[820] H. Chung et al., „Digital forensic investigation of cloud storage services", *Digital Investigation* 9/2012, 87.

[821] Нарочито је корисна могућност да се оваквом анализом уоче малвери који су заразили систем. Аналитичка способност поменутих алата се све више развија и користе се у разне сврхе: за анализу са даљине (M. Cohen, D. Bilby, G. Caronni, „Distributed forensics and incident response in the enterprise", *Digital Investigation* 8/2011, 101–102.), за класификацију малвера чак и за самоизлечење компромитованог рачунара (J. Grizzard Towards self-healing systems: re-establishing trust incompromised systems, Georgia Institute of Technology, 2006, 55.). Осим тога, поједини аутори указују на корисност аутоматизације процеса прикупљања података из „живог" система јер она умањује потребу за интервенцијом лица које примењује алате а тиме се обезбеђује интегритет тако прикупљених доказа.

[822] Када истражитељ прикупља податке из активног система, правилно ће поступити уколико их не буде чувао у уређајима за складиштење података тог рачунарског система него у претходно припремљеном спољном уређају за складиштење података који повезује са рачунаром: *USB* стикови са што већим меморијским капацитетом, екстерни хард-дискови са што више могућности конектовања са рачунаром (*USB/eSATA/FW*), *DVD* са заштитом од даљег снимања података (*write protection)* или екстерни хард-диск са виртуелним *DVD*.

[823] Више томе, CERT Training and Education handbook, *First Responders Guide to Computer Forensics*, http://www.sei.cmu.edu/reports/05hb001.pdf , 94-102.

[824] О примерима таквог редоледа, Vacca, *op.cit*, 223.

Битно је имати на уму да технике прикупљања непостојаних података свакако проузрокују одређене промене у рачунару, али се односе само на датотеке оперативног система, а не мењају садржај похрањен у *RAM* меморији. Иако је пожељно да форензичар прикупи и сачува што више непостојаних података, то мора чинити на начин да остави што мање трагова својих акција у систему, а да то не би представљало проблем у погледу прихватљивости доказа, корисно је тачно регистровати све промене у уређају настале употребом софтверских алата[825], како би се могло утврдити који је ефекат техника за прикупљање непостојаних података произвела у оперативном меморије рачунарског система. Како је у таквим ситуацијама ризик од измене, оштећења или губитка података веома висок, форензички преглед „живог" система захтева посебну обуку, практично искуство и скуп проверених форензичких алата, и потребан је знатно виши ниво специјализованости лица од лица која поступају у „*dead box"* сценарију, па само стручна, квалификована и компетентна лица могу да спроведе неопходне кораке и при томе да користе технике које изазивају најмањи утицај на систем. Ако се не може обезбедити присуство специјализованог форензичара, треба тражити промптну подршку специјализоване јединице[826], а ако се ни ово не може обезбедити, боље је решење извући кабел уређаја из утичнице, него манипулисти непостојаним подацима што може резултатирати контаминацијом доказа и немогућношћу његове употребе на суду. Иако је уобичајено поступање органа на лицу места у случају наиласка на рачунарску мрежу позив у помоћ стручнх лица, услед недовољног броја лица обучених за рачунарску и мрежну форензику у односу на све већу количину дигиталних садржаја, може се појавити проблем неадкватне стручне подршка на лицу места због све веће заступљености малих рачунарских мрежа[827]. Из тог разлога сматрамо да је неопходно да лица која

[825] На рачунарски систем се повеже софтверски алат за прикупљање *RAM* меморије (на *CD-ROM* или *USB*), креира се *snapshot* почетног стања меморије, потом се алату издаје наредба за аутоматско прикупљање непостојаних података, креира се *snapshot* измењеног стања меморије, а прикупљени подаци се потом похрањују на посебном уређају за складиштење. B. Lempereur, M. Merabti, Q. Shi, „Pypette: A Framework for the Evaluation of Live Digital Forensic Acquisition Techniques", *Proceedings of the Seventh International Workshop on Digital Forensics & Incident Analysis (WDFIA 2012),* 93-94.

[826] https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, 25

[827] У конкретном случају убиства извршен је претрес стана оштећеног ради проналаска мотива и трагова које је осумњичени оставио за собом и том приликом је пронађен укључен рачунар. Да је истражитељ поступио у складу са традиционалном методологијом и искључио рачунар и транспортовао га у лабораторију на анализу од стране стручеака дигиталне форензике,

предузимају радње првог захвата буду оспособљена да прикупе потенцијалне доказе у покренутом рачунарском систему на самом лицу места. Свакако да ово могу извршити само обучена лица, али је потребно да овим знањима располажу лица која излазе на лица места, јер одбрана може довести у питање тачност и поузданост сваког метода прикупљања доказа и коришћених алата. Како би се обезбедила прихватљивост доказа који су прикупљени на овај начин, полиција и тужилаштво морају у случају потребе да се врши форензичка анализа живог система располагати знањима и вештинама као и доказ о валидности употребљеног алата.

Приказане су само неке опште препоруке, али не постоји стандардна *Live Data Forensics* процедура која би била уноформна за све ситуације и све уређаје, што је један од проблема прихватљивости доказа прикупљених на овај начин, но ову методологију је потребно пратити без обзира на то који форензички алат и технике се користи за анализу меморије рачунара. Међутим, у вези са прикупљањем непостојаних података из активног система, важно је указати да нису у свим националним прописима дозвољене активности које се могу применом ових алата предузети[828]. У појединим законодавствима наредба за претресање рачунара садржи овлашћење, како за иницијалну претрагу рачунара тако и за накнадну форензичку анализу, док је у другим система потребно издавање две наредбе за ове две фазе. Како је прикупљање непостојаних података ограниченог обухвата и сврхе (а то је обезбеђење података који би заувек били изгубљени искључивањем рачунара) сматрамо да није потребно посебно овлашћење поред наредбе за претрес рачунара, осим у случају када околности прикупљања непостојаних података захтевају додатно време или проширују обухват извршења првобитно одобреног претресања. Такође, треба имати у виду да се овај процедура не односи на прикупљање у реалном времену садржаја комуникације путем рачунарске мреже. Заправо, прикупљање непостојаних

бесповратно би били изгубљени корисни подаци. Да је истражитељ био обучен да прикупи непостојане податке у RAM меморији а између осталог и инстант поруке између оштећеног оосумњиченог које би га повезале са учиниоцем. Наведено према: Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, https://www.ncjrs.gov/App/publications.aspx?ID=237673

[828] K. Amari, „Techniques and Tools for Recovering and Analyzing Data from Volatile Memory“, 2009, http://www.sans.org/reading-room/whitepapers/forensics/techniques-tools-recovering-analyzing-data-volatile-memory-33049.

података применом приказане методологије треба посматрати само као једну од фаза у претресу рачунарског система, јер се претходно описани кораци односе само на прикупљање, обезбеђење и регистровање посебно осетиљивих (у смислу губитка и измене) рачунарских података, који су већ присутни у рачунару (аналогно прикупљању трагова на увиђају лица места) а који могу у случају да се не предузму наведени кораци бити трајно изгубљени. *Из тог разлога било би оправдано да наредба за претрес рачунара садржи овлашћење* да се документује и сачува стање рачунарске мреже и електронских уређаја за складиштење података и да се изврши преглед меморије рачунара ради прикупљања непостојаних података на лицу места.

Међутим, иако *in situ* прегледање живог рачунарског окружења омогућава прикупљање рачунарских података који би се трајно и бесповратно изгубили и били недоступни за накнадну анлазу (нарочито информације о оперативном стању рачунара у тренутку када се њему приступило) поступањем у складу са принципима дигиталне форензике, ипак се може довести у питање оправданост дигиталне форензике „живих" рачунарских система (*live digital forensics*) која са собом носи изазов у погледу да ли су докази прикупљени на овај начин изгубили на кредибилности. И поред тога што постоје напори да се тестирају форензички алати за прикупљање меморије[829] и да се створе критеријуми по којима би их требало тестирати[830], до сада није није утврђена отпорност алата на антифорензичке технике[831] (чак шта више, показало се да постојећи бесплатни и комерцијални софтвери не садрже механизме за заштиту процеса прикупљања од деловања примењних антифорензичких техника[832]), *мишљења смо да прикупљање меморије у живом систему у погледу стандардизације, а тиме и валидности прикупљених доказа далеко од прикупаљања података у идеалним условима*

[829] H. Inoue, F. Adelstein, R. Joyce, „Visualization in testing a volatile memory forensic tool", *Digital Investigation* 8/2011, 44.
[830] Carrier, *op.cit*, 56. Упор. S.Vömel, C. Freiling, „A survey of main memory acquisition and analysis techniques for the windows operating system", Digital Investigation 1/2011; 3–22.
[831] M.Wundram, F. Freiling, C. Moch, „Anti-forensics: the next step in digital forensics tool testing", Proceedings 7th International Conference on IT Security Incident Management & IT Forensics (IMF), 2013, 15.
[832] S. Rekhis, N. Boudriga, „A Hierarchical Visibility theory for formal digital investigation of anti-forensic attacks", *Computers & security* 31/2012, 968.

форензичке лабораторије[833]. Као потврду за тај став наводимо да, иако се у научној и стручној литератури могу пронаћи истраживања о стандардизацији техника прикупаљања података из живих система[834], *још увек преовладава став да се подаци прикупљени на овај начин не могу прихватити као доказ*. Како би докази добијени применом оваквог приступа могли представљати значајан допринос истрази, потребно је у будућности посветити пажњу ефектима и прецизности ових техника прикупљања података[835].

3.2.4. Фаза анализе

Након што се прикупе рачунари и други уређаји, следи најважнија и најзахтевнија фаза дигиталне истраге – фаза анализе, чији циљ је да се издвоје релевантни рачунарски подаци који могу бити докази у кривичном поступку, односно да се пронађу електронски докази. Дакле, управо кроз ову фазу се рачунарски подаци, који су похрањени у прикупљеним рачунарским системима или се преносе кроз рачунарску мрежу, трансформишу у електронске доказе. Форензичка анализа је *мукотрпан и спор* процес који треба да буде реализован темељно, како би се утврдили обрасци активности осумњиченог, аномалије дигиталног потписа, необична понашања, трансфер датотека и слично. Анализа свих прикупљених рачунарских података је *тежак и компликован* процес, јер се обично прикупи велика количина података који су у сировом неразумљивом формату и који се применом одређених алата преводе у апстрактнији разумљивији формат. Како је пред ову фазу дигиталне истраге постављен

[833] Бројна истраживања су посвећена изналажењу теоријски и научно потврђених метода за проверу техника које се користе у прикупљању рачунарских података из живих система, а који могу бити електорнски доказ. B. Carrier, E. Spafford, „Categories of digital investigation analysis techniques based on the computer history model“, *Digital Investigation* 3/2006, 128; P. Stephenson, „Modeling of post-incident root cause analysis“, *International Journal of Digital Evidence* 2/2003, 13; A. Arasteha et al, “ Analyzing multiple logs for forensic evidence“, Digital Investigation 1/2007, 85.

[834] Упор. G.G. Richard III, Roussev V., „Next-generation digital forensics“, *Communications of the ACM* 2 /2006, 77; F. Adelstein, „Live forensics: diagnosing your system without killing it first“, *Communications of the ACM* 2/2006, 64; B. Hay, M. Bishop, K. Nance, „Live Analysis: Progress and Challenges“, *IEEE Security and Privacy* 2/2009, 36; B. Schatz, „BodySnatcher: Towards reliable volatile memory acquisition by software“, *Digital Investigation* 4/2007, 130.

[835] Истраживања посвећена проблему форензичких алата за прикупљање непостојаних података приказана су у радовима: J. Stüttgen, M. Cohen, “Anti-forensic resilient memory acquisition”, Digital Investigation 10/ 2013, 108.; A. Walters, N. Petroni, “Volatools: Integrating Volatile Memory into the Digital Investigation Process”, Black Hat Briefings DC 2007, 15.

изузетно захтеван циљ, а то је да податке у бинарном облику доведе у везу са осумњиченим за потребе кривичног поступка, нужно је да се одвија у постојећим законским оквирима и уз уважавање научних постулата и смерница практичног поступања дигиталне форензике. За разлику од већине форензичких наука које су компаративне у природи и заснивају се на упоређивању узорака (нпр. балистичко вештачње, вештачење трагова боја...), дигитална форензика се може описати као археологија, јер се бави првенствено трагањем за дигиталним траговима ради одговора на питање ко је створио и користио одређене електронске записе и у коју сврху[836].

Процес уочавања, издвајања и анализе података са собом носи бројне изазове: током ове фазе може се изменити извор податка или релевантни метаподаци чиме се у знатној мери може умањити доказна вредност прикупљеног материјала[837], електроноки уређаји имају огромне меморијске капацитете за складиштење података, рачунарским мрежама се преносе бројни подаци великом брзином[838], а постоји и проблем превазилажења механизама заштите података у систему, као и непоседовања одговарајућих ресурса за поступање у законским временским оквирима[839].

С обзиром на постављени циљ и тешкоће које постоје ка остварењу тог циља, сматрамо да је неопходно постојање одређених **општих принципа** којим је потребно да се форензичар руководи приликом фазе форензичке анализе, а превасходно се односе на: *Интегритет података*[840]*, прецизно документовање*[841]*,*

---

[836] S. McQuade (ed.), *Encyclopedia of cybercrime,* Westport, Conn. : Greenwood Press 2009, 29.

[837] О значају метаподатака, F. Buchholz, E. Spafford, „On the role of file system metadata in digital forensics“, Digital Investigation 1/2004, 300.

[838] У студији *An International Data Corporation (IDC*) било је предвиђено да ће у 2011. години бити генерисано укупно 1.8 зета бајтова података биће широм света – што је представљало повећање од 50% у односу на претходне године. Наведено према: “Digital Univers Study 2011”, http://www.emc.com/digital_universe.

[839] Да би се извршила најједноставнија форензичка анализа једног десктоп рачунара потребно је у просеку 25-35 часова, при чему је за детаљну претрагу хард драјва по кључним речима потребно око 8 часова. Наведено према: Brown, *op.cit*, 9.

[840] Приликом анализе података рачунарског уређаја форензичар мора да буде опрезан да не оштети или модификује неки од електронских података који су донети у форензику лабораторију. Чак и просто прављење листе садржаја датотека у директоријуму или отварање датотека модификује поље "последњег приступа" (*last accessed” field*) које се често користи као доказ, и тако „корумпира“ доказ јер он више није у првобитном стању. Стога форензичар мора применити методе и технике којима се обезбеђује да се електронски подаци не мењају у току анализе. Метод који се најчешће примењује како би се то осигурало јесте да форензики истражитељ приступа уређају за складиштење података само док се налази у "*read-only* " моду, јер та технички поставка спречава да садржај уређаја за складиштење података буде измењен. Друга предострожност коју

подршку специјалисте[842] *и легалитет*[843]. Постојање и поштовање општих принципа обезбеђује да се електронски докази прикупе на начин који се може верификовати као поуздан, законит и истинит[844]. При томе, форензичар би био дужан да потврди да се приликом анализе придржавао ових принципа, у супротном би суд могао одлучити да се ради о недозвољеном доказу. Иако постоји велики број електонских уређаја и рачунарских мрежа који су

форензичари могу да предузму да би поштовали принцип интегритета података је да спроведе њихово испитивање у идентичној копији оригиналног уређаја за складиштење података тако да увек чувају оригиналне податке или аутентичну копију из које се прави радна копија која се користи за анализу. На крају, као део принципа интегритета података, искусни истражитељи треба да испитају да ли су подаци аутентични и да ли има трагова да су модификовани или им је неовлашћено приступљено пре него што је обезбеђен, односно да није примењена нека од *антифорензичких* техника са намером да измењени подаци наведу на погрешан траг. B. Carrier, „Risks of live digital forensic analysis“, *Communications of the ACM* 2/2006, 58.

[841] Да се не би довео у питање интегритет електронских доказа који настају као резултат радњи из претходно описаних фаза, потребно је припремити исцрпну документацију о свим предузетим активностима (Bayuk, *op.cit,* 137.) Током анализе је потребно створити тзв. *audit trail*, као својеврсни записник, којим се региструју све активности на рачунару који је предмет обраде и који на тај начин доприноси уочавању трагова тих активности, односно који подаци и који делови рачунарског система су анализирани, што суду помаже да разуме и провери поузданост резултата анализе. Како би се осигурало да се правилно направи такав записник, форензичари користе стандардизоване обрасце да документују своје анализе и ка подсетник да не забораве да обаве све фазе испитивања за добијање исцрпног прегледа рачунарског система. Истражитељ треба да белешкама покрије све фазе истражних активности а управо се ово може обезбедити коришћењем унапред припређених формулара. Овом својеврсном записнику је корисно прикључити снимак садржаја екрана, фотографије и видео записе, јер ови додаци омогућавају бржи и бољи опис корака које је истражитељ у фази анализе предузео (G. Richard, V. Roussev, L. Marziale. “Forensic discovery auditing of digital evidence containers“, *Digital Investigation* 4/2007, 89.)

[842] Техничка природа електронских доказа чини да је неопходно да се ангажују стручњаци дигиталне форензике а данас је тешко, ако не и немогуће, да један форензичар буде специјализован у свим областима компјутерске форензике. Неки могу имати генерална знања, али други су уско специјализовани у областима као што су жива форензике или у опоравак података из оштећених рачунарским системима. Део стручне подршке осигурава да форензичари имају опрему која им је потребна за анализу, као и приступ форензичким лабораторијама (која може да обухвати алатке за аутоматизацију одређених истражних активности или инсталације као што су монтиране камере које служе за стварање и одржавање *audit trail*).

[843] Како се рачунари све више користе као уређаји за комуникацију између физичких лица, количина личних података који се складиште у њима су порасла. Неминовност је да рачунарски систем појединца садржи личне податке и податке о приватном животу који су ирелевантни за истрагу, а који су поверљиви и можда чак и правно привилеговани, што може бити велики изазов. Форензичар не зна где се у рачунарском систему налазе подаци и који су подаци поверљиви јер нису често означени као такви. У оквиру истог фолдера могу да постоје поруке које су од интереса за истрагу и неке који су правно заштићене, а нису релевантне. Ако у току анализе истражитељ наиђе на личне податке ван опсега истраге, у неким правним системима су дужни да одмах зауставе даље активности у погледу тих података и означе их као личне податке ради даље орјентације. Такође, није незамислива ситуација у којој лице у фолдер са ознаком лично сакрије инкриминишући материјал што додатно показује комплексност разматрања са којим се форензичари аналитичари суочавају. Да би се решила дилема, постоји неколико могућности да се заштите и интереси истраге и приватност и право на одбрану осумњиченог и лица чији су лични подаци у питању. Једна од тих могућности је да се заплењени подаци ставе у судски депозит, а лица разговарају о садржају и потреби да се исти прегледа, као и да лице на које се подаци односе стави конкретне примедбе на суду пре него што их специјалисти анализирају.

[844] Више о потреби поштовања фундаменталних принципа форензичке анализе, Casey, *op.cit*, 6-9.

потенцијални извори дигиталних доказа (имајући у виду њихове специфичности), а тиме и више врста форензичке анализе, уважавање општих принципа било би неопходан услов прихватљивости резултата анализе у сваком случају.

Иако постоје бројни алати за форезичку анализу, који су у знатној мери аутоматизовани, и даље су неопходни знање и вештине стручног лица, која не само што морају знати како да добију податке користећи одређене форензичке алате, него је потребно солидно разумевање како основна технологија функционише, како су подаци распоређени и како алати тумаче и приказују анализиране податке. Полазећи од контекста случаја, а ослањајући се на знање, искуство и вештине, форензичар би неизоставно требало да *примени научни метод*[845] на резултате анализе које настају употребом алата, анализирајући доступне податке, како би утврдио корисне карактеристике и могуће недостатке резултата, упоређујући доказе са познатим узорцима за издвајање више информација, и обављањем експеримената за боље разумевање контекста доказа[846]. Лице које врши форензичку анализу а на ком је одговорност да пронађе електронске доказе, мора да буде непристрасно и објективно, а то постиже на најбољи могући начин уколико користи научни метод. Примена научног метода започиње прикупљањем чињеница и постављањем почетних претпоставки, али је ради провере хипотезе нужно да лице буде спремно да пронађе и грешке и одступања и размотри алтернативне могућности, односно да чак уложи напор да оповргне своје хипотезе ради потпунијег разумевања дигиталних трагова и изналажења поузданог дигиталног доказа.

---

[845] Casey, *op.cit*, 5.

[846] Примена научног метода подразумева следеће кораке: 1. Прикупљање информација (посматрање и форензички преглед дигиталних доказа); 2. Стварање хипотезе; 3. Провера хипотезе; 4. Извођење закључака. Casey, *op.cit.*, 24. Ови кораци се заправо предузимају тако што форензичар наизменично предузима следеће активности: 1. *Процењује садржај и контекст*- дигитални подаци који су у облику да су видљиви и читљиви имају одређени садржај који је разумљив за човека, па се тај садржај најпре прегледа ради утврђивања интегритета и аутентичности, те испитује како би се утврдиле претпоставке о одређеним околностима случаја (као што су коришћена средства, мотивација, околности и слично); 2. *Врши експерименте* - уопштен појам који у овом случају означава да постоји потреба да се примене неуобичајене или претходно непримењене методе и технике за време дигиталне истраге (што није неправилно, јер су све доказане методологије у почетку настале као експеримент) ради потврђивања или оповгравања постављених претпоставки, при чему је неопходно да експеримент буде ригорозно документован, тако да научна и стручна заједница, као и судови, имају прилику да примењени метод или технику тестирају; 3. *Доводи у везу прикупљене податке* - како су подаци током истраге прикупљени из многих извора (дигиталних и аналогних), вероватно је да један дигитални доказ сам за себи не значи ништа, па је потребно да буду доведени у везу са другим подацима; 4. *Проверава* резултате фазе анализе (Casey, *op.cit*, 22).

3.2.4.1. Стварање форензичке копије уређаја

Имајући у виду да се рачунарски подаци лако могу оштетити, изменити или уништити, и то или намерно (људском активношћу) или услед аутоматских процеса у самом систему, да би се очувао интегритет података похрањених у одређеном уређају и спречиле било какве манипулације, на оригиналном диску уређаја не врше се никакава испитивања. Стога је први приоритет по пријему уређаја у лабораторију у којој се врши форензичка анализа уређаја који садржи електронске доказе и пре приступања анализи, потребно обезбедити оригинални материјал од измене и губитка на одговарајући начин. То се постиже *стварањем форензичке копије* уређаја, односно *клона*, који је у потпуности идентичан оригиналном електронском уређају. Процес стварања форензичке копије уређаја назива се *Disk imaging* (назива се још и *Disk cloning* и *Disk ghosting*), при чему је потребно водити рачуна о томе да, када се копира један диск на други, то буде верна копија оригиналног диска[847]. „Клонирање“ диска је широко прихваћена, односно стандардна пракса у дигиталној форензици са циљем стварања форензичке копије која је у потпуности идентична оригиналу и садржи бит сваког податка који је похрањен у уређају за складиштење података, укључујући скривене податке, привремене датотеке, покварене датотеке, фрагменте датотека, избрисане датотеке који нису још увек преснимљене (оваква копија назива се још и *bit-for-bit image,* јер се клонира бит по бит диска)[848].

[847] Тако се, на пример, показало да форензички алат *Ghost* (прузвођача *Norton,* www.symantec.com*)* који је био у широкој употреби од стране форензичара за клонирање диска заправо не ствара поптуну копију хард диска, већ само садржи информације о партицијама диска и копира садржај датотека на тим партицијама, што не представља форензичку копију оригинала.

[848] *Disk imaging* се разликује од простог копирања свих датотека са једног диска на други диск (нпр. опцијом *copy/paste*), јер на тај начин копирани подаци могу наизглед бити идентични, али се разликује начин на који су подаци похрањени а и не копирају се сви постојећи подаци. Такође, *Disk imaging* није исто што и стварање *backup* -а диска (нпр. коришћењем *backup* опције у *Windows* оперативном систему или алата за *backup*, као што је *Norton Ghost*), јер се тим техникама копирају само активне датотеке, па резултат њихове примене није потпуно идентични дупликат диска. Када се ствара форензичка копија диска, сваки физички сектор диска се копира тако што се подаци похрањују, односно дистрибуирају на исти начин као у оригиналном диску, па је резултат и физички и логички клон оригиналног диска. Иако је могуће копирати појединалне датотеке или партиције у диску уређаја, клонирање целокупоног рачунара пружа далеко више информација јер се ствара комплетна слика уређаја и свих података похрањених у њему (нарочито оних на први поглед невидљивих), и на тај начин се обезбеђује могућност за рад на идентичном дупликату диска.

Постоје више метода за стварање клона диска[849], а одабир зависи од околности случаја (опреме којом располаже форензичар, да ли је форензичар био на лицу места приликом одузимања уређаја или је уређај допремљен у лабораторију и слично). Међутим, који год метод био коришћен, пре него што се створи форензичка копија диска, исти се издваја из уређаја, при чему се користи се тзв. техника *write protection* (заштита од измене садржаја оригиналног диска) употребом одговарајућих хардвера и софтвера[850], креираних са наменом да омогуће форензичару да прегледа и прикупља податке са диска који треба да се анализира, без ризика да се било шта измени на оригиналном диску.

Наиме, након што се хард диск физички издвоји из предметног уређаја, спаја се са радним рачунаром преко стандардних каблова за конверзију (*USB-to-Integrated Drive Electronics (IDE) conversion cable*) при чему се корисити одговарајући *write-blocking* уређај[851] који је повезан са радним рачунаром[852], и након тога покреће се процес прикупљања хард диска (који траје неколико сати, у зависности од његове величине) [853] а након што је процес окончан, хард диск се се уклања и похрањује на сигурно место и тек тада се може приступити клонирању диска. У сврху креирања идентичне копије уређаја користе се посебни *Disk imaging* форензички алати[854], како софтверски[855], тако и хардверски[856], при чему се могу поделити према томе да ли је резултат дупликат у сировом или компресованом формату[857].

---

[849] Ради се о следећим методама: уклањање хард диска из рачунара и прикључивање на други, радни рачунар који користи форензичар у лабораторији; прикључивање другог хард диска (преносног рачунара који форензичар има са собом на терену) на рачунар који се прегледа и стварање копије; употреба посебног уређаја за клонирање диска (као што је нпр. *DIBS Rapid Action Imaging Device*) или коришћењем мрежне конекције (ентранета, каблова, *USB* и слично). Више о методама клонирања диска Cross, Shinder, *op.cit*, 236. За опис процедуре стварања форензичке слике, Middleton, *op.cit*, 10-15; Brown, *op.cit*, 270-275.

[850] Како се основни улазни и излазни систем (*basic input/output System:BIOS*), оперативни систем, и други периферни уређаји могу директно повезивати на хард диск, најбоље решење је да се техника *write-blocking* користи када форензичар директно приступа хард диску. Наведено према: Brown, *op.cit*, 64.

[851] Најчешће се користе следећи уређаји: *FastBloc* (за рад у лабораторији), *FastBloc FE portable (*који се може користити на терену) и *Tableau Forensic SATA Bridge* (Више о томе, Cross, Shinder, *op.cit*, 65. и 235).

[852] Веома је важно да хард диск радног рачунара, на ком се ствара клон уређаја који се прегледа, буде или нов и некоришћен или у потпуности „очишћен", односно да се трајно и бесповратно обришу сви подаци који су претходно били похрањени на њему, како клон који се ствара не би био „контаминиран" подацима из ранијих случајева. У ту сврху, у зависности од околности конкретног случаја, користе се три технике: преснимавање диска (*overwriting*), размагнетисање (*degaussing/demagnetizing*) и физичко уништење диска (*physically destroying the disk*).

[853] О техници прикупљања хард диск, Easttom, Taylor, *op.cit*, 259-260. и 265-266.

[854] Могуће је предвидети неколико захтева које алати морају испуњавати: да креирају бит по бит слику оригиналног диска или партиције диска, да ни на који начин не производе промене на

Међународна организација за рачунарске доказе препознаје следеће појмове: „ оригинални дигитални доказ“ за означавање физичких предмета и података пре одузимања са лица места, „дупликат дигиталног доказа“ као потпуну дигиталну репродукцију свих рачунарских података садржаних у оригиналном физичком предмету и „копија“ као тачну репродукцију информација садржаних у рачунарским подацима независно од оригиналних физичких предмета. Дакле, електронски докази нису „оригинални“ јер се из изворног облика (нуле и јединице) прерађују у „читљив“ формат од стране алата за анализу ради представљања на суду[858]. Да би се показала аутентичност, интегритет а пре свега оправданост употребе електронских доказа, неопходно је испитивање стручног лица које је спроводило дигиталну истрагу, а нарочито о правилности функционисања опреме која је произвела дигиталне доказе и о коришћеној методологији. С обзиром на то да се, дакле, анализа не обавља на оригиналном диску, него на његовој копији, веома је важно питање аутентичности, односно како потврдити да се заиста ради о идентичном дупликату оригиналног диска насталом применом поменутих хардверских и софтверских алата.

Аутентификација има за циљ да се обезбеди потврда да је прикупљени рачунарски податак у потпуности идентичан оном који је оригинално изузет из извора. Ако се измени податак или се изгуби током процеса стварања клона, како

оригиналном диску, да верификују интегритет клона и сл. Више о томе, у публикацији „*Imaging Tool Specification*” Програма за тестирање форензичких алата : http://www.cftt.nist.gov/disk_imaging.htm.

[855] Постоји неколико за ову сврху креираних форензичких алата: *Dc3dd* и *Dcfldd*, који стварају *.dd* формат; *Ddrescue*, који је подобан за клонирање диска са меморијом великог капацитета, а има и могућност уочавања грешака и прикупљања података из оштећених сектора диска; *Aimage*, за стварање напредног форензичког формата (*Advanced Forensic Format:AFF*); *Ewfacquire*, за стварање формата за вештаке (*Expert Witness Format: EWF*). Више о алатима који се користе за стварање форензичке копије хард диска, Cross, Shinder, *op.cit*, 245-248.

[856] У употреби је већи број хардверских уређаја за стварање дупликата диска, који интегришу у себи заштиту оригиналних података (*write blocking*), стварају клон диска на радном рачунару и пружају потврду да је форензичка слика верна у потпуности оригиналном диску, а поједини аутматски генеришу извештаје о процесу. Такви су нпр. следећи уређаји: *Logicube Forensic Talon, Intelligent Computer Solutions ImageMASSter, Solo-III, Voom Technologies Hardcopy II, DIBS RAID: Rapid Action Imaging Device* итд.

[857] Изворно се метод за форензичко дупликовање диска заснивао на „*dd“* команди *Unix* софтвера којом се за копирање диска од 250 *GB* било потребан диск капацитета од 250 *GB* или више. Новије методе стварања форензичке копије заснивају се на компресовању, при чему копирају и компресују све датотеке са оригиналног диска, али и све метаподатке, тако да дубликат који настаје као резултат иако заузима мање меморијског капацитета на диску на ком је копиран, ипак представља идентичну копију оригиналног диска.

[858] Barbara, *op.cit*, 117.

је могуће тврдити да постоји идентитет између оригиналног извора и копије на којој се заправо врши сва форензичка обрада? Зато тек када се утврди да је клон, односно дупликат у потпуности идентичан са оригиналом, односно да постоји аутентичност, могу се предузимати даљи кораци[859]. У ту сврху, осим што се за стварање форензичке копије неопходна правилна примена описаних техника (*write-blocking* и *disk imaging*), нужно је применити и технику којом се ствара својеврсни отисак оригиналног диска, употребом тзв. *Hash Function*[860] којом се обезбеђује неизмењеност садржаја диска, а тиме и интегритет доказа. Наиме, пре клонирања диска се израчунава одређена математичка (*hash*) вредност диска, као индивидуални и непоновљиви идентификатор диска[861] (што се може упоредити са папиларним линијама јединственим за човека), односно својеврсни дигитални отисак. То је вредност која се додељује појединачној датотеци, партицији, односно диску на основу математичког алгоритма, који се израчунава на основу прегледа датотеке, партиције, диска бит по бит а свака промена било ког податка резултираће и променом *hash* вредности. Након клонирања се упоређује *hash* вредност оригиналног диска и *hash* вредност насталог клона, па њихово подударање представља потврду да је створена идентична *bit-for-bit* копија оригиналног диска. Ако се *hash* вредност клона разликује од оригинала, потребно је избрисати креирани клон и поновити поступак, док год *hash* вредност оригинала и клона нису идентичне[862]. Осим израчунавања *hash* вредности диска, ова техника се примењује и на појединалне датотеке, директоријуме или

[859] Cross, Shinder, *op.cit*, 210.

[860] *Hash* функција је математички криптографски алгоритам који од почетног бита одређене дужине (*input*) производи низ од фиксне дужине карактера (*output*), при чему *input* увек даје идентични *output* који се назива *hash*. Уколико се почетни *input* измени, мења се и *hash в*редност. Осим тога, не постоји начн да се из *hash* као резултата повратно добије оригинални *input.* Најчешће се користе два криптографска алгортима*: Message Digest 5* (*MD5*) који израчунава вредност од 128 бита и *Secure Hashing Algorithm (SHA-1)* који израчунава вредност од 160 бита. Наведено према: Stephenson, *op.cit*, 252. Више о томе, Brown, *op.cit*, 281-284.

[861] *Hash* вредност израчунава форензички алат тако што оригиналној датотеци додељује одређену енкриптовану вредност, низ од 32 бита (нпр. 6b605a8x218ac7923kl73c8082c529l9). Наведено према: Moore, *Search and seizure of digital evidence*, 71. При томе, за сваку датотеку се додељује јединствену вредност, односно јединствени дигитални траг. Вероватноћа да две датотеке имају исти дигитални отисак је 1: 3.402.821.038 (наведено према: Easttom, Taylor , *op.cit*, 269.) Валидација употребом 32-битног математичког процеса (израчунавањем тзв. *32-bit CRC* вредности) је у употреби од 1989. године, са тачношћу у односу 1: 4.3 милијарде, међутим, имајући у виду све већи меморијски капацитетет и брзину процесуирања у савременим рачунарима, овај степен тачности се показао као недовољан, па је решење пронађено у *Hash* функцији. Наведено према: Vacca, *op.cit*, 243.

[862] Easttom, Taylor, *op.cit*, 230-231.

партиције диска, како би се осигурало да форензичар по пријему а током анализе није ни на који начин изменио податке у њима. Међутим, у овој фази није могуће израчунавати *hash* вредност свих датотека, него се предузима у фази претраге клона диска. Већина аутора се слаже у томе да је израчунавање и упоређивање *hash* вредности оригинала и клона најбољи начин аутентификације, тј. потврда да се ради о потпуно идентичном диску и да је обезбеђена аутентичност копије диска, односно у случају израчунавања и упоређивања *hash* вредности датотеке, да није било никаквих промена и да је тиме интегритет доказа очуван у току дигиталне истраге (чиме се онемогућава да окривљени у току поступка изјави да су му подметнути докази, односно да су измењени подаци[863]).

Уобичајено се стварају најмање три копије уређаја: једна на којој се врши анализа, друга која се представља на суду и трећа која се доставља осумњиченом у сврху анализе и прегледа података, односно електронских доказа који постоје против њега. Овакав начин анализе и презентовања електронских доказа на суду је широко распрострањен и прихваћен као аутентични и тачан приказ дигиталног уређаја[864].

3.2.4.2. Стадијуми форензичке анализе

Након издавајања хард диска и његовог клонирања, на створеној форензичкој копији врши се анализа релевантних података. Форензичка анализа се врши на радном рачунару који је опремљен одговарајућим софтверским алатима, који омогућавају претрагу, екстраховање и штампање релевантних података, као и аутоматизвано приказивање и састављање извештаја о процесу анализе[865]. Међутим, и поред употребе форензичких алата, велики део посла у фази анализе података (претрага, екстракција и анализа) је и даље задатак стручног лица.

Након *иницијалног прегледа*, који се предузима ради уочавања очигледних доказа и процене знања и вештина које је осумњичени применио, врши се е*кстракција података применом одговарајућих техника*[866], а тек потом се врши

[863] Vacca, *op.cit*, 39-40; Britz, *op.cit*, 39; Easttom, Taylor, *op.cit*, 255; Casey, *op.cit*, 185.
[864] Walden, *op.cit*, 609.
[865] *ACPO*, 29.
[866] N. Beebe, J. Clark, „A hierarchical, objectives-based framework for the digital investigations process“, *Digital Investigation* 2/2005, 151.

анализа и реконструкција догађаја како би се дошло до одговара на битна криминалиситичка питања и саставио извештај са налазом и интерпретацијом резултата анализе. На основу свега изнетог, може се уочити да се фаза анализе одвија кроз неколико стадијума:

1. Претрага података похрањених у одузетим уређајима;
2. Издвајање релевантних података (екстракција);
3. Анализа (у ужем смислу) и реконструкција догађаја;
4. Састављање извештаја о току и резултатима анализе.

Уобичајено је да у оквиру ове фазе први корак буде *почетна претрага,* у којој се полази од неких *иницијалних трагова* који су почетна тачка анализе (примера ради, поједине кључне речи у претрази текстуалних датотека, спорни запис о активностима или порнографски приказ). Почетна претрага је прилично неодређена и обично даје десетине стотина резултата. Форензичар проверава добијене резултате, одбацује небитне ставке и уколико је потребно додатно рафинира термине за претраживање. У случају да се пронађе релевантан траг, анализира се како би се дошло до других повезаних и релевантних трагова. Ови нови налази се користе за изградњу нове листе за *накнадну претрагу*. Цео поступак претраге је итеративан, како би се прикупило што више релевантних доказа потребних за каснију реконструкцију догађаја. Фаза анализе података је отуда дуготрајна и захтева значајну стручност и искуство форензичара[867].

Једно од утврђених стандардних правила поступања јесте да се цела структура система датотека прегледа (*in toto*[868]), што, међутим, постаје практично неизводљиво, с обзиром на комплексност оперативног система и повећан

[867] На пример, код избора иницијалних трагова корисно је да форензичар одржава колекцију листе за претрагу из претходних случајева, како би у случају на ком тренутно ради могао да оформи листу за претрагу на основу ове колекције или чак да поново употреби листу коју је користио у сличном случају. Поједини форензички софтверски алати омогућавају кориснику увоз и извоз листе за претраге за брзо покретање иницијалне претраге. Из тог разлога је корисно стварање систематског механизма за прикупљање, управљање, размену и поновно коришћење знања унутар форензичке лабораторије, пружајући подршку за доношење одлука форензичарима у конкретним случајевима. О корисности стварања аутоматизованог, ефективног механизма за коришћење знања из претходних дигиталних истрага у оквиру форензичке лабораторије, више о томе, G. Ruibin, Z. Yun, „Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework“, *International Journal of Digital Evidence* 1/2005, 3-4.

[868] Преглед *in toto* је предвиђен у свим познатим смерницама добре праксе, као и у већини постојећих модела дигиталне истраге.

меморијски капацитет уређаја за складиштење података[869]. Да би се превазишао проблем великог броја података прикупљених током претходне фазе, потребно је материјал свести на обим и облик који је подобан за анализу. У ту сврху поједини аутори предлажу употребу технике која се назива *тријажа*. Иако сваки преглед почиње од тоталитета дигиталних доказа, да би лоцирали и екстраховали потребне податке, форензичари у пракси циљано прегледају систем, одабирају специфичне датотеке и типове података и игноришу ирелевантне типове и садржаје. При томе се користе *два приступа* прегледу: селекција и редукција[870]. Наиме, потребно је да форензичар најпре састави листу питања на која настоји да пронађе одговор а потом изабере технику или алат који служи за лоцирање информације, како би форензички преглед резултирао релевантним електронксим доказима[871].

Претрага и издвајање података нису ограничени само на датотеке које постоје у оперативном систему и другим софтверима који су инсталирани у рачунарском систему и другим уређајима, него се прегледом различитих делова диска може приступити фрагментима датотека и подацима који су оштећени или избрисани. Зато се преглед и издвајање података из хард диска врши на два нивоа: на логичком и физичком нивоу.

1) *Преглед и екстракција на логичком нивоу* подразумева идентификовање и/или опоравак датотека у оперативном систему, систему датотека и инсталираним апликацијама, на који начин се прикупљају подаци похрањени у активним и избрисаним датотекама, укључујући: а) екстракцију података о систему датотека, да би се утврдила структура директоријума, као и називи, локација, величина, атрибути и временски идентификатори у њима похрањених датотека; б) екстракцију датотека које су на први поглед релевантне за истрагу, на

---

[869] Типични хард дискови садржи више од стотину гигабајта података (па и више од хиљаду гигабајта). Уређаји за складиштење ове величине могу да садржи стотине хиљада фотографија, текстуалних датотека и других докумената за које је немогуће да истражитељ прегледа један по један.

[870] *Селекција* подразумева трагање за подацима ради лоцирања информације са доказном вредношћу, пру чему је потребно да форензичар са одређеним степеном одређености зна за чим трага и где то може пронаћи. *Редукција* подразумева уклањање информација које немају доказну вредност, при чему и након примене овог приступа остаје и даље велика количина података које треба обрадити. Да би се превазишли основни недостаци приказаних приступа, потребно је да форензичар примени комбинацију оба, узимајући у обзир све околности случаја како би преглед био ефикасан и ефективан.

[871] Више о приступима форензичком прегледу, Pollitt, *op.cit*, 17-29.

основу назива, есктензије, садржаја и/или локације у диску[872]; в) издавајање података који су заштићени енкрипцијом, лозинкама[873] и/или компресовани; г) издавајање података у неискоришћеном простору диска (*slack*)[874]; д) издавајање података у недодељеном простору (*unallocated file space*)[875]; ђ) поврат избрисаних података[876].

2) *Преглед и екстракција на физичком нивоу* подразумева идентификовање и/или опоравак свих података који су похрањени било где у хард диску рачунара, а употребом разних метода, укључујући: а) претрагу по кључним речима (*keyword searching*); б) претрагу по одређеним идентификаторима датотеке (нпр. заглављу) да би се повратиле датотеке или фрагменти датотека, нарочито ако су оштећене, избрисане или похрањене у покваренim директоријумима или оштећеном уређају за складиштење података (тзв. реконструкција датотека, односно *File carving*[877]); в) претрагу по партицијама диска и неискоришћеног простора.

Поједини аутори указају на потребу развоја, тестирања и примене нових аутоматизованих техника и алата, указујући на предности проактивног приступа форензичкој анализи. Неки од њих експлицитно користе термин проактивни приступ, критикујући претежно реактивни карактер постојећих приступа[878], док остали имплицитно указују на неопходност постојања претходних фаза пре прикупљања и анализе података[879].

---

[872] У зависности од околности конкретног случаја, врши се претрага: историје активности на Интернету (листа *Uniform Resource Locators:URL* преко привремених *Internet* датотека, *Web cache* и *History* директоријума); електронске поште и именика; текстуалних датотека (екстензија *.doc, .wpd, .wps, .rtf, txt* и сл*);* табеларних датотека (екстензија *xls, .wg1, .wk1* и сл*);* графичких датотека (екстензија *.jpg, .gif, .bmp,.tif* и слично) итд. Наведено према: Cross, Shinder, *op. cit*, 638.

[873] За опис процедуре откривања шифри, Middleton, *op.cit*, 139-142.

[874] Кластер је група сектора у хард диску у ком се похрањују подаци, а ком оперативни систем додељује јединствени број како би имао траг до датотека сачуваним у том простору. Како је кластер фиксне величине у оперативном систему, кластер је „задужен" за датотеку, чак и да она не попуни ту количину простора.Тај неискоришћени део простора назива се *slack space.* Cross, Shinder, *op.cit*, 140-141.

[875] Ради се о делу хард диска који није део ниједне партиције диска, али може да садржи оштећене и избрисане податке.

[876] Постоји више техника које се користе за повраћај избрисаних података. Више о томе, Cross, Shinder, *op.cit*, 307-312.

[877] Да би се реконструисао пун садржај оштећених датотека или фрагмената датотека, користе се посебни форензички алати као што су: *Foremost, Scalpel, DataLifter* и *PhotoRec.* Casey, *op.cit*, 36.

[878] W. Ren, H. Jin: "Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation", *2005 ACM Symposium on Applied Computing*, Santa Fe 2005, 435.

[879] Тако *Tan* уводи појам форензичке спремности ради повећања способности органа да прибављају кредибилне дигиталне доказе уз истовремено смањење трошкова форензичке обраде (Rowlingson, *op.cit*, 3). *Carrier* и *Spafford* препознају потребу посебне фазе спремности у оквиру предложеног модела (Carrier, *op.cit*, 6-12). *Rowlingson* истиче да поједина организације имају

Након прегледа хард диска (на физичком и логичком нивоу), врши се *претрага података у периферним уређајима и другим уређајима* за складиштење података, а онда се приступа анализи. Из свега наведеног је јасно да је циљ претраге диска да се прикупе информације потребне да би се одлучило којој врсти анализе (у ужем смислу) приступити.

3.2.4.3. Врсте форензичке анализе

Форензичка анализа система датотека[880] има за циљ откривање да ли одређени подаци постоје у уређајима за складиштење података. Обично се користи када је за добијање доказа о извршењу радње кривичног дела довољно да се утврди да су незаконити садржаји били у поседу осумњиченог (нпр. фотографије на којима су прикази злостављања деце, списак бројева украдених кредитних картица, датотеке настале повредом ауторских права), односно када су

тимове за реаговање на инциденте који прикупљају доказе на основу интерних правила (Rowlingson, *op.cit*, 1-28.). Исто тако, *Orebaugh* истиче да је много више времена потребно када се прво прикупљају подаци а потом анализирају у реактивној фази, док уколико се проактвно приступи прикупљању само потенцијалних доказа и само они се потом анализирају, то је и ефикасније и одузима мање времена. Из тог разлога сматра да је пажњу потребно посветити развоју проактивних техника (A. Orebaugh, "Proactive forensics" *Journal of Digital Forensic Practice* 1/2006, 38). Као пример алата, који проактивно прикупља податке, наводи се тзв. *Proactive Object Fingerprinting and Storage (PROOFS).* Алат се заснива на креирању и праћењу својеврсних „потписа" датотека које чине „отисци" створени на основу садржаја датотеке (C. Shields et al., „A system for the proactive, continuous, and efficient collection of digital forensic evidence", *Digital Investigation* 8/2011, 7).

[880] Уређаји за складиштење података (као што су магнетни дискови, силиконски чипови, или чак обични пластични дискови) чувају све информације у бинарном формату (нула и јединица). Да би се структуирали подаци, тако да рачунарски систем може да препозна који битови се односе на исту датотеку, односно који битови чине заједно директоријум, осмишљен је систем датотека. Као што у библиотеци постоји систем картица који идентификује сваку књигу у ком реду и полици се налази и помаже да се књиге пронађу и врате после употребе на место, тако и систем датотека у уређају за складиштење података служи да се подаци у датотекама могу једноставно пронаћи. Уређаји се могу поделити у партиције од којих свака има свој систем датотека како би се омогућило „смештање" датотека у њима. Партиционисање хард диска је аналогно подели зграде библиотеке тако да се створе две одвојене библиотеке, на пример, једна за средњу школу и један за основну школу, свака са својим системима картица. Када је хард диск подељен у два дела, односно партиције, оне ће се појавити као два различита диска у софтверу (на пример, у оперативном систему *Windows* се обично налазе диск *c:>* и диск *d:>*, иако су оба система датотека физички налазе на истом хард диску). Осим тога, могуће је да се једна партиција није ограничена на један хард диск, него се налази на неколико физички одвојених дискова (на пример, рачунарски корисник види само један диск у софтверском интерфејсу, рецимо диск *c:>*, али у стварности обухвата два или више физичких хард диска). Оно што повезује све заједно је систем датотека који је део хард диска или вишеструки хард диск чини да изгледа као јединствена целина за оперативни систем. Више о томе, М. Хајдуковић, *Оперативни системи (проблеми и структура),* ФТН Издаваштво, Нови Сад 2013, 167.

подаци у поседу осумњиченог доказ да је предузео радњу извршења кривичног дела (нпр. постојање датотеке који садржи изворни код за рачунарски вирус који је проузроковао штету великих размера). Ова форензичка анализа је најједноставнија анализа, у смислу да је њен циљ ограничен на утврђивање присуства података без њихове даље анализе. Но, понекад је само проналажење података компликовано, јер је лице употребило одређене анти-форензичке технике.

Форензичар претражује уређај за складиштење да идентификује колико партиција постоји и који систем датотека је коришћен[881], како би се испитале датотеке и пронашли потребни подаци[882]. Системи датотека садрже вредне и форензички значајне информације, али претраживање може представљати изазов. Наиме, ради прегледности великог броја података у меморији уређаја, оперативни системи и апликације користе системе за идентификовање и организовање података у виду назива датотека, екстензија, фолдера и директоријума, а велики меморијски капацитет уређаја за складиштење података готово немогућим чини прегледања садржаја свих датотека појединачно. Из тог разлога, да би *убрзали фазу анализе*, већина аналитичара прво прегледа уобичајене директоријуме за складиштење података, тражећи датотеке са сумњивим називом. Други метод за бржу анализе је да се систем датотека претражи преко кључних речи које су релевантне, а одрђени рачунари имају и сопствене претаживаче (нпр. реч „дете“ ако се трага за приказима дечје порнографије), који имају могућност препознавања слике (а не само преко кључних речи у имену датотеке), а постоје и софтверски алати за препознавање фотогафија на којима су уобичајени прикази дечјег злостављања (чак и преуређене копије тих приказа)[883]. Осим тога, за анализу система датотека у великим рачунарским системима користи се *Data*

[881] Најчешће заступљен систем датотека је Табела за алокацију датотека (*File Allocation Table: FAT*), настао 1980. године и коришћен у првим персоналним рачунарима, и још увек се користи у разним електронским уређајима (у музичким плејерима, камерама, мобилним телефонима итд.) а у широкој је употреби због робусности и широке компатибилности (*Apple* рачунари, *Windows PCs, Linux)* па већина других софтвера може да очита *FAT* партиције. Модерни оперативни системи садрже новије системе датотека које нуде додатне карактеристике, као што су сигурносни приступ кориснику, компресија, енкрипција, дефрагментација и сл, тако *Microsoft Windows* користи *NTFS* систем датотека, *Apple* рачунари користе *HFS+*, док *Linux* може да користи неколико различитих система датотека, као што су *EXT, BTRFS, XFS* или *ReiserFS*. Више о томе, Хајдуковић, *op.cit*, 155-157.

[882] Cross, Shinder, *op.cit*, 238.

[883] Као што је *NetClean Analyze.* https://www.netclean.com/en/analyze/investigations/overview/.

mining, техника анализе података која се заснива на екстраховању значења информације из велике количине података похрањених у базама података[884] применом одређених математичких функција[885].

Посебну пажњу је потребно посветити *избисаним подацима*[886]. Када систем датотека уклања датотеку из рачунарског система, то не значи да датотеку физички брише из меморије уређаја за складиштење података, већ из система датотека уклања референцу ка локацији избрисане датотеке[887]. Но, постоје одређени софтверски алати за трајно (неопозиво) брисање датотека из хард диска, а функционишу на тај начин што се врши непрекидно преснимавање физичког простора за складиштење (где је датотека била ускладиштена) различитим лажним датотекама, како би се осигурало да не остане траг избрисаних датотека.

Осим наведеног, потребно утврдити да ли је корисник применио неку од *антифорензичких техника* у циљу компромитовања доступности или корисности

---

[884] P. Chen, „Discovering investigation clues through mining criminal databases“, *Intelligence and Security Informatics Studies in Computational Intelligence* 135/2008, 179.

[885] Више о овој техници и могућности коришћења у дигиталној истрази, Y. Ku, Y. Chen, C. Chiu, "A Proposed Data Mining Approach for Internet Auction Fraud Detection", *Intelligence and Security Informatics Lecture Notes in Computer Science*, 4430/2007, 240; R. Al-Zaidy et al, „Mining criminal networks from unstructured text documents „, Digital Investigation 8 /2012, 153.

[886] Већина уређаја има четири функције којима се омогућава да се подаци снимају, очитавају, мењају и бришу. Међутим, брисање података из меморије уређаја може бити у различитим формама. У стандардним апликацијама брисање датотеке значи само да се уклањају подаци о путањи ка месту у меморији где се чувају подаци или се подаци просто сматрају избрисаним а преименовани се чувају на другој локацији (нпр. у *Recycle Bin*-у), па се као такви још увек налазе у меморији уређаја и постоји могућност да се они „опораве“ док код нису пребрисани или избрисани трајно. Добра техника за идентификовање садржаја који корисници рачунара покушавају да сакрију је прегледање директоријума обрисаних датотека у оперативном систему (то је, на пример, *Recycle Bin* директоријум у *Windows* оперативном систему). Уколико се уочи незаконити садржај, форензичар може идентификовати из ког директоријума избрисана датотека потиче (на пример, преко наредбе *Restore*) а потом га прегледати ради уочавања додатних датотека са незаконитим садржајем. Чак и када корисници рачунар "испразне“ директоријум обрисаних датотека (на пример, преко наредбе *Empty the Recycle Bin*), ипак постоји могућност за опоравак обрисаних датотека.

[887] Део на хард диску у ком се налази датотека је означена као доступна у систему датотека, као да не постоји датотека у њему. Прегледом свих сектора на уређају за складиштење података које систем датотека препознаје као доступне за чување података и проверавањем да ли постоје ускладиштени подаци у том сектору, могуће је опоравити избрисане датотеке, чак и када је систем датотека више нема референце ка њима. Постоје форензички алати који аутоматки обављају поменуте функције, као што су *TestDisk* и *PhotoRec* које је могуће применити на различитим оперативним системима и системима датотека. У случају физичког оштећења хард диска (на пример, ако је запаљен или изломљен) још увек је могуће да се опораве неке датотеке ускладиштене на њему, испитивањем да ли су магнетни дискови нетакнути, те утврђивањем да ли је могуће повратити магнетне информације кроз растављање дискове и пажљиво читање магнетних информације. У случају оштећења флеш меморије за складиштење, као што *SSD* дискови, које су робуснији од магнетних дискова, поједине флеш ћелије од којих се диск састоји се такође могу испитати, да би се утврдило које од њих још увек функционишу па се са њих могу оправити подаци. Хајдуковић, *op.cit* 167-168.

доказа до који се може доћи применом дигиталне форензике[888]. Учиниоци кривичних дела настоје да отежају рад надлежних органа откривања и гоњења па предузимају кораке како би прикрили трагове свог деловања у виртуелном окружењу, јер је интерес учиниоца да онемогуће прикупљање трагова и доказа против њих, да се време откривања повећа, да оставе трагове који воде до погрешног закључка и слично. Дакле, сврха антифорензичких техника, дакле, може бити онемогућавање прикупљања доказа (сакривањем или уништењем података) или уклањање садржаја из прикупљених података што чини њихову анализу некорисном[889]. Постоји више таквих техника, а најчешће се користе *технике за сакривање података* у систему датотека[890]. Осим тога, садржаје је могуће прикрити употребом енкрипције, компресовања, стеганографије и сл. Наиме, да би се сакриле датотека са подацима, користе се технологије *енкрипције* за шифровање датотека па чак и целог хард-диска[891], којим се онемогућава приступ садржајима неовлашћеним корисницима односно онима којима није

[888] R. Harris, „Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem, *Digital Investigation* 3/2006, 44-45.

[889] *Garfinkel* указује да, уколико се настоји да се прикупе подаци упркос примењеним анти-форензичким техникама, потребно је претходно и правовремено утврдити који подаци имају приоритет приликом прикупљања и обезбеђења и пажњу посветити развијању алата и техника који проактивно приступају прикупљању података (Garfinkel, "Anti-forensics: Techniques, detection and countermeasures, 78). Ипак, иако је за откривање појединих техника за сакривање података потребно користи специјалне алате, за већину је довољна свест да постоји могућност прикривања и логична употреба уобичајених техника. Cross, Shinder, *op.cit*, 238.

[890] Подаци се могу сакрити у меморији уређаја и тиме бити невидљиви приликом прегледа меморије коришћењем уобичајених системских наредби и програма (H. Khan, M. Javed, SA. Khayam, F.Mirza, „Designing a cluster-based covert channel to evade disk investigation and forensics“, *Computers and Security* 1/2011, 38). Осим скривања у *slack* простору, постоје скривене партиције које оперативни систем не препознаје одмах, али које је рачунарски корисник поставио тако да само он може приступити њиховом садржају. Корисници могу створити фалсификоване податке (нпр. креирањем лажних заглавља у електронској поруци или изменом тачног времена у метаподатку датотеке) или користити *прикривене канале у протоколима за комуникацију* (изменом неколико поља у заглављу поруке приликом остваривања комуникације) и тиме сакрити податке који се преносе у рачунарској мрежи. Могуће је применити технику којом се валидни подаци током процеса прикупљања замењују фабрикованим подацима (D.Bilby, „Low down and dirty: anti-forensic rootkits“, Proceedings of Black Hat Japan 2006, 17; L. Milkovic, *Defeating Windows memory forensics*, http://events.ccc.de/congress/2012/Fahrplan/events/5301.en.html). Осим тога, малвер у рачунарском систему може бити тако инсталиран да, уколико уочи присуство форензичког алата за прикупљање *RAM* меморије (јер је подешен да надледа систем), „заблокира“ хардвер на ком је инсталиран алат и тиме онемогући процес прикупљања података или пак да прикрије постојеће датотеке лажним. (C. Malin, E. Casey, , J. Aquilina, *Malware Forensics: Investigating and Analyzing Malicious Code*, Syngress, Boston 2008, 37-38).

[891] Технологије енкрипције су уграђене у већину модерних оперативних система (*Bitlocker* у *Windows*-у 7, *FileVaul*t у *MacOS X*-у, *eCryptFS* у Linux-у), док је у ранијим верзијама оперативних система енкрипцију било могуће извршити инсталирањем софтвера као што су *TrueCrypt* и *PGP*.

познат кључ за декприцију[892]. Иако је готово немогуће дешифровање без приступа кључу. Постоји неколико могућности за покушај идентификације кључа[893], а у појединим државама постоји законска могућност да надлежни органи под принудом затраже од корисника да им открије лозинку за приступ њиховим уређајима за складиштење.[894] Уколико су, пак, коришћене технике *стеганографије*, не само да је садржај податка недоступан, него је непозната и чињеница да податак постоји[895], јер је стеганографија техника сакривања одређене поруке или других садржаја у одређеној датотеци, које није могуће уочити простим увидом у датотеку (као што је дигитална фотографија, али их форензичар може открити кроз статистичку анализу сликовних датотека како би се утврдило да ли садрже необичне поставке)[896]. Уколико се сумња на присуство

[892] Енкрипција је математичка техника модификовања дигиталног садржаја тако што се мењају битови (нула и јединица) кроз примену математичких операција, што чини дигитални садржај неразумљивим. Једини начин да се промени садржај односно врати у оригинални јесте применом обрнуте математичке операције. За сваку операцију шифровања, постоји само једна операција дешифровања, јер су математичке формуле шифровања и дешифровања јединствено повезане и упарене, као брава и кључ за ту браву. C. Hargreaves, H. Chivers, „Recovery of encryption keys from memory using a linear Scan", *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. IEEE Computer Society*, 1374. Форензички истражитељ који не зна или нема приступ математичкој формули за декрипцију, заправо нема кључ за дешифровање и неће практично никад моћи да приступи шифром заштићеним подацима. Могуће је пробати различите шифре, једну по једну, и могуће је да ће у неком тренутку истражитељ пронаћи прави јединствени кључ за дешифровање, али у је пракси ово неизводљиво, покушај дешифровања података би могао да потраје неколико година, ако не и много дуже, чак и када би се користили најмоћнији рачунари у свету. Више о значењу енкрипције и криптографије,.McQuade, *op.cit*, 39-41.

[893] Уколико истражитељ има списак познатих лозинки осумњиченог, прво треба да покуша са њима, у супротном, може да покуша са уобичајеним лозинкама, које су често састављене од речи из речника. Неке студије су показала да многи корисници користе лозинке једноставне за памћење и, као што су 123456, пассворд, Суперман, или фудбал и списак најчешће коришћених лозинки се лако може добити претраживањем Интернета. Друго, за кључеве за шифровање које снабдева рачунарска мрежа, администратор мреже има копије кључа и може бити у стању да дешифрује шифровани диск. Ово је случај за *BitLocker* шифровање рачунара у *Windows Active Directory*. Више о томе, A. Marcella, D. Menendez, *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Auerbach Publications, New York 2002, 278-286.

[894] Као на пример, у Великој Британији. C Soghoian, „Caught in the cloud: privacy,encryption, and Government back doors in the Web 2.0 era", *Journal on communication and high technology law* 2/2010, 378. Упор. B. Chatterjee, „New but not improved: revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions", *International Journal of Law and Information Technology* 3/2011, 267. Више о томе биће речи у Четвртом делу.

[895] Rekhis, Boudriga, *op.cit*, 970.

[896] О стеганографији, В. Куњадић, „Стеганографија као метод у супростављању високотехнолошком криминалитету, *Криминалистичко форензичка истраживања* 1/ 2011, 217-230.

скривених садржаја у датотеци, могуће је употребом одговарајућих софтвера за стеганографију екстраховати те делове датотеке[897].

Форензичка анализа датотеке разликује се у односу на анализу система датотека по томе што се овом анализом не утврђује да ли одређена датотека, односно документ постоји, него је њен циљ сазнавање што је више могуће информација о датотеци пронађеној у рачунару, те може да да одговор на питање ко је створио датотеку, да ли је датотека измењена и да ли постоје скривени подаци у датотеци. Наиме, систем датотека у ком су складиштене датотеке садржи о њима метаподатке (односно податке о податку) а које се односе на све остале информације о датотеци осим садржаја датотеке, као на пример датуме и време када је датотека креирана, да ли је и када датотека последњи пут модификована и када јој је последњи пут приступљено. За анализу метаподатака најчешће се користе две технике: *Time frame analysis*[898] и *Ownership and possession analysis*[899]. Сви ови подаци су веома корисни, јер се уз помоћ њих се може идентификовати извор датотеке, односно корисник који је датотеку створио[900].

---

[897] За опис техника на којима се заснивају доступни софтвери за стеганографско прикривање, Vacca, *op.cit*, 498.

[898] Анализа временских метаподатака датотеке показује датум и време када је датотека креирана, измењена, када јој је последњи пут корисник приступио, преузео са Интернета и слично. Ови метаподаци су корисни да се утврде временски периоди релевантни за одређени догађај, а у вези са подацима о времену и датуму који се чувају у логовима система датотека, могуће је показати који од улогованих корисника је предузео одређене радњу на датотеци. Cross, Shinder, *op.cit*, 237. Више о томе, C.Hosmer, „Proving the Integrity of Digital Evidence with Time", I*nternational Journal of Digital Evidence* 1/2002, 3-4.

[899] Анализа „власништва" може да укаже на корисника који је створио, изменио или приступио датотеци. Cross, Shinder, *op.cit*, 239. О анализи, C. Chasky, „Who's At the Keyboard? Authorship Attribution in Digital Evidence Investigations", *International Journal of Digital Evidence* 1/2005, 5-6.

[900] На пример, датотека једне фотогарије у *EXIF* секцији садржи као метаподатке информације о томе када је фотографија снимљена, у којој експозицији, серијски број дигиталне камере, географксе координате места где је фотографија снимљена (дигиталне камере које немају уграђен *GPS* не генеришу ове метаподатке, али мобилни телефони са дигиталним камерама то чине без обзира на то да ли је у тренутку настанка фотографије *GPS* био активиран, и то са прецизношћу до 10 метара у односу на тачно место настанка фотографије, односно израчунавајући географске кооридинате са прецизношћу до неколико километара) и слично. Ове податке аутоматски очитава сваки софтвер за преглед и уређивање фотографија, као и оперативни систем, па ако би се код осумњиченог лица пронашла дигитална камера са истим серијским бројем као што је серијски број у метаподацима одређене фотографије, та подударност би могла указивати на идентитет креатора фотографије. Међутим, лице може покушати да те метаподатке измени, али се свака измена може уочити анализом *EXIF* секције у датотеци, с обзиром на то да технички подаци о фотографији у *EXIF* секцији остају неизмењени. За датотеке са текстуалним садржајем, на пример, могуће је из метаподатака утврдити колико дуго је текст преуређиван, историју едитовања, укључујући имена корисника који су их едитовали, назив штампача који је одштамап текстуални документ и слично.

Форензичка анализа непостојаних података и оперативног регистра датотека[901] за разлику од форензичке анализе система датотека која за циљ има утврђивање да ли постоје одређене датотеке у рачунару, и форензичке анализе датотеке, којој је сврха утврђивање што више података о датотекама, служи да се утврди што више информација о рачунарском систему. Док резултат прве анализе може бити идентификовање присуства одређеног незаконитог садржаја, као што је рачунарски вирус, а друге анализе да је вирус креиран на рачунару осумњиченог, трећа врста анализе може да помогне у решавању ситуације у којој осумњичени тврди да није он тај који је креирао вирус пронађен на његовом рачунару. Форензичка анализа непостојаних података и регистра датотека резултира доказима о томе који софтвери, процеси и услуге су били покренути, односно коришћени, који корисници су били пријављени на систем и у ком тренутку, па је ова форензичка анализа нарочито корисна када постоји сумња да је треће лице (не корисник) приступило неовлашћено рачунарском систему. Међутим, форензичка анализа непостојаних података је могућа само ако се врши прикупљање података из „живог“ система[902], јер је овом форензичком техником могуће анализирати само податке који се тренутно налазе у рачунарском систему (односно, када се врши *in situ* прикупљање података)[903], док анализа регистра датотека има својеврсни историјски контекст, односно применом ове технике се утврђује чињенице из прошлости[904].

---

[901] *Live data forensics and log file forensic analysis.*

[902] Више о форензичкој анализи непостојаних података, M. Kiley, S. Dankner, M. Rogers, „Forensic Analysis of Volatile Instant Messaging“, Ray, *op.cit*, 129-139.

[903] Форензика „живог“ система (*Live forensics*) подразумева обраду покренутог рачунарског система и прикупљање непостојаних података (као што су подаци о тренутној конфигурацији уређаја, подаци из *RAM* меморије који се губе моментом искључења уређаја) и уочавање свих активних процеса у рачунару (на пример, да ли је одређени рачунарски вирус тренутно активан у систему). Примера ради, уколико осумњичено тврди да није поставио недозвољен садржај у рачунар него да је неовлашћено лице приступило у рачунар и у њему складиштио те садржаје, применом ове форензичке технике може се утврдити да ли су се други корисници пријавили у систем или да је био покренут одређени софтвер који је омогућио приступ рачунару преко Интернета. Постоје бројни алати за форензичку анализу живог система, а један од најчешће коришћених и доступних преко Интерпола је софтверски алат *COFEE*. Овај софтвер садржи преко 100 тестова, може се користити преко *USB*-а и даје станрадизован извештај који омогућава анализу прикупљених података и презентовање на суду.

[904] Оперативни регистар датотека је део оперативног система и служи за праћење и снимање процеса који се одвијају у рачунару и у њему је садржан својеврсни хронолошки распоред дешавања у рачунару, а осим тога чува податке о приступу рачунару. Према томе, у регистру се могу пронаћи докази о томе који корисник и када се логовао у систем, који софтвер и која услуга је покренута и у ком тренутку, што су корисни подаци у случају сумње да је неовлашћено лице приступило рачунарском систему.

Форензичка анализа података из рачунарске мреже има за циљ да се идентификује извор/одредиште комуникације остварене преко рачунарске мреже, односно извор напада преко Интернета. Иако је на Интернету на први поглед изражена анонимност (исказана кроз афоризам: *On the Internet nobody knows you are a dog*) која се огледа у могућности коришћења пседуоанонимних и лажних корисничких налога, у случају истраживања кривичног дела почињеног употребом ове рачунарске мреже, надлежни органи настоје да утврде прави идентитет лица који је осумњичени учинилац кривичног дела, при чему овај процес утврђивања везе између виртуелног и стварног идентитета пред органе намеће оперативне и процедуралне компликације. Постоје два основна извора података који се користе у процесу идентификације лица у вези са активностима на Интернету: подаци створени коришћењем услуга електронских комуникација и подаци који се односе на садржај комуникационих активности осумњиченог. Помоћу прве врсте података може се идентификовати извор и одредиште комуникације на основу неког јединственог параметра, односно уређај са ког је упућен комуникациони садржај а тиме и одређеног корисника (нпр. адресу електронске поште). Међутим, уколико више корисника користи уређај за остваривање приступа мрежи, изазов може бити како доказати да је одређено лице користило опрему или уређај у релевантно време. Од успешног утврђивања ових веза у фази истраживања зависи могућност одбране да се позива на аргумент да је било које лице могло у одређено време бити повезано на мрежу и извршити кривично дело а не само осумњичени[905].

У највећем броју случајева форензичар је кроз анализу оперативног регистра датотека дошао до одрђене *IP* адресе преко које је остварена малициозна комуниакција ка рачунару или *FQDN* име домена и *IP* адресу сајта са ког је преузет илегални садржај или заглавље електронске поште које садржи одредиште. Полазећи од овога, форензичар анализом *IP* адресе и имена домена које је извршилац користио трага за везама са другим Интернет ресурсима, да би идентификовао учиниоца или да би пронашао трагове других кривичних дела. Када је потребно идентификовати осумњиченог, надлежни органи могу наићи на одређене препреке, чак и уколико су познате *IP* адресе помоћу којих се остварује

[905] D. Chaikin, „Network investigation of cyber attacks: the limits of digital evidence“, *Crime, Law and Social Change* 4-5/2006, 250.

комуникација између корисника рачунарске мреже. То неће бити проблем када се користе стататичке *IP* адресе (које су логички повезане са неким псеудонимом и именом домена и једним уређајем), али *IP* адресе се, као што је објашњено, додељују динамички сваки пут када се корисник пријави на мрежу. Стога је идентификацију помоћу познате *IP* адресе потребно вршити кроз четири фазе[906].

Најпре се утврђује изворна *IP* адреса коју треба повезати са уређајем, односно корисником. Проблем проистиче из чињенице да изворна *IP* адреса може понекад бити намерно прикривена *(spoofed IP address*[907]), тако што се у заглављу пакета који је шаље наводи лажна *IP* адреса[908], међутим изворна *IP* адреса одредишта се применом одговарајућих алата увек може утврдити[909]. Потом се утврђује ком ентитету је одређена *IP* адреса додељена, а то може бити пружалац услуга електронских комуникација или одређена компанија која има своју мрежу или појединац уколико има фиксну, статичку *IP* адресу[910]. Следећој фази се приступа уколико се утврди да блок *IP* адреса припада одређеном ентитету, како би се утврђена *IP* адреса повезала са тачно одређеним корисником, проучавањем

---

[906] R. Clayton, *Anonymity and Traceability in Cyberspace*, University of Cambridge 2005: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf.

[907] *http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm.*

[908] Прикривање *IP* адресе може учинити појединац на више начина, а ове услуге се и комерцијално нуде, што је карактеристично за *darknet (*таква се услуга пружа на сајту *www.anonymizer.com)*

[909] *Софтвер за електорнску пошту* садржи у заглављу сваке поруке одређене техничке информације, које нису видљиве на први поглед. Поруке се шаљу преко више сервера (који се зову агенти за слање поште: *Mail Transfer Agent* (MTA) и сваки њих оставља траг у заглављу поруке у виду информације са које *IP* адресе и у које време је порука прошла кроз тај сервер на путу ка свом одредишту, тако да је анализом података у заглављу поруке могуће утврдити хронолошку путању којом се порука кретала до сандучета за пријем поште. Заглавље поруке је у стандардизованом Интернет формату (RFC 2822) и садржи *IP* адресе са које је порука послата и у које време. Међутим, није у свим случајевима једноставно утврдити *IP* адресу пошиљоца: уколико је пошиљалац „упао“ у нечији рачунар употребом ботнета и са његове *IP* адресе послао поруку (у случају сумње да је тај рачунар хакован, анализом регистра датотека могуће је утврдити извор са ког је напад на рачунарски систем извршен) или је послао преко јавно доступне мреже (нпр. у лобију хотела или у Интернет кафеу) и тада је корисно прегледати снимке камера за видео надзор простора који је покривен том рачунарском мрежом, уколико су доступни или остварити увид у регистар корисиника, да би се идентификовала лица која су приступила мреже у одређено време. О техникама прикупљања података о саобраћају на Интернету, Garrison, *op.cit*, 24-58.

[910] Коришћењем одређених софтвера се прегледају базе података реистратора (који додељују *IP* адресе на локалном, регионалном и националном нивоу), што може бити проблем јер они нису дужни да проверавају тачност података регистрованих ималаца *IP* адреса. Алтернативно се може користити апликација за утврђивање којим путањама се шаљу пакети преко Интеренета (нпр. *http://www.webopedia.com/TERM/T/traceroute.html*).

регистра пријављивања на мрежу[911]. Ова фаза не може дати резултате ако се ради о мрежи која корисницима гарантује анонимност, као што је у Интернет кафеу, ако се корисник пријавио на необезбеђену бежичну мрежу или ако ентитет не одржава регистар пријављивања на мрежу[912]. У последњој фази се долази до података о кориснику налога који су регистровани код пружалаца комуникационих услуга (а постојање тих регистара зависе од природе улуга које се пружају и начина плаћања тих услуга[913]). Из наведеног се може уочити да идентификација лица на основу *IP* адресе није увек једноставан метод нити представља свемогући магични штапић[914], већ зависи првенствено од регистара и евиденција које воде поменути субјекти (из тога разлога је и разматрано прописивање обавеза задржавања података[915])

3.2.5. Припрема електронских доказа за презентовање у кривичном поступку

Највећи изазов када се говори о електронским доказима јесте питање њихове аутентичности:

- Да ли су рачунарски подаци, који се могу употребити као доказ, измењени?
- Да ли је програм, коришћен као форензички алат за обраду рачунарских података, поуздан?
- Да ли је осумњичени аутор података, који се могу употребити као доказ?

Методологија развијена у оквиру дигиталне форензике, која се и даље усавршава, директно је усмерена ка превазилажењу поменутих изазова. Одређене

[911] Постоје системи који региструју почетак и крај сесије, као што је *Dynamic Host Configuration Protocol: DHCP* који региструје динамичко додељивање *IP* адреса.
[912] Више о форензичкој обради *wireless* мрежа, Kipper, *op.cit*, 57-62.
[913] Код бесплатне услуге приступа Интернету од кључног значаја за идентификацију корисника је тзв. *Calling Line Identity (CLI)* број.
[914] Идентитет осумњиченог се може утврдити и помоћу друге врсте података које лице свесно или несвесно оставља као траг обављањем активности на Интернету. Примера ради, „колачићи“ могу бити тако конфигурисани да укључују имена корисника, његове лозинке и друге идентификационе податке. Креатор вируса у једном случају је био идентификован уз помоћ коментара о својим активностима које је остављао на разним форумима користећи псеудоним. G.Gupta et. al, „Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol“, *International Journal of Digital Evidence* 4/2004, 7.
[915] Више о томе у Осмом делу.

компоненте те методологије (првенствено *Chain of custody,* креирање клона и рад на њему, документација и верификација резултата употребом приказаних криптографских функција, односно *hash* вредности) су и осмишљене да би се обезбедило да изворни подаци не буду измењени.

У погледу форензичких алата који су у употреби, треба имати на уму да су они дизајнирани тако да аутоматски и аутономно извршавају задатке у оквиру форензичке анализе. Ти алати су програмирани тако што су се на основу знања програмера користили алгоритми у коду за писање софтвера, али ако ти кодови нису доступни форензичару који употребљава тај алат у току дигиталне истраге, питање је са колико поузданости он може тврдити да су резултати валидни. Што се тиче поузданости софтверских алата, иста се може проверити кроз меру прихваћености алата, поновни преглед (*peer review*) и индивидуално тестирање. Наиме, у појединим случајевима као резултат форензичке анализе може се појавити велики број доказа, док у другим резултат може бити свега неколико или чак једна датотека или неколико бајтова података. У овим случајевима се препоручује да се понови испитивање са потпуно другачијем алатом. Наиме, у сваком софтверу постоје минорне аномалије у програмирању (тзв. *bug*) које могу да доведу до нетачних чињеница у извештају који генеришу (нпр. датум и време). Да би се обезбедила већа поузданост и веродостојност резултата, потребно је поновити испитивање које треба да да потпуно исти извештај[916]. Употреба софтверских алата и поступање по креираним процедурама, учинила је прикупљање података из рачунарских система и мрежа стандардизованим, али изазов представља преглед и анализа прикупљених података са ограниченим временским оквирима и осталим ресурсима, а нарочито некритичко прихватање резултата рада алата, што је недопустиво јер се може поставити питање, да ли резултате даје форензички алат или стручно лице.

Још један изазов у области дигиталне форензике односи се на начин који су докази представљени у извештајима. Наиме, уобичајено је да форензичари користите више рачунарских форензичких алата у току форензичке анализе (као фазе дигиталне истраге) како би проверили постављене хипотезе кроз добијене

[916] Понављање испитивања употребом другог софтверског алата (тзв. Dual Tool Verification) препоручују и смернице добре праксе. ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf, 50.

резултате, при чему се може десити да коришћени алати генеришу различите ставке у извештајима о дигиталним доказима, јер не постоје стандарди у функцији за извештавање форензичких алата. Исто тако, форензичар се може сусрети и са проблемом интеграције софтверски генерисаних извештаја о дигиталним доказима у званичне извештаје о дигиталној истрази. Из тог разлога се као неопходност указује на потребу да се кроз преглед различитих форензичких алата створе стандардне функције за генерисање извештаја како би се очувао валидност резултата, а тиме и интегритет дигиталних доказа [917].

Проблем може настати и у вези са пребрзим и олаким доношењем закључака. Као пример пребрзог доношења закључка, може се навести ситуација у којој форензичар испитујући доказе на диску једне корпорације, прегледа рачунар осумњиченог лица А. ком је додељено име „*jasuspect*“ за идентификацију корисника рачунарске мреже у корпорацији, наведе у извештају „Корисник лице А. је извршио одређену радњу у рачунару, јер запис о догађајима (*event log)* показује да је корисник приступио датотеци ... “. Међутим, овакав закључак није исправан. Запис о догађају показује само да је датотеци приступљено са рачунара који је у мрежи регистрован као *jasuspect,* али не повезује извршење радње са физичким лицем које је за тим рачунаром фактички предузимало радње. Исправан закључак би био: „Корисник са идентификацијом *jasuspect* (која је додељена лицу А.) је извршио одређену радњу у рачунару...“ [918].

У суштини, са електронским доказом је потребно поступати као са сваким другим доказом, јер у случају сумње да је доказ незаконит или неаутентичан, окривљени и бранилац могу довести у питање прихватљивост употребе доказа, па је на тужилаштву да ту сумњу отклони. Уколико тужилаштво поднесе суду телефонски рачун или уговор који доказује да је осумњичени био корисник услуга одређеног пружаоца услуге електронске комуникације, ово ће суд обично прихватити, али ако тужилаштво тврди да је осумњичени избрисао све податке на хард диску, форматирао га и онда избацио кроз прозор са десетог спрата, али су подаци опорављени коришћењем услуга одређене фирме за опоравак рачунарских

[917] О предлозима за такве стандарде, I. Baggili (ed.), *Digital Forensics and Cyber Crime* (Second International ICST Conference ICDF2C 2010 Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers), Springer, Heidelberg-Dordrecht 2011, 78-95.
[918] Наведено према: Brown, *op.cit*, 21.

података, бранилац окривљеног може довести у питање оправданост и прихватљивост оваквог метода опоравка података, па ја на тужилаштву задатак да коришћену методологију прикаже прихватљивим. У том смислу је корисно да као сведок буде позвано лице које је руковало електронским доказима, да би се приказала објективност у поступању са потенцијалним изворима електронских доказа, као и континуитет и интегритет доказа, приказивањем начина како се до доказа дошло, односно сваке фазе у прикупљању и обради података. Из тог разлога је цео процес прикупљања и обраде доказа потребно документовати, а доказ као резултат процеса сачувати у таквој екстензији да треће лице може поновити исти процес и доћи до истих резултата. Наиме, може се ангажовати вештак који даје научно и стручно поткрепљена објашњења процеса и резултата како би се утврдило да је интегритет електронског доказа очуван, да му се може поклонити вера и да се на њему може засновати осуђујућа пресуда.

У вези са могућим улогама лица са стручним знањем, потребно је да постоји одређена равнотежа, јер ниједна од екстремних ситуације није прихватљива – нити се може очекивати од суда да разуме до детаља техничке ствари нити, пак, да прихвата без поговора и преиспитивања технике и методе које су коришћене у обради рачунарских података као магију. Могуће решење је *peer review* – да ако други стручњак у релевантној области проучи технику, тестира је и верификује резултате, суд прихвати доказ. Ни у једној области није прихватљиво да суд слепо верује вештаку (што важи и у погледу информационих технологија), него је дужан да и налаз и мишљење вештака, као и исказ сведока (стручног лица), здраворазумски и критички у складу са слободном оценом доказа процењује.

У вези са оценом резултата вештачења и коришћених метода, у англосаксонској литератури, која обрађује питање валидности појединих научних техника које се могу користити за добијање прихватљивих научних доказа на суду, аутори указују на потребу примене тзв. Фрај стандарда (*Frye test*), по ком суд може прихватити доказ до ког се дошло применом нове научне технике само уколико је она генерално прихваћена у широј научној заједници[919]. Да би се

[919] Ради се о стандарду који је установљен прецедентом у случају *Frye v. U.S.* Фрај је име окривљеног у поступку у ком је као прецедент усвојен захтев да се нова техника може прихватити након што се, најпре одреди научна област којој техника припада, а потом утврди да ли принципе на којима се техника заснива прихата већина представника те научне области. Наведедно према:

утврдило да ли постоји потреба за ангажовањем вештака у кривичном поступку, амерички судови од 1923. године користе овај стандард постављањем два питања: да ли је доказ релевантан за случај и да ли је доказ генерално прихватљив у научној заједници. Врховни суд САД је 1993. године допунио овај стандард за оцену прихватљивости научног доказа тако што установио да су „судије дужне да процењују прихватљивост научног доказа", јер постоји потреба не само да је доказ релевантан, него и да је коришћени научни метод поуздан. Наиме, одређени научни метод може резултирати прихватљивим доказом у кривичном поступку под условом да задовољава захтеве постављене у оквиру тзв. Доберт теста (*Daubert test*[920]*),* а ти захтеви су следећи: да ли теорија или техника може бити (односно, да ли је била) емпиријски проверена; да ли је теорија или техника била подвргнута рецензији и да ли је публикована; да ли је позната потенцијална стопа погрешних резултата; да ли се техника заснива на специјализованим вештинама и опреми коју је примени један стручњак или је могу применити, односно поновити на исти начин и други стручњаци; да ли се техника и резултати њене примене могу објаснити на довољно јасан и једноставан начин тако да суд може разумети суштину?[921] Осим ових, постоји још стандарда који су значајна за оцену да ли је одређена научна метода прихватљива, а то су: Кополино стандард (*Coppolino standard* утврђен у прецеденту *Coppolino v. State* из 1968. године), по ком „суд може дозволити коришћење метода нове, чак контроверзне, односно непотврђене научне дисциплине, уколико се традиционалним потврђеним методама не може одређени проблем објаснити", и Маркс стандард (*Marx standard* утврђен у прецеденту *People v. Marx* из 1975. године), по ком је „суд задовољен уколико не постоји потреба да „жртвује" здрав разум да би разумео и проценио научну експертизу која је представљена у поступку доказивања"[922].

О прихватљивости и доказној вредности електронског доказа у нашој судској пракси тешко је за сада говорити, с обзиром да је незнтатан број предмета за кривична дела која се доказују електронским доказима. И поред постојања

House of Commons Science and Technology Committee, *„Forensic Science on Trial"* 2005, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf, 75.

[920] Ради се о стандарду који је установљен прецедентом у случају *Daubert v. Merrell Dow Pharmaceuticals Inc (509 US 579/1992).*

[921] Brown, *op.cit*, 31-32.

[922] Vacca, *op.cit*, 55.

слободне оцене доказа, сматрамо да је корисно постављање јасних усмеравајућих правила у погледу оцене од стране суда[923]. Ако се поузданост и/или потпуност потенцијалног доказа доведу у питање, његова доказна вредност се умањује, а тиме се доводи у сумњу и прихватљивост употребе као доказа. Питање да ли је доказ прихватљив и колика је његова доказна вредност је правно питање које решава суд. Из тога разлога је потребно да је дигитална истрага спроведена тако да се не умањује аутентичност доказа који су њен резултат, а суд може неколико критеријума користити за процену да ли је процес форензичке анализе задовољио захтеве у оквиру концепта научног доказа:

1. У погледу тумачења значаја електронског доказа, суд треба да утврди да ли су и на који начин коришћене технике утицале на измену оригиналног формата електронског записа;
2. Грешке, недоследности и губици у току форензичке анализе нису реткост и на њих је потребно указати у извештају о резултатима, па суд може поставити питање: да ли су све грешке идентификоване и на задовољавајући начин објашњен њихов утицај на тачност и поузданост доказа?
3. Требало би да буде задовољен и критеријум транспаретности, односно да се одговори на следеће питање: да ли резултати процеса дигиталне форензике могу бити прегледани и потврђени од стране трећег лица? Да би се омогућила провера поузданости и тачности резултата форензичке анализе, потребно је да тај процес буде транспарентан и подобан за проверу и потврду резултата, што се се може постићи документвањем свих предузетих корака, навођење котишћених хардверских и софтверских алата, описивањем окружења у ком је анализа вршена, навођењем проблема, грешака и недоследности.
4. Осим наведеног, суд би требало да процени и да ли је анализу извршило лице са довољно релевантног искуства у дигиталној форензици[924].

[923] Потреба унифицираног поступања у погледу услова прихватања електронских доказа од стране суда истакнута је и у Препоруци Савета Европе – *Recommendation 95 (13) relating to problems of criminal procedural law connected with information technology*, Sept. 1995.
[924] R. McKemmish, „When is Digital Evidence Forensically Sound?“, Ray, Shenoi, *op.cit*, 29-31.

С обзиром на то да је неминовно да дигитални докази постају све присутнији у кривичним поступцима, а да орган поступка не поседује потребно знање за разумевање метода дигиталне форензике, све ће значајнија бити улога стручњака ове ове научне дисциплине. Тежња за „научним“ доказима је оправдана, нарочито у све већем броју случајева у којима је извршена дигитална истрага за чије разумевање је потребно специјално уско техничко знање. Са друге стране, постоји ризик од олаког прихватања нових научних метода којим се долази до доказа за потребе кривичног поступка а који нису претходно на одговарајући начин проверени и потврђени, каква је ситуација са дигиталном форензиком. Из тог разлога је потребно да и суд, на коме је и даље одговорност за оцену доказа, да када пред собом има доказе – налаз и мишљење вештака или исказ сведока (стручног лица које је учествовало у увиђају или непосредном извршењу радњи и мера а које се односе на поступање са електронским доказима), да процењује валидност и поклања веру спрам свог уверења, а не да узима олако и без резерве исказе лица ма у којој мери се односили на техничке детаље. Да би то могао да уради, сматрамо да је неопходно да судија има минимална знања и о дигиталној истрази, а да процесно законодавство у довољној мери и на одговарајући начин уреди предузимање приказаних активности дигиталне форензике, прописивањем одређених радњи и мера за прикупљање електронских доказа.

Осми део

СУПРОТСТАВЉАЊЕ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛУ И ЉУДСКА ПРАВА

Право на приватност је означено као „право појединца да буде остављен на миру“[925] пре више од сто година, али овакво посматрање може и даље да буде полазна основа за одређивање суштине концепта приватности, као динамичке категорије коју је потребно прилагодити вредностима у измењеном окружењу. Употреба достигнућа информационих технологија изменила је начин на који појединци обављају свакодневне активности и комуницирају у кибер простору а при томе су спремни да се дела своје приватности одрекну[926]. Међутим, *полазимо од тога да је заштиту* права на правну личност, те права на слободан развој личности кроз право на приватност и заштиту података о личности у *online* окружењу, *нужно обезбедити правним прописима који садрже чак строжа и прецизнија правила* у односу на правила која штите те вредности у *offline* окружењу. Наведене права је могуће ограничити само ради заштите општег интереса а ово ограничење треба да буде сразмерно и одређено законом. С тим у вези се поставља питање до које мере и у којим случајевима је ова права могуће и оправдано ограничити, односно који је *обухват овлашћење* надлежних органа *да прикупљају доказе* за потребе кривичног поступка за дела високотехнолошког криминала (чије радње се остварују у кибер простору) *предузимањем одређених*

[925] S. Warren, L. Brandeis, ‘The Right to Privacy’, *Harvard Law Review*, 5/1890. Наведено према D. Ritchie,”Is it possible to define ‘privacies’ within the law? Reflections on the ‘securitisation’ debate and the interception of communications”, *International Review of Law, Computers & Technology* 1–2/2009, 29. У често цитираном делу аутора који означавају приватност на овај начин, наведено је да су „фотографије угрозиле светост приватног и породичног живота, а да ће ова угроженост бити још израженија са даљим развојем механичких уређаја .... да ће се појединац повлачити у осаму и сферу приватности, која штити људски интегритет, а да закон треба да штити ту сферу ради слободног развоја личности“. Ова предвиђања су се показала као делимично тачна. С једне стране, технолошки развој јесте са собом донео могућност високог степена ризика од нарушавања приватне (и најинтимније) сфере појединца, али се, са друге стране, однос према приватности појединца променио.

[926] Иако прописи гарантују лицима право на заштиту података, корисници информационих технологија се својевољно одричу те заштите прихватањем услова коришћења појединих услуга и производа. Више о томе, T. Dreier, ‘‘Opt in’’ and ‘‘opt out’’ mechanisms in the Internet era – towards a common theory“, *Computer Law and security Review* 26/2010, 145-146.

радњи и мера којим у великој мери могу задирати у приватну сферу појединаца и прикупљати велики број података о њима.

Након терористичких напада током 2000-тих година, прописивање посебних оперативних и процесних овлашћења потребних за сузбијање тешких облика криминала, међу њима и високотехнолошког криминала, постало је законодавни тренд у великом броју држава, као вид респресивног реаговања (али са проактивним елементима) на повећан ризик по општу безбедности. За прописивање интрузивних специјалних истражних техника у циљу јачања механизама кривичног правосуђа за одговор на претње тероризма и других нарочито тешких кривичних дела била је обезбеђена подршка јавности. Но, терористички напади се чак могу посматрати као повод, а не узрок оваквог легислативног тренда и захтева јавности за виши степен секуритизације[927], јер су идеје о увођењу посебних истражних техника и употреби информационих технологија за појачан надзор активности корисника биле на политичкој агенди одређених држава и пре 2001. године, а ови догађаји су послужили као катализатор за оправдање проактивности у супротстављању одређеним безбедносним ризицима[928]. Као последица наведеног, осим у САД, и на европском контитенту се може уочити повећан број легислативних иницијатива које су имале за циљ омогућавања прекограничне полицијске и правосудне сарадње у кривичним стварима, а међу њима је и усвајање и широка подршка Конвенцији о високотехнолошком крииминалу.

Осим тога, легитимност је стекла и употреба тзв. благих безбедносних мера (*soft security*[929]) које се остварују кроз надзор и праћење активности корисника рачунарских уређаја и мрежа, те анализу и коришћење података садржаних у разним базама података. Могућности надзора активности грађана су са развојем технологије постајале све шире: од прислушкивања статичног телефона, пресретања електронске поште, праћења преко паметних мобилних телефона са *GPS* додатком, до надзора у реалном времену *VoiP* комуникација и употребе

[927] О концепту „друштво максималне сигурности“ (*maximum security society),* S. Gutwirth, *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002, 71-78.
[928] *Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs* (LIBE)-Technical Report Series, 2003, ftp://ftp.jrc.es/pub/EURdoc/eur2O823en.pdf, 95-96.
[929] K. Ball, F. Webster, *The Intensification of surveillance: crime, terrorism and warfare in the information age*, Pluto Press, New York 2003, 3-4.

техника предиктивног профилирања корисника и слично[930]. Истовремено, огромне количине личних података корисника Интернета се прикупљају и обрађују од стране различитих актера (при чему се подаци разним техникама укрштају и сравњују) кроз различите механизме којих појединац често није ни свестан. Како се радње дела високотехнолошког криминала предузимају и њихове последице наступају у техничком окружењу, може се рећи да *употреба информационих технологија* (без које радње не би ни могле бити извршене) представља *битну карактеристику* овог вида криминала, па је *за откривање и доказивање дела је неопходно применити управо методе и технике информационих технологија*.

Постоји, међутим, *дилема* је да ли приликом регулисања природе и обима овлашћења надлежних органа откривања и доказивања кривичних дела високотехнолошког криминала *дозволити примену поменутих метода и техника*, те да ли поћи од реактивног или проактивног приступа, како се не би створио орвелијански систем електронског надзора у телекомуникационом окружењу. *Некритичко регулисање и примена* напредних метода и техника надзора и праћења активности корисника, у чијим свакодневним активностима је све пристуније ослањање на информационе технологије, створило би *реалну опасност од проширивања и продубљивања обухвата сфера живота које се надгледају*, у много већем обиму од легитимног надгледања у оквиру концепта проактивности и стварања својеврсног потпуног и паноптичког надзора података о личности[931] (тзв. *dataveillance*[932]) што се не може оправдати чак ни потребама супротстављања најтежим облицима кривичних дела, па ни високотехнолошком криминалу (јер податке о распрострањености и свеопштој претњи овог облика криминала треба узети са резервом услед непоуздане методологије прикупљања и обраде). Како ове технологије омогућавају надзор са високим степеном интрузивности у приватну сферу појединаца, неопходно је *успоставити баланс* у

[930] О питањима угрожавња приватности у *online* окружењу, *Cloud computing and its implication on data protection*, 2010, *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp.*

[931] Више о томе, M. Levi, Wall D., "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society* 2/2004, 194-200.

[932] О овом концепту, Clarke R., „Information Technology and Dataveillance", *Communications of the ACM* 5/1988, 500.

њиховој примени у сврху сузбијања дела високотехнолошког криминала, односно, од пресудног значаја је пронаћи одговор на питање *на који начин постићи равнотежу између индивидуалних интереса* (заштите права приватности и података о личности) и општег интереса (прикупљање доказа за потребе кривичног поступка за дела високотехнолошког криминала).

Пред државом је изазов како да одговарајућим правним оквиром обезбеди да *надзор активности* које се остварују употребом савремених метода и техника (пресретање комуникација, надгледање и праћење, задржавања података, декрипција и друго[933]) за потребе спречавања и откривања дела високотехнолошког криминала и гоњења учинилаца *буде у балансу са заштитом права на приватност*[934]. Како би се постигла неопходна равнотежа између интереса кривичног поступка и интереса (и права) окривљеног и других лица у поступку, *релевантна су не само ограничења обухвата приликом прописивања овлашћења*, те *врста радњи* које су органи овлашћени да предузму, него и *начин остваривања тих овлашћења*. Да би рачунарски подаци који се прикупљају ради откривања и доказивања кривичних дела могли да буду употребљени као доказ у кривичном поступку, потребно је на одговарајући начин уредити дужност надлежних органа да воде рачуна о томе да приликом предузимања радњи и мера, не повреде права појединаца у вези са прикупљањем и обрадом тих података у складу са важећим прописима на националном и међународном нивоу[935].

Оваква парадигма је инкорпорисана и у Конвенецији о високотехнолошком криминалу, у чијој Преамбули је као један од циљева наведено остваривање

---

[933] О угрожавању права приватности прописивањем механизама за сузбијање тешких облика криминала, M. Klang, Murray A., *Human rights in the digital age*, Routledge-Cavendish, London-Portland 2005, 147-153.

[934] Тако је у саопштењу Комсије ЕУ 2004. године истакнуто да у истраживању могућих безедносних решења пажњу потребно посветити и људским правима и слободама и другим демократским вредностима, да би се пронашла потребна равнотежа између надзора и контроле у циљу смањења потенцијалног ризика од терористичких аката и поштовања људских права и приватности. *Communication Security Research : The Next Steps*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0590:FIN:EN:PDF. Такође, у ЕУ као простору слободе, безбедности и правде треба да буде обезбеђено поштовање и заштите основних људских права и слобода, а нарочито пажњу је потребно посветити питању заштите приватности у вези са применом савремених технологија, *Commission Communication: A strategy on the external dimension of the area of freedom, security and justice*, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l16014_en.htm.

[935] M.V.P. Asinary, „Legal Constraints for the Protection of Privacy and Personal Data in Electronic Evidence Handling“, *International journal of Law, Computers and Technology* 2/2004, 235.

равнотеже између интереса кривичног поступка и поштовања основних људских права. Конвенција обавезује државе потписнице да у националном законодавству инкриминишу одређена понашања и да предвиде одређена овлашћења надлежним органима ради откривања и доказивања, не само дела високотехнолошког криминала (у смислу чланова 2-11), него и свих других кривичних дела која су извршена употребом рачунарског система, односно ради прикупљања електронских доказа за сва кривична дела. Иако Конвенција предвиђа да се прописивање радњи и мера и њихово одређивање и примена у конкретним случајевима остварују у складу са домаћим правним системом, *члан 15.* Конвенције садржи изричиту обавезу за државе да то чине у складу са *одређеним условима и ограничењима* и на начин да се *обезбеди одговарајућа заштита основних права и слобода грађана, водећи рачуна о принципу сразмерности*[936]. У том смислу, члан 15. поставља принципе и захтеве које имају за циљ да државе *испоштују обавезу да се* приликом прописивања овлашћења (и процедура), односно предузимања радњи и мера на које су надлежни органи овлашћени (у складу са процесним одредбама Конвенције) *заштите појединци и њихова права.* Услови и ограничења у смислу члана 15. Конвенције су доведени у везу са стандардима постављеним у међународноправним инструментима, укључујући права гарантована Конвенцијом Савета Европе о основним људским правима и слободама, Међународним пактом о грађанским и политичким правима и другим инструментима међународног права.

Поред тога, модалитет и примена услова и ограничења се огледа у прописивању услова за одређивање доказних радње сходно националним прописима, па могу бити одређени и у Уставу или релевантним законима, а у складу са природом овлашћења или процедура. То значи услови и ограничења да у националном правном систему могу бити дефинисани као протективни у далеко већој мери у односу на члан 15. Конвенција као *минималне стандарде* наводи:

[936] Док коначан текст Конвенције није био представљен на скупу у Будимпешти 2001. године 27 нацрта је било израђено, при чему је тек 19. верзија постала доступна широј јавности. Од те верзије па до усвајања коначног нацрта, доста пажње је било посвећено управо члану 15. Конвенције, с обзиром на ризик које процесне одредбе могу представљати по права на приватност. Више о томе, *Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf. Текст члана 15, у облику у ком је усвојен и саставни је део Конвенције, представља компромис између општег интереса и интереса заштите права појединаца.

судску контролу или контролу од стране другог независног тела[937], навођење образложења за предузимање радњи и мера на основу просецних овлашћења, као и ограничење обима (обухвата) и временског трајања поступања по основу тог овлашћења, односно у оквире те процедуре, а са посебним нагласком је истакнут *принцип сразмерности*, у смислу да прописивање овлашћења и процедура, односно примена радњи и мера буде пропорционално природи и околностима кривичног дела[938]. Дакле, од држава се очекује да обезбеде равнотежу између општег интереса (за потребе кривичног поступка, а у складу са обухватом процесних овлашћења предвиђеним чланом 14) и интереса појединаца (заштита основних људских права и слобода, у складу са чланом 15). Имајући у виду природу процесних овлашћења, њихово прописивање, те одређивање и примена радњи и мера на основу тих овлашћења, може имати утицаја превасходно на два основна права, а то су *право на приватност* и *право на заштиту података о личности*[939].

Стога је у имплементацији одредаба Конвенције у прописима кривичног процесног права, који уређују предузимање радњи и мера са циљем да се обезбеде електронски докази, *нужно посебну пажњу посветити заштити ова два права.* Како бисмо разумели утицај процесних овлашћења која у општем интересу могу ограничити гарантована права на приватност и заштиту података о личности, потребно је размотрити поимање ових права у изворном облику и потом прилагођена изазовима употребе савремених технологија од стране надлежних државних органа.

1. ПРАВО НА ПРИВАТНОСТ

Концепт приватности настао у САД у великој мери је утицао на схватање европске јуриспруденције и јудикатуре, па сматрамо да је за разумевања његове

[937] Мисли се заправо на механизме са надзорним овлашћењима (као што је институт обудсмана или парламентарни истражни одбори) у циљу успостављања одговарајућег баланса између права приватности појединаца и општих интереса. Kleve P., De Mulder R., "Privacy protection and the right to information: In search of a new balance", *Computer Law& Security Report* 24/2008, 230.

[938] Параграф 146. Пратећег извештаја уз Конвенцију (*Explanatory report*), http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[939] L. Bygrave, „Data protection pursuant to the right to privacy in human rights treaties", *International journal of law and information technology* 3/1998, 257.

суштине корисно узети у обзир најзначајнија становишта америчких правосудних органа о ограничењу права на приватност у вези са кривичним поступком. Правни оквир за заштиту приватности лица у САД налази се у 4. Амандману на Устав (ратификован 1791. године) по ком се појединцу гарантује да може да очекује заштиту приватности (у погледу личности, дома и својине) од мешања државе. Врховни суд САД[940] је у својој прецедентној историји у неколико одлука потврдио право на приватност применом 4. Амандмана[941], а одлука која представља камен темељац америчког концепта приватности је донета 1967. у предмету *Katz v. United States*[942]. Пресуда је значајна из разлога што је у њој установљен стандард „разумног очекивања приватности" (*reasonable expectation of privacy*[943]). Да би се применио овај стандард, у конкретном случају се постављају два питања: 1. Да ли је лице имало *стварно очекивање приватности*, и 2. Да ли друштво такво очекивање препознаје као *оправдано*. Уколико су одговари на оба питања потврдни, државни орган може приступити заштићеној сфери приватности, а *ради заштите општих интереса*, само *на основу налога*

[940] Судска пракса Суда је претраживана преко јавности доступне базе података:http://www.supremecourt.gov/case_documents.aspx

[941] Суд је обезбедио право на приватност први пут применом 4. амандмана 1886. године у предмету *Boyd v. United States,* а 1928. је први пут разматрао питање уставности надзора комуникација у предмету *Olmstead v. United States.* Решавајући питање да ли се докази прикупљени прислушкивањем телефонских разговора окривљеног могу употребити против њега у кривичном поступку, Суд је утврдио да тајно прислушкивање представља кршење 4. Амандмана. Занимљиво је да је управо један од аутора научног рада у ком је право на приватност 1890. први пут одређено у смислу права грађана да буду остављени на миру од радњи других лица, касније у улози судије (*Louis Brandeis*) у предмету из 1928. проширио дејство права и на заштиту од активности државе, јер наводи да свако неоправдано мешање државе у приватност појединца без обзира на употребљена средства може да представља повреду 4. Амандмана. Отуда се судија *Brandeis* сматра творцем концепта приватности. У предмету *Goldman v. United States* из 1942. заузет је став да употреба детектафона (уређај који се поставља на зид зграде ради прислушкивања разговора унутар просторија у згради) не представља повреду права на приватност, а у предмету *Silverman v. United States* да је употреба уређаја *spike mike* за прислушкивање противуставна јер је потребан улазак у стан ради његовог инсталирања. У предмету *Berger v. New York* заузет је став по ком је електронско прислушкивање од стране полиције у складу са Уставом уколико је задовољен принцип одређености (да би налог био издат потребно је да буду предочени прецизни подаци о лицу и месту који се претресају и предметима који се имају одузети, као и природа кривичног дела које се истражује), а да се претрес без претходног добијања налога може извршити само у изузетним околностима. У предмету *Griswold v. Connecticut* Суд је потврдио да гаранције из Првог, Четвртог, Петог и Деветог амандмана стварају зоне приватности које Устав штити.

[942] 389 U.S. 347 (1967). У пресуди је наведено да је тиме што је овлашћено лице полиције прислушкивало и снимало разговор окривљеног који је обављао у јавној телефонској говорници прекршена гаранција приватности појединца (то што је лице прислушкивано у јавној телефонској говорници, а не у свом дому не значи да лице не ужива заштиту, јер 4. Амандман штити људе, а не места).

[943] Више о томе, R. Dunne., *Computers and the Law: An Introduction to Basic Legal Principles and Their Application in Cyberspace*, Cambridge University Press, Cambridge 2009, 198-202.

добијеног од суда (но, постоје и изузеци у којима се стандард оправданог очекивања приватности не примењује). Суд је стандард утврђен у овој пресуди почео да примењује и у другим предметима, при чему је користио и термине као што су „оправдано“ (*justifiable*) и „легитимно“ (*legitimate*) очекивање приватности[944]. Стандард је и данас примењив у пракси Суда, без обзира на промене у нивоу технолошког развоја и представља темељ модерног схватања концепта приватности[945].

Да бисмо „заштиту општих интереса“, као правни стандард који оправдава ограничење поштовања приватности, потпуније разумели, потребно га је посматрати у контексту релевантних инструмената који штите право на приватност. С обзиром на то се да се у Конвенцији о високотехнолошком криминалу као стандард који се узима у обзир (и одређује меру ограничења процесних овлашћења надлежних органа), првенствено указује на Европску конвенцију о заштити људских права и основних слобода (у даљем тексту: ЕКЉП[946]), пажњу је потребно усмерити на анализу релевантних одредаба ЕКЉП кроз приказ праксе Европског суда за људска права[947], која у великој мери утиче на обликовање прописа у европским државама. Наиме, члан 8. ЕКЉП *штити појединце од неоправданог и арбитрерног мешања државних органа у сферу приватности*, у смислу да свако има право на поштовање приватног и породичног живота, дома и преписке, што може бити ограничено у појединим случајевима уколико су испуњени одређени услови. Наиме, државни органи могу својим радњама ограничити гарантована права уколико је таква могућност предвиђена законом и потребна у демократском друштву ради заштите одређених

[944] Kyllo v. United States, 533 U.S. 27, 33 (2001); Bond v. United States,529 U.S. 334, 338 (2000); California v. Greenwood,486 U.S. 35, 41 (1988); California v. Ciraolo, 476 U.S. 207, 211 (1986); Smith v.Maryland, 442 U.S. 735, 740 (1979). Више о томе, Dunne, *op.cit*, 202-220.

[945] Тако је у пресуди *United States v. Jones* из 2012. године Суд заузео став да је надзор аутомобила осумњиченог лица употребом система за глобално позиционирање без издатог налога од стране суда повреда гаранција из 4. Амандмана. Значајан је став по ком је неприхватљиво поједностављено гледиште полиције да све што се дешава на улицама није приватна сфера, као и да надзор и праћење на овај начин представља повреду оправданог очекивања приватности. О критичкој анализи ове пресуде, више о томе, P. Smith, *"*Much a do about mosaics: how original principles apply to evolving technology *in United States v. Jones",* North Carolina Journal of Law and Technology 2/ 2013, 567; O. Kerr, *"*The Mosaic Theory of the Fourth Amendment Amendment", *Michigan Law Review* 3/2012, 311-354.

[946] *Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, CETS* No. 005, 1950, http://conventions.coe.int/treaty/en/treaties/html/005.htm.

[947] Судска пракса Европског суда је претраживана преко јавности доступне базе података: http://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

општих интереса. Дакле, у погледу *могућности ограничења права*, Суд је утврдио следеће *критеријуме*: 1. *предвиђеност* законом; 2. *оправданост* постојањем легитимног циља, и 3. *неоходност* у демократском друштву ради остварења легитимног циља. Да би ограничење гарантованих права било оправдано, треба да има основ у закону[948] који је усклађеним са принципом владавине права, а чије одредбе су формулисане на довољно прецизан начин да би их адресати могли разумети и поступати по њима[949], са јасно предоченим последицама непоступања[950], тако да се обезбеђује заштита од арбитрерног мешања државних органа у сферу приватности[951].

Ради процене да ли се ради о потребном и неопходном ограничењу које одређена мера представља по гарантована права, потребно је да се утврди постојање притисака у демократском друштву за увођењем таквих мера[952], а ограничавање права приватности треба да је сразмерно легитимном циљу због ког је мера уведена[953] . Приликом процене потребе да ли је одређена мера потребна, од држава се очекује да буде објективна, те да приликом *разматрања принципа сразмерности* једнаку пажњу посвети како природи легитимног циља, тако и природи права које се ограничава[954]. Да би се установило да ли је принцип сразмерности испоштован, потребно је *одговорити на следећа три питања*: 1. Да ли постоји доказ да се радњама државних органа може остварити предвиђен легитимни циљ, 2. Да ли су радње апсолутно неопходне или се исти циљ може остварири и предузимањем друге радње која узрокује мање негативних последица по право приватности; 3. Чак и да није могуће остварити легитимни циљ предузимањем алтернативне радње, да ли су негативне последице по приватност толико тешке да није оправдано предузимање радње[955]. У пракси Европског суда за људска права се може пронаћи више пресуда које су донете поводом кршења права на поштовање приватног и породичног права прописивањем процесних

[948] Пресуда у предметима *Kruslin v. France, (1990)* и *Kopp v. Switzerland, (1998-II).*
[949] Пресуда у предмету *Sunday Times v. the United Kingdom, (1979).*
[950] Пресуда у предмету *Amman v. Switzerland, (2000-II).*
[951] Пресуда у предмету *Ollson v. Sweden, (1988).*
[952] Пресуда у предмету *Norris v. Ireland, (198)* и *Dudgeon v. The United Kingdom (1988).*
[953] Пресуда у предмету *Gillow v. The United Kingdom, (1986).*
[954] Пресуда у предмету *Lingens v. Austria, (1986).*
[955] F. Bignami, „The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts“, *Cornell International Law Journal* 2/2008, 220.

овлашћења, односно одређивањем и применом радњи и мера надлежних органа јер у конкретном случају нису испуњени претходно наведени услови.

У контексту употребе нових технологија од стране државних органа, Суд је у својој пракси недвосмислено препознао да то може представљати ризик по вредности које су заштићене чланом 8. Конвенције. У пресуди у предмету *Saunders v United Kingdom* модерно друштво је означено као „информационо друштво“[956], које зависи од информација, а које је могуће сакрити у компјутеризованом свету коришћењем крипотографских функција уређаја.

О односу нових технологија и криминалитета, Суд је истакао да је брз развој телекомуникационих технологија, нарочито Интернета, у последњих неколико деценија условио појаву нових облика кривичних дела и модалитета постојећих[957], док је истовремено препознао да сузбијање кривичних дела (нарочито организованог криминала и тероризма) зависи у великој мери од употребе савремених научно-потврђених техника и метода за потребе откривања и доказивања[958]. Суд наводи да се гаранција слободе од самооптуживања у смислу члана 6. Конвенције не односи на употребу материјала који се може добити од окривљеног употребом мера процесне принуде а који постоје независно од воље окривљеног (као што су крв или урин за потребе ДНК анализе), па се сходно томе, могу се користити и инкриминишући подаци које окривљени оставља за собом у виду дигиталних трагова а који се могу пронаћи предузимањем радњи и мера којима се врши прикупљање електронских доказа[959]. Тако је употреба *CCTV* камера корисна у превенцији кривичних дела [960], а прихваћено је као оправдано и коришћење мера тајног надзора комуникација[961], али је нужно да у закону постоје јасне и одговарајуће гаранције од злоупотреба, а да процена да ли се у конректном случају ради о повреди права из члана 8. зависи од околности случаја, односно од природе, обима и трајања мере, те овлашћења органа који одређују, примењују и

[956] Пресуда у предмету *Saunders v United Kingdom1996-VI; 23 EHRR 313.*
[957] Пресуда у предмету *K.U. v. Finland (No.2872/02*).
[958] Пресуда у предмету *S and Marper v United Kingdom 48 EHRR 50*.
[959] С тим у вези, у пресуду у предмету *Timurtas v Turkey 2000-VI; 33 EHRR 121* Суд истиче да је потребно проверити аутентичност фотокопије исправе пре него што буде прихваћена као копија оригинала, а тим пре је потребно то учинити са свим дигиталним изворима јер модерне технологије у дигиталним уређајима омогућавају фалсификовање података у електронском облику.
[960] Пресуда у предмету *Peck v United Kingdom 2003-I.*
[961] Пресуда у предмету *Klass and Others v Germany 28 (1978).*

надгледају извршење мере[962]. Потребно је да државе у својим законодавствима прилагоде одредбе које уређују ове нестандардне мере тајног надзора[963] и обезбеде контролу над њиховим спровођењем[964]. Да само постојање законског овлашћења за предузимање ових мера не би представљало претњу по приватност грађана, Суд је заузео веома стриктан став у погледу принципа „усклађености са законом" приликом процене да ли је применом овлашћења повређено право појединца у смислу члана 8. Конвенције. Стога државе треба да се суздрже од коришћења нових технологија за потребе кривичног поступка на начин којим се девалвира постојање права на приватност (негативна обавеза државе). Тако је у пресуди у случају *Kruslin v France*[965], Суд истакао потребу за стварањем јасних, прецизних правила за надзор и снимање комуникација које се остварују техничким средствима, с обзиром да технике за примену ове мере постају високософистициране и тиме интрузивне у све већој мери, јер право на приватност подразумева заштиту интегритета личности и његову могућност да одбије да се у потпуности учини транспарентним у савременом друштву.

У погледу аспекта приватности комуникација, у пресуди у предмету *Copland v United Kingdom*[966] је јасно указано на то да уколико лице није упознато са тим да се његова комуникација надгледа, има право на оправдано очекивање приватности и заштите у том смислу, односно да прикупљање података о личности надзором средстава општења представља неовлашћено мешање у приватност дома и преписке[967]. У овом предмету је први пут разматрано питање надзора комуникација које се остварују употребом телефона и других техничких средстава као и активности корисника на Интернету. Суд је истакао да и просто складиштење тих података представља повреду права из члана 8. без обзира на то што подаци нису употребљени. Ипак, иако су слобода изражавања и поверљивост комуникација важне вредности у демократском друштву на основу чега корисник услуга електронских комуникација има право да очекује да се његова приватност

[962] K. Aquilina, „Public security versus privacy in technology law: balancing act?", *Law computers & Security Report* 26/2010, 134.
[963] Пресуде у предметима *Weber and Saravia v Germany 2006-XI* и *Liberty and Others v United Kingdom Application No. 58243/00*.
[964] Пресуда у предмету *Kennedy v United Kingdom Application No. 26839/05*.
[965] Пресуда у предмету *Kruslin v France A 176 (1990); Kopp v Switzerland 1998-II.*
[966] Пресуда у предмету *Peck v United Kingdom 2003-I; 36 EHRR 41*.
[967] Пресуда у предмету *Niemietz v Germany A 251-B (1992*) у којој је хард диск рачунара први пут препознат као средство општења.

штити, таква гаранција није апсолутна и та права могу бити ограничена када то захтевају интереси кривичног поступка и заштита права и слобода других лица[968]. Тако, примера ради, праћење лица употребом система за глобално позиционирање није одређено као повреда права на приватност у случају на то да је ова мера одређена због заштите националне безбедности, спречавања извршења кривичних дела и заштите права оштећених лица, што је и пропорционално легитимном циљу у демократском друштву[969].

Да је заштита права гарантованих у члану 8. Конвенције од кључног значаја за владавину права у демократском друштву јасно произлази из чињенице да држава може имати не само негативне, него и позитивне обавезе, у смислу да инкриминише прикупљање података и надзор комуникација уколико се остварују на начин да представљају повреду права на приватност[970], односно да створи ефикасан механизам за санкционисање понашања која вређају гарантована права појединаца[971]. Осим тога, поступање у складу са таквом позитивном обавезом подразумева да се у појединим случајевима може ограничити неко друго право гарантовано Конвенцијом[972].

Историја судске праксе у погледу члана 8. ЕКЉП је богата и пуна неочекиваних праваца развоја услед креативне примене метода тумачења, па се може рећи да пракса овог Суда има изражену динамичку црту *(the dynamic character of the Strasbourg case law*[973]). Суд полази од тога да је Конвенција „живи“ инструмент који треба да се тумачи у складу са условима савременог окружења, како би се одредбе прилагодиле технолошком развоју, који представља изазов по гаранатована права. Нарочито из разлога што последице таквог развоја нису могле бити предвиђене у време усвајања текста Конвенције. Како је то истакнуто још 1984. године, Суд као „бранич“ Конвенције има задатак да штити право из члана 8. у његовој пуној димензији, а посебно због тога што постоји опасност да неограничена и неоправдана употреба савремених технологија од

[968] Пресуда у предмету *K.U. v. Finland (No.2872/02*).
[969] Пресуда у предмету *Uzun v. Germany* (*No* 35623/05).
[970] Пресуда у предмету *X andY v The Netherlands A 91 (1985*).
[971] Пресуда у предметима *August v. the United Kingdom No. 36505/02*; *M.C. v. Bulgaria No. 39272/98*.
[972] Вид . пресуду у предмету *Von Hannover v Germany 2004-VI; 43*. У овом предмету је Суд заузео јасан став да је ради заштите права приватности могуће и оправдано ограничити слободу извештавањ из члана 10. Конвенције.
[973] A. Chedraui,“Analysis of the Exclusion of Evidence Obtained in Violation of Human Rights in Light of the Jurisprudence of the European Court of Human Rights“, *Tilburg Law Review* 2 /2011, 207.

стране државе произведе све већу рањивост појединца у окружењу „Великог брата“[974].

Оправдано је очекивати да ће се, услед дивергенције технологија и њиховог коришћења од стране овлашћених државних органа, у пракси Суда у будућности све чешће појављивати захтеви за испитивање оправданости мешања државних органа у све аспекте приватне сфере појединаца, нарочито у вези са надзором активности корисника услуга електронских комуникација за потребе кривичног поступка, као и захтеви за заштиту података о личности од обраде која није у складу са општеприхваћеним принципима.

2. ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ

Концепт приватности садржи неколико елемената: личну приватност, којом се штити физички интегритет појединца (тзв. *телесна приватност*); приватност личног понашања, које се односи на заштиту свих аспеката понашања појединца (нарочито на осетљиве аспекте, као што су сексуално опредељење и навике, политичка активност, религијска уверења и слично) како у приватним тако и на јавним местима (тзв. *медијска приватност*); приватност личног општења (комуникација), којом се штити право појединаца да међусобно комуницирају употребом различитих средстава, без надгледања тих активности од стране неовлашћених лица (тзв. *комуникациона приватност*); приватност података о личности, на основу ког појединци имају оправдано очекивање да подаци о њима не буду аутоматски доступни другим појединцима и организацијама, као и могућност да врше контролу над обрадом и употребом тих података (тзв. *приватност информација*)[975].

Услед конвергенције технологија дошло је до промена у процесу прикупљања и обраде података, и то не само по обиму (подаци се прикупљају и обрађују у великом броју база података, нпр. *Google*, базе корисника *online* продаја, друштвених мрежа итд), него и по квалитету (прикупљају се и обрађују потпуно

[974] Ibidem.
[975] Више о томе, R. Clarke, “Privacy impact assessment: Its origins and development”, *Computer Law and Security Review* 2/2009, 124; R. Clarke, “Technology, Criminology and Crime Science“, *European Journal on Criminal Policy and Research*, 1/2004, 57.

нове врсте података о личности, као нпр. подаци о локацији корисника електронксих уређаја, подаци о активностима корисника на Интернету, *RFID* итд), а осим тога технике и методе за прикупљање и обраду података су учиниле овај процес далеко интрузивнијим (нпр. аутоматско препознавање, размена података, профилирање и слично[976]). С тим у вези се може сматрати да је дошло до међусобног приближавања последња два аспекта (комуникационе приватности и приватности информација) у тзв. *информациону приватност*.[977] Уколико пођемо од тога да право на приватност подразумева право појединаца да самостално донесу одлуку о томе када, како и у ком обиму је спреман да подаци о њима буду доступни другим појединцима и јавности, *информациону приватност* можемо одредити као право индивидуе да се својевољно одрекне појединих елемената права на приватност у информационом окружењу[978] и изједначити је са *правом на информационо самоопредељење* (*Recht auf informationelle Selbstbestimmung*) које је први пут одређено у одлуци немачког Уставног суда 1983. године[979]. У овој одлуци је Суд утврдио неколико битних принципа који се сматрају темељом европског система заштите података о личности с обзиром на то да су уграђени у кључне правне иснтрументе у Европској унији који регулишу ова питања[980]. Право на информационо самоопредељење је схваћено као право појединца да донесе одлуку о употреби и приступачности података о личности , а као такво је изведено из права на слободан развој личности (*allgemeines Personlichkeitsrecht*) и на заштиту људског достојанства (*Menschenwurde*), што одговара схватању приватности у смислу да лице одлучи када, како, коме и до које мере је спремно да податке о себи учини доступним другима[981].

---

[976] Flint D., „Law shaping technology: Technology shaping the law“, *International Review of Law, Computers & Technology* 1–2/ 2009, 6.

[977] Y. Poullet, „Data protection legislation: What is at stake for our society and democracy“, *Computer Law and security review* 25/2009, 215.

[978] Могуће је уочити још једну врсту приватности, а то је приватност локације. Wright D., „The state of the art in privacy impact assessment“, *Computer Law and security Review* 28/2012, 55.

[979] Судска пракса Уставног суда Немачке: http://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/EN/Entscheidungensuche_Formular.html?language_=en.

[980] G. Hornung, C. Schnabel, „Data protection in Germany I: The population census decision and the right to informational self-determination“, *Computer Law&Security Review* 25/2009, 87.

[981] Одлука је донета поводом пописивања грађана и потребе да се приликом прикупљања података о њима обезбеди њихово право на слободан развој личности. Више о томе, Hilgendorf E., Valerius B., *Computer- und Internetstrafrecht:Ein Grundiss*, Springer, Heidelberg 2012, 6-7.

Што се тиче односа права правтности и заштите података о личности, несумњиво је да заштита података о личности (као право појединца да има одређене гаранције у погледу обраде података који га одређују, односно могу одредити) своју основну легитимност изводи из заштите права на приватност[982]. Може поставити питање да ли су заштита података о личности «синоними» [983] или су «близанци, али не идентични» [984], као и које право произлази из ког: да ли је заштита података о личности само аспект права на приватност или се пак заштита права на приватност постиже заштитом података о личности.

Питање заштите података први пут се помиње током 1960-их године прошлог века у САД, услед ризика који је са собом донео технолошки развој, тачније са појавом рачунара који су омогућили аутоматизацију процеса прикупљања и обраде података о појединцима[985]. Убрзо након уочавања потребе заштите информационе приватности појединаца у америчкој правној науци, на европском континенту је уследило нормативно реаговање. Први закон којим се уређује заштита података о личности усвојен је у немачкој држави Хесе 1970. године, а потом су слични закони усвојени и у другим европском државама (1973. у Шведској, 1976. у Немачкој, 1978. у Француској, Данској, Норвешкој и Аустрији итд.[986]). Иако заштита података о личности није била изричито предвиђена *у најзначајнијим међународним уговорима о људским правима* усвојеним после

[982] R. Polcak, „Aims, methods and achievements in European data protection“, International Review of Law, Computers & Technology, 3/ 2009, 181.
[983] K. McCullagh, “Protecting ‘privacy’ through control of ‘personal’ data processing: A flawed approach”, *International Review of Law, Computers & Technology* 1–2/ 2009, 17.
[984] C. Kuner, “An international legal framework for data protection: Issues and prospects”, *Computer Law& Security Review* 25/2009, 308.
[985] Потреба за правилима о заштити података о личности је настала са појавом рачунара и коришћењем могућности аутоматске обраде података од стране државних органа. У поређењу са датотекама у физичком свету које су се мануелно обрађивале, датотеке ускладиштене у рачунарима све већих меморијских капацитета, омогућавају обраду података о личности на начин који може угрози заштиту на приватност у далеко већој мери. Да аутоматизација обраде података не би омогућила најразноврсније злоупотребе, постало је јасно да би држава требало да обезбеди квалитетан ниво заштите података о личности на тај начин да се не прикупљају подаци који нису неопходни за остваривање одређене сврхе, те да се неовлашћено не откривају и не користе прикупљени подаци.
[986] P. De Hert, Papakonstantinou V., Riehle C., “Data protection in 3rd pillar – cautious pessimism”, *Crime, Rights and the EU: the future of police and judicial cooperation* (ed.Martin M.), London 2008,123.

Другог светског рата, не може се оспорити да ови инструменти не гарантују заштиту података о личности у оквиру права на приватност[987].

Први међународни извор права који се непосредно односи на заштиту података о личности је *Конвенција о заштити лица у вези са аутоматском обрадом података о личности*[988] (са Додатним протоколом у вези са надзорним органима и прекограничним протоком података о личности[989]) усвојена у оквиру Савета Европе 1981. године. Међу пионирским актима посвећеним уређењу заштите података на наднационалном нивоу вредне помена су 1990. године усвојене Смернице *OECD-a* за заштиту приватности и прекогранични промет података о личности[990] и Смернице УН о компјутерозованим подацима о личности[991].

Концепт приватности који је развијен у ***америчкој*** јудикатури кроз низ прецизних правних правила и стандарда и заштићен у пракси кроз систем прецедената, у својој структури садржи и заштиту података о личности[992]. Што се тиче прикупљања података о личности као аспекта приватности, Врховни суд САД је 1977. године први пут указао на могућност претње по приватност услед прикупљања велике количине података у компјутеризованим базама података у поседу државних органа[993]. Иако је у поменутој пресуди посредно разматрао питање информационе приватности, Суд до сада ни у једном предмету није јасно

---

[987] Релевантне су следеће одредбе: члан 12. Универзалне декларације о људским правима, члан 17. Међународног пакта о грађанским и политичким правима и члан 8. Европске коневнције о заштити људских права и основних слобода.

[988] *CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS* No. 108, 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. Република Србија је ратификовала ову Конвенцију, Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података („Сл. лист СРЈ - Међународни уговори", бр. 1/92, "Сл. лист СЦГ - Међународни уговори", бр. 11/2005 - др. закон и "Сл. гласник РС - Међународни уговори", бр. 98/2008 - др. закон и 12/2010).

[989] *CoE, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001, http://conventions.coe.int/Treaty/EN/Treaties/HTML/181.htm.* Република Србија је ратификовала овај Протокол, Закон о о потврђивању додатног протокола уз Конвенцију о заштити лица у односу на аутоматску обраду личних података, у вези са надзорним органима и прекограничним протоком података („Сл. гласник РС - Међународни уговори", бр. 98/2008).

[990] *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, усвојене 1990. а последњи пут измењене 2013. године, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Working party on information security and privacy: the evolving privacy landscape: 30 years after the OECD privacy guidelines, *http://www.oecd.org/internet/interneteconomy/47683378.pdf*;

[991] *UN Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990)*, усвојене 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.

[992] Kuner, *op.cit*, 310.

[993] Whalen v. Roe, 429 U.S. 589, 605 (1977).

одредио право на заштиту података о личности које прикупљају државни органи, него се више концентрисао на заштиту других аспеката приватности[994], а информациону приватност је препустио законодавцу да регулише.[995]

Иначе, актуелно питање у америчкој правној науци јесте преиспитивање адекватности примене концепта приватности (у смислу 4. Амандмана) у обезбеђењу права на информациону приватност у савременом технолошком окружењу[996]. Да би доктрина 4. Амандмана била подобна да буде основ у разматрању уставности електронског надзора и праћења применом других високотехнолоших техника, потребно је да Суд утврди као минимум основне стандарде које би примењивао у оцени да ли је конкретним радњама државних органа повређено право на информациону приватност[997], што Суд није учинио, јер преовладава мишљење да је право на информациону приватност далеко шире од концепта приватности које штити Устав и да је потребно обезбедити његову заштиту у компјутеризованом савременом окружењу, не само кроз деловање

[994] C. Arzt, "Data protection versus 4th Amendment: a new approach towards police serach and seizure", *Criminal Law Forum* 16/2005, 192.

[995] Од почетка 1990-их уочавају се критике овако уског третирања концепта приватности од стране Суда, јер је „прикупљање података о личности нови вид интрузије државе, па схватање 4. Амандмана мора да буде проширено тако да обезебди заштиту информационе приватности" (Katz L, „In Search of a Fourth Amendment for the Twenty-first Century", *Indiana Law Journal* 2/1990, 553). Такође се указује да је „право појединца да буде остављен на миру" концепт другачији у односу на право појединца да захтева заштиту података о себи од државе (Colb S.,, The Qualitative Dimension of Fourth Amendment ''Reasonableness'', *Columbia Law Review* 3/1998, 1645).

[996] Тако постоје мишљења по ком се информациона приватност може посматрати и као *право својине над подацима (information property*) (J. Litman, "Information Privacy/Information Property", *Stanford Law Review*, 5/2000, 1289.). Поједини аутори тврде да су такви ставови неприхватљиви, јер податак о личности одређује или може да одреди појединца на директан начин у много већем обиму него својина над одређеним предметом и стога је свака аналогија непримерена. Подаци о личности се доводе у везу са имовином лица нарочито у погледу кривичног дела крађе идентитета (о томе више, J. Clough, „Data theft? Cybercrime and the increasing criminalization of access to data", *Criminal Law Forum* 2/2011, 147-150; K. Jaishankar, „Identity related crime in the cyberspace: Examining Phishing and its impact", *International Journal of Cyber Criminology* 1/2008, 13). Према мишљењу професора Кера 4. Амандман штити појединца само од неоправданог мешања у уживању својине (оправдано очекивање заштите од неоснованог физиког претреса стана и предмета у стану) али не и слободан развој личности а тиме ни приватност (о томе више, J. Lerner, D. Mulliga, "Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home", *Stanford Technology Law Review* 3/2008, 4-5). Из наведених разлога је примена 4. Амандмана (*property-based approach*) неподобна да заштити информациону приватност појединца (O. Kerr, „The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution", *Michigan Law Review* 5/2004, 871. Упор. P. Swire, „Katz Is Dead. Long Live Katz", *Michigan law review* 5/2004, 906.). Како нове технологије могу угрозити право приватности тако да ни на који начин не угрожавају приватну својину, постоји потреба за преиспитивањем дејства 4. Амандамана и могућности да заштити информациону приватност (S. Colb, „A World without Privacy: Why Property Does Not Define the Limits of the Right against Unreasonable Searches and Seizures", *Michigan Law Review* 5/2004, 894).

[997] О томе више, P. Swire, „Katz Is Dead. Long Live Katz", *Michigan law review* 5/2004, 923-931.

Суда, него кроз прописе са прецизирајућом улогом нарочито у погледу заштите приватности у вези са кривичним поступком. Ово је потребно посебно ако се узму у обзир прописи који државним органима омогућавају употребу интрузивних техника надзора ради прикупљања доказа за потребе кривичног поступка.

У том смислу релевантан је Закон о приватности електронских комуникација[998], који се ослања на 4. Амандман јер регулише прикупљање рачунарских података који се чувају и преносе у рачунарским мрежама. Међутим, тзв. *USA Patriot*[999] који је у великој мери одступио од гаранција из 4. Амандмана, изменио је одредбе првопоменутог Закона. Најконтроверзније одредбе овог Закона су садржане у другом одељку, који је насловљен као „Процедуре појачаног надзора" (*Enhanced Surveillance Procedures)* које овлашћују државне органе да употребом напредних техника за надзор активности у вези са информационим технологијама прикупљају податке (у виду обавештајних података) о држављанима САД, као и од страним држављанима. Истовремено су проширена овлашћења полиције и тужилаштва, тиме што се уводи могућност неограниченог прислушкивања, надзора заштићених рачунара, издавања *sneak and peak* налога, обавезивања пружалаца услуга електронских комуникација на откривање великог броја података о корисницима[1000]. Употреба напредних техника тајног надзора оправдана је као „поштен компромис"[1001] између традиционално схваћене приватности и ризика по општу безбедност, нарочито од будућих терористичких напада, међу којима се истиче *cyber warfare* и претња високотехнолошког криминала уопште. Неке од контроверзних одредаба су биле временски ограничене до краја 2005. године, но истовремено је предвиђена годишња валидација потребе да се одредбе и даље примењују. Поједине одредбе су биле предмет преиспитивања у погледу сагласности са Уставом (нарочито са 4. Амандманом), али у већини случајева је Суд заузео став да је интерес заштите од

[998] *Electronic Communication Privacy Act 1986*, Pub. L. No. 99-508, 100 Stat. 1848, https://it.ojp.gov/default.aspx?area=privacy&page=1285. Овим законом су измењене и допуњене одредбе Закона о прислушкивању телефона и скривеним микрофонима(*Federal Wiretap Act*) из 1968.

[999] *USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act* of 2001, Pub. L. No. 107-56, 115 Stat. 272 , http://www.americanlaw.com/patriotact.html.

[1000] Rashbaum, *op.cit*, 50-51.

[1001] J. Soma et al, Balance of Privacy vs. Security:a historical perspective of the USA Patriot Act, *Rutgers Computer and Technology Law Journal* 4/2005, 314.

могућих терористичких напада претежнији од интереса заштите приватности и слободе[1002]. Како се из кратког приказа развоја и савременог схватања концепта приватности у САД може закључити да друштво појединчево очекивање приватности уопште и у погледу заштите података о личности не препознаје као оправдано услед сталне претње по општу безбедност, која је претежнији интерес од заштите права појединаца гарантованих Уставом, сматрамо да, иако је концепт приватности (и у оквиру њега заштита података о личности) настао у оквиру америчке правне традиције, узор не треба тражити у овом правном систему, него се кретати у оквирима у којима је наш правни систем настао и развијао се, те пажњу посветити европској правној традицији.

У прилог тврдњи да међународни уговори познају заштиту података о личности као право које се изводи из зајемчених права на приватност је пракса ***Европског суда за људска права*** која потврђује да заштита приватног живота обухвата и заштиту у погледу прикупљања, складиштења и употребе података о личности[1003]. Суд је у пресуди у предмету *K.U. v. Finland*[1004] јасно истакао да је заштита података о личности од кључног значаја за поштовање приватног и породичног живота, и тиме потврдио став који је у претходном периоду заузео у неколико пресуда[1005]. У пресуди у случају *Peck v. United Kingdom* Суд је поставио критеријуме за одређивање да ли се ради о податку о личности који ужива заштиту у смислу члана 8. Конвенције, при томе јасно истичући *да иако прикупљање података може бити оправдано, то не значи да је прихватљиво задржавање података дуже него што је потребно за остваривање сврхе у коју*

[1002] Тако у предмету *In re: Sealed Case*, суд надлежан за одобравање надзора страних обавештајних података је инсистирао да се поштују ограничења налога за електронски надзор у складу са Законом о надзору страних обавештајних података (*FISA*) али је Врховни суд утврдио да та ограничења нису дозвољена јер су у супротности са *USA Patriot* законом (који је изменио одредбе *FISA*-а) по ком државни орган нема обавезу да образлаже потребу за издавањем таквог налога. На овај начин је за добијање налога за претрес и надзор комуникација довољно се позвати у предлогу суду на одредбе поменутог закона. У предмету *United States v. Sattar* је окривљени безуспешно покушао да издејствује да се докази који су прибављени против њега на основу судског налога за тајни електронски надзор буду проглашени као недозвољени.

[1003] Више о пракси Европског суда за људска права, S. Gutwirth, Y. Poullet, P. De Hert (eds.), *Data protection in profiled world*, Springer , Heidelberg 2010, 42-43.

[1004] Пресуда у предмету *K.U. v. Finland* (*No.*2872/02).

[1005] Концепт приватног живота обухвата заштиту лица у погледу фотографија и видео снимака које садржи његов приказ (пресуда у предмету *Sciacca v. Italy* (*No.* 50774/99), у погледу снимања гласа ради даље анализе (пресуда у предмету *P.G. and J.H. v. the United Kingdom* (*No* 44787/98); података који су објављени а настали су снимањем на јавним местима (пресуда у предмету *Peck v. the United Kingdom* (*No* 44647/98); праћења лица путем *GPS*- а и обраде тих податак без знања лица (пресуда у предмету *Uzun v. Germany* (*No* 35623/05).

су се подаци прикупљали[1006]. Чак штавише, *само складиштење података који се односе на приватну сферу појединца може представљати повреду права* из члана 8. Конвенције[1007], као и *накнадна употреба сачуваног податка од стране лица које није за то овлашћено*[1008], те *онемогућавање лица да буде информисано да ли се подаци о њему прикупљају*[1009]. Осим тога, Суд је заузео јасан став да *стварање база података у којима се неограничено чувају подаци о личности*, а чије укрштање може омогућити стварање профила личности, *представља неоправдано мешање* у приватност појединца[1010]. Ипак, уколико се подаци о личности прикупљају и складиште за потребе националне безбедности у складу са прописима који садржа адекватне и ефективне гаранције од злоупотребе података, Суд је заузео став да не постоји повреда права из члана 8. Конвенције[1011], при чему ти *прописи треба да довољно јасан начин одреде обухват и услове коришћења таквих овлашћења надлежних органа*[1012]. Иако је у више пресуда заузео став о појединим аспектима заштите података о личности, може се приметити да је *Суд суздржан у погледу оцене усклађености појединих техника за прикупљање и обраду података о личности,* а које су у средишту стратегија за борбу против тероризма и других тешких облика кривичних дела.

Што се тиче регулисања ове проблематике у оквиру ***Европске уније***, треба истаћи да је заштита података о личности препозната као људско право у члану 8. Повеље о основним правима[1013], и предмет је регулисања у неколико правних иструмента, од којих су најзначајније: Директива ЕУ о заштити појединаца у вези са обрадом података о личности и слободним кретањем тих података[1014] и

[1006] Пресуда у предмету *Peck v. the United Kingdom* (*No* 44647/98).
[1007] Пресуда у предмету *Leander v. Sweden* (*No* 116/1987).
[1008] Пресуда у предмету *Amann v Switzerland* (*No* 843/2000*).* Ипак, накнадна употреба не би представљала повреду овог права уколико је предвиђена законом ради заштите оправданих интереса у демократском друштву.
[1009] Пресуда у предмету *Rotaru v Romania* (*No* 46/2000).
[1010] Пресуда у предмету *S. and Marper v United Kingdom* (*Nos* 30562/04, 30566/04).
[1011] P. Breyer, „Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR“, *European Law Journal* 3/2005, 368.
[1012] Пресуда у предмету *Niemietz v Germany* (*No* 251/1992).
[1013] *Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.*
[1014] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.*

Директива о приватности електронских комуникација[1015]. Ипак, ови прописи се односе на заштиту података о личности у некадашњем првом стубу ЕУ. Прикупљање и обрада података о личности за потребе кривичног поступка регулисани су Оквирном одлуком ЕУ о заштити података о личности обрађених у оквиру полицијске и правосудне сарадње у кривичним предметима[1016] (који се непосредно односи на питање заштите података о личности али не у вези са кривичним поступком унутар граница државе него у оквиру прекограничне сарадње у кривичним стварима[1017]) као и у различитим секторским прописима[1018]. Ови прописи су у недовољној мери међусобно усаглашени, али сви садрже основне принципе заштите у складу са поменутом Конвенцијом СЕ, па се може рећи да је систем заштите података о личности у Европској унији прилично комплексан, непотпун и некохерентан[1019].

У погледу прописа у ***националном законодавству*** који садрже одредбе о заштити података о личности, могли бисмо разликовати више категорија [1020], при

[1015] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.*

[1016] *Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF.*

[1017] Ова Оквирна одлука уређује обраду података о личности који су пренесени или стављени на располагање између држава чланица, а донета је како би размена података о личности у оквиру полицијске и правосудне сарадње у кривичним стварима била подржана јасним правилима којима се повећава узајамно поверење између надлежних органа држава чланица уз истовремено потпуно уважавање основних права појединаца. Више о томе, M. Pisarić, „Data protection within police and judicial cooperation in EU", *European Legal Studies and Research*, 2011, 444; P, De Hert, C. Riehle, „Data protection in the area of freedom, security and justice. A short introduction and many questions left unanswered", *ERA Forum* 11/2010, 159–167.

[1018] Ради се о следећим актима: Шенгнески споразум (*Schengen Agreement, http://eur-lex.europa.eu/search.html?qid=1429091166702&text=schengen&scope=EURLEX&type=quick&lang=en*), Одлука о оснивању *Europol*-а (*Council Decision of 6 April 2009 establishing the European Police Office*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0371) , Одлука о оснивању *Eurojust*-а (*Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime*, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1429091092084&uri=CELEX:52008AP0384), Одлука 2008/615/JHA о унапређењу прекограничне сарадње, посебно у борби против тероризма и прекограничног криминала (*Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF)

[1019] О критици система заштите података о личности у Европској унији, R. Jones, D. Tahri., "An overview of EU data protection rules on use of data collected online", *Computer Law and security review* 27/2012, 635; F. Wang, N. Griffiths, „Protecting privacy in automated transaction systems: a legal and technological perspective in the European Union", *International review of law, computers & technology* 2/2010, 157.

[1020] Најопштији и најсвебухватнији слој у регулативи чини низ општих одредаба које садрже основне принципе заштите и правила о обради података о личности (одредбе садржане у уставу

чему се они међусобно нужно не искључују, али је потребно да постоји кохерентност између њих, односно да чине јасно дефинисану и ка истом циљу усмерену структуру, тако да се прописи у различитим гранама права који регулишу различите аспекте друштвеног живота примењују на конзистентан начин[1021]. Да би се то обезбедило, потребно је да постоје ***одређени руководећи принципи*** у виду смерница за успостављање јединственог система заштите података о личности. У том смислу, приликом регулисања права појединца на заштиту података о личности у вези са кривичним поступком за дела високотехнолошког криминала, треба имати у виду поједине принципе који су заједнички поменутим инструментима, који иако ако су усвојени у оквиру различитих организација и имају различиту правну снагу[1022], садрже мање – више исте гаранције заштите појединаца у вези са обрадом података о личности[1023].

Међутим, како су принципи заштите података о личности настали у време када је обрада података о личности у технолошком смислу била коначна и уочљива,

---

које предвиђају гаранцију права на заштиту података о личности и одредбе „кровног“ закона). Други слој садржи слична правила а која уређују различите секторе у друштву (нпр. одредбе о заштити података о личности у законима који уређују систем здравствене заштите). Трећи слој обухвата одредбе које овлашћују одређене субјекте да прикупљају податке о личности у различитим областима друштвеног живота, али су у односу на претходни слој мање систематичне и ужег обухвата (нпр. прописи о вођењу криминалистичких евиденција и коришћењу података за потребе кривичног поступка). Следећи слој чине разни прописи који између осталог садрже одредбе, које регулишу поједине аспекте заштите података о личности (као нпр. права на приступ подацима о личности). Пети слој садржи казненоправне одредбе које инкриминишу одређена понашања која повређују заштиту података о личности као кривично дело (у кривичном закону), односно као прекршај (у казненоправним одредбама појединих прописа).

[1021] D. W, Schartum, „ Designing and Formulating Data Protection Laws“, *International Journal of Law and Information Technology* 1/2008, 10.

[1022] За Републику Србију је правно обавезујућа само Конвенција Савета Европе коју је наша држава ратификовала, а што се тиче извора права Европске уније, како Републици Србији као земљи кандидату за чланство предстоји процес усклађивања правног система са системом те организације, одредбе поменутих инструмената свакако треба имати у виду.

[1023] Ради се о следећим принципима: 1. Подаци о личности се прикупљају и обрађују законом дозвољеним и правичним средствима (*принцип законитости прикупљања и обраде података о личности*); 2. Обим података о личности је ограничен на меру која је потребна за остваривање сврхе прикупљања (*принцип минималности*); 3. Подаци о личности се прикупљају за одређену и законом дозвољену сврху и обрађују се на начин који одговара сврси прикупљања (*принцип одређености сврхе*); 4. Подаци о личности се могу употребити за друге сврхе (осим сврхе прикупљања) само уз изричит пристанак лица или овлашћење у складу са законом (*принцип ограничене употребе*); 5. Подаци о личности треба да буду тачни, потпуни и у вези су са сврхом обраде (*принцип квалитета података*); 6. Безбедносне мере се предузимају ради заштите података о личности од ненамерног и/или неовлашћеног откривања, уништења или измене (*принцип безбедности података о личности*); 7. Лица о којима се прикупљају подаци се обавештавају и омогућава им се приступ подацима ради отклањања/исправке нетачних и непотпуних података (*принцип учешћа појединаца*); 8. Стране овлашћене за обраду података о личности су одговорне за усклађеност обраде са наведени принципима (*принцип одговорности*).

односно ограничена (што у савременом окружењу свакако да није случај) неоправдано је очекивати да исти могу бити применљиви и даље, макар не на исти начин и у истом смислу како су изворно настали. У време кад су међународни инструменти били усвојени, технологије које су данас у уобичајеној и широкој употреби (Интернет, социлајне мреже, биометријски системи) су биле непознате и можда чак незамисливе. У савременом технолошком окружењу различити субјекти за различите потребе податке о личности прикупљају и обрађују применом разних, често скривених техника, без знања лица, а постоји повећана опасност да се подаци из разних извора укрштају и формирају својеврсни профили личности[1024]. Са снижавањем трошкова аутоматске обраде, повећањем меморијских капацитета рачунара[1025], те употребом интелигентних високософистицираних техника за прикупљање, обраду и анализу података, ризик од неоправданог задирања у права приватности, у смислу заштите података о личности, постаје све очигледнији[1026]. Осим тога, корисници неке од поменутих технологија олако користе у свакодневном животу и њихово поимање приватности је сасвим другачије у односу на традиционално схватање приватности, те оправданог очекивања приватности[1027]. Из овога, међутим, не произлази закључак да од заштите података треба одустати, већ да је, тим пре, неопходно унапредити правни механизам који би појединцима обезбедио одређена права у циљу заштите њихових података, јер концепт приватности није превазиђен, нарочито не концепт информационе приватности који директно везујемо за заштиту података о личности.

[1024] Технике за профилирање користе статистичке методе које аутоматским укрштањем наизменично одабраних информација у различитим изворима (великим базама података) изводе закључке о понашању лица, односно створити његов профил. На овај се, рецимо, може на основу куповине одређеног предмета одређеног дана у одређено време са 89% сигурности утврдити да купац нема партнера. Наведено према: Poullet, *op.cit*, 214.

[1025] Према Муровом закону *(Moore's law*) меморијски капацитет ће се дупло повећавати сваких 18 месеци (повећање од 1000 пута за 15 година) уз истовремено смањење трокова за овако побољшан капацитет ће се смањивати за 50 %. *Moore's Law at 50: Its past and its future*, http://www.extremetech.com/extreme/203031-moores-law-at-50-its-past-and-its-future.

[1026] J. Esayas, "A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data", *Computer Law and security review* 28/2012, 341.

[1027] P. De Filippi, S. McCarthy, "Cloud Computing: Centralization and Data Sovereignty", *European Journal for Law and Technology* 2/2012, 13-14.

2.1. Информациона приватност и нове технологије

С обзиром на то да се не сме занемарити да се услед свеопште дигитализације свакодневног живота и конвергенције рачунарских и комуникационих технологија променило и окружење у ком је гарантована заштита првобитно настала, истичемо потребу да се постојећи механизми прилагоде променама условљеним развојем информационих технологија[1028]. У вези са коришћењем савремених електронских уређаја за аутоматску обраду и пренос података о личности и у *online* окружењу у ком појединци немају ефективну контролу над обрадом података о њима[1029], поставља се питање *да ли се информациона приватност може посматрати на исти начин* као у физичком свету или су оваква схватања изгубила смисао у ери Интернета па се може говорити о тзв. *online информационој приватности* као новој парадигми? Даље се можемо запититати, *да ли се* заштита тзв. *online информационе* приватности *може обезбедити на исти начин*, односно регулисати истим правилима као приватност у физичком свету?

Супротно од некадашњих схватања о анонимности корисника Интернета и неограниченој слободи поступања, ниједна активност на Интернету није у потпуности приватна сфера појединца без обзира на све мере заштите које корисник употреби. У том смислу, *online приватност* се може посматрати кроз *две компоненте*: 1) *приватност која се односи на податке о личности*, а подразумева да корисник има контролу Интернета у погледу тога ко, када и како

[1028] Да би одређена правила у вези за заштитом података о личности била довољно уопштена, тј. да би се могла сматрати принципима, потребно их је креирати тако да буду технолошки неутрална, како не би промене у технолошком развоју угрожавале зајемечени ниво права лица. M. Hildebrandt , L.Tielemans, „Data protection by design and technology neutral law“, *Computer Law and Security Review* 29/2013, 510.

[1029] Информациону приватност као такву је пре појаве Интернета било лако штитити из разлога: нису прикупљане велике количине података о личности; прикупљени подаци су били чувани и одржавани на децентрализованим основама; подаци су имали површни карактер до мере некорисности; без одговарајућих технологија није било могућности за праћење активности појединаца у великом обиму; из прикупљених података без одговарајућих техника није било једноставно извести информацију. У компјутеризованом умреженом окружењу, пак, моћ контроле над протоком података о личности може бити компромитована на најмање два начина: (1) омогућавање увида у податке о прошлим и садашњим радњама ширем кругу лица у односу на првобитно дат пристанак лица у тренутку када је добровољно предао одређене информације (депривација контроле приступа подацима), и (2) стварањем фактичких или контекстуалних нетачности које доводе до погрешне представе о понашању појединца (депривација контроле тачности података). A. Miller, “Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information -Oriented Society”, *Michigan Law Review* 6/1969, 1109.

је приступио његовим подацима[1030] (у циљу заштите *online* идентитета[1031]), и 2) *приватност општења* која подразумева заштиту од мешања у његове комуникације и друге активности које остварује на Интернету[1032]. Обе ове компоненте имају свој пандан у реалном свету, па је могуће правила која их штите применити и у погледу вредности које се испољавају и виртуелном окружењу, јер се у сваком случају односе на појединца чије права могу бити угрожена и поништена неоправданим мешањем разних субјеката[1033]. Наиме, с обзиром на то да се велики број активности које је појединац предузимао у реалном свету „преселио" у виртуелни, концепт приватности у виду „оправданог очекивања неузмениравања од неоправданог надгледања тих активности"[1034] такође треба да буде пресељена из *offline* у *online* окружење[1035]. Ово је потребно тим пре што је податке о личности на основу којих се могу идентификовати корисници услуга електронских комуникација (без обзира на то да ли се ради о подацима које свесно чини доступним јавности или настају независно од његове воље) могуће употребом савремених техника и метода искористити на неслућене начине - до стварања виртуелног идентитета појединаца – аватара чијег постојања

[1030] C. Bennett, „In Defence of Privacy: the concept and the regime", Surveillance & Society 4/2011, 486. Упор. L. Duranti, C. Rogers, „Trust in digital records: An increasingly cloudy legal area", *Computer law & security review* 28/ 2012, 525.

[1031] D. Svantesson, „The significance and protection of identity in the online world", *Computer Law and security Review* 27/2011, 2.

[1032] M. Watney, „The Legal conflict between Security and Privacy in Addressing Crime and Terrorism in Internet", ISSE Conference, Warsaw, Poland: 25 September 2007, 32.

[1033] У Препорукама Савета Европе из 1999. године које се односи на заштиту права приватности корисника Интернета, пажња је била у том тренутку посвећена само обавезама које пружаоци Интернет услуга имају према корисницима (Y. Akdeniz, *op.cit*, 57). У том периоду није се указивало на опасности обраде података о личности од стране државних органа, већ се заштита овог права остваривала само у односу на приватни сектор.

[1034] Оправдано очекивање се мења током времена у зависности од тога колико су појединци спремни да се одрекну дела своје приватности у одређеном контексту, што се усложњава јер појединци полазе од очекивања приватности коју су имали у физичком свету а нису свесни да је њихово понашање предмет надзора и праћења. Примера ради, појединци су могли имати оправдано очекивање приватносту када су у својим домовима слушали радио станице на аналогном уређају, међутим, када слушају *webradio* нису свесни да је та активност надгледана односно да постоји могућност да се преко *IP* адресе *дође до појединачног слушаоца и да се анализом записа изведу закључци о његовим музичким преференцијама*. R. Leenes, B. Koops, "Code: Privacy death or saviour?" *International journal of Law, Computers and Technology* 3/2005, 322.

[1035] Веће за људска права Уједињених нација је 2012. године усвојило Резолуцију о промоцији, заштити и уживању људских права на Интернету, у којој је афирмисан принцип да се иста права које појединци имају у *offline* свету, *морају бити заштићена* и у *online* окружењу. *Resolution L13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet*, http://geneva.usmission.gov/2012/07/05/Internet-resolution.

лице није ни свесно[1036]. Гарантовање права на приватност штити појединце од претераног мешања друштва и контроле других појединаца у погледу развоја и испољавања његове личности, али истовремено омогућава слободно учешће у социјалном животу[1037]. У том смислу, *online* приватна сфера није просто „инфосфера" која окружује свако лице, већ обухвата „друштвене и контекстуалне комплексности које се мешају и дешавају у техничким системима"[1038] и због тога се подаци о активностима не смеју прикупљати на начин да угрозе његово право на слободан развој личности.

У вези са наведеним, корисно је указати на „*теорију мозиака*"[1039], по којој појединачни подаци који сами по себи немају никакву или имају ограничену вредност у обради, када се доведу у везу са другим подацима добијају додату вредност, односно постају информације, чијим комбиновањем се долази до новог схватања њихових међусобних односа и јача се њихова аналитичка синергија, тако да резултирајући мозаик информација постаје много вреднији него појединачни подаци сами по себи[1040]. Уколико ову теорију применимо на ситуацију у ком се подаци о личности неограничено прикупљају , ма колико појединачно безначајни били (мада тако не би требало третирати ниједан податак који одређује или може да одреди лице), њиховим укрштањем и комбиновањем долази се мозаика информација о појединцу, као дигиталног идентитета чијег постојања лице није свесно па нема ни котролу на њима и чиме се поништава информациона приватност, што је недопустиво[1041]. *Online* приватност је легитимно посматрати као право појединца „да буде заборављен"[1042], „да буде

[1036] Осим постојања такве виртуелне личности, које лице није свесно, у литератури се расправља и о могућности заштите (па и путем кривичног права) аватара (као облика имовине), које је лице створило у виртуелном окружењу са намером и одређеном сврхом. A. Guinchard, „Crime in virtual worlds: The limits of criminal law", *International Review of Law, Computers & Technology* 2/ 2010, 178;
[1037] F. Regan, „Response to Bennett: Also in Defense of Privacy", *Surveillance & Society* 4/2011, 499.
[1038] Bignami, *op.cit*, 220.
[1039] D. Pozen, „The Mozaic theory, national security and the freedom of national act", *The Yale Law Journal* 1/2005, 630.
[1040] О критици теорије мозаика, Kerr, „The Mosaic Theory of the Fourth Amendment Amendment", 347.
[1041] „*Дигитални идентитет*" је концепт који се разматра у америчкој научној литераути, као скуп дигиталних информација о лицу које су подобне да га идентификуу, односно одреде у виртуелном окружењу. C. Sullivan, „Digital identity, privacy and the right to identity in the United States of America", *Computer Law and Security Review* 29/2013, 349.
[1042] D. Goldrick, „Developments in the Right to be Forgotten", *Human Rights Law Review* 4/2013, 762. Исто, P. Castellano, 'A Test for Data Protection Rights Effectiveness: Charting the Future of the ''Right to Be Forgotten'' under European Law', *The Colombia Journal of European Law Online* 1/2012, 3; J.

остављен на миру“ [1043], „да се обрише његов електронски идентитет“[1044] у свету дивергенције информационо-комуникационих технологија у смислу очувања контроле појединца над подацима који се о њему прикупљају и обрађују, односно да се независно од његовог знања и воље не ствара „електронски идентитет“[1045]. Контрола над подацима о личности у смислу ограничавања приступа истим, огледа се у очекивању појединаца да се онемогући њихово тајно праћење и надгледање њихових активности, а произлази из дубоке потребе за аутономним развојем идентитета и индивидуалности и отуда још израженија потреба за информационом приватношћу и у виртуелном окружењу[1046].

Имајући у виду промене у друштвеном, технолошком и правном окружењу које је произвела конвергенције инфрмационо-комуникационих технологија а ради одговора на изазове које која примена ових технологија може имати на основна људска права и слободе, Комитет министара Савета Европе је 2005. године усвојио *Декларацију о људских правима и владавини права у информационом друштву*[1047].У овој Декларацији се истиче потреба за прилагођавањем постојећих механизама заштите људских права и слобода, а нарочито у погледу радњи и мера које предузимају надлежни државни органи у сузбијању савремених облика тешког криминала употребом технолошких достигнућа (пре свега се мисли на електронску обраду, прикупаљње, снимање, складиштење података о личности) која могу имати негативне последице по достигнути ниво заштите права лица. Те радње треба да буду прописане и примењене у складу са принципима одређености, потребности, сразмерности, и уз

Ausloos., „The ‘Right to be Forgotten’-Worth remembering?“, *Computer Law and security Review* 28/2012, 146.

[1043] Према Извештају о ставовима о подацима о личности и електронском идентитету у Европској унији, 70% анкетираних је забринуто јер одређене приватне компаније складиште и користе податке о њима за друге сврхе осим у односу на сврху због које су прикупљени, а 75% њих изражава жељу да има могућност да тражи брисање података о њима који се појављују на одређеним веб страницама. *Attitudes on Data Protection and Electronic Identity in the European Union*, http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm.

[1044] P. Bernal, ‘A Right to Delete?, *European Journal of Law and Technology* 2/2011, 2. О техничким проблемима у осрваривању вог права, *European Network and Information Security Agency, The Right to Be Forgotten: Between Expectations and Practic*e 2011, www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten.

[1045] Y. Poulett, „The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!“, *International Law Computers& Technology Review* 2/ 2004, 254.

[1046] D. Michelfelder, “The moral value of informational privacy in cyberspace”, *Ethics and Information Technology* 3/2001, 133.

[1047] *Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society*, https://wcd.coe.int/ViewDoc.jsp?id=849061.

контролу судских органа, како право на поштовање приватног живота и слобода општења не би били угрожени. Осим тога, Комитет је децембра 2014. године представио нацрт измена Конвенције СЕ бр.108. (који је у време писања овог рада прослеђен на усвајање). Измене се предлажу у циљу модернизације принципа заштите података о личности ради прилагођавања постојећем технолошком и друштвеном окружењу. Нагласак је на потреби да се правним механизмима пронађе одговор на изазове које нове информационе и комуникационе технологије, те *глобализација процеса обраде података о личности и њихов олакшан проток* постављају пред заштиту приватности лица[1048].

На овом месту указујемо и да је режим заштите података о личности у Европској унији тренутно у процесу реформе[1049] - ради стварања јединственог система заштите података о личности процедури је усвајање Опште уредбе о заштити појединаца у вези са обрадом података о личности и слободним протоком тих подтака[1050] и Директиве о заштити појединаца у вези са обрадом података о личности од стране надлежних органа за потребе спречавања, откривања и истраге кривичних дела и гоњења учинилаца или извршења кривичних санкција [1051], која садржи правила о заштити података о личности у кривичном поступку и у вези са прекограничном разменом података између надлежних органа у систему кривичног правосуђа[1052].

[1048] Више о томе, http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp. О потреби модернизације Конвенције СЕ, S. Kierkegaard et al., "30 years on -The review of the Council of Europe Data Protection Convention 108", *Computer Law and security Review* 27/2011, 223-225.

[1049] *Interparliamentary Committee Meeting, "The reform of the EU Data Protection framework – Building trust in a digital and global world*, 2012, http://www.europarl.europa.eu/document/activities/cont/201210/20121003ATT52831/20121003ATT52831EN.pdf.

[1050] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation*), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=en.

[1051] *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0010&from=en.

[1052] О критичкој анализи предлога Директиве, M. Backer, G. Hornung, „Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure", *Computer Law & Security Review* 28/2012, 630; P. De Hert, Papakonstantinou V., "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Magazine of the Society for Computers & Law. Computers & Law* 6/2012, 22; P. De Hert, V. Papakonstantinou, "The proposed data protection Regulation replacing Directive 95/46/EC: A sound

3. ОБРАДА ПОДАТАКА О ЛИЧНОСТИ И КРИВИЧНИ ПОСТУПАК

Како је окружење у ком се предузимају радње дела високотехнолошког криминала технолошко, то што се корисници технологија својевољно одричу дела своје приватности (што је суштина права на информационо самоопредељење), постојећа правила о заштити података о личности је потребно прилагодити измењеним околностима и узети их у обзиром приликом прописивања радњи и мера које ради откривања и доказивања надлежни органи предузимају.

Свако лице има право на заштиту података о личности, а то право може бити ограничено ради заштите општег интереса, односно очувања битних вредности у друштву. У погледу лица против ког постоји одређен степен сумње да је учинило одређено кривично дело, надлежни органи су овлашћени да предузимањем одређених радњи и мера у складу са законом прикупљају и обрађују податке о личности за потребе кривичног поступка. Подаци о личности се прикупљају на основу овлашћења за предузимање редовних и посебних доказних радњи и мера (коришћење криминалистичких евиденција, посматрање, систематско прикупљање информације од стране прикривеног иследника, надзор и снимање комуникација одређеним техничким уређајима, претрес уређаја за електронску обраду и складиштење података и друго), а прикупљање података би требало да буде ограничено у мери која је потребна за сузбијање конкретног кривичног дела[1053] у складу са принципом сразмерности. У погледу овлашћења надлежних органа на предузимање радњи и мера које је потребно установити у националним прописима а ради имплементације процесних одредаба Конвенције о високотехнолошком криминалу (водећи рачуна о широком обухвату тих одредаба), *потребно је проценити могући ризик од предузимања појединих радњи и мера на заштиту података о личности и приватност лица*.

---

system for the protection of individuals", *Computer Law & Security Review* 2/2012, 135; R. Wong, "Data protection: The future of privacy", *Computer Law and security Review* 27/2011, 55.

[1053] Препорука Савета Европе која се односи на употребу података о личности у полицијском скетору (*Recommendation N° R (87) 15 regulating the use of personal data in the police sector*), http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf. Иако усвојена пре више од 25 година ова Препорука садржи битне принципе за заштиту података о личности од неоправданог мешања државних органа. *Report: Recommendation R (87) 15 – Twenty–five years down the line, 2013,* http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf.

Када се разматра заштита података о личности у вези са прикупљањем података за потребе кривичног поступка, потребно је обратити пажњу на следеће изазове:

1. Како обезбедити поштовање суштине општих принципа заштите података о личности у случају када су ограничења овог права дозвољена у вези са предузимањем радњи и мера којима се прикупљају подаци о личности (с обзиром на то да приликом ограничења људског права државни органи дужни да воде рачуна о томе да не задиру у суштину права)?
2. Како регулисати (да ли дозволити, у којим случајевима и под којим условима) употребу савремених техника надзора (као што су *data mining* и *profiling*[1054]) које задиру у саму суштину заштите података о личности?
3. Да ли правни оквир пружа заштиту и у погледу одређених података који се непосредно не односе на лица (при чему треба имати у виду да ти подаци могу послужити за утврђивање идентитета лица (*identifiable data*) па их треба третирати као податке о личности)?
4. Који правни оквир се примењује за заштиту података о личности који се прикупљају у комерцијалне природе (подаци који проистичу из уговорног односа лица и привредних субјеката у вези са пружањем услуга електронских комуникација и сл) а које су пружаоци услуга електронских комуникација дужни да предају у одређеним случајевима надлежним државним органима;
5. Како обезедити да се гарантовани ниво заштите података о личности поштује у вези са остваривањем одређених облика међународне сарадње надлежних органа?

Да би се ови изазови превазишли на начин да се заштита података о личности обезбеди на одговарајући начин, сматрамо да потребно прецизно дефинисати у којим случајевима, под којим условима и на који начин су поједини државни органи овлашћени да прикупљају, обрађују и користе податке о личности, а нарочито је потребно регулисати механизме размене података о личности између различитих државних органа (као и прекограничне размене података), као и

[1054] О опасностима ове технике по приватност лица, Schermer B., „The limits of privacy in automated profiling and data mining“, *Computer Law and security Review* 27/2011, 46.

између државних органа и приватног сектора (првенствено мислимо на пружаоце услуга електрнских комуникација[1055]).

Основни принципи заштите података о личности могу се уочити у основи правног регулисања у Републици Србији. Тако је чланом 42. Устава[1056] зајемчена заштита података о личности у поглављу којим се уређују људска права и слободе, а одређено је да се прикупљање, држање, обрада и коришћење података о личности уређују се законом (*принцип законитости прикупљања и обраде података о личности)*. Осим тога, изричито је прописано да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (*принцип одређености сврхе* и *принцип ограничене употребе*)[1057].

На основу поменуте одредбе усвојен је Закон о заштити података о личности[1058]. Закон у члану 8. одређује случајеве у којима обрада[1059] података о личности[1060] није дозвољена[1061] (што треба довести у везу са Кривичним закоником РС[1062] који у члану 146. предвиђа кривично дело Неовлашћено

[1055] Више о томе, Law enforcement challenges in transborder acquisition of electronic evidence from "cloud computing providers" (prepared for the Council of Europe/Global Project on Cybercrime), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp.

[1056] „Сл. гласник РС“, бр. 98/2006.

[1057] У Нацрту измена Конвенције СЕ се уводи *и за потребе „спречавања“ кривичних дела*.

[1058] „Сл. гласник РС“, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012.

[1059] Обрада података је свака радња предузета у вези са подацима као што су: прикупљање, бележење, преписивање, умножавање, копирање, преношење, претраживање, разврставање, похрањивање, раздвајање, укрштање, обједињавање, уподобљавање, мењање, обезбеђивање, коришћење, стављање на увид, откривање, објављивање, ширење, снимање, организовање, чување, прилагођавање, откривање путем преноса или на други начин чињење доступним, прикривање, измештање и на други начин чињење недоступним, као и спровођење других радњи у вези са наведеним подацима, без обзира да ли се врши аутоматски, полуаутоматски или на други начин (члан 3. Закона).

[1060] Податак о личности је свака информација која се односи на физичко лице, без обзира на облик у коме је изражена и на носач информације (папир, трака, филм, електронски медиј и сл.), по чијем налогу, у чије име, односно за чији рачун је информација похрањена, датум настанка информације, место похрањивања информације, начин сазнавања информације (непосредно, путем слушања, гледања и сл, односно посредно, путем увида у документ у којем је информација садржана и сл.), или без обзира на друго својство информације (члан 3. Закона).

[1061] Између осталог, предвиђају се ситуације у којим не постоји правни основ за обраду, а то су: 1) физичко лице није дало пристанак за обраду, и 2) обрада се врши без законског овлашћења. Дакле, да би обрада била дозвољена потребно је или да је лице на које се подаци односе дало пристанак за обраду (у складу чланом 11. Закона) или да постоји законско овлашћење које замењује пристанак лица о коме се подаци прикупљају (које произлази з чланова 12. и 13 Закона).

прикупљање личних података[1063]). Члан 13. изричито овлашћује органе власти да обрађују податке без пристанка лица, ако је обрада неопходна ради обављања послова из надлежности одређених законом а у циљу (између осталог) *спречавања, откривања, истраге и гоњења за кривична дела*, што је у складу са поменутом одредбом Устава. Устав садржи још један од принципа заштите података о личности јер гарантује да свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом (члан 42. став 4). С тим у вези, Закон о заштити података о личности утврђује да лице о коме се подаци обрађују има право на обавештење о обради (члан 19), увид (члан 20) и копију (21. и 22)[1064], али да се то право може ограничити ако би давање обавештења озбиљно угрозило радње спречавања, откривања, истраге и гоњења за кривична дела (члан 23)[1065]. Ова одредба је законски основ за ограничење заштите података о личности као људског права гарантованог Уставом, а да би ова одредба имала смисао законитог ограничења поменутог људског права, нужно је довести у везу са чланом 20. Устава. Наиме, људска права зајемчена Уставом могу законом бити ограничена ако ограничење допушта Устав, у сврхе ради којих га Устав допушта, *у обиму неопходном да се уставна сврха ограничења задовољи* у демократском друштву и *без задирања у суштину зајемченог права*. Истовремено, треба имати на уму и то да су сви државни органи, а нарочито судови, при ограничавању људских права, дужни *да воде рачуна о* суштини права које се ограничава, важности сврхе ограничења, природи и обиму ограничења, односу ограничења са сврхом ограничења и о томе да ли постоји начин да се сврха ограничења постигне мањим ограничењем права. Иако Устав предвиђа овакву дужност државних органа, *Законик о кривичном поступку* као пропис који би требало детаљније да разради могућност ограничења овог права ради заштите интереса кривичног поступка, међутим, *не садржи ниједну одредбу која има за*

[1063] "Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.

[1063] Радњу извршења овог кривичног дела чини лице које: 1) неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени податке о личности који се прикупљају, обрађују и користе на основу закона; 2) противно закону прикупља податке о личности грађана или тако прикупљене податке користи.

[1064] Предвиђање ових права је обавеза државе потписнице Конвенције (права су гарантована у складу са чланом 8. Конвенције).

[1065] Члан 9. Конвенције предвиђа могућност ограничења гарантованих права уколико је такво одступање предвиђено законом и представља неопходну меру ради заштите важних интереса, између којих се наводи и сузбијање кривичних дела.

циљ заштиту података о личности. Стога *сматрамо да је ради веће правне сигурности потребно у Законику о кривичном поступку предвидети изричите одредбе које би се односиле на прикупљање, коришћење и заштиту података о личности за потребе кривичног поступка, а нарочито на обавештавање лица да се о њему обрађују подаци за потребе кривичног поступка.*

У погледу ***обавештења лица*** да се о њему прикупљају подаци за потребе кривичног поступка, ради изналажења могућег решења, можемо узети у обзир поменуту Оквирну одлуку ЕУ[1066] која у члану 17. предвиђа право лица да буде упознато са тим да су подаци о личности били прикупљани и обрађивани за потребе кривичног поступка, али да се такво право приступа може ограничити ако је потребно и у сразмери са заштитом одређених интереса, а између осталог, и како се не би ометао кривични поступак. При томе, свако одбијање или ограничавање приступа даје се се у писаном облику лицу чији се подаци обрађују. Писана одлука треба која садржи образложење (које може да изостане у случајевима у којима постоји разлог за ограничење права приступа информацијама)[1067]. Сматрамо да је потребно у Законик унети одредбу по којој би јавно тужилаштво или суд били дужни да лицу на основу поднетог захтева *доставе обавештење* о томе да *ли су подаци о личности били предмет прикупљања и обраде за потребе кривичног поступка*. Ради заштите интереса кривичног поступка, остваривање права на обавештење се може ограничити, односно временски одложити до истека одређеног рока[1068].

[1066] *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF*.

[1067] Предлог Директиве садржи обавезу прописивања одредбе у закону о кривичном поступку којом се лице о коме су подаци прикупљани и обрађивани обавештава о прикупљању података, о сврси, периоду у ком се подаци намеравају чувати, праву да захтева остваривање увида, исправку и брисање нетачних и непотпуних података, лицима којима су прикупљени подаци прослеђени, те о праву на правно средство, Осим тога, лице може да тражи остварвање увида у податке који се о њему прикупљају (и то у погледу сврхе обраде, категорије податаке, периода чувања, те лица којима су подаци прослеђени). Међутим, обавеза обавештавања лица и омогућавања приступа обрађиваним подацима може бити одложена, односно ограничена у потребној и сразмерној мери а из оправданих разлога - да се не би угрозило откривање и доказивање кривичног дела, те повредила права других лица. У случају да државни орган одбије или ограничава обавештење, односно омогућавање остваривања увида лицу о коме се подаци прикупљају, дужан је да изда писану и образложену одлуку са поуком о правном леку, при чему образложење може бити изостављено уколико би се образложење угрозило кривични поступак. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0010&from=en..

[1068] Тако чл. 188. Закона о кривичном поступку Хрватске предвиђа да јавно тужилаштво или суд лицу, на његов лични захтев, доставља обавештење о томе да ли су лични подаци били предмет прикупљања, похране и обраде за потребе кривичног поступка, али се то обавештење не може

Обавеза обавештавња лица је од *нарочитог значаја у вези са посебним доказним радњама које су тајног и интрузиваног карактера*[1069]. У складу са чланом 60. Закона о мерама процесне принуде у Финској постоји обавеза надлежних органа да о примени тајних мера надзора (пресретање телекомуникација, прикупљање података на други начин осим пресретањем, надзор података о саобраћају, проширено прислушкивање, прикривено прикупљање информација, технички надзор) обевесте осумњиченог након што је јавни тужилац донео одлуку о отварању истраге или о непредузимању даљих радњи, али у сваком случају најкасније у року од годину дана од окончања примене мере надзора. Међутим, на захтев јавног тужиоца суд може додатно одложити обавезу обавештавања лица, и то до две године од отварања истраге, уколико је то оправдано интересима заштите безбедности државе или живота и тела. Уколико су радње примењене према неидентификованом лицу, обавеза постоји од момента утврђивања идентите лица према коме су радње одређене. Немачки Законик о кривичном поступку садржи још детаљније одредбе. Члан 101. став 4. предвиђа обавезу надлежних органа да обавесте лице да је примењена мера надзора према њему, као и других лица који су погођена мером надзора[1070], а дужност обавештавња постоји од тренутка када више не постоји опасност да би обавештење угрозило интересе кривичног гоњења, заштите живота, физичког интегритета, слободе и имовине других лица. О одлагању обавештења побројаних лица саставља се писано образложење. Уколико одлагање траје дуже од 12 месеци (односно 6 месеци у погледу радње тајнод надзора и снимања лица из члана 100ц) од тренутка окончања мере, даље одгалање је могуће само на основу одлуке суда

доставити пре истека рока од године дана након доношења решења о спровођењу истраге (али се лицу доставља одлука у писаном облику, која не садржи образложење).

[1069] F. Boehm, P. De Hert, „Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law“, *European Journal of Law and Technology* 3/2012, 12. Више о томе, P. De Hert, F. Boehm, „The Rights of notification after Surveillance is over: ready for recognition?“, *Digital Enlightment Yearbook* (eds: J.Bus et.al), 2012, 37-38.

[1070] Тако се о радњи аутоматског поређења и преношења података о личности обавештавају лица против којих се након процене резултата примене мере донета одлука о кривичном гоњењу; о радњи пресретања комунуникација, обавештавају се учесници у комуникацији која је надзирана; о радњи тајног акустичког и оптичког надзора, обавештавају се окривљени против кога је радња одређена, лица која су обухваћена надзором, као и лица који су власници или држаоци приватних просторија које су надзиране; о мери акустичког снимања разговора у јавнсти употребом техничких средстава и фотографисања, лица против којих је мера одређена и друга лица значајније погођена мером; о мери провере успостављања телекомуникационе везе, лица који су учесници у тој комуникацији; о мери утврђивања *IMSI* броја, лице идентификовано као власник телефона.

који је надлежан за одређивање радње. Када лице буде обавештено да је према њему примењена мера, има право у року од 2 недеље од обавештења да од суда који је одредио меру захтева да преиспита законитост одређивања мере, као и метода и средстава који су коришћени у примени мере. Уколико је, пак, покренут поступак, суд о овом захтеву окривљеног одлучује у пресуди којом решава кривичну ствар. Изузетно је важна и одредба у којој је изричито наведено да се сви подаци о личности прикупљени применом поменутих мера а који нису више потребни у сврхе кривичног гоњења или за могућу контролу законитости мере од стране суде, уништавају по обавештењу лица и то без одлагања, о чему се саставља одговарајући записник, а уколико се подаци чувају само за потребе судске контроле законитости мере по обавештењу лица, они се не могу користи ни за једну другу сврху без сагласности лица а приступ тим подацима је ограничен.

Законик о кривичном поступку Србије предвиђа *могућност* обавештавања лица само у једном члану, и то у члану 163, којим уређује поступање са прикупљеним материјалом који је настао применом посебне доказне радње тајног надзора комуникација а који се свакако неће користити у кривичном поступку. Наиме, ако јавни тужилац не покрене кривични поступак у року од шест месеци од дана када се упознао са материјалом прикупљеним коришћењем посебних доказних радњи или ако изјави да га неће користити у поступку, односно да против осумњиченог неће захтевати вођење поступка, судија за претходни поступак доноси решење о уништењу прикупљеног материјала, о чему може обавестити лице према коме је спроведена посебна доказна радња ако је у току спровођења радње утврђена његова истоветност и ако то не би угрозило могућност вођења кривичног поступка. Сматрамо да је овакво решење није у складу са принципима и стандардима заштите података о личности, из више разлога. Обавештавање је предвиђено само као *могућност али не и обавеза*, при чему може у потпуности изостати – адекватније би било предвидети обавезу, коју је могуће временски одложити док постоји опасност угрожавања вођења кривичног поступка, али и то одлагање везати за одређени рок. Даље, могућност обавештавања се односи само на примену тајног надзора комуникација, али не и друге посебне доказне радње, што сматрамо да је неоправдано. Осим тога, лице се обавештава само о доношењу

решења о уништењу материјала, што значи да му није могућено ни правним ни фактичким средством да оствари увид у прикупљене податке и тиме такво обавештавање нема никакав смисао у погледу правне заштите података о личности. Чак штавише, члан 165. предвиђа да подаци о предлагању, одлучивању и спровођењу посебних доказних радњи представљају тајне податке у смислу Закона о тајности података[1071].

С обзиром на то да је сама чињеница спровођења посебних доказних радњи тајни податак ком је остваривање приступа могуће само на начин и под условима утврђеним Законом[1072], произлази да лице према коме се посебна доказна радња не може ни на који начин бити обавештено о томе да су се подаци о личности прикупљали применом радње тајног надзора комуникација докле год материјал не буде уништен у складу са чланом 163. Законика о кривичном поступку (односно, протеком две године од добијања статуса тајног податка, подаци о предлагању, одлучивању и спровођењу посебних доказних радњи престају да буду тајни, па би лице могло да тражи те податке, што опет не би имало никаквог смисла јер би до тад материјал настао применом радње тајног надзора већ могао бити уништен у складу са поменутом одредбом Законика).

Имајући у виду праксу ЕСЉП да повреду права приватности (и заштиту података о личности) представља онемогућавање лица да буде информисано да ли се подаци о њему прикупљају као и чување података дуже него што је потребно за остваривање сврхе у коју су се подаци прикупљали, сматрамо да је у Законик у кривичном поступку неопхдоно унети одговарајуће одредбе које се односе на заштиту података о личности у вези са кривичном процедуром, а у складу са основним принципима заштите података о личности.

[1071] „Сл.гласник РС“, бр. 104/2009.

[1072] У складу са тим Законом, тајним податком се сматра податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности. Податак је означен са "ИНТЕРНО" ради спречавања настанка штете за рад, односно *обављање задатака и послова* органа јавне власти који их је одредио. Ако престанак тајности податка није одређен датумом утврђеним у документу у коме је садржан тајни податак или наступањем одређеног догађаја утврђеног у документу у коме је садржан тајни податак, *тајност престаје истеком рока одређеног законом* (према степену тајности), а тај рок за податак са ознаком "ИНТЕРНО" *износи две године од дана одређивања тајности податка*. Тајни подаци чувају се на начин тако да је приступ тим подацима дозвољен само овлашћеним корисницима, с тим да тајним подацима означеним степеном тајности "ИНТЕРНО" приступ имају само функционери, запослена лица, односно лица која обављају послове у органима јавне власти.

Осим непостојањем одговорајућих одредаба у закону који уређује кривичну процедуру, право на приватност и правп на заштиту података о личности могу бити неоправдано ограничени неадекватним прописивањем овлашћења надлежних органа за предузимање радњи и мера у циљу откривања и доказивања дела високотехнолошког криминала, па бисмо на овом месту указали на неколико механизама чији ефекти су подобни да у значајној мери повреде, односно обезбевреде ова права.

3.1. Неоправдано прикупљање података о комуникацијама

Иако се у складу са Директивом *95/46/EC* очекивало од држава чланица ЕУ да обезбеде заштиту права на приватност лица у вези са обрадом података о личности и у вези са електронским комуникацијама (у складу са Директивом 2002/58/EC), у Декларацији о борби против тероризма 2004. године се указало на потребу стварања правила о задржавању података о комуникицијама које се остварују посредством пружалаца јавно доступних услуга електронских комуникација, као потребно и ефикасно средство у сузбијању тешких облика криминала. Наредне године усвојена је Директива 2006/24/EC о задржавању података[1073] која обавезује државе да усвоје прописе којим се пружаоци услуга електронских комуникација обавезују да за одређени временски период задрже и чувају велики број података који се односе на комуникације које корисници тих услуга остварују, те да их учине доступним државним органима у случају потребе вођења кривичне истраге за тешка кривична дела[1074]. Обавезивање на задржавање тих података је правдано значајем тих података за истраживање кривичних дела јер су посматрани аналогно „отиску прстију на лицу места“ у физичком свету[1075]. Бројни аргументи су истицани против ове контроверзне Директиве[1076], а уставни

[1073] *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.

[1074] Директива је заменила одредбу члана 15. Директве о приватности електронских комуникација и предвидела обавено задржавања бројних података о саобраћају електронских комуникација.

[1075] Brown, *op.cit*, 98.

[1076] A. Monti, "The Legal Duty of IAPs to Preserve Traffic Data: A Dream or a Nightmare?", *International Review of Law Computers & Technology* 2/2004, 224-225; S. Toeniskoetter, „Preventing A

судови у у неколико европских држава су законе донете ради имплементације ове Директиве огласили неуставним[1077], а на основу захтева Уставног суда Ирске и Уставног суда Аустрије, Суд правде Европске уније је разматрао валидност Директиве. Суд је заузео став да Директива није у складу са принципом пропорционалности и да не садржи довољно гаранција за заштиту приватности и заштиту података о личности као права гарантованих у Повељи ЕУ о фундаменталним људски правима. Иако би се задржавање података које је одредила Директива могло схватити као одговарајућа мера за остваривање циља, а то је сузбијање тешких кривичних дела, начин на који се Директива услед недостатка јасних и прецизних услова у њеним одредбама меша у основна људска права није адекватан да се оправда то мешање као неопхдно потребно. Најпре, односи се на податке о свим лицима који су корисници услуга електронских комуникација, без икаквог ближег одређивања или прецизирања. Осим тога, Директива не предвиђа ниједан критеријум који би обезбедио да надлежни органи добију приступ подацима и да их користе само у сврхе спречавања и откривања тешких кривичних дела и гоњења учинилаца тих дела, односно на основу ког се може проценити сразмерност и оправданост таквог озбиљног мешања у основна људска права. Осим тога, Директива не предвиђа ни материјалне ни формалне услове под којима надлежни органи могу од пружалаца услуга захтевати остваривање приступа задржаним подацима, чак шта више такав приступ ни на који начин није условљен прехтодном судском одлуком или другог независног тела. Такође је проблематичан и период задржавања података јер се није правила разлика између различитих категорија података нити одређује критеријум за одређивање периода задржавања између минималних шест и максималних 24 месеца чиме се не обезбеђује да мера задрђавања података буде ограничена на неопходно време трајања. На основу свега изнетог, Суд је 8. априла 2014. године огласио Директиву неважећом[1078].

Modern Panopticon: Law Enforcement Acquisition Of Real-Time Cellular Tracking Data“, *The Richmond Journal of Law and Technology* 4/2007, 32-35.

[1077] L. Feiler, "The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", *European Journal of Law and Technology* 3/2010, 27-28; T.J. McIntyre., “Data retention in Ireland: Privacy, policy and proportionality”, *Computer law & security report* 24/2008, 327.

[1078] C-293/12 и C-594/12, http://curia.europa.eu/juris/documents.jsf?num=C-293/12.

Слични, ако не и исти, аргументи би могли бити употребљени и за критику решења садржаних у Закону о електронским комуникацијама, нарочито у погледу заштите података о личности. Задржавање података о саобраћају може представљати инструзивнију меру од пресретања садржаја комуникације или прикупљању података о саобраћају у реалном времену (у смислу Конвенције о високотехнолошком криминалу), јер је неспорно да подаци о саобраћају представљају податке о личности (јер могу идентификовати лице) у погледу којих је, такође, неопходно испоштовати прописане принципе заштите[1079]. Уколико бисмо применили стандарде утврђене у пракси ЕСЉП, могли бисмо закључити да примена ове мере није ни потребна нити одговарајуће уређена, а није ни сразмерна и оправдано у демократском друштву. Оваква мера је изузетно интрузивна у погледу права гарантованог чланом 8. ЕКЉП, с обзиром на то да држава право на поштовање приватног живота и комуникација може ограничити само у мери која је потребна у демократском друштву, и у складу са принципом пропорционалности. Закон чак не садржи ограничење у погледу тешких кривичних дела, па је принцип пропорционалности готово поништен. Задржавање података је далеко ширег обухвата у односу на радњу прикупљања података о саобраћају у реалном времену или пресретња комуникација (надлежни орган прикупља или снима податке применом техничких средстава или обавезује пружаоце услуга електронских комуникација да у складу са својим техничким могућностима прикупе или сниме или да помогну и сарађују са надлежним органом у прикупљању података који се односе на *конкретну одређену комуникацију* која се остварује посредством рачунарског система) док се задржавање односе на неодређене комуникације. Ако је ЕСЉП установио да просто чување података о личности представља угрожавање слободе грађана[1080], тим пре захтев за задржавањем података од стране пружалаца услуга представља још већу опасност по права гарантована у члану 8. Конвенције. Иако прикупљање података о личности може бити оправдано потребама кривичном поступка, имајући у виду опште принципе заштите података о личности (те праксу ЕСЉП и Одлуку суда ЕУ), те да повреду права приватности може представљати просто

[1079] J. Moiny, ''Are Internet protocol addresses personal data? The fight against online copyright infringement'', *Computer Law and security Review* 27/2011, 349.
[1080] На пример, у пресудама у предметима *Klaas, Ludi,Rotaru, Ammann.*

складиштење података о саобраћају комуникације (који представљају податке о личности), сматрамо да би било неопходно преиспитати уставност појединих одредаба Закона о електронским комуникацијама (које се односе на обавезу задржавања података).

3.2. Прекогранична размена података о личности

Потребно је на указати на још једно, изузетно важно питање у вези са заштитом података о личности, а то је уређивање могућности прекограничне размене података о личности у вези са спонтаном разменом података између надлежних органа и других видова достављања података у оквиру пружања међународне правне помоћи у кривичним стварима, која је неопходна за супртостављање високотехнолошком криминалу.

Иако је изношење података о личности дозвољено и на сличан начин уређено у Конвенцији СЕ и актима ЕУ, занимљиво је поменути да је пре усвајања ових прописа постојала дебата о кривичноправној орговорности за прекогранични трансфер података у оквиру рачунарских мрежа[1081]. Док се размена података о личности између држава чланица ЕУ остварује у складу са поменутим прописима, изношење података о личности из земаља чланица ЕУ у треће земље регулисано је чланом 25. Директиве 95/46 о заштити података о личности у вези са обрадом података о личности и слободним протоком тих података[1082], а може се реализовати само уколико је Одлуком Комисије ЕУ а на основу прибављеног мишљења тела надлежног за заштиту података о личности (члан 29. Директиве) утврђено да су у прописима односне државе испоштовани принципи заштите приватности, односно да се гарантује адекватан ниво заштите података о личности.

[1081] U. Sieber, "Criminal liability for the transfer of the data in international computer network", *European Journal of Crime, Criminal Law and Criminal Justice* 2/1997, 135.

[1082] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Изношење података о личности се остварује на основу билатералних уговора који гарантују висок степен заштите података[1083], а подаци се могу размењивати између надлежних органа уговорних страна само за потребе спречавања и сузбијања најтежих облика кривичних дела[1084]. Тако је Одлуком Комисије 2000. године[1085] утврђено да у САД гарантован потребан степен заштите података о личности (*Safe Harbor privacy principles*[1086]). Међутим, на овом месту је потребно истаћи да је Суд Европске Уније у пресуди од 6. октобра 2015. године[1087] поништио Одлуку Комисије из 2000. године (тзв. *Safe Harbour Decision*). Максимилијан Шремс, држављанин Аустрије и корисник Фејсбука, поднео је представку ирском поверенику за заштиту података о личности[1088], за из разлога што сматра да закони и пракса у САД (а нарочито имајући у виду активности Едварда Сноудена током 2013. године) не постоји одговарајући степен заштите података о личности пренетих у САД, посебно у погледу заштите од надзора од стране обавештајних служби (од масовног и неселективног приступа подацима о личности). Повереник је одбио представку Шремса као неосновану, са образложењем да Одлука Комисије потврђује постојање адекватног нивоа

[1083] Две врсте таквих билетарелних уговора су закључени са одређеним државама: ради изношења података о имену путника (*Passenger Name Record (PNR) Agreement*) и података о финансијским трансаксијама за које постоји сумња да се користе за финансирање тероризма (*Terrorist Finance Tracking Programme*). Након терористичких напада у САД започети између земаља ЕУ и САД постигнут је споразум о преносу података о путницима (тзв. *Passenger Name Record*:*PNR*) које авио компаније прикупљају у једну сврху америчким царинским органима за другу сврху (*data-mining* за безбедносне сврхе). Иако је Комисија 2004. у складу са Директивом донела одлуку да амерички царински органи исшуњавају услов адекватности, Европски суд правде је 2006. године заузео став да није могуће у овом случају позвати се на изузетак „адекватности" од захтева које поставља Директива о приватности, те да је пренос података о путницима које прикупљају авио компаније недозвољен.

[1084] G. Gunasekara „The Final Privacy Frontier? Regulating Trans-Border Data Flows", *International Journal of Law and Information Technology* 2/2007, 149. Осим тога, од 2011. се воде преговори између ЕУ и САД о стварању „кровног" споразума који би омогућио размену свих података о личности за потребе спречавања и сузбијања свих кривичних дела. http://ec.europa.eu/justice/data-protection/document/international-transfers/pnr-tftp/pnr-and-tftp_en.htm.

[1085] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215).

[1086] http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[1087] Пресуда у предмету *Maximillian Schrems v. Data Protection Commissioner* (Case C-362/14), http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=250967.

[1088] Свако лице с боравиштем на државном подручју Уније која жели користити Фејсбуком дужно је приликом регистрирања склопити уговор с Фејсбук Иркса, друштвом кћери Фејсбук који има седиште у САД. Подаци о личности корисника који бораве на државном подручју Уније преносе се у целости или делимично на севере који припадају Фејсуку а који су смештени на државном подручју САД-а, где су предмет обраде.

заштите података о личности у САД[1089]. Последица одлуке Суда у конкретном случају биће дужност ирског повереника да пажљиво размотри наводе у представки Шремса и да одлучи да ли је потребно суспендовати трансфер података корисника Фејсбука са територије Европске уније у САД по основу налаза да се у тој земљи не пружа потребан степен заштите података о личности. Суд је најпре заузео став по ком постојање Одлуке Комисије не може да смањи нити онемогући утицај националних органа за заштиту података о личности, с обзиром да им је Повељеом о људским правима ЕУ у надлежност поверена неприкосновена заштита података о личности држављана. Отуда су национални органи овлашћени да, без обзира на постојање Одлуке Комисије, надзиру трансфер података о личности у треће земље. У погледу валидности Одлуке, Суд је утврдио да Комисија приликом њеног доношења није на одговарајући начин утврдила адекватност система заштите података о личности у САД, а нарочито у погледу непостојања правне заштите лица чији подаци се преносе у ову земљу.

Потреба за вишим степеном заштите података о личности у вези са прекограничном сарадњом надлежних органа у сузбијању кривичних дела препозната је у предлозима аката у оквиру реформе система заштите података. Тако се у предлогу Директиве (члан 60) наводи да ће се усвојени међународни уговори у области правосудне и полицијске сарадње преиспитати ради усклађивања за новим системом заштитите података о личности (у року од 5 година од ступања на снагу Директиве), па постоје мишљења да би усвајање прописа овако протективне оријентације онемогућило ефективну међународну сарадњу надлежних државних органа[1090]. Овакво решење би имало утицаја и на КВК, с обзиром на то да иста предвиђа да државе чланице сарађују у најширем могућем обиму и ограничава основе за одбијање указивања помоћи, у смислу да се поступање по молби друге државе може одбити позивањем на заштиту података о личности само у изузетним случајевима (у складу са чланом 23. КВК).

[1089] Повереник је сматрао да нису постојали докази да је служба безбедности САД приступила подацима подносиоца представке и додао је да приговори нису могли бити ваљано истакнути јер је о сваком питању у вези с одговарајућом заштитом података у САД-у требало одлучити у складу с Одлуком 2000/520 те да је Комисија у тој одлуци утврдила да САД осигурава одговарајући степен заштите.

[1090] Interparliamentary Committee Meeting, "*The reform of the EU Data Protection framework – Building trust in a digital and global world*, 2012, http://www.europarl.europa.eu/document/activities/cont/201210/20121003ATT52831/20121003ATT52831EN.pdf.

Како је међународна сарадње кључни елемент у ефикасном супротстављању високотехнолошком криминалу, а размена података о личности битан вид сарадње, у прописивању система заштите података о личности треба на одговорајући усагласити и постићи равнотежу између општих и појединачних интереса.

Полазећи од преузетих обавеза ратификовањем Конвенције о заштити лица у односу на аутоматску обраду личних података Савета Европе[1091], Закон о заштити података о личности у члану 53. изричито дозвољава *изношење података* о личности из Републике Србије у државу чланицу Конвенције, а у друге државе, односно међународну организацију, под условом да је у тој држави/међународној организацији прописом, односно уговором о преносу података, *обезбеђен степен заштите података у складу са Конвенцијом*. Испуњеност ових услова утврђује Повереник за заштиту података, те уколико су ти услови испуњени, издаје дозволу за изношење података. Овај „протективни" елемент произлази из тога што се заштита података о личности третира као основно људско право[1092]. Из тог разлога законодавац, судови и орган надлежни за заштиту податак треба да воде рачуна да подаци о личности буду заштићени и након што буду пренети у другу државу, односно међународну организацију[1093]. Отуда приликом доношења

[1091] У вези са овим потребно је нагласити да Конвенција предвиђа да држава не може само *само ради заштите приватности*, да забрани или да услови (издавањем некакве специјалне дозволе) прекогранични проток личних података на територију неке друге стране уговорнице, али да то може да уради ако у њеном законодавству постоје посебни прописи за неке категорије личних података или аутоматизованих збирки са личним подацима, због карактера тих података или збирки, осим у случају да је у прописима друге стране уговорнице истоветна заштита већ предвиђена.

[1092] C. Kuner, „Data Protection Law and International Jurisdiction on the Internet (Part 1)", *International Journal of Law and Information Technology* 2/2010, 180.

[1093] Три случаја које описују различите ситуације у којима се подаци о личности обрађивани изван ЕУ са различитим последицама у смислу примене Директиве, а поводом којих је одлуку донео рган надлежан за заштиту података о личности у Италији (*Garante per la protezione dei dati personali*). У првом случају су се на вебсајту лоцираном у САД на непрофесионалан начин критиковао рад појединих италијанксих научника (у вези са експериментима на животињама), поводом чега је орган изнео мишљење да се италијански прописи о заштити података о личности не могу примењивати с обзиром на то да су радње предузете на Интернет страници која се налази изван граница ЕУ. У другом случају размтрана је легалност аутоматског преноса фотографија италијанских улица на сервер лоциран у САД за унос у апликацију *Google Street View* и утврђено је да се на овакву обраду података о личности од *стране Google Inc.* примењују италијански прописи с обзиром на то да се опрема налазила на територији Италије (у складу са чл.4.Директиве). Трећи случај односио се на оцену дозвољености софтвера *Heinz 360 Feedback* који је уведен као нови модел за побољшање пословних способности запослених у једној фирми (са чим су се запослени сагласили потписивањем уговора о раду). Тај софтвер функционише тако што се оцене рада запослених преносе у рачунарски систем који аутоматски анализира те податке

одлуке да ли дозволити изношење података о личности у иностранство, надлежни орган своју дужност треба да оствари вршећи ефективну контролу у погледу степена заштите података о личности која може да буде обезбеђена у иностранству[1094].

Што се тиче размене података о личности за потребе кривичног поступка, релевантна је Закон о међународној правној помоћи о кривичним стварима[1095]. Овај Закон у члану 83. међу осталим облицима међународне правне помоћи просто наводи и: „достављање података без замолнице". За пружање овог вида међународне правне помоћи (осим испуњености општих претпоставки за пружање помоћи из члана 7), потребно је и да су испуњени услови предвиђени Закоником о кривичном поступку. Законик о кривичном поступку, међутим, не садржи ниједну одредбу о овоме. На основу наведеног, сматрамо да *заштита података од личности у погледу изношења ових података ван Републике Србије није на адкеватан начин регулисана*, те да је потребно у Законику о кривичном поступку предвидети одредбе којима би се ова питања уредила. Уношење одредаба би било потребно из најмање два разлога: 1) ради заштите података о личности у вези са члановима 25-35. Конвенције СЕ о високотехнолошком криминалу (које се односе на омогућавање међународне сарадње) 2) ради усаглашавања са Конвенцијом СЕ о заштити лица у односу на аутоматску обраду личних података, 3) ради усаглашавања правног система са Оквирном одлуком ЕУ (који уређује прекограничну размену података за потребе кривичним поступака)[1096]. У супротном, обраду података о личности за потребе кривичног поступка и размену тих података између надлежних органа држава можемо означити и као *директно поништавање принципа одређености сврхе*

а који се налази у САД а који је усклађен са Safe Harbor правилима и стога је легално обрађује податке о личности. У овом случају је прекогранични трансфер података о личности законит. A. Mantelero, „Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *European Journal for Law and Technology* 2/2012, 4.

[1094] D. Svantesson, „Privacy, Internet and Transborder Data Flows", *Masaryk University Law and Technology journal* 1/2010, 2.

[1095] „Сл. гласник РС", бр. 20/2009.

[1096] Ипак, треба имати у виду да већина држава чланица примењује опште прописе о заштити података о личности (а у вези са законом о кривичном поступку) и на обраду података за потребе кривичног поступка и у националном и прекограничном контексту. Иако у овим државама нису усвојени посебни прописи који би ова питања непосредно регулисали (што је учињено у свега 7 држава), сматра се да су и на тај начин испунили обавезу из Оквирне одлуке. Наведено према Извештају о имплементацији Оквирне одлуке: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_12_en.pdf , 4.

прикупљања[1097]. Међутим, сматрамо да је у вези са регулисањем ових питања потребно *задржати резерву* и бити нарочито обазрив. Требало би имати у виду да је осетљиво питање прекограничне размене података предмет актуелне научне и стручне расправе[1098], да је посебна пажња размени података посвећена како у нацрту Измена Конвенције СЕ, тако и у предлогу Директиве ЕУ, али да је постизање концензуса и даље под знаком питања.

Не чекајући даљи развој догађаја, потребно је осим одредабама у ЗКП, размену података о личности детљаније регулисати и у ЗМПП. Одредбе би требало да буду усклађене са Законом о заштити података (да се у процедуру одобравања пружања овог вида помоћи укључи надлежни орган за заштиту података о личности[1099]), те да ограничи могућност пружања овог вида помоћи за одређену сврху (слично начелу специјалитета за изручење из члана 13. и 14).

Осим наведених проблема *у вези са прекограничним приступом и претрагом рачунарског система и мреже који се налази у иностранству*, важно питање је који прописи се примењују у погледу заштите појединаца чији се подаци прикупљају: да ли државе у којој се рачунар ком се са даљине приступа или прописи државе чији надлежни органи остварују прекогранични приступ? Прописи држава се могу значајно разликовати, примера ради, у погледу слободе изражавања или услова који треба да буду испуњени да би полиција добила одобрење за остваривање приступа похрањеним рачунарским подацима. Такође, може се десити да надлежни органи прикупљају електронске доказе на начин који није законит у складу са прописима државе у којој је претраживани рачунар лоциран – рецимо у једној држави одобрење за предузимање радње даје јавни тужилац док је у другој неопходно судска наредба или чак држава забрањује надзор електронских комуникација па не дозволи држави чији органи остварују приступ да користи прикупљене рачунарске податке. Појединци уочибачајено и легитимно очекују да надлежни органи према њима предузимају радње у складу

[1097] Подршку за ово становиште проналазимо и код појединих аутора, који су у разматрању ове регулативе пажњу посветили суштини заштите података о личности. Тако, Cannatacia, Mifsud, *op.cit*, 104.

[1098] E. De Busser, „EU data protection in transatlantic cooperation in criminal matters: Will the EU be serving its citizens an American meal? “, *Utrecht Law Review* 1/2010, 92; Упор. E. Dretzka, S. Mildner, „Anything but SWIFT: Why Data Sharing is Still a Problem for the EU“, *American Institute for Contemprorary German Studies* 35/2010, 5.

[1099] C. Kuner, „Data Protection Law and International Jurisdiction on the Internet (Part 2)“, *International Journal of Law and Information Technology* 3/2010, 231.

са прописима државе у којој живе. Како појединци очекују примену предвидиљивог режима заштите, примена услова и гаранција предвиђених прописима друге државе веома је проблематично питање. С тим у вези се може поставити питање, како обезбедити да државни органи који врше прекогранични приступ поштују прописе и постигнути и за појединце очекивани ниво заштите података о личности државе у којој се налази претраживани рачунар? Полазећи од тога да радње надлежних органа држава потписница ЕКЉП могу бити доведене у питање пред ЕСЉП у смислу проширења екстратериторијалне надлежности државе у складу са чланом 1 ЕКЉП[1100], овај механизам се показује као крајње решење у заштити права појединаца. Ипак, хармонизација прописа у циљу приближавања гарантованог нивоа заштите података о личности и других људских права би представљала идеално решење.

Осим тога, *у ситуацији када надлежни државни органи једне државе траже од пружалаца услуга електронских комуникација* (нарочито услуга *cloud computing*-а) да предају рачунарске податке који су похрањени у другој држави, прописи о заштити података о личности те друге државе могу бити доведени у питање. Недостатак поузданости захтева упућених директно пружаоцу услуге од стране надлежних органа држава, доводи до настанка ризика да подаци о личности који се обрађују буду предати органима државе у којој не постоји одговарајући правни основ и тиме долази до повреде прописа држава чланица (и прописа ЕУ) који обезбеђују заштиту појединца у погледу података који се о њему обрађују[1101]. Тако се предлогу Опште уредбе о заштити појединаца у вези са обрадом података о личности и слободним протоком тих података наводи да се трансфер података надлежним органима других држава које остварују прекогранични приступ рачунарима на територији држава чланица ЕУ може дозволити само уколико се утврди да у тој држави постоје исте или сличне гаранције утврђене овом Уредбом[1102] (у супротном ће се сматрати да

[1100] http://www.echr.coe.int/NR/rdonlyres/DD99396C-3853-448C-AFB4-67240B1B48AE/0/FICHES_Juridiction_Extraterritoriale_EN.pdf.

[1101] Article 29 Data Protection Working Party, *Opinion on Cloud Computing*, 2012, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20120701_wp_196_cloud_computing_en.pdf.

[1102] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=en.

екстратериторијална примена прописа тих држава представља повреду правила међународног јавног права).

3. Прикупљање података напредним техникама надзора

Прикупљање података похрањених у рачунарским системима и базама података је легитиман начин докле год је у складу са националним прописима (којима је обезбешена имплементација процесних одредаба КВК), међутим, *може се поставити питање легитимности прикупљања података из јавно доступних (open source) извора*, првенствено са Интернета. Наиме, постоје неколико метода за прикупљање података коришћењем база података или јавно доступних извора који нису у складу са процесним одредбама Конвенције. Неограничено прикупљање података о личности без постојања одређеног степена сумње да је лице извршило кривично дело, складиштење тих података и сравњивање података из различитих извора ради профилирања личности је у супртоности са поменутим принципима заштите података (одређености свхре, сразмерности итд). Нарочито је проблематично коришћење дигитализованог индуктивног профилирања за предиктивни надзор активности лица – ради се о методу заснованом на форензичким доказима, процесно-орјентисаном ка уочавању каракетиричног понашања учиниоца и предвиђању будућих радњи[1103]. Да би се ове технике примениле у складу са принципима заштите података о личности, процедуре за њихову примену морају бити јасно и транспарентно прописане законом и одобрене од стране независног органа.

На овом месту је потребно указати на пресуду немачког Савезног уставног суда којом се установљено право на поверљивост и целовитост информационих система (*der Vertraulichkeit und Integritaet Informationstechnischer Systeme*), које је изведено из основног права на правну личност[1104]. У оцени уставности *online* претрага (*die Online Durchsuschung*) електронских информационих система, Суд је 2008. године у пресуди огласио неуставном одредбу Закона о заштити уставног

[1103] R. Van Brakel, P. De Hert, „Policing, surveillance and a law in pre-crime society: understanding the consequences of technology based strategies“, *Cahiers Politiestudies. Jaargang* 20/ 2011, 173-174.
[1104] Пресуда (BVerfG, 1 BvR 370/07 vom 27.2.2008) је у целости доступна на следећем линку: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html .

поретка државе Северне рајнске Вестфалије по којој је било омогућен тајни (прикривени) надзор Интернета и тајни (прикривени) приступ информационим системима[1105], ради прегледа садржаја похрањењеног у рачунарском систему повезаном на Интернет. Из значаја употребе система информацине технологије за развој личности и потребе да се та употреба заштити од угрожавања, Уставни суд је извео право појединца на поверљивост и целовитост информационих система. Ово право подразумева оправдано очекивање појединца да слободно и без узнемиравања од стране других лица а нарочито државних органа користи све предности тих система. Оспорена овлашћења државних органа су неуставна јер нису у складу са принципом јасног дефинисања ограничења гарантованх права, принципом пропорциналности и тиме не садрже довољно потребне предострожности у циљу заштите приватног живота појединца[1106]. С обзиром на то да прикривена инфилтрација у рачунарски систем на овај начин може омогућити државним органима да несметано „шпијунирају" грађане у свакодневним активностима (које се не односе све на сумњива понашања) оваква одредба је потпуно недопустива у једном демократском друштву[1107].

Иако је ограничење одређених људских права правдано потребама кривичног поступка у потпуности легитимно, имајући у виду да мере и радње које се предузимају ради откривања и доказивања дела високотехнолошког криминала у себи носе ризик од незапамћеног задирање у сферу приватности[1108], сматрамо да је гарантовање заштите информационе приватности веома важно питање. Ако се колективна безбедност (у оквиру које је је важан елемент сузбијање кривичних дела) не може постићи на други начин осим неоправданим надзором и праћењем свих активности корисника електронских услуга и прикупљањем и обрадом података о њима, о слободи појединаца се више не може говорити, јер „потпуна транспарентност (радњи државних органа) парализује планирање и акцију, а потпуна тајновитост угрожава и слободу и безбедност"[1109].

[1105] B. Schroeder, C. Schroeder, *Die Online Durchsuschung: Rectliche Grundlagen*, Technik, Medienecho, Hannover 2008, 101.
[1106] F. Roggan, *Online-Durchsushungen: Rectliche und tatsachliche Konsequenzen des BVerfG-Urteils vom 27. Febraur 2008*, Berliner Wissenschafts-Verlag, Berlin 2008, 79.
[1107] Roggan*, op.cit*, 106.
[1108] О могућем утицају савремених техника и метода надзора, види D. Wright, M. Friedewald „Sorting out Smart Surveillance", *Computer Law& Security report* 26/2010, 348.
[1109] Posner R., „Privacy, Surveillance, and Law", *The University of Chicago Law Review* 1/2008, 246.

С обзиром на способност савременог рачунарства за прикупљање, обраду и складиштење података великог броја података и њихово укрштање и анализу, као нужност се појавило питање контроле тог процеса чије димензије и обухват су пре развоја рачунара било незамисливи. Рачунарске технологије константним развојем повећавају потенцијал за надзор појединаца, до те мере да дистопијска предвиђања нису више у домену књижевности и научне фантастике[1110]. Томе доприноси не само количина података који се прикупљају него и чињеница да појединци не знају који то државни органи, привредни и други субјекти прикупљају податке о њима и због чега, због чега сматрамо да се такво друштво не може сматрати друштвом које се заснива на слободи и владавини права.

Свеобухватан и неселективни надзор комуникација и понашања појединаца није оправдан, већ је неопходно предвидети одређена процедурална ограничења и гаранције: За откривање и доказивање дела високотехнолошког криминала је неопходно применити методе и технике информационих технологија, међутим, некритичко регулисање и примена напредних метода и техника надзора и праћења активности корисника, у чијим свакодневним активностима је све присутније ослањање на информационе технологије, створило би реалну опасност од проширивања и продубљивања обухвата сфера живота које се надгледају, далеко од оправданости надгледања у оквиру концепта проактивности и стварања својеврсног потпуног и паноптичког надзора података о личности, што се не може оправдати чак ни потребама супротстављања најтежим облицима кривичних дела, па ни високотехнолошком криминалу. Стога радње које се заснивају на употреби тих техника и метода треба да буду прописане и примењене у складу са принципима одређености, потребности, сразмерности, и уз контролу судских органа, како право на поштовање приватног живота и слобода општења не би били угрожени.

У прописима је потребно постићи равнотежу између потреба вођења кривичног поступка и поштовања људских права, односно овлашћења истражних органа у циљу прикупљања података и обима заштите права на приватност појединаца: Заштиту права на правну личност, те права на слободан развој личности кроз право на приватност и заштиту података о личности у *online*

[1110] О поређењу са Орвеловом „1984“ и Кафкиним „Процесом“, види Solove D., „Privacy and Power: Computer Databases and Metaphors for Information Privacy“, *Stanford Law Review* 6/2001, 1420.

окружењу, нужно је обезбедити правним прописима који садрже строга и прецизна правила која одређују обухват овлашћења надлежних органа да прикупљају доказе за потребе кривичног поступка за дела високотехнолошког криминала јер се предузимањем одређених радњи у великој мери може задирати у приватну сферу појединаца и прикупљати велики број података о њима. Наведене права је могуће ограничити само ради заштите општег интереса, ово ограничење треба да буде сразмерно и одређено законом, у мери и у случајевима је ова права могуће и оправдано ограничити.

ЗАКЉУЧАК

Одредбе кривичног процесног права које се односе на откривање и доказивање дела високотехнолошког криминала потребно је прилагодити специфичностима злоупотреба информационе технологије у кибер простору, с обзиром на то да сматрамо да постојећи прописи не регулишу радње надлежних органа на начин одговарајући за откривање и обезбеђење електронских доказа. Неадекватност постојећих решења произлази, не толико из природе недозвољених активности, већ из својстава информационих технологија које су омогућиле њихово извршење на начин у квантитативно и квалитативно другачији у односу на традиционална кривична дела, а што није узето у обзир приликом уређивања доказних радњи. С тим у вези, потребно је прецизирати овлашћења надлежних органа неопходна за истрагу не само дела високотехнолошког криминала, него и других кривичних дела за истрагу којих је неопходно прикупити електронске доказе.

Електронске доказе могли бисмо одредити као рачунарске податке који су похрањени или се преносе у рачунарском систему, рачунарској мрежи или другом уређају и опреми за електронску обраду, пренос и/или складиштење података, а који, након што су прикупљени, обрађени и анализирани у складу са правилима дигиталне форензике а у законском оквиру који уређује правила кривичне процедуре, могу имати значај доказа у кривичном поступку. Постоји велики број потенцијалних извора електронских доказа, па је са сваким од њих је потребно поступати узимајући у обзир специфичности начина на који се подаци у њима похрањују/преносе, као и природу тих података. Треба имати у виду да су рачунарски подаци ускладиштени на медијумима који се разликују по величини и начину употребе, начину складиштења података (на физичком и логичком нивоу) и меморијским капацитетима, што има утицаја на начин прикупљања података и анализу прикупљених податка.

У настојању да се пронађу инспиративна решења, анализирана су законодавства појединих држава, а анализа је потврдила изузетан допринос Конвенције о високотехнолошком криминалу, као свеобухватног оквира за прилагођавање кривичног процесног законодавства посебностима доказивања дела високотехнолошког криминала. 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.

Осим преиспитивања потребе унапређења постојећих и предлагања увођења нових решења у кривичном процесном праву која би била одговарајућа и истовремено и технолошки неутрална, нарочиту пажњу је потребно посветити превазилажењу транснационалне природе високотехнолошког криминала. Наиме, високотехнолошки криминал је феномен са израженом транснационалном, глобалном димензијом која органима гоњења намеће потребу за прикупљањем доказа и хватањем учиниоца који се налазе на територији других држава, уколико се извршилац радње кривичног дела налази на територији једне државе, а последице радње и оштећена лица на територији једне или више других држава, па надлежни органи једне државе не могу без сарадње са надлежним органима друге државе да се ефикасно супротставе овом облику криминала. Међутим, механизми пружања међународне правне помоћи су спори а у појединим случајевима и непостојећи, док ефикасна борба против транснационалних облика злоупотреба информационих технологија, а нарочито прикупљање електронских доказа, захтева хитно и брзо реаговање. Из тог разлога је постојеће опште оквире сарадње надлежних органа потребно прилагодити специфичним изазовима које пред њих поставља посебна природа дела високотехнолошког криминала, а мишљења смо да би најделотворнији начин за постизање ефективне и ефикасне сарадње надлежних државних органа у супротстављању високотехнолошком криминалу *кроз потпуно искоришћавање могућности које предвиђа Конвенција Савета Европе о високотехнолошком криминалу.*

Приликом нормирања овлашћења потребних за откривање и доказивање дела високотехнолошког криминала *потребно водити рачуна о заштити права лица према којима су радње предузете,* с обзиром на то да се применом технички савремених метода и средстава откривања и доказивања кривичних дела може се у великој мери задирати у приватну сферу појединца. Наиме, услед конвергенције технологија дошло је до промена у процесу прикупљања и обраде података, и то

не само по обиму, него и по квалитету, а осим тога, технике и методе за прикупљање и обраду података су учиниле овај процес далеко интрузивнијим.

Неспорно је да би одредбама кривичног процесног права требало надлежним органима дати овлашћења потребна за адекватно реаговање на изазове високотехнолошког криминала у смислу употребе техника и метода информационе технологије јер би без тога дела високотехнолошког криминала било немогуће открити и доказати. Ипак, с обзиром на то да потребне мере и радње могу бити високог степена интрузивности, приликом прописивања овлашћења надлежних органа потребно је водити рачуна о одређеним *ограничењима* чији је *смисао спречавање самовоље у поступању од стране тих органа и неоправданог и прекомерног задирања у гарантована права приватности* (уз потребу критичког преиспитивања услова неопходности таквих овлашћења у демократском друштву). Равнотежа између интереса супротстављања високотехнолошком криминалу и заштите права на приватност је непостојана. Промене у технолошком развоју олакшавају извршење тешких кривичних дела, што заузврат захтева и спремнији одговор државе, да би се у том смислу осигурала заштита општих интереса, држава добија од грађана легитимитет за ограничавање права и слобода, а са све жустријим одговором државе, повећава се и могућност угрожавања приватности грађана. Са престанком претњи, због којих грађани дају подршку држави за спровођење мера већег степена репресивности или са разумевањем тих претњи, држава губи легитимитет за превагу општег интереса над правима грађана и равнотежу је потребно поново успоставити. Дакле, услед интензивног инсистирања на стварању механизама за супротстављање тешким облицима криминала (међу њима је и високотехнолошки криминал) применом интрузивних радњи, равнотежа између општег интереса и заштите гарантованих људских права у савременом информационом друштву може да буде поремећена. Иако постоје аргументи да се примена поменутих метода надзора и контроле података у дивергентном технолошком окружењу оправда као заиста потребна, сматрамо да је штета од олаког и неопрезног омогућавања њихове примене која би наступила по права приватности много већа од њихове апстрактне корисности. Да би се та штетност свела на најмању могућу меру, процес прикупљања и обраде података о личности треба да буде усклађен са

стриктним правилима о заштити истих. Легитимност обраде података о личности за потребе кривичног поступка процењује се у вези са принципом пропорционалности: у којој мери ризик по општу безбедност може и у којој мери да оправда задирање у права приватности. Може се поставити питање, да ли постоји доказ који потврђује тезу да примена тако интрузивних мера од стране надлежних државни органа заиста доприноси откривању и доказивању тешких кривичних дела што је употребљено као основни циљ и оправдање увођење могућности за примену мера надзора, као и мера ограничења у виду принципа сразмерности. Не постоји. Иако се у потпуности слажемо са изреком Бенџамина Френклина по којој „друштво које је спремно да се одрекне мало слободе зарад мало безбедности не заслужују ни слободе ни безбедност“ [1111], нереално је очекивати да ће држава одустати од могућности примене тих мера и наставити да их њихово постојање правда потребом за очувањем безбедности и спречавања и сузбијања кривичних дела. На овом месту се ни не залажемо за укидање ових радњи и мера, него инсистирамо да се принципи сразмерности, потребности, предвиђености и легалности узму у обзир приликом њиховог прописивања као и одређивања у сваком конкретном случају. Неопходна судска контрола сваке мере а да би таква контрола била ефективна, од изузетне важности је судијско разумевање техничких могућности који се остварују у оквиру сваке од мера и импликација које по податке о личности и приватност лица те мере имају. Иако се принцип пропорционалности везује за посебне доказне радње, сматрамо да је дејство овог принципа потребно проширити на све радње које имају за циљ прикупљање електронских доказа, чак и на оне које нису посебне доказне радње у смислу схватања у нашој литератури и пракси (па и законодавтсву). Наше мишљење је да третман посебности треба да добију све радње које имају потенцијал да угрожавају права приватности, односно то су све радње у оквиру којих се врше дигиталне истраге. Полазећи од суштине права приватности, да би могућност његовог ограничења била оправдана, сматрамо да је одредбама кривичног процесног права потребно што прецизније уредити сва релевантна питања како би радња одређивале само као неопходно потребне.

* * *

[1111] Наведено према, Levi, Wall , *op.cit*, 206.

Из наведених разлога дајемо следеће предлоге ***de lege ferenda,*** те сматрамо да је у ***Законик о кривичном поступку,*** потребно је унети, односно изменити одређен број одредаба.

1. Сматрамо да је у *члану 2*. потребно брисати тачку 29 („Електронски запис“) и уместо ње додати тачку „Електронски доказ“: рачунарски податак прибављен применом чланова 286. став 3. и 4., члана 286 а, 286 б, 148 а, 160а, 160 б, 161. и 167а, а који може имати значај доказа. Осим тога, потребно је додати тачке „Рачунарски податак“, „Рачунарска мрежа“, „Рачунар“, „Рачунарски систем“ како је то одређено Кривичним закоником у члану 112. ставови 17,18, 33. и 34, с обзиром на то да су исти усклађени са Конвенцијом о високотехнолошком криминалу, да се не непотребно стварале језичке недоумице). Сходно томе, у одговарајућим члановима заменити речи „уређаји за аутоматску обраду података“ речју „рачунар (јер обухвата и уређаје за пренос рачунарских података).

2. У погледу ***хитног чувања ускладиштених рачунарских података,*** потребно је у вези са радњама и мерама које полиција предузима следеће *у члану 286*. став 3. заменити речи: „По налогу судије за претходни поступак” речима: „*По наредби судије за претходни поступак*”.

Како се у складу са постојећом одредбом овлашћење дато полицији у циљу остварења дужности из члана 286.став 1, односи се само на прибављање појединих података о саобраћају у погледу *телефонске комуникације*, не и осталих видова електронске комуникације, потребно је реч: „телефонске“ заменити речју: „електронске“. Осим тога, потребно је додати став који би предвиђао да наредба садржи податке о кривичном делу, опис околности из којих произлази да су испуњени услови за одређивање радње, временски период за који се траже подаци и одређивање електронске комуникације, односно базне станице која је предмет радње. Мишљења смо да би ради омогућавања експедитивног деловања у нарочито хитним околностима било оправдано предвидети да јавни тужилац може издати налог, а евентуално за такво поступање обезбедити контролу суда у виду потврде законитости тако издатог налога, тим пре што се не ради о прикупљању података у реалном времену (прикупљање података у

реалном времену покривено је посебном доказном радњом), него података о оствареној комуникацији (што би се могло остварити издавањем одговарајуће наредбе). С тим у вези, корисно је предвидети да у случају опасности од одлагања јавни тужилац може да изда налог, ако верује да на време неће моћи прибавити наредбу судије за претходни поступак, али је дужан да о томе одмах, а најкасније у року од 24 сата, поднесе извештај судији за претходни поступак у ком образлаже разлоге за такво поступање. Судија за претходни поступак цени да ли је издавање налога од стране јавног тужиоца било оправдано и доноси решење о потврђивању налога или о одбијању захтева тужиоца за потврду налога, на које јавни тужилац нема право жалбе. Уколико су подаци прибављени без наредбе судије за претходни поступак, односно ако јавни тужилац није у року доставио судији за претходни поступак извештај или ако је одбијен захтев јавног тужиоца за потврду налога, тако прикупљени подаци не могу се употребити као доказ у поступку.

3. Такође, сматрамо да је потребно додати нови члан који би се непосредно односио на ***меру хитног чувања ускладиштених рачунарских података***.

Овим чланом би било предвиђено да када постоји опасност да ће се рачунарски подаци похрањени у рачунарском систему, који могу бити од значаја за кривични поступак, изгубити или изменити, јавни тужилац издаје наредбу да се ти подаци сачувају у неизмењеном облику за рок до деведесет дана. Рок може бити продужен по одобрењу јавног тужиоца за још деведесет дана. Мера хитно чување ускладиштених рачунарских података би се могла наредити према било ком физичком или правном лицу који има у поседу или врши контролу над рачунарским системом у ком су ускладиштени потребни подаци, осим према окривљеном и лицима из члана 93, члана 94. став 1. и члана 95. став 2. Законика. Наредба би се могла односити на све врсте података који су похрањени у систему, укључујући и податке о оствареним електронским комуникацијама који су у поседу пружалаца услуга електронских комуникација. Наредба се издаје у писаном облику и садржи следеће елементе: лице према коме се наредба издаје, одређење података које је потребно сачувати, временски период за који се захтева чување података и образложење. 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 предавање података или наредбе за претрес уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи.

С тим у вези, потребно је додати нови члан који би се непосредно односио на меру *хитног чувања и делимичног откривања података о саобраћају комуникација*. Наиме, 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, дужан је да надлежном органу пружи довољно података потребних за утврђивање идентитета свих пружалаца коришћењем чијих услуга је комуникација остварена.

4. У погледу остваривања приступа и увида у садржај похрањених рачунарских података ***у току вршења увиђаја,*** потребно је у *члану 135***.** који уређује увиђај над стварима предвидети да у току вршења увиђаја лица места на ком се налази рачунар, а за које постоји вероватноћа да садрже електронске доказе, орган поступка уз помоћ стручног лица предузима техничке мере ради спречавања губитка, оштећења или измене рачунарских података на начин да се поштују гарантована права држаоца рачунара.

Ако се врши увиђај над уређајима и опремом из члана 152. став 3. овог законика, држалац предмета, осим окривљеног, дужно је да омогући приступ и да пружи обавештења потребна за њихову употребу, изузев ако не постоји неки од разлога из члана 93, члана 94. став 1. и члана 95. став 2. овог законика. 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.).

5. Што се тиче **претресања рачунара,** сматрамо да је једино адекватно решење брисати у члану 152. став 3. и у члану 157. став 3, а додати одредбе

које би се односиле на претресање рачунара ради проналаска и одузимања рачунарских података који могу бити доказ у кривичном поступку**.**

Конкретно, уколико се *у* току претресања стана и других просторија пронађе рачунар и/или опрема на којој се могу чувати рачунарски подаци, а за које постоји вероватноћа да садрже рачунарске податке који могу имати значај доказа (електронске доказе), полиција уз помоћ стручног лица предузима техничке мере ради спречавања губитка, оштећења или измене рачунарских података. Претресање рачунара и опреме предузима се *на основу наредбе суда* уколико постоји вероватноћа да ће се претресањем пронаћи рачунарски подаци који могу имати значај доказа (електронски докази), уз помоћ стручног лица.

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 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 прикупљеним доказним материјалом ради накнадног одобрења радње и могућности коришћења прикупљених доказа. Наиме, целисходно је предвидети да јавни тужилац или овлашћена службена лица полиције могу изузетно без наредбе суда предузети претресање рачунара уз сагласност у писаном облику држаоца рачунара или лица под чијом је рачунар, или ради отклањања непосредне и озбиљне опасности за људе или имовину. Кад јавни тужилац или овлашћена службена лица полиције предузму претресање без наредбе суда, дужна су да о томе одмах, а најкасније у року од 24 часа, поднесу извештај судији за претходни поступак који цени да ли су били испуњени услови за претресање. Уколико судија процени да нису били испуњени услови за претресање, прикупљени рачунарски подаци се не могу користити као доказ.

После предаје наредбе о претресању, држалац рачунара и опреме на коме ће се претресање предузети позива се да добровољно преда рачунарске податке који се траже. Претресању рачунара и рачунара и опреме се може *приступити и без*

претходне предаје наредбе, очигледно припрема или је отпочело уништавање рачунарских података важних за поступак или је држалац недоступан.

Ако се врши претресање рачунара и опреме, држалац предмета или присутно лице (члан 156. став 4.), осим окривљеног, дужно је да омогући приступ и да пружи обавештења потребна за њихову употребу, изузев ако не постоји неки од разлога из члана 93, члана 94. став 1. и члана 95. став 2. овог законика. Према лицу које одбије да поступи по наведеној обавези, сходно се примењује одредба члана 148. став. 2. Ток претресања се тонски и оптички снима, а снимци и фотографије се прилажу записнику о претресању.

Уколико током вршења претреса постоји вероватноћа да су тражени рачунарски подаци похрањени у другом просторно удаљеном рачунарском систему или делу система ком се може законито приступити из рачунарског система који је предмет претреса, претресање се може проширити и на тај други рачунарски систем или део система, уколико је то неопходно за утврђивање чињеница што се не може остварити предузимањем других радњи и ако постоји опасности да ће у супротном доћи до губитка тражених података, а за то постоји пристанак лица из става 3. или наредба суда. Судија у наредби ограничава проширену претрагу на тачно одређене делове рачунарског система ком се може приступити преко првобитно претраживаног рачунара.

Уколико околности указују да су потребни рачунарски подаци похрањени у рачунару који је на територији друге државе, подаци којима се приступило се копирају ради обезбеђења (али се не би могао остварити увид у њихов садржај до одлуке суда стране државе). О том судија обавештава Министарство правосуђа, а Министарство државу на чијој територији се налази рачунарски систем на који је проширен претрес, ради поштовања правила о пружању узајамне правне помоћи у кривичним стварима и територијалног суверенитета стране државе.

6. У вези са претресањем рачунара, треба предвидети у посебном члану ***одузимање рачунарских података.***

У вези са одузимањем предмета потребно је предвидети сходну примену правила о одузимању предмета и на похрањене рачунарске податке. Тако је у

члану који предвиђа који предмети могу бити одузети (члан 147) потребно је поред уређаја за аутоматску обраду података и уређаја и опреме на којој се чувају или се могу чувати електронски записи, додати да то могу бити *и рачунарски подаци похрањени у њима*.

Наиме, потребно је изричито прописати да наредба о претресању рачунара обухвата и овлашћење за одузимање рачунарских података који могу имати значај доказа. 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. 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).

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. У зависности од околности случаја, потребни рачунарски подаци се одузимају тако што се: рачунарски систем и уређаји за складиштење података одузимају са лица места и прослеђују на форензичку обраду, или се на лицу места у присуству држаоца рачунара или два сведока стварају копије потребних рачунарских података, при чему се једна копија предаје у судски депозит и оверава дигиталним потписом, а друга се прослеђује на форензичку обраду. Копирање рачунарских података врши стручно лице на одговарајућем медијуму у процедури која обезбеђује потпуну саобразност оригинала и копије. Сматрамо да је нужно у посебном члану уредити *дужности држаоца рачунарских података*. Наиме, лице које у поседу или под контролом

има рачунарске податке који могу имати значај доказа треба обавезати да органу поступка на основу наредбе суда преда податке у целовитом, изворном, видљивом и опипљивом облику подобном да се изузму са лица места или у облику из ког се могу превести у видљиву и читљиву форму. Истим чланом потребно је обавезати пружаоце услуга електронских комуникација да предају податке о кориснику услуга, а који су у поседу или под контролом пружаоца, и то: податке о врсти комуникационе услуге, техничким условима и периоду коришћења услуга; податке о идентитету корисника, адреси, броју телефона, плаћању услуге на основу уговора са корисником; и податке о опреми која је предата кориснику на основу уговора са корисником. 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 *предавање комуникације које су у 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

7. У погледу ***тајног надзора комуникација,*** потребно је проширити круг кривичних дела у погледу којих се радња може одредити.

То би значило да се у *члану 162. став 3,* уврсте и следећа кривична дела: Оштећење рачунарских података и програма (члан 298.ставови 1.и 2), Прављење и уношење рачунарских вируса (члан 300), Рачунарска превара (члан 301. став 1. и 2), Спречавање и ограничавање приступа јавној рачунарској мрежи (члан 303) и Неовлашћено коришћење рачунара или рачунарске мреже (члан 304). Алтернативно, предвидети могућност одређивања ове посебне доказне радње за сва кривична дела која су у надлежности тужиоца за високотехнолошки

криминал. Осим тога, сматрамо да је неопходно уколико је, наравно испуњен услов из члана 161, омогућити одређивање радње и за друга кривична дела која су извршена употребом рачунарског система, или у погледу који је потребно прикупљање електронских доказа.

Осим тога, у *члану 166,* неопходно је предвидети могућност заплене не само писама и других пошиљким него и порука електронске комуникације“. Такође, потребно је додати став по ком се тајни надзор комуникација се може одредити и према лицу за које постоји основи сумње да у име осумњиченог или од осумњиченог прима или прослеђује поруке или да осумњичени користи њихов телефонски број, односно адресу, или које крије осумњиченог или му прикривањем средстава којима је кривично дело учињено, трагова кривично дела или предмета насталих или прибављених кривичним делом или на други начин помаже да не буде откривен.

У *члану 167. став 2.* међу елементима наредбе за одређивање тајног надзора комуникација, после речи обим, неопходно је додати одређење који подаци се прикупљају.

Поред правила да се радња одређуеј наредбом судије за претходни поступка, сматрамо да је оправдано предвидети изузетак, по ком би уколико постоји опасност од одлагања и ако јавни тужилац процени да на време неће моћи прибавити наредбу судије за претходни поступак, наредбу могао на време од двадесет четири сата издати јавни тужилац. Наредбу са означеним временом издавања, допис у којем образлаже разлоге за издавање наредбе и образложени предлог за даље спровођење радње јавни тужилац би доставио судији за претходни поступак у року од шест часова од издавања, који би испитао да ли су постојали услови за издавање наредбе и да ли је постојала опасност од одлагања. Судија за претходни поступак би одмах, а најкасније у року од шест часова по пријему наредбе и дописа одлучио решењем о законитости наредбе јавног тужиоца. Уколико одобри наредбу, а јавни тужилац је поднео предлог за даље спровођење доказне радње, доноси наредбу, а уколико се не сложи с наредбом, о томе одлуку доноси веће из члана 21. став 4. Ако је поднет предлог за даље спровођење доказне радње одређене, оно се наставља до одлуке већа. Веће о захтеву судије за претходни поступак одлучује у року од 12 часова од пријема

захтева. Уколико веће потврди наредбу јавног тужиоца, а поднет је предлог за даље спровођење доказне радње, доноси наредбу, а уколико не одобри наредбу, решењем налаже да се одмах обустави спровођење радње, а подаци прикупљени на основу налога јавног тужиоца се предају судији за претходни поступак који поступа у складу са чланом 163. став 1.

Мишљења смо да нема разлога да у спровођењу тајног ндазора комуникација могу учествовати Безбедносно-информативна агенција или Војнобезбедносна агенција јер су те службе безбедности нису орган кривичног поступка. Осим тога, потребно је ради заштите података о личности, што представља уставно право грађана, предвидети да по завршетку тајног надзора комуникације јавни тужилац обавештава лице да је према њему била спроведена доказна радња, осим уколико постоји опасност да би такво обавештење угрозило интересе кривичног гоњења или живот, физички интегритет, слободе и права и имовину других лица. О одлагању обавештења лица би састављала писана белешка а одлагање не би могло да траје дуже од шест месеци од дана када се јавни тужилац упознао са материјалом прикупљеним коришћењем посебне доказне радње.

Како ова посебна доказна радња обухвата само *заплену писама и других пошиљки,* се не односи на, сматрамо да је целисходно проширити могући обухват ове радње и на поруке електронске поште, односно друге поруке које се преносе коришћењем услуга електронских комуникација. У оквиру посебне доказне радње тајног надзора комуникације, оправдано је посебним чланом уредити ***заплену порука електронске комуникације.*** Наиме, судија за претходни поступак би могао захтевати од пружалаца услуга електронских комуникација да заплене поруке електронске комуникације, уколико се процени да је у комуникацији учествовао окривљени или је повезана са извршењем кривичног дела из члана 161. Ако то налажу разлози хитности, јавни тужилац би могао до добијања наредбе суда наредити заплену, односно зауставити прослеђивање порука електронске комуникације, али за то морао обезбедити сагласност судије за претходни поступак у року од 48 часова, док би се у супротном мера обуставила. Уколико би заплену наредио јавни тужилац, дужан би био да поруку у одговарајућем облику преда суду без одлагања, без измена и без сазнавања садржаја комуникације, док би остваривање увида у задржане поруке било могуће

само у присуству судије за претходни поступак. Уколико би јавни тужилац утврдио да поруке немају значај доказа, оне би се проследиле пошиљаоцу без одлагања, док би се, у случају да поруке имају значај доказа, пошиљалац и прималац о томе обавештавали, под условом да то не би угрозило истрагу.

8. У погледу ***рачунарског претраживања података,*** предвиђено је да се радња може одредити само у погледу кривичних дела из члана 162. став 1 и 2. међу којима није ниједно кривчно дело из групе кривичних дела против безебдности рачунарских података, па сматрамо да би било сасвим оправдано предвидети могућност одређивања ове посебне доказне радње према делима која спадају у високотехнолошки криминал у смислу члана 3. Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (према постојећем решењу радња се не може одредити ни према једном из ове групе кривичних дела.)

Осим тога, како претраживање може вршити не само државни орган него и правно лице *које на основу закона врши јавна овлашћења* (члан 180), у члану коју уређује садржај наредбе (*члан 170. став 2*), потребно је предвидети да се осим државног органа означи и то правно лице. Осим тога, потребно је јасно назначити који субјект је овлашћен за претраживање (као претходну активност), а који за упоређивање (као накнадну активност).

9. У ***Закону о судским вештацима,*** у погледу начина на који кандидат за вештака доказује поседовање стручног знања, потребно је у *члану 7. став 1*, на крају реченице додати: „*и поседовањем одређених сертификата издатих од стране међународно признатих удружења и организација.*“ Осим тога, у *члану 9*, који одређује под којим условима правно лице може обављати послове вештачења, оправдано је додати став по ком правно лице у ком се вештачење обавља у лабораторијама мора да *испуни стандарде квалитета у складу са ILAC-G19 и ISO/IEC 17025.*

* * *

Држава може усвојити добре законе у циљу супротстављања високотехнолошком криминалу, међутим, један од основних изазова у тумачењу

и примени тих закона је недостатак техничког знања од стране лица које законе тумаче и примењују. Држава може формирати посебну организациону јединицу полиције надлежну за високотехнолошки криминал и прописати да се форензичка анализа електронских доказа обавља од стране посебних форензичких одељења, може формирати посебно јавно тужилаштво у чијој ексклузивној надлежности је гоњење учинилаца дела високотехнолошког криминала, међутим, ако се не обезбеде технички и људски ресурси, ове јединице не могу остваривати своју функцију. Запослени у специјализованој јединици нису нити ће бити по природи ствари у могућности да у изађу на свако лице места ради вршења увиђаја или претреса стана приликом којих се пронађе рачунар који би могао садржати корисне електронске доказе. То значи да уколико полицајац који је присутан на лицу места приликом вршења радњи првог захвата не поседује знања о природи електронских доказа нити познаје основна техничка и тактичка правила поступања, једним погрешним кораком може угрозити, па и онемогућити употребу електронских доказа. При томе чак ни ступање у контакт са посебним одељењем полиције/тужилаштва или чекање до њиховог изласка на лице места није у сваком случају адекватно решење, јер време понекад игра кључну улогу, што доводи до другог, по нашем мишљењу битнијег проблема, а то је непоседовање основних знања дигиталне форензике од стране запослених у „неспецијализованим“ државним органима.

Рачунари и информационе технологије су увелико постале део свакодневице великог броја појединаца и нису више апстракција и луксуз малобројних, а с обзиром на свеприсутност информационих технологија у свакодневном окружењу, неминовно је да ће у будућности радње све већег броја кривичних дела остављати одређени електронски траг у виду рачунарских података који могу бити електронски доказ у кривичном поступку (не само у кривичних дела извршених против безбедности рачунарских података и рачунарских система и мрежа, односно посредством информационе технологије, него и других кривичних дела), а то значи да ће се повећавати и број случајева који би могли бити у надлежности специјализованих јединица. Истовремено, услед све већег броја кривичних дела која ће, с обзиром на околности случаја, моћи бити доказана у кривичном поступку употребом електронских доказа, кривична дела која за

објект напада/средство извршења имају рачунарски систем/мреже изгубиће на својој „специјалности“, изазови откривања и доказивања ће бити превазиђени, а надлежни органи ће их посматрати и решавати као и сва друга кривична дела.

За разлику од мање или веће лакоће у прихватању предности које је технолошки развој донео, међу запосленим у надлежним правосудним органима постоји незаинтересованост/ отпор за разумевања основних принципа функционисања ових технологија. Проблем постоји уколико се полиција или јавно тужилаштво суздрже чак од покушаја да истражују случај у ком се као средство извршења појаве рачунари. Међутим, игнорисање од стране надлежних органа је недопустиво из разлога што је услед свеприсутности информационе технологија све већа вероватноћа да у све већем броју предмета трагови и докази буду у електронском облику. Полазећи од тога да страх и отпор углавном потичу од незнања, односно недовољног поимања одређене појаве (као што су људске заједнице страховале и поштовале природне појаве које нису разумеле и из тог разлога им придавале божанска својства), мишљења смо да је битан корак ка супротстављању високотехнолошком криминалу управо демистификација одређених аспеката рачунарства, а тиме и високотехнолошког криминала. Отуда је један од кључних предуслова да би надлежни органи гоњења успешно истражили високотехнолошки криминал усвајање основног знања и вештина за разумевања како функционишу рачунарски системи, на којим принципима се заснива рачунарска мрежа, шта се може а шта не може постићи применом информационе технологије и на који начин је употребом информационе технологије омогућено извршење радње кривичних дела. Није потребно да полиција, јавно тужилаштво и суд познају како хакер користи конфигурационе поставке да оствари неовлашћени приступ у рачунар или како се ствара и користи мрежа ботнетова за извршење дистрибуираног напада на информационе системе. У разумевању ових питања надлежним органима помоћ пружају лица са стручним знањем у одређеним процесним улогама (у улози вештака, стручног лица и/или стручног саветника). Иако форензичку обраду рачунара могу обављати само за то оспособљена лица, сматрамо да је познавање основа архитектуре рачунара ради сазнавања извора потенцијалних електронских доказа неопходно овлашћеним службеним лицима криминалистичке полиције који поступају на лицу места на

ком се налази рачунари (нарочито ако није обезбеђено присуство стручних лица) како би на правилан начин обезбедили рачунарске податке који могу послужити као доказ у кривичном поступку. Изузетно је важно да јавни тужилац познаје ове специфичности да би уопште могао да руководи истрагом, предложи вештачење и заступа оптужбу, а неопходно је разумевање чињеница о техничким детаљима предузетих доказних радњи чије резултате у виду електронских доказа презентује против оптуженог. Што се тиче суда, фундаментална техничка знања су потребна ради разумевања суштине материјалноправних одредаба које садрже инкриминацију дела високотехнолошког криминала, а нарочито у погледу процесних одредаба које се односе на специфичности доказних радњи које само суд може да одреди (нпр. претресање рачунара), као и слободне оцене електронских доказа који настају као резултат тих радњи. Уколико судији недостаје техничко знање потребно за примену закона, помоћ у разумевању техничких детаља може му пружити вештак информационе технологија, међутим, неопходно је да судија поседује макар минимум знања да би могао поставити питања на које вештак треба да одговори, односно да би могао одредити правац вештачења, те критички и по свом слободном судијском уверењу оценити налаз и мишљење вештака (а не да га некритички прихвата). Такође, сматрамо да је, осим поменутог, важно да судија разуме и могуће последица доказних радњи предузетих у вези са рачунарским системима и мрежама, с обзиром на знатан степен интрузивности у право приватности корисника рачунара.

На основу свега наведеног, сматрамо да је специјализација државних органа (полиције и тужилаштва) надлежних за високотехнолошки криминал тренутно оправдано решење, али да је у циљу ефикасног реаговања у будућности, од изузетне важности, чак и нужно познавање основа дигиталне форензике од стране свих надлежних органа откривања, гоњења и суђења, као и од стране бранилаца ради остваривања функције одбране у кривичном поступку.

СПИСАК БИБЛИОГРАФСКИХ ЈЕДИНИЦА

1. ЛИТЕРАТУРА

1.1. Књиге

1. Алексић Ж., Шкулић М., *Криминалистика*, Београд 2002;
2. Алексић Ж., Шкулић М., *Криминалистика*, Београд 2011;
3. Baggili I. (ed.), *Digital Forensics and Cyber Crime* (Second International ICST Conference ICDF2C 2010 Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers), Springer, Heidelberg-Dordrecht 2011;
4. Ball K., Webster F., *The Intensification of surveillance: crime, terrorism and warfare in the information age,* Pluto Press, New York 2003;
5. Barbara J., *Handbook of Digital and Multimedia Forensic Evidence,* Springer, Heidelberg-Dordrecht 2008;
6. Barrett D., Kipper G., *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments,* Elsevier Science & Technology, Heidelberg 2010;
7. Bayer V., *Jugoslovensko krivično procesno pravo, knjiga druga, Pravo o činjenicama i njihovom utvrđivanju u krivičnom postupku*, Zagreb 1989;
8. Bayuk J., *Cyber Forensics: Understanding Information Security Investigations*, Springer, New York-Dordrecht 2010;
9. Бајовић В., *О чињеницама и истини у кривичном поступку*, Београд 2015;
10. Бејатовић С., *Кривично процесно право*, Београд 2014;
11. Brenner S., *Cybercrime: Criminal Threats from Cyberspace (Crime, Media, and Popular Culture)*, Praeger, Santa Barbara 2010;
12. Brenner S., *Cybercrime and the Law: Challenges, Issues, and Outcomes*, Northeastern University Press, Boston 2012;
13. Britz M., *Computer Forensics and Cyber Crime: An Introduction*, Prentice Hall, New Jersey 2008;

14. Бркић С., *Кривично процесно право I*, Центар за издавачку делатност Правног факултета у Новом Саду, Нови Сад 2014;

15. Brown C., *Computer Evidence: Collection and Preservation*, Charles River Media, Boston 2009;

16. Bryant R., Bryan S. (eds.), *Investigating Digital Crime*, John Wiley&Sons, Chichester 2008;

17. Bryant R., Bryan S. (eds.), *Policing Digital Crime*, Ashgate Publishing Limited, Surrey 2014;

18. Бугарски Т., *Доказне радње у кривичном поступку*, Центар за издавачку делатност Правног факултета у Новом Саду, Нови Сад 2014;

19. Васиљевић Т., *Систем кривичног процесног права СФРЈ*, Београд 1981;

20. Васиљевић Т., М. Грубач, Коментар Законика о кривичном поступку, Београд 2011;

21. Vacca J., *Computer forensics: Computer Crime Scene Investigation*, Charles River Media, Boston 2005;

22. Водинелић В., К*риминалистика*, Београд 1996;

23. Walden I., *Computer Crimes and Digital Investigations*, Oxford University Press, Oxford 2007;

24. Wall D., *Crime and the Internet*, Routledge, London 2001;

25. Wall D., *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge University Press, Cambridge 2010;

26. Watson D, Jones A., *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*, Syngress, Waltham 2013;

27. Garland D., *The culture of control*, Oxford University press, Oxford, 2001;

28. Garrison C, Lillard T., Schiller C., Steele J., *Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data*, Elsevier Science & Technology, Boston 2010;

29. Gercke M., Brunst P., *Praxishandbuch Internetstrafrecht*, Kohlhammer; Auflage, Stuttgart 2010;

30. Gertz M., *Integrity and Internal Control in Information Systems V*, Springer, Bonn, 2003;

31. Geschonneck A., *Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklaren*, Springer, Heidelberg 2012;

32. Grabosky P., *Electronic Crime*, Pearson Education Inc, New Jersey 2007;

33. Грубач М., *Кривично процесно право*, Београд 2011;

34. Gutwirth S., *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002;

35. Gutwirth S., Poullet Y., De Hert P. (eds.), *Data protection in profiled world*, Springer, Heidelberg 2010;

36. Darell K., *Issues in Internet Law: Society, Technology, and the Law*, Amber Book Company, London 2013;

37. Делић Н., *Нова решења у посебном делу КЗ Србије*, Београду 2014;

38. Dunne R., *Computers and the Law: An Introduction to Basic Legal Principles and Their Application in Cyberspace*, Cambridge University Press, Cambridge 2009;

39. Ђурђић В., *Кривични поступак Србије*, Ниш 2006;

40. Ђурђић В., *Основи криминалистике*, Ниш 2012 ;

41. Easttom C, Taylor J., *Computer Crime, Investigation, and the Law*, Course Technology, Boston 2010;

42. Игњатовић Ђ., *Компарација криминалитета и казнене реакције: Србија- Европа*, Правни факултет Универзитета у Београду, Београд 2013;

43. Јекић З., *Кривично процесно право*, осмо измењено и допуњено издање, Београд 2003;

44. Jewkes Y., Yar M., *Handbook of Internet Crime*, Willan, Devon 2010;

45. Johnson T., *Forensic Computer Crime Investigation (International Forensic Science and Investigation)*, CRC Press, Chicago 2005;

46. Kamal A., *The Law of Cyber-Space: An Invitation to the Table of Negotiations*, United Nations Institute for Training and Research, New York 2005;

47. Kipper G., *Wireless Crime and Forensic Investigation*, Auerbach Publications, New York 2007;

48. Kizza J. , *Guide to Computer Network Security*, Springer Science & Business Media, Berlin 2013;

49. Klang M., Murray A., *Human rights in the digital age*, Routledge-Cavendish, London-Portland 2005;

50. Кнежевић С., *Кривично процесно право, Општи део*, Ниш 2015;

51. Knetzger M., Muraski J., *Investigating High-Tech Crime*, Prentice Hall, New Jersey 2007;

52. Комлен Николић Л. et al, *Сузбијање високотехнолошког криминала*, Удружење јавних тужилаца и заменика јавнх тужилаца Србије, Београд 2010;

53. Koops B., Brenner S., (eds.), *Cybercrime Jurisdiction: A Global Survey*, T.M.C. Asser Press, Amsterdam 2006;

54. Kruse W, Heiser , *Computer Forensics: Incident Response Essentials*, Addison Wesley, London 2001;

55. Kshetri, N., *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer, Amsterdam 2010;

56. Lee H. et al., *Crime Scene Handbook*, Academic Press, San Diego 2001;

57. Li C., *Handbook of research on computational forensics, digital crime, and investigation : methods and solutions*, Information Science Reference, New York 2010;

58. Лукић Т., *Посебности кривичног поступка за организовани криминал, тероризам и корупцију*, Нови Сад 2008;

59. Malin C, Casey E., Aquilina, J., *Malware Forensics: Investigating and Analyzing Malicious Code*, Syngress, Boston 2008;

60. Marcella A., Menendez D., *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Auerbach Publications, New York 2002;

61. Marcella A., Menendez D., *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Second edition, Auerbach Publications, New York 2008;

62. Марковић Б., *Уџбеник кривичног судског поступка Краљевине Југославије*, Београд 1937;

63. Marsden C.T., *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge 2011;

64. Marshall A., *Digital Forensic*, Wiley, Chichester 2008 (263, 286);

65. Martin D., *La Criminalite Informatique*, Presses Universitaires De France, Paris 1997;

66. Middleton B., *Cybercrime investigator's field guide*, Auerbach Publications, Boca Raton 2005;

67. Moore R., *Cybercrime: Investigating High-Technology Computer Crime*, Anderson, Oxford 2011;

68. Moore R., *Search and seizure of digital evidence*, LFB Scholarly Pub., New York 2005;

69. Mueller M.L., *Networks and States: the Global Politics of Internet Governance*, MIT Press, Cambridge 2010;

70. McGuire M., *Hyper-crime: the New Geometry of Harm*, Abingdon, Oxford 2007;

71. McQuade S. (ed.), *Encyclopedia of cybercrime*, Westport, Conn. : Greenwood Press 2009;

72. McQuade S., *Understanding and Managing Cybercrime*, Allyn & Bacon, Boston 2005;

73. Naughton J, *A Brief History of Future: Origins and History of the Internet*, London, Weidenfeld and Nicolson 1999;

74. Pittaro M., *Cybercrime: Current Perspectives from InfoTrac*, 2 edition , Wadsworth Publishing, Andover 2009;

75. Prosise C., Mandia K, *Incident Response: Investigating Computer Crime*, McGraw Hill Osborne Media, 2001;

76. Путник Н., Сајбер простор и безбедносни изазови, Београд 2009 (8);

77. Радуловић Д., *Кривично процесно право*, Подгорица 2002;

78. Радуловић Д., *Коментар Законика о кривичном поступку Црне Горе*, Подгорица 2009;

79. Ray I., Shenoi S., *Advances in Digital Forensics IV*, Springer, Boston 2008;

80. Roggan F., *Online-Durchsushungen: Rectliche und tatsachliche Konsequenzen des BVerfG-Urteils vom 27.Febraur 2008*, Berliner Wissenschafts-Verlag, Berlin 2008;

81. Roxin C., B. Schunemann, Strafverfahrensrecht, 27. Auflage, Munchen 2012;

82. Ruh J. (ed.), *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, Computer Law Association, Stanford 1996;

83. Rustad M., *Global Internet law in a nutshell*, St. Paul, MN: West, Boston 2013;

84. Ruyver B., Vermeulen G., Beken T., *Strategies of the EU and the US in combating transnational organized crime*, Maklu 2002;

85. Sieber U., *Information Technology Crime – National Legislations and International Initiatives*, Carl Heymanns Verlag, Köln 1994;

86. Sieber U., *Legal Aspects of Computer-Related Crime in the Information Society* (COMCRIME Study), European Commission, 1998;

87. Симоновић Б., *Криминалистика*, Крагујевац 2004 ;

88. Sorell M, *Forensics in Telecommunications, Information and Multimedia*, Springer-Verlag, Berlin - Heidelberg 2009;

89. Sofaer A., Goodman S., *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution Press, Stanford 2001;

90. Spinello R., *Regulating Cyberspace: The Policies and Technologies of Control*, Praeger,Westport 2002;

91. Стевановић Ч., Ђурђић В., *Кривично процесно право (Општи део)*, Ниш 2006;

92. Stephenson P., *Investigating computer-related crime*, CRC Press, Boca Raton 2000;

93. Стојановић З., *Коментар Кривичног законика*, Београд 2006;

94. Стојановић З., *Кривично право (општи део)*, Правна књига, Београд 2010;

95. Стојановић З., Делић Н., *Кривично право (посебни део*) друго издање, Београд 2014;

96. Schjolberg S., *Computers and Penal Legislation – A Study of the Legal Politics of a new Technology,* Scandinavian University Press, Oslo 1984;

97. Schjolberg S., *The History of Cybercrime: 1976-2014*, Koln 2014;

98. Schroeder B., Schroeder C., *Die Online Durchsuschung: Rectliche Grundlagen*, Technik, Medienecho, Hannover 2008;

99. Урошевић В. (ур.), *Везе cyberкриминала са иregуларном миграцијом и трговином људима*, Министарство унутрашњих послова Републике Србије, Београд 2014;

100. Урошевић В, Ивановић З, Уљанов С., *Мач у World Wide Web-у: изазови високотехнолошког криминала*, *Eternal mix*, Београд 2012;

101. Yar M., *Cybercrime and Society*, SAGE Publications, New York 2006;

102. Фејеш И., *Савремени криминалитет и доказно право*, Нови Сад 2002;

103. Ferrera G., *CyberLaw: Text and Cases*, Cengage Learning, Independence 2011;

104. Franklin C., *The Investigator's Guide to Computer Crime*, Charles C. Thomas Pub. Ltd, Springfield 2006;

105. Furedi S., *Culture of fear*, Continuum, London 2002;

106. Хајдуковић М., *Оперативни системи (проблеми и структура),* ФТН Издаваштво, Нови Сад 2013;

107. Хајдуковић М., Живанов Ж., *Архитектура рачунара (преглед принципа и еволуције)*, ФТН Издаваштво, Нови Сад 2013;

108. Hennessy J., Patterson D, *Computer Architecture: A Quantitative Approach*, Elsevier, Waltham 2011;

109. Hilgendorf E., Valerius B., *Computer- und Internetstrafrecht:Ein Grundiss*, Springer, Heidelberg 2012;

110. Caloyannides M., *Privacy protection and computer forensics*, Artech House, Boston 2004;

111. Casey E., *Handbook of Digital Forensics and Investigation*, Academic, Amsterdam-Boston 2010;

112. Casey, E., *Digital evidence and computer crime: forensic science, computers and the Internet*, Academic Press, Amsterdam-Boston 2011;

113. Clark F., Diliberto K., *Investigating Computer Crime*, CRC Press, New York 1996;

114. Clarke N., *Computer forensic*, IT Governance Publishing, London 2010;

115. Clifford R., *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime*, Carolina Academic Press, Durham 2011;

116. Clough J., *Principles of Cybercrime*, Cambridge University Press, Cambridge 2010;

117. Craig B., *Cyberlaw: The Law of the Internet and Information Technology*, Prentice Hall, New Jersey 2012;

118. *Criminological aspects of economic crime*: Reports Presented to the Twelfth Conference of Directors of Criminological Research Institutes, Strasbourg 1977;

119. Cross M., Shinder D. L., *Scene of the Cybercrime*, Syngress, Burlington 2008;

120. Curtis G., *The Law of Cybercrime and their Investigation*, Taylor&Francis, Boca Raton 2012;

121. Шкулић М., *Међународни кривични суд – надлежност и поступак*, Београд 2005;

122. Шкулић М., *Кривично процесно право*, Правни факултет у Београду, Београд 2014;

123. Шкулић М., *Организовани криминалитет: појам и кривичнопроцесни аспекти,* Београд 2015;

124. Шкулић М. *et al, Усаглашеност домаћих прописа са институтима Европске уније у области међународне правне помоћи у кривичним стварима и препоруке за хармонизацију*, Удружење јавних тужилаца и заменика јавних тужилаца, Београд 2011;

125. Шкулић М., Бугарски Т., *Кривично процесно право*, Нови Сад 2015;

126. Шкулић М., Илић Г., *Водич за примену новог Законика о кривичном поступку*, Београд 2013.

1.2. Радови у часописима и другим публикцијама

1. Abel W., „Agents, Trojans and tags: The next generation of investigators“, *International Review of Law, Computers & Technology* 1-2/2009, 99-108;

2. Adelstein F, „Live forensics: diagnosing your system without killing it first“, *Communications of the ACM* 2/2006, 63-66;

3. Adler M., „Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net- Wide Search“, *The Yale Law Journal* 4/1996, 1093-1120;

4. Akdeniz Y., „New Privacy Concerns: ISPs, Crime Prevention and Consumers' Rights,“ *Journal of Law, Computers and Technology* 1/2001, 55-61;

5. Aldesco A., „The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime“, *Loyola of Los Angeles Entertainment Law Review* 1/2002, 81-123;

6. Al-Zaidy R. et al, „Mining criminal networks from unstructured text documents“, *Digital Investigation* 8 /2012, 147–160;

7. Aquilina K., „Public security versus privacy in technology law: balancing act?“, *Law computers & Security Report* 26/2010, 130-143;

8. Arasteha A et al, “Analyzing multiple logs for forensic evidence“, Digital Investigation 1/2007, 82-91;

9. Ard C., „Botnet Analysis“, *International Journal of Computer Forensics Science* 1/2007, 65-74;

10. Arzt C., “Data protection versus 4th Amendment: a new approach towards police serach and seizure”, *Criminal Law Forum* 16/2005, 183-230;

11. Asinary M.V.P., „Legal Constraints for the Protection of Privacy and Personal Data in Electronic Evidence Handling“, *International journal of Law, Computers and Technology* 2/2004, 231-250;

12. Atchison C., „Emerging Styles of Social Control on Internet: Justice denied“, *Humanities, Social Sciences and Law, Critical Criminology* 1-2/2000, 85-100;

13. Atchison C., „The Internet and the State: Instrument of Social Control or Subversive Technology“, *Humanities, Social Sciences and Law, Critical Criminology* 1-2/2000, 163-170;

14. Ausloos J., „The ‘Right to be Forgotten’-Worth remembering?“, *Computer Law and security Review* 28/2012, 143-152;

15. Ayers D., „A second generation computer forensic analysis system“, *Digital Investigation* 6/2009, 34-42;

16. Ballou S., „Emerging paper standards in computer forensics“, *Digital Investigation* 8/2012, 96-97;

17. Бановић Б., „Електронски докази“, *Ревија за криминологију и кривично право* 3/2006, 223-232;

18. Backer M, Hornung G., „Data processing by police and criminal justice authorities in Europe - The influence of the Commission’s draft on the national police laws and laws of criminal procedure“, *Computer Law & Security Review* 28/2012, 627-633;

19. Bachmaier L., „European Investigation Order for obtaining evidence in the criminal proceedings: study of the Proposal for a European Directive“, *Zeitschrift für Internationale Strafrechtsdogmatik* 9/2010;

20. Beebe N., Clark J., „A hierarchical, objectives-based framework for the digital investigations process“, *Digital Investigation* 2/2005, 147-167;

21. Bellia P., „Chasing bits across borders“, *University of Chicago Legal Forum*, 2/2001, pp. 35–101;

22. Bem D, et al, „Computer Forensics: Past, Present and Future“, Journal of information science and Technology 3/2008, 43-59;

23. Bennett D., „The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations“, *Information Security Journal: A Global Perspective* 1/2012, 159–168;

24. Berg T., „The Impact of the Internet on state power to enforce the law“, *Brigham Young University Law Review* 4/2000, 1305-1362;

25. Berman P., „The globalization of jurisdiction“, *University of Pennsylvania Law Review* 12/2002, 311–529;

26. Bernal P, „ A Right to Delete? “, *European Journal of Law and Technology* 2/2011, 1-15;

27. Bignami F., „The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts“, *Cornell International Law Journal* 2/2008, 211-250;

28. Bilby D., „Low down and dirty: anti-forensic rootkits”, Proceedings of Black Hat Japan, Tokyo 2006, 1-40;

29. Boehm F., De Hert P., „Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law“, *European Journal of Law and Technology* 3/2012, 1-15;

30. Borisevich S. et al, „A comparative review of cybercrime law and digital forensics in Russia, the United States and under the Convention on cybercrime of the Council of Europe“, *Northern Kentucky Law Review* 39/2012, 267-326;

31. Bradbury D., „When borders collide: legislating against cybercrime“, *Computer Fraud & Security* 2/2012, 11–15;

32. Brand M., „Internet and the Law: An Article Examining the Problems and Questions Concerning the Regulation of Cyberspace“, *Tilburg Foreign Law Review* 3/2002, 259-278;

33. Brenner S., „Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law“, *Murdoch University Electronic Journal of Law* 2/2001, 1-46;

34. Brenner S., „Cybercrime metrics: Old wine, new bottles?’ *Virginia Journal of Law and Technology* 13/2004, 1-52;

35. Brenner S., „Cybercrime jurisdiction”, *Crime, Law and Social Change* 46/2006, 189–206;

36. Brenner S., „Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model“, *Journal of International Commercial Law and* Technology 2/2007, 58-67;

37. Brenner S., „Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force“, *Mississippi Law Journal* 1/2011, 1229-1259;

38. Brenner S., Koops B., „Approaches to cybercrime jurisdiction“, *Journal of High Technology Law* 1/2004, 1-46;

39. Brenner S., Schwerha J., „Transnational evidence gathering and local prosecution of international cybercrime", *John Marshall Journal of Computer and International Law* 3/2002, 347–395;

40. Brenner S., Schwerha J., „Introduction—Cybercrime: A Note on International Issues", *Information Systems Frontiers* 2/2004, 111–114;

41. Breyer P., „Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR", *European Law Journal* 3/2005, 365-375;

42. Brinson A. et al., „A cyber forensics ontology: Creating a new approach to studying cyber forensics", *Digital Investigation* 3/2006, 37 –43;

43. Broadhurst R., „Developments in the global law enforcement of cyber-crime", *Policing: An International Journal of Police Strategies and Management* 2/2006, 408-433;

44. Brown I., „Communications Data Retention in an Evolving Internet", *International Journal of Law and Information Technology* 2/2010, 95-109;

45. Buono H., „Gearing up the fight against cybercrime in the European Union: a new set of rules and the establishment of the European cybercrime center (ec3)", *New journal of European criminal Law* 3/2012, 222-244;

46. Buchholz F., Spafford E., „On the role of file system metadata in digital forensics", Digital Investigation 1/2004, 298-309;

47. Bygrave L., „Data protection pursuant to the right to privacy in human rights treaties", *International journal of law and information technology* 3/1998, 247-284;

48. Вићентијевић М., „Кривична дела против безбедности рачунарских података", *Избор судске праксе* 7-8/2008, 12-16;

49. Walden I., „Communication service providers: Forensic source and investigatory tool", *Information security technical report* 11/ 2006, 10–17;

50. Wall D., „Catching cybercriminals: Policing the Internet", *International Review of Law Computers & Technology* 2/1998, 201-218;

51. Wall D., „Introduction to Cybercrime, Cyberspeech and Cyberliberties", *International journal of Law, Computers and Technology* 1/2000, 5-9;

52. Wall D., „Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace“, *Police Practice and Research* 2/2007, 183-205;

53. Wall D., „Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime“, *International Review of Law Computers & Technology* 1-2/2008, 45-63;

54. Walters A., Petroni N., „Volatools: Integrating Volatile Memory into the Digital Investigation Process”, *Black Hat Briefings DC* 2007, 1-18;

55. Wang S., „Measures of retaining digital evidence to prosecute computer-based cyber-crimes“, *Computer Standards & Interfaces* 29/2007, 216–223;

56. Watney M., „The Legal conflict between Security and Privacy in Addressing Crime and Terrorism in Internet, ” ISSE Conference, Warsaw, Poland: 25 September 2007, 32-38;

57. Watney M,. „The Way Forward in Addressing Cybercrime Regulation on a Global Level”, *Journal of Internet Technology and Secured Transactions* 1-2/ 2012, 61-68;

58. Weber R., „Internet of Things – New security and privacy challenges”, *Computer Law and security Review* 26/2010, 23-30;

59. Weir B., „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;

60. Williams M., „Policing and Cybersociety: The Maturation of Regulation within an Online Community“, *Policing & Society* 1/ 2007, 59-82;

61. Wittow M., Buller D., „Cloud Computing: emerging legal issues for access to data, anywhere, anytime“, *Journal of Internet Law* 1/2010, 1-5;

62. Wittzack R., *„*Principles of International Internet Law*“, German Law Journal* 11/2010, 1245-1263;

63. Wolfson A., „Electronic fingerprints: doing away with conception of computer-generated records as hearsay“, *Michigan Law review* l/2005, 151-173;

64. Wong R., „Data protection: The future of privacy”, *Computer Law and security Review* 27/2011, 53-57;

65. Wright D., Friedewald M., „Sorting out Smart Surveillance“, *Computer Law& Security report* 26/2010, 343-354;

66. Wright D., „The state of the art in privacy impact assessment“, *Computer Law and security Review* 28/2012, 54-61;

67. Whitcomb C.M., „An Historical Perspective of Digital Evidence“, I*nternational Journal of Digital Evidence* 1/2002, 1- 9;

68. Gable K., „Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent“, *Vanderbilt Journal of Transnational Law* 1/ 2009, 57-118;

69. Garfinkel S, „Anti-forensics: Techniques, detection and countermeasures," *2nd International Conference on i-Warfare and Security* (Armistead L.), Edith Cowan University, Monterey 2007, 77-84;

70. Garfinkel S. et al., „Bringing science to digital forensics with standardized forensic corpora“, *Digital Investigation* 6/2009, 2 –11;

71. Garfinkel S, „Digital forensics research: The next 10 years”, *Digital Investigation* 7/2010, 64-73;

72. Garicano L., Heaton P., „Computing Crime: Information Technology, Police Effectiveness, and the Organization of Policing“, CEPR Discussion Paper 5837/2006, 1-10;

73. Gercke M., „Europe's legal approaches to cybercrime“, *ERA forum* No. 10/2009, 49-120;

74. Gillespie A., *„*Jurisdictional issues concerning online child pornography*“, International Journal of Law and Information Technology* 3/2012, 151-177;

75. Goldrick D, „Developments in the Right to be Forgotten“, *Human Rights Law Review* 4/2013, 761-776;

76. Goldsmith J., „The Internet and the Abiding Significance of Territorial Sovereignty“, *Indiana Journal of global legal studies* 2/1998, 475-491;

77. Goldsmith J., „The Internet and the Legitimacy of Remote Cross-Border Searches“, *The University of Chicago Legal Forum* 103/2001, 1-16;

78. Goncalves M., „Technological Change, Globalization and the Europeanization of Rights“, *International review of Law Computers& Technology* 3/2002, 301-316;

79. Goodman M., Brenner S., „The emerging Consensus in on Criminal Conduct in Cyberspace“, *International Journal of Law and Information Technology* 2/2002, 139-223;

80. Gordon S., Ford R., „On the definition and Classification of cybercimes“, *Journal in Computer Virology* 1/2006, 13-20;

81. Grivna T., „Virtual crimes“, *Masaryk University Journal of Law and Technology* 1/2008, 97-104;

82. Guinchard A., „Crime in virtual worlds: The limits of criminal law“, *International Review of Law, Computers & Technology* 2/ 2010, 175–182;

83. Gunasekara G. „The Final Privacy Frontier? Regulating Trans-Border Data Flows“, *International Journal of Law and Information Technology* 2/2007, 147-179;

84. Guo Y., Slay J., Beckett J., „Validation and verification of computer forensic software tool - searching Function“, Digital investigation 6/2009, 12–22;

85. Gupta G. et. al, „Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol“, *International Journal of Digital Evidence* 4/2004, 1-11;

86. De Busser E, „EU data protection in transatlantic cooperation in criminal matters: Will the EU be serving its citizens an American meal? “, *Utrecht Law Review* 1/2010, 86-100;

87. De Filippi P., Belli L., „Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation“, *European Journal for Law and Technology* 2/2012, 1-17;

88. De Hert P., Boehm F., „The Rights of notification after Surveillance is over: ready for recognition?“, *Digital Enlightment Yearbook* (eds: J.Bus et.al), 2012, 19-39;

89. De Hert P., Kloza D., „Internet (access) as a new fundamental right. Inflating the current rights framework?“, *European Journal of Law and Technology* 3/2012, 1-27;

90. De Hert P., Kopcheva M., „International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! Case“, *Computer Law and security Review* 27/11, 291-297;

91. De Filippi P., McCarthy S., „Cloud Computing: Centralization and Data Sovereignty“, *European Journal for Law and Technology* 2/2012, 1-18;

92. De Hert P, Papakonstantinou V., Riehle C., „Data protection in 3rd pillar – cautious pessimism”, *Crime, Rights and the EU: the future of police and judicial cooperation* (ed.Martin M.), London 2008, 121-194;

93. De Hert P., Papakonstantinou V., „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, *Computer Law & Security Review* 2/2012, 130 – 142;

94. De Hert P., Papakonstantinou V., „The Police and Criminal Justice Data Protection Directive: Comment and Analysis”, *Magazine of the Society for Computers & Law. Computers & Law* 6/2012, 21 – 25;

95. Dinant J.-M., „The Long Way from Electronic Traces to Electronic Evidence“, *International Review of Law Computers & Technology* 2/2004, 173-183;

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

97. Dreier T., „Opt in and ‘‘opt out’’ mechanisms in the Internet era – towards a common theory“, *Computer Law and security Review 26/2010,* 144-150;

98. Dretzka E., Mildner S., „Anything but SWIFT: Why Data Sharing is Still a Problem for the EU“, *American Institute for Contemprorary German Studies* 35/2010, 1-7;

99. Duranti L., Rogers C., „Trust in digital records: An increasingly cloudy legal area“, *Computer law & security review* 28/ 2012, 522-531;

100. Esayas J., „A walk in to the cloud and cloudy it remains: The challenges and prospects of ‘processing’ and ‘transferring’ personal data”, *Computer Law and security review* 28/2012, 336-678;

101. Живановић С., „Практични аспекти високотехнолошког криминала“, *Криминалистичко форензичка истраживања* 1/ 2011, 138-152;

102. Zavrsnik A., „Cybercrime - definitional challenges and criminological particularities“, *Masaryk University Journal of Law and Technology* 2/2008, 1-29;

103. Zavrsnik A., „Towards an overregulated cyberspace: criminal law perspective“, *Masaryk University Law and Technology journal* 2/2010, 173-190;

104. Zavrsnik A., „The absence of body in Cyberspace Criminal Justice Impact", *Masaryk University Journal of Law and Technology* 1/2007, 43-52;

105. Zekos G., „State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction", *International Journal of Law and Information Technology* 1/2005, 1-37;

106. Ianelli N., „Botnets as a Vehicle for Online Crime", *International Journal of Computer Forensics Science* 1/2007, 19-39;

107. Игњатовић Ђ, „Појмовно одређење компјутерског криминалитета", Анали Правног факултета у Београду 1-3/91, 136-144;

108. Inoue H., Adelstein F., Joyce R, „Visualization in testing a volatile memory forensic tool", *Digital Investigation* 8/2011, 42–51;

109. Jaishankar K., „Establishing a Theory of Cyber Crimes", *International Journal of Cyber Criminology* 2/20007, 1-9;

110. Jaishankar K., „Identity related crime in the cyberspace: Examining Phishing and its impact", *International Journal of Cyber Criminology* 1/2008, 10-15;

111. Jones R., Tahri D., „An overview of EU data protection rules on use of data collected online", *Computer Law and security review* 27/2012, 630-636;

112. Kalbande D, Jain N., „Comparative digital forensic model", *International Journal of Innovative Research in Science, Engineering and Technology* 8/ 2013, 3414-3419;

113. Katyal N.K., „Criminal Law in Cyberspace", *University of Pennsylvania Law Review* 4/2001, 1003-1114;

114. Katz L, „In Search of a Fourth Amendment for the Twenty-first Century", *Indiana Law Journal* 2/1990, 549-583;

115. Kahvedzic D., Kechadi T., „Dialog: A framework for modeling, analysis and reuse of digital forensic knowledge", *Digital Investigation* 6/2009, 23-33;

116. Kenneally E., „Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection*", UCLA Journal of Law and technology* 5/2005, 1-35;

117. Kenneally E., Brown C., „Risk sensitive digital evidence collection", *Digital Investigation* 2/ 2005, 101-119;

118. Kerlin- Karnell K., „The Treaty of Lisbon and the Criminal Law: Anything New Under the Sun?“, *European Journal of Law Reform*, 3/2008, 1-10;

119. Kerr O., „The problem of perspective in Internet Law, Georgetown Law Journal 2/2003, 357-405;

120. Kerr O., „The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution“, *Michigan Law Review* 5/2004, 801-888;

121. Kerr O., „Digital Evidence and the New Criminal Procedure“, *Columbia Law Review* 1/2005, 279-318;

122. Kerr O., „Searches and Seizures in Digital World“, *Harvard Law Review* 2/2005, 531-585;

123. Kerr O., „Enforcing Law Online“, *The University of Chicago Law review* 2/2007, 745-760;

124. Kerr O., „Ex Ante Regulation of Computer Search and Seizure“, *Virginia Law Review* 6/2010, 1241-1293;

125. Kerr O., „The Mosaic Theory of the Fourth Amendment Amendment“, *Michigan Law Review* 3/2012, 311-354;

126. Kierkegaard S. et al., „30 years on -The review of the Council of Europe Data Protection Convention 108“, *Computer Law and security Review* 27/2011, 223-231;

127. Kleinschmidt R., „An International Comparison of ISP's Liabilities for Unlawful Third Party Content“, *International Journal of Law and Information Technology* 4/2010, 332-355;

128. Kleve P., De Mulder R., „Privacy protection and the right to information: In search of a new balance”, *Computer Law& Security Report* 24/2008, 223-232;

129. Koepsell D., „An emerging ontology of jurisdiction in cyberspace”, *Ethics and Information Technology* 2/2000, 99–10;

130. Koops B., „The Internet and its Opportunities for Cybercrime“, Tilburg Law School Legal Studies Research Paper Series 9/2011, 735-754;

131. Kristoff J., „Botnets and Packet Flooding DDoS Attacks on the Domain Name System”, *International Journal of Computer Forensics Science*1/2007, 9-18;

132. Ku Y., Chen Y., Chiu C, „A Proposed Data Mining Approach for Internet Auction Fraud Detection", *Intelligence and Security Informatics Lecture Notes in Computer Science*, 4430/2007, 238-243;

133. Kuner C., „An international legal framework for data protection: Issues and prospects", *Computer Law& Security Review* 25/2009, 307-317;

134. Kuner C., „Data Protection Law and International Jurisdiction on the Internet (Part 1)", *International Journal of Law and Information Technology* 2/2010, 176-193;

135. Kuner C., „Data Protection Law and International Jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology* 3/2010, 227-247;

136. Kurek K., „How to achieve balance between effective crime preventing and protecting privacy of citizens, Online search as a new challenge for e-justice", *Masaryk University Journal of Law and Technology* 3/2009, 377-386;

137. Khan H., Javed M, Khayam SA, Mirza F., „Designing a cluster-based covert channel to evade disk investigation and forensics", *Computers and Security* 1/2011, 35-49;

138. Lathoud B., „Formalization of the Processing of Electronic traces", *International journal of Law, Computers and Technology* 2/2004, 185-192;

139. Laykock G., „New Challenges for Law Enforcement", *European Journal on Criminal Policy and Research* 1/2004, 39-53;

140. Leenes R., Koops B., „Code: Privacy death or saviour?" *International journal of Law, Computers and Technology* 3/2005, 329-340;

141. Lempereur B., Merabti M., Shi Q., „Pypette: A Framework for the Evaluation of Live Digital Forensic Acquisition Techniques", *Proceedings of the Seventh International Workshop on Digital Forensics & Incident Analysis*, 2012, 87-96;

142. Лепојевић Б., Ковачевић-Лепојевић М., „Међународни стандарди у супротстављању компјутерском криминалу и њихова примена у Србији", *Зборник Института за криминолошка и социолошка истраживања* 1-2/2007, 265-291;

143. Lerner J., Mulliga D., „Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home", *Stanford Technology Law Review* 3/2008, 1-20;

144. Leroux O., „Legal Admissibility of Electronic Evidence", *International journal of Law, Computers and Technology* 2/2004, 193-220;

145. Lessig L., „The Path of Cyberlaw", *The Yale Law Journal* 7/1995, 1743-1755;

146. Levi M., Wall D., „Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society* 2/2004,194-220;

147. Litman J., „Information Privacy/Information Property", *Stanford Law Review*, 5/2000, 1283-1313;

148. Losavio M., Adams J., „Gap Analysis: Judicial Experience and Perception of Electronic Evidence", *Journal of Digital Forensic Practice* 1/2006, 13–17;

149. Louwrens G., Von Solms S. H., „A Multi-component View of Digital Forensics," in: Availability, Reliability, and Security, ARES '10 International Conference on, 2010, 647-652;

150. Лукић Т., „Дигитални докази", *Зборник радова Правног факултета у Новом Саду* 2/2012, 177-192;

151. Лукић Т, „Прислушкивање и задржавање телекомуникационих података", *Правни живот* 9/2011, 837-853;

152. Maier B., „How Has the Law Attempted to Tackle the Borderless Nature of the Internet?", *International Journal of Law and Information Technology* 2/2010, 142-175;

153. Mantelero A., „Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution", *European Journal for Law and Technology* 2/2012, 1-6;

154. Marshal A., „Standards, regulation & quality in digital investigations: The state we are in", *Digital Investigation* 8/2011, 141-144;

155. Martini B., Choo K., „An integrated conceptual digital forensic framework for cloud computing", *Digital Investigation* 9/2012, 71-80;

156. Mason S., George E., „Digital evidence and ‘cloud’ computing”, *Computer law & security review* 27/2011, 524-528;

157. McCullagh K., „Protecting ‘privacy’ through control of ‘personal’ data processing: A flawed approach”, *International Review of Law, Computers & Technology* 1–2/ 2009, 13–24;

158. Meyers M., Rogers M., „Computer Forensics: The Need for Standardization and Certification”, *International Journal of Digital Evidence* 2/2004, 1-11;

159. Michelfelder D., „The moral value of informational privacy in cyberspace”, *Ethics and Information Technology* 3/2001, 129-135;

160. Miller A., „Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information -Oriented Society”, *Michigan Law Review* 6/1969, 1089-1246;

161. Милошевић М., „Актуелни проблеми сузбијања компјутерског криминала“, *Наука, безбедност, полиција* 1/2007, 57-74;

162. Miquelon-Weismann M., „The Convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process?” *John Marshall Journal of Computer & Information Law* 2/2005, 329-363;

163. Mislan R, Casey E, Kessler G, „The growing need for on-scene triage of mobile devices”, *Digital Investigation* 6/2010, 112-124;

164. Moiny J., „Are Internet protocol addresses personal data? The fight against online copyright infringement’’, *Computer Law and security Review* 27/2011, 348-361 (380);

165. Moitra S., „Developing policies for cybercrime”, *European Journal of Crime, criminal law and criminal justice,* 13/3, 2005, 436-464;

166. Monterosso F., „Protecting The Children: Challenges That Result In, And Consequences Resulting From, Inconsistent Prosecution Of Child Pornography Cases In A Technical World”, *The Richmond Journal of Law and Technology* 3/2010, 1-23;

167. Monti A., „The Legal Duty of IAPs to Preserve Traffic Data: A Dream or a Nightmare?”, *International Review of Law Computers & Technology* 2/2004, 221-230;

168. Moore R., „To view or not to view: examining the plain view doctrine and digital evidence", *American Journal of Criminal Justice* 1/2004, 55-73;

169. Mulligan C., „Perfect Enforcement Of Law: When To Limit And When To Use Technology", *The Richmond Journal of Law and Technology* 4/2008, 1-49;

170. Murdoch W., „Regulation of State Surveillance of the Internet human rights infringement or e-security mechanism?", *International Journal of Electronic Security and Digital Forensics*, 1/ 2007, 42-54;

171. Murdoch W., „The Evolution of Legal Regulation of the Internet to Address Terrorism and Other Crimes", *The Journal of South African Law* 1/2007, 494-512;

172. McIntyre T.J., „Data retention in Ireland: Privacy, policy and proportionality", *Computer law & security report* 24/2008, 326–334;

173. McIntyre T.J., „Blocking child pornography on the Internet: European Union Developments", *International Review of Law, Computers & Technology* 3/2010, 209–221;

174. Николић В., „Откривање и праћење компјутерског криминала", *Безбедност* 2/2004, 252-276;

175. Novikoviene L., Bileviciute E., „Application of IT Examination in Investigation of Crimes on Safety of Electronic Data and Information Systems", *Jurisprudence* 1/2010, 317-329;

176. Nogueira J., „Mobile Intelligent Agents to Fight Cyber Intrusions", *International Journal of Forensic Computer Science* 1/2006, 28-32;

177. Nogueira J., „Ontology for Complex Mission Scenarios in Forensic Computing", *The International Journal of Forensic Computer Science* 1/2008, 42-50;

178. Nogueira J., Celestino J., „Autonomic Forensics a New Frontier to Computer Crime Investigation Management", *International Journal of Forensic Computer Science* 1/2009, 29-41;

179. Orebaugh A., „Proactive forensics" *Journal of Digital Forensic Practice* 1/2006, 37-41;

180. O'Reilly C., „Finding jurisdiction to regulate Google and the Internet", *European Journal of Law and Technology* 1/2011, 1-13;

181. Ohm P, „Massive Hard Drives, General Warrants, and the Power of Magistrate Judges“, *Virginia Law Review* 1/2011, 97-130;

182. Петровић С., „Дилема: сајбер или кибер“, *Страни правни живот* 2/2012, 368-378;

183. Pisarić M., „Data protection within police and judicial cooperation in EU“, *European Legal Studies and Research*, 2011, 441-447;

184. Писарић М., „Унапређење размене података у оквиру прекограничне полицијске и правосудне сарадње у кривичним стварима на нивоу Европске уније - "Прумски процес", *Зборник радова Правног факултета у Новом Саду* 3/ 2010, 557-572;

185. Писарић М., „Мера хитног чувања ускладиштених рачунарских података“, *Зборник радова Правног факултета у Новом Саду* 1/2014, 229-251;

186. Pozen D., „The Mozaic theory, national security and the freedom of national act“, *The Yale Law Journal* 1/2005, 628-679;

187. Polcak R., „Aims, methods and achievements in European data protection“, International Review of Law, Computers & Technology, 3/ 2009, 179–182;

188. Posner R., „Privacy, Surveillance, and Law“, *The University of Chicago Law Review* 1/2008, 245-260;

189. Poulett Y., „The Fight against Crime and/or the Protection of Privacy: A Thorny Debate!“, *International Law Computers& Technology Review* 2/ 2004, 251-273;

190. Poullet Y., „Data protection legislation: What is at stake for our society and democracy“, *Computer Law and security review* 25/2009, 211-226;

191. Pocar F., „New challenges for international rules against cyber crime“, *European Journal on Criminal Policy and Research* 1/2004, 27-37;

192. Pradillo J., „Fighting against cybercrime in Europe: the admissibility of remote searches in Spain“, *European journal of crime, criminal law and criminal justice*, 19/2011, 363–395;

193. Прља Д., Рељановић М., „Високотехнолошки криминал - упоредна искуства“, *Страни правни живот* 3/2009, 161-184;

194. Quirchmayr G., „Internet, WWW and beyond“, *Information Technology and Lawyers* 1/2006, 137-163;

195. Ранђеловић Д., Богдановић Т., „Алати за дигиталну форензику“, *Наука, безбедност, полиција* 2/2010, 25-47;

196. Rashbaum K. et al., „Admissibility of non-U.S. Electronic Evidence“, *The Richmond Journal of Law and Technology* 5/2011, 1-76;

197. Rahman R., „The legal measure against Denial of Service (DoS) attacks adopted by the United Kingdom legislature: should Malaysia follow suit?“, *International Journal of Law and Information Technology* 2/2012, 85-101;

198. Regan F., „Response to Bennett: Also in Defense of Privacy“, *Surveillance & Society* 4/2011, 497-499;

199. Reid A., „Online protection of the child within Europe“, *International Review of Law, Computers & Technology* 3/2009, 217–230;

200. Reidenberg J., „Technology and Internet Jurisdiction“, University of Pennsylvania Law Review, 6/2005, 1951-1974;

201. Reith M., Carr C, Gunsch G., „An Examination of Digital Forensic Models“, *International Journal of Digital Evidence* 3/2002, 1-12;

202. Rekhis S., Boudriga N., „A Hierarchical Visibility theory for formal digital investigation of anti-forensic attacks“, *Computers & security* 31/2012, 967-982;

203. Рељановић М., „Високотехнолошки криминал - појам, регулатива, искуства“, *Страни правни живот* 3/2007, 75-98;

204. Richard G., Roussev V., „Next-generation digital forensics“, *Communications of the ACM* 2 /2006, 76-80;

205. Richard G., Roussev V., Marziale L. „Forensic discovery auditing of digital evidence containers“, *Digital Investigation* 4/2007, 88 – 97;

206. Ritchie D., „Is it possible to define ‘privacies’ within the law? Reflections on the ‘securitisation’ debate and the interception of communications”, *International Review of Law, Computers & Technology* 1–2/2009, 25–34;

207. Roberts J., „A Practitioner's Primer on Computer-Generated Evidence“, *The University of Chicago Law Review* 2 /1974, 254-280;

208. Rowlingson R.., „A Ten Step Process for Forensic Readiness“, *International Journal of Digital Evidence* 3/2004, 1-28;

209. Rogers M. K. et al, “Computer Forensic Field Triage Process Model”, *Conference on Digital Forensics, Security and Law*, 2006, 27-40;

210. Ruibin G., Yun Z., „Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework“, *International Journal of Digital Evidence* 1/2005, 1-13;

211. Rustad M., „Private Enforcement of Cybercrime on the Electronic Frontier“, *Southern California Interdisciplinary Law Journal* 11/2001, 63-116;

212. Saylor J., „Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches“, *Fordham Law Review* 6/ 2011, 2809-2858;

213. Svantesson D., „Privacy, Internet and Transborder Data Flows“, *Masaryk University Law and Technology journal* 1/2010, 1-20;

214. Swire P., „Katz Is Dead. Long Live Katz“, *Michigan law review* 5/2004, 904-932;

215. Seitz N., „Transborder search: a new perspective in law enforcement?“, *Yale journal of law and technology* 7/ 2005, 22-50;

216. Sieber U., „Criminal liability for the transfer of the data in international computer network”, *European Journal of Crime, Criminal Law and Criminal Justice* 2/1997, 134-143;

217. Simpson B, „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 , 21-50;

218. Singh M., „Cybercrime Convention and transborder Criminality“, *Masaryk University Journal of Law and Technology* 1/2007, 53-66;

219. Smith P., „Much a do about mosaics: how original principles apply to evolving technology *in United States v. Jones”,* North Carolina Journal of Law and Technology 2/ 2013, 557- 598 ;

220. Soghoian C., „Caught in the cloud: privacy,encryption, and Government back doors in the Web 2.0 era“, *Journal on communication and high technology law* 2/2010, 360-424;

221. Solove D., „Privacy and Power: Computer Databases and Metaphors for Information Privacy“, *Stanford Law Review* 6/2001,1393-1462;

222. Soma J. et al, „Balance of Privacy vs. Security:a historical perspective of the USA Patriot Act”, *Rutgers Computer and Technology Law Journal* 4/2005, 285-346;

223. Sommer P., „The Future for the Policing the Cybercrime“, *Computer Fraud & Security* 1/2004, 8-12;

224. Sommer P., „Forensic science standards in fast-changing environments“, *Science and Justice* 1/2010, 12-17;

225. Sommer P., „Certification, registration and assessment of digital forensic experts: The UK experience“, *Digital Investigation* 8/2011, 98-105;

226. Спасић В., „Сајбер криминал у светлу нове регулативе“, *Правни живот* 9/2005, 947-964;

227. Спасић В., „Актуелна питања у области сајбер криминала“, *Билтен судске праксе Врховног суда Србије* 1/2006, 107-130;

228. Stalla-Bourdillon S., „The flip side of ISP’s liability regimes: The ambiguous protection of fundamental rights and liberties in private digital spaces“, *Computer Law & Security Review* 5/2010, 492–501;

229. Stalla-Bourdillon S., „Chilling ISPs. when private regulators act without adequate public framework“, *Computer Law and security Review* 26/2010, 290-297;

230. Stephenson P., „Modeling of post-incident root cause analysis“, *International Journal of Digital Evidence* 2/2003, 1-16;

231. Stinsman J, „Computers and Searches, Rethinking the Applicability of the Plain View Doctrine“, *Temple Law Review* 4/2011, 1097-1120;

232. Stol W.Ph. et al., „Governmental filtering of websites: the Dutch case“, *Computer law & security review* 25/2009, 251-262;

233. Strossen N., „Cybercrime v. Cyberliberties“, *International journal of Law, Computers and Technology* 1/2000, 11-24;

234. Stüttgen J., Cohen M., „Anti-forensic resilient memory acquisition”, Digital Investigation 10/ 2013, 105–115;

235. Sullivan C., „Digital identity, privacy and the right to identity in the United States of America“, *Computer Law and Security Review* 29/2013, 348-358;

236. Shields C. et al., „A system for the proactive, continuous, and efficient collection of digital forensic evidence“, *Digital Investigation* 8/2011, 3-13;

237. Schartum D. W, „Designing and Formulating Data Protection Laws“, *International Journal of Law and Information Technology*1/2008, 1-27;

238. Schatz B, „BodySnatcher: Towards reliable volatile memory acquisition by software“, *Digital Investigation* 4/2007, 126-134;

239. Schermer B., „The limits of privacy in automated profiling and data mining“, *Computer Law and security Review* 27/2011, 45-52;

240. Schmitknecht D., „Building FBI computer forensics capacity: one lab at a time“, Digital Investigation 1/2004, 177-182;

241. Schulz T., „Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface“, *The European Journal of International Law* 4/2008, 799-839;

242. Schumacher P., „Fighting illegal Internet content - May access providers be required to ban foreign websites? A recent German approach“, *International Journal of Communications Law and Policy*, 8/2004, 1- 22;

243. Schwerha J., „Cybercrime: Legal Standards Governing the Collection of Digital Evidence“, *Information Systems Frontiers* 2/2004, 133-151;

244. Talleur T., „Digital evidence: moral challenge“, *International Journal of Digital Evidence* 1/2002,1-16;

245. Taylor M. et al, „Digital evidence from peer-to-peer networks“, Computer law & security review 27/2011, 647-652;

246. Taylor M. et al., „Digital evidence in cloud computing systems“, *Computer Law& security review* 26/2010, 304-308;

247. Tikk E., Kaska K., „Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons”, *Proceedings of the 9th European Conference of Information Warfare and Security – Thessaloniki*, 2010, 288-295;

248. Toeniskoetter S., „Preventing A Modern Panopticon: Law Enforcement Acquisition Of Real-Time Cellular Tracking Data“, *The Richmond Journal of Law and Technology* 4/2007, 1-49;

249. Trepel S., „Digital Searches, General Warrants, And The Case For The Courts," *Yale Journal of Law and Technology* 10/2008, 122-150;

250. Урошевић, В. Уљанов, С. Вуковић, Р. „Полиција и високотехнолошки криминал – Примери из праксе и проблеми у раду МУП-а Републике Србије“, ZITEH 2006, 338-346;

251. Урошевић В., Којадиновић И., „Правни аспекти несталних података као доказа прикупљених приликом он лине анализе активног рачунара“, *Криминалистичко форензичка истраживања* 1/ 2011, 520-529;

252. Yusoff Y., Ismail R., Hassan Z., „Common phases of computer forensics investigation models“, *International Journal of Computer Science & Information Technology* 3/2011, 17-31;

253. Fafinsky S., „The UK Legislative Position on Cybercrime: A 20-Year Retrospective“, *The Journal of Internet Law* 10/2009, 1-12;

254. Feiler L., „The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection", *European Journal of Law and Technology* 3/2010, 1-34;

255. Flaglien A., „Storage and exchange formats for digital evidence“, *Digital Investigation* 8/2011, 122-128;

256. Flint D., „Law shaping technology: Technology shaping the law“, *International Review of Law, Computers & Technology* 1–2/ 2009, 5–11;

257. Foggetti N., „Transnational Cyber crime, differences between national laws and developments of european legislation: by repression?“, *Masaryk University journal of Law and technology* 2/2008, 31-45;

258. Hall G., „Toward Defining the Intersection of Forensics and Information Technology“, *International Journal of Digital Evidence* l/2005, 1-20;

259. Hannan M., „To revisit: What is forensic computing?“, *Proceedings of the Second Australian Computer, Network and Information Forensics Conference*, 2004, 103–111;

260. Hargreaves C., Chivers H., „Recovery of encryption keys from memory using a linear Scan“, *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. IEEE Computer Society*, 1369–1376;

261. Harris R., „Arriving at an anti-forensics consensus: examining how to define and control the anti-forensics problem, *Digital Investigation* 3/2006, 44–49;

262. Harrison W. et al, „A Lessons Learned Repository for Computer Forensics", *International Journal of Digital Evidence* 3/2002, 1-9;

263. Hay B, Bishop M, Nance K, „Live Analysis: Progress and Challenges", *IEEE Security and Privacy* 2/2009, 30–37;

264. Heissl G., „Jurisdiction for Human Rights Violations on the Internet", *European Journal of Law and Technology* 1/2011, 1-15;

265. Hilbert M., „How to Measure "How Much Information"? Theoretical, Methodological, and Statistical Challenges for the Social Sciences", *International Journal of Communication* 6/2012, 1042–1055;

266. Hildebrandt M., Tielemans L., „Data protection by design and technology neutral law", *Computer Law and Security Review* 29/2013, 509-521;

267. Hoey A., „Techno-Cops: Information Technology and Law Enforcement", *International Journal of Law and Information Technology*, l/1998, 69-90;

268. Hopkins S., „Cybercrime Convention: a positive beginning to a long road ahead", *The Journal of High technology Law* l/2002, 101-121;

269. Hornung G., Schnabel C., „Data protection in Germany I: The population census decision and the right to informational self-determination", *Computer Law&Security Review* 25/2009, 84-88;

270. Hosmer C., „Proving the Integrity of Digital Evidence with Time", I*nternational Journal of Digital Evidence* 1/2002, 1-12;

271. Huey L., Rosenberg R., „Watching the Web: Thoughts on expanding police surveillance opportunities under the Cyber-crime Convention", *Canadian Journal of Criminology and Criminal Justice* 10/2004, 597-606;

272. Hunter D., „Cyberspace as place and the Tragedy of the Digital Anticommons", *California Law Review* 2/2003, 439-519;

273. Hunton P., „The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model", *Computer Law & Security Report* 25/2009, 528-535;

274. Hunton P., „Cybercrime and security: A new model of Law enforcement", *Investigation* 4/2010, 385-395;

275. Hunton P., „A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment", *Digital Investigation* 7/2011, 105-113;

276. Hunton P., „The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation", *Computer Law and security Review* 2 7 / 2 0 1 1 , 6 1 - 6 7;

277. Hunton P., „Data attack of the cybercriminal: Investigating the digital currency of cybercrime", *Computer Law and security Review* 28/2012, 201-207;

278. Cade N., „An adaptive approach for an evolving crime: the case for an International cyber court and penal code", *Brooklyn Journal of International Law* 37/2012, 1139-1175;

279. Calderoni F., „The European legal framework on cybercrime: striving for an effective implementation", *Crime, Law and Social Change* 54/2010, 339-357;

280. Cangemi D., „Procedural Law Provisions of the Council of Europe Convention on Cybercrime, international review of law computers & technology", 2/ 2004, 165–171;

281. Cannatacia J., Mifsud J., „The end of the purpose-specification principle in data protection?", *International Review of Law, Computers & Technology* 1/ 2010, 101–117;

282. Carrier B., „Defining digital forensic examination and analysis tools using abstraction layers", *International Journal of Digital Evidence* 1/2003, 1-12;

283. Carrier B., „Risks of live digital forensic analysis", *Communications of the ACM* 2/2006, 56–61;

284. Carrier B, Grand J., „A hardware-based memory acquisition procedure for digital investigations", Digital Investigation 1/2004, 50–60;

285. Carrier B., Spafford, E., „Getting Physical with the Digital Investigation Process", *International Journal of Digital Evidence*, 2/2003, 1-20;

286. Carrier B., Spafford E., „Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence", *Digital Forensic Research Workshop*, 2005, 1-10;

287. Carrier B, Spafford E., „Categories of digital investigation analysis techniques based on the computer history model“, *Digital Investigation 3*/2006, 121-130;

288. Casey E, Ferraro M, Nguyen L. „Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence“, *Journal of Forensic Sciences* 6/2009,1353-1364;

289. Casey E. et al, „The growing impact of full disk encryption on digital forensics”, *Digital Investigation* 2/2011, 129–134;

290. Cassim F., „Formulating specialized legislation to address the growing spectre of cybercrime: a comparative study“, *Potchefstroom electronic law journal*, 12/2009, 35-79;

291. Castellano P, „A Test for Data Protection Rights Effectiveness: Charting the Future of the ‘‘Right to Be Forgotten’’ under European Law’, *The Colombia Journal of European Law Online* 1/2012, 1-5;

292. Цветковић З., „Компјутерски криминал“, *Бранич* 2-3/2001, 5-11;

293. Ciardhuáin S., „An Extended Model of Cybercrime Investigations“, *International Journal of Digital Evidence* 1/2004/, 1-22;

294. Clarke R., „Information Technology and Dataveillance“, *Communications of the ACM* 5/1988, 498-512;

295. Clarke R., „Technology, Criminology and Crime Science“, *European Journal on Criminal Policy and Research*, 1/2004, 55-63;

296. Clarke R., „Privacy impact assessment: Its origins and development”, *Computer Law and Security Review* 2/2009, 123-135;

297. Clough J., „Data theft? Cybercrime and the increasing criminalization of access to data“, *Criminal Law Forum* 2/2011, 145–170;

298. Colb S. „The Qualitative Dimension of Fourth Amendment ‘‘Reasonableness’’, *Columbia Law Review* 3/1998, 1642-1666;

299. Colb S., „A World without Privacy: Why Property Does Not Define the Limits of the Right against Unreasonable Searches and Seizures“, *Michigan Law Review* 5/2004, 889-903;

300. Cottim A., „Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime", *European Journal of Legal Studies* 3/2010, 1-23;

301. Chaikin D., „Network investigation of cyber attacks: the limits of digital evidence", *Crime, Law and Social Change* 4-5/2006, 239-256;

302. Chang R., „Why the plain view doctrine should not apply to digital evidence", *Suffolk journal of trial and appellate advocacy* 1/2007, 31-67;

303. Chasky C., „Who's At the Keyboard? Authorship Attribution in Digital Evidence Investigations", *International Journal of Digital Evidence* 1/2005, 1-14;

304. Chatterjee B., „New but not improved: revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions", *International Journal of Law and Information Technology* 3/2011, 264-284;

305. Chedraui, A., „Analysis of the Exclusion of Evidence Obtained in Violation of Human Rights in Light of the Jurisprudence of the European Court of Human Rights", *Tilburg Law Review* 2 /2011, 205-234;

306. Chen P., „Discovering investigation clues through mining criminal databases", *Intelligence and Security Informatics Studies in Computational Intelligence* 135/2008, 173-198;

307. Chung H. et al., „Digital forensic investigation of cloud storage services", *Digital Investigation* 9/2012, 81-95.

2. ПРОПИСИ

2.1. Прописи Републике Србије

1. Устав Републике Србије („Сл. гласник РС", бр. 98/2006);

2. Кривични законик („Сл. гласник РС", бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014);

3. Законик о кривичном поступку („Сл. гласник РС", бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014);

4. Закон о изменама и допунама Законика о кривичном поступку („Сл. гласник РС", бр. 55/2014);

5. Закон о јавном тужилаштву („Сл. гласник РС“, бр. 116/2008, 104/2009, 101/2010, 78/2011 – др.закон, 101/2011, 38/2012 – одлука УС, 121/2012, 101/2013, 111/2014 – одлука УС и 117/2014);

6. Закон о организацији и надлежности државних органа у сузбијању организованог криминала, корупције и других посебно тешких кривичних дела („Сл. гласник РС“, бр. 42/2002, 27/2003, 39/2003, 67/2003, 29/2004, 58/2004 - др. закон, 45/2005, 61/2005, 72/2009, 72/2011 - др. закон, 101/2011 - др. закон и 32/2013);

7. Закон о организацији и надлежности државних органа у поступку против учинилаца ратних злочина („Сл. гласник РС“, бр. 67/2003);

8. Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Сл. гласник РС“, бр. 61/2005 и 104/2009);

9. Закон о судским вештацима („Сл. гласник РС“, бр. 44/2010);

10. Закон о међународној правној помоћи о кривичним стварима („Сл. гласник РС“, бр. 20/2009);

11. Закон о електронским комуникацијама („Сл. гласник РС“, бр. 44/2010, 60/2013 – одлука Уставног суда и 62/2014);

12. Закон о заштити података о личности („Сл. гласник РС“, бр. 97/2008, 104/2009 - др. закон, 68/2012 - одлука УС и 107/2012);

13. Закон о тајности података („Сл.гласник РС“, бр. 104/2009);

14. Закон о потврђивању Конвенције о високотехнолошком криминалу („Сл. гласник РС“, бр.19/2009);

15. Закон о потврђивању Конвенције о заштити лица у односу на аутоматску обраду личних података („Сл. лист СРЈ - Међународни уговори", бр. 1/92, "Сл. лист СЦГ - Међународни уговори“, бр. 11/2005 - др. закон и "Сл. гласник РС - Међународни уговори", бр. 98/2008 - др. закон и 12/2010);

16. Закон о о потврђивању додатног протокола уз Конвенцију о заштити лица у односу на аутоматску обраду личних података, у вези са надзорним органима и прекограничним протоком података („Сл. гласник РС - Међународни уговори“, бр. 98/2008);

17. Закон о потврђивању Европске Конвенције о узајамној правној помоћи у кривичним стварима, са додатним протоколом („Сл. лист СРЈ-Међународни уговори“, бр.10/2001);

18. Закон о потврђивању Европске конвенције о екстрадицији са додатним протоколима („Сл. лист СРЈ – Међународни уговори“, бр. 10/2001).

2.2. Прописи међународних организација

1. Charter of United Nations, http://www.un.org/en/documents/charter/;
2. United Nations Millennium Declaration, 2000, http://www.un.org/millennium/declaration/ares552e.pdf;
3. United Nations Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990), http://www.un.org/documents/ga/res/45/a45r095.htm;
4. United Nations Resolution L13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet, http://geneva.usmission.gov/2012/07/05/Internet-resolution.
5. ECOSOC Resolution 2007/20 International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related crime http://www.un.org/en/ecosoc/docs/2007/resolution%202007-20.pdf;
6. ITU Resolution: Combating the criminal misuse of information technologies, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf;
7. ITU Resolution: Combating the criminal misuse of information technologies, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf;
8. OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, 1990, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm;

9. Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 005, 1950, http://conventions.coe.int/treaty/en/treaties/html/005.htm;

10. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm;

11. Council of Europe Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001, http://conventions.coe.int/Treaty/EN/Treaties/HTML/181.htm;

12. Council of Europe Convention No. 185 on cybercrime, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm;

13. Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm;

14. Council of Europe Recommendation No. R. (89) 9, Computer-related crime: https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2;

15. Council of Europe Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995, https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2;.

16. Council of Europe Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, https://wcd.coe.int/ViewDoc.jsp?id=849061;

17. The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:FULL:EN:PDF;

18. Charter of Fundamental Rights of the European Union, http://www.europarl.europa.eu/charter/pdf/text_en.pdf;

19. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01): http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:EN:PDF

20. Directive 91/250/EEC on legal protection of computer programs, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31991L0250;

21. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

22. Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:en:PDF;

23. Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000D0520;

24. 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);

25. Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF
;

26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML;

27. Framework Decision 2004/68/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography, OJ L 13, 20.1.2004, p.44; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004F0068:EN:NOT;

28. Framework Decision 2005/222/JHA on attacks against information systems, Official Journal of the European Union, L 69/67, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF;

29. Council Decision 2008/616/JHA f 23 June 2008 n the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008D0616.

30. Council Decision of 6 April 2009 establishing the European Police Office, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32009D0371

31. Council Decision on the strengthening of Eurojust and amending Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1429091092084&uri=CELEX:52008AP0384

32. Recommendation N° R (87) 15 regulating the use of personal data in the police sector), http://ec.europa.eu/justice/data-protection/law/files/coe-fra-rpt-2670-en-471.pdf;

33. Resolution L13 on the Promotion, Protection and Enjoyment of Human Rights on the Internet, http://geneva.usmission.gov/2012/07/05/Internet-resolution..

2.3. **Прописи појединих држава**

1. Anti-Terrorism, Crime & Security Act (ATCS) 2001, http://www.legislation.gov.uk/ukpga/2001/24/contents;
2. Wetboek van Strafvordering, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html;
3. Gesetz über die internationale Rechtshilfe in Strafsachen, http://www.gesetze-im-internet.de/englisch_irg/englisch_irg.html.
4. Законик о кривичном поступку Републике Црне Горе ("Службени лист ЦГ", бр. 57/2009, 49/2010, 47/2014 - Одлука УС ЦГ, 2/2015 - Одлука УС ЦГ и 35/2015);
5. Закон о кривичном поступку Републике Српске (Сл. гласник РС 53/2012)
6. Zakon o kaznenom postupku Republike Hrvatske (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13).
7. Electronic Communication Privacy Act 1986, Pub. L. No. 99-508, 100 Stat. 1848, https://it.ojp.gov/default.aspx?area=privacy&page=1285
8. Electronic Communication Privacy Act, https://it.ojp.gov/default.aspx?area=privacy&page=1285
9. Kriminālprocesa likum, http://www.knab.gov.lv/uploads/eng/criminal_procedure_law_2014.pdf.
10. Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf;
11. Ley 25/2007 de conservación de datos comunicaciones electrónicas, http://www.boe.es/boe_gallego/dias/2007/10/23/pdfs/A03094-03100.pdf.
12. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725:
13. Lov om rettergangsmaten i straffesaker (Straffeprosessloven) 53/2006, http://www.ub.uio.no/ujur/ulovdata/lov-19810522-025-eng.pdf.

14. Pakkokeinolaki 806/2011, http://www.finlex.fi/fi/laki/kaannokset/2011/en20110806.pdf.

15. Police and Criminal Evidence Act 1984, http://www.legislation.gov.uk/ukpga/1984/60.

16. Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, http://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf.

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

18. Strafprozessordnung,http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0430.

19. Testo del decreto-legge 23 maggio 2008, n. 92 (in Gazzetta Ufficiale - serie generale - n. 122 del 26 maggio 2008), coordinato con la legge di conversione 24 luglio 2008, n. 125 (in questa stessa Gazzetta Ufficiale alla pag. 6), recante: «Misure urgenti in materia di sicurezza pubblica», http://www.altalex.com/index.php?idnot=41643.

20. The U.S. Federal Criminal Code, http://www.law.cornell.edu/uscode/text/18/2703.

21. Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 , http://www.americanlaw.com/patriotact.html.

22. USA Electronic Communication Privacy Act 1986, Pub. L. No. 99-508, 100 Stat. 1848, https://it.ojp.gov/default.aspx?area=privacy&page=1285.

23. USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 , http://www.americanlaw.com/patriotact.html.

24. Federal Rules of Criminal Procedure, http://www.law.cornell.edu/rules/frcrmp.

25. Foreign Intelligence Surveillance Act, 1978, https://www.law.cornell.edu/uscode/text/50/chapter-36.

26. Code de procédure pénale, http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&dateTexte=20051213;

27. Code of practice for searches of premises by police officers and the seizure of property found by police officers on persons or premises, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117591/pace-code-b-2011.pdf

28. 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.

29. 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.

3. СУДСКА ПРАКСА

3.1. **Коришћене базе судске праксе:**

1. Судска пракса Уставног суда Србије: http://www.ustavni.sud.rs/page/jurisprudence/35/.
2. Судска пракса Европског суда за људска права: http://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=
3. Судска пракса Суда правде Европске уније: http://curia.europa.eu/juris/recherche.jsf.
4. Судска пракса Уставног суда Немачке: http://www.bundesverfassungsgericht.de/SiteGlobals/Forms/Suche/EN/Entscheidungensuche_Formular.html?language_=en.
5. Судска пракса Врховног суда САД: http://www.supremecourt.gov/case_documents.aspx

3.2. Попис цитираних одлука домаћих судова

1. Пресуда Вишег суда у Београду, *Кв.По1 бр. 601/13* од 13. 08.2013.године

2. Пресуда Апелационог суда у Београду Кж. По3 5/2014 од 19.02.2014. године

3. Пресуда Апелационог суда у Београду Кж. По3 8/2015 од 11.06.2015. године

4. Пресуда Врховног суда Србије Кж. Кж. бр. 1547/04 од 22. 11.2004. године

5. Пресуда Врховног суда Србије Кж. Кж1. бр. 493/05 од 8.06. 2005. године

6. Пресуда Врховног суда Србије Кж. 1309/06 од 11. 09.2006. и пресуда Окружног суда у Јагодини К. 185/05 од 27. 01. 2006. године

7. Пресуда Врховног суда Србије Кзз 280/2015 од 26.03.2015. године

8. Решење Апелационог суда у Београду Кж. 1 бр. 3201/13 од 23. 01. 2014. године и решење Вишег суда у Београду К. Бр. 61/11 од 19.12.2012. године

9. Решење Апелационог суда у Београду Кж2. 3000/11 од 13. 09. 2011. и решење Вишег суда у Београду К. 1875/10 од 7. 07 2011 године

10. Решење већа Вишег суда у Београду – Посебног одељења Кв-По1. 682/12 од 25. 10.2012. и решење председника већа Вишег суда у Београду – Посебног одељења К-По1. 302/10 од 5. 10.2012. године

11. Решење Врховног суда Србије Кж. 1060/05 од 19. 09. 2005. и пресуда Окружног суда у Крушевцу К. 153/04 од 14. 04. 2005. године

12. Решење Врховног суда Србије Кж. 1876/03 од 26. јануара 2004. и пресуда Окружног суда у Београду К. 52/03 од 11. 07. 2003. године

13. Решење Врховног суда Србије Кж. 2253/05 од 30. 01. 2006. и пресуда Окружног суда у Зрењанину К. 89/05 од 19. С09. 2005. Године

14. Одлука Уставног суда Републике Србије, ИУз 149/2008 од 28.05.2009.

3.3. Попис цитираних одлука Европског суда за људска права

1. Пресуда у предмету *Amman v. Switzerland, (2000-II).*
2. Пресуда у предмету *August v. the United Kingdom No. 36505/02*;

3. Пресуда у предмету *Gillow v. The United Kingdom, (1986).*
4. Пресуда у предмету *K.U. v. Finland (No.2872/02*).
5. Пресуда у предмету *Kennedy v United Kingdom (No. 26839/05*)
6. Пресуда у предмету *Klass and Others v Germany 28 (1978).*
7. Пресуда у предмету *Kruslin v France A 176 (1990);*
8. Пресуда у предмету *Leander v. Sweden* (*No* 116/1987).
9. Пресуда у предмету *Liberty and Others v United Kingdom Application No. 58243/00*
10. Пресуда у предмету *Lingens v. Austria, (1986).*
11. Пресуда у предмету *Norris v. Ireland, (198)* и *Dudgeon v. The United Kingdom (1988).*
12. Пресуда у предмету *Ollson v. Sweden, (1988).*
13. Пресуда у предмету *P.G. and J.H. v. the United Kingdom* (*No* 44787/98);
14. Пресуда у предмету *Peck v United Kingdom 2003-I.*
15. Пресуда у предмету *Rotaru v Romania* (*No* 46/2000).
16. Пресуда у предмету *S. and Marper v United Kingdom* (*Nos* 30562/04, 30566/04).
17. Пресуда у предмету *Saunders v United Kingdom1996-VI; 23 EHRR 313.*
18. Пресуда у предмету *Sciacca v. Italy* (*No.* 50774/99);
19. Пресуда у предмету *Sunday Times v. the United Kingdom, (1979).*
20. Пресуда у предмету *Timurtas v Turkey 2000-VI;*
21. Пресуда у предмету *Uzun v. Germany* (*No* 35623/05)
22. Пресуда у предмету *Von Hannover v Germany 2004-VI;*
23. Пресуда у предмету *Weber and Saravia v Germany 2006-XI*
24. Пресуда у предмету *X andY v The Netherlands A 91 (1985*);

4. ИЗВОРИ СА ИНТЕРНЕТА

4.1. **Публикације:**

1. ACPO, Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.npcc.police.uk/;

2. Article 29 Data Protection Working Party, Opinion on Cloud Computing, 2012, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20120701_wp_196_cloud_computing_en.pdf;

3. Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime, 2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_10_Assess_report_v30_public.pdf;

4. Association of Chief Police Officers: Good Practice Guide for Computer-Based electronic Evidence , 2012, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf;

5. Attitudes on Data Protection and Electronic Identity in the European Union, http://ec.europa.eu/public_opinion/archives/eb_special_359_340_en.htm;

6. BS 10008:2008 " Evidential weight & legal admissibility of electronic information", http://shop.bsigroup.com/Browse-By-Subject/ICT/Legal-Admissibility/;

7. CERT Training and Education Handbook, First Responders Guide to Computer Forensics, 2005, http://www.sei.cmu.edu/reports/05hb001.pdf;

8. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf;

9. Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal? http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf;

10. Cloud computing and its implication on data protection, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp;

11. Cloud Computing and privacy, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp;

12. Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf;

13. COE: Transborder access and jurisdiction: What are the options?2012, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf;

14. Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, 2006, http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf;

15. Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf;;

16. Commission Communication: A strategy on the external dimension of the area of freedom, security and justice, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l16014_en.htm;

17. Commission Communication: A strategy on the external dimension of the area of freedom, security and justice, http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l16014_en.htm;

18. Commission Communication: Building an open and secure Europe, 2014, http://europa.eu/pol/pdf/flipbook/en/borders_and_security_en.pdf:

19. Commission Communication: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime, http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf;

20. Commission Communication: Towards a general policy on the fight against cyber crime, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF;

21. Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, „Strengthening Forensic Science in the United States: A Path Forward“, 2009, http://www.nap.edu/catalog/12589.html;

22. Communication Security Research : The Next Steps, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0590:FIN:EN:PDF;

23. Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf;

24. Council of Europe Ad hoc Committee on Data Protection, http://www.coe.int/t/dghl/standardsetting/dataprotection/Cahdata_en.asp;

25. Council of Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp;

26. Council of Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges, 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp;

27. Cybercrime Model Laws, 2014, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Reports/2014_Zahid/3021_model_law_study_v15.pdf;

28. Cybercrime: current threats and trends, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp;

29. Cybercrime: where we are and where could, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Update/cyber_octopus_PS_alexander_mosaic1e.pdf;

30. DFRWS technical report: A Road Map for Digital Forensic Research, New York 2001, http://www.dfrws.org/2001/dfrws-rm-final.pdf**;**

31. Digital Univers Study, 2011, http://www.emc.com/digital_universe;

32. European Committee on Crime Problems, Final Report, http://www.oas.org/juridico/english/89-9&final%20Report.pdf;

33. European Network and Information Security Agency, The Right to Be Forgotten: Between Expectations and Practice 2011, www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten;

34. European Union: Council conclusions on a concerted work strategy and practical measures against cybercrime, http://www.eu2008.fr/webdav/site/PFUE/shared/import/1127_JAI/Conclusions/JHA_Council_conclusions_Cybercrime_EN.pdf;

35. Explanatory Report of the Convention on Cybercrime (185), No. 10, http://conventions.coe.int;

36. Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice, Office of Justice Programs National Institute of Justice, http://www.ojp.usdoj.gov/nij;

37. Forensic Science on Trial, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf;

38. Gareth S., Website Location: Cyberspace vs. Geographic Space, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/Gareth%20Samson%20Website%20Location.pdf;

39. Good Practice and Advice Guide for Managers of e-Crime Investigation, http://www.met.police.uk/pceu/documents/managers_guide_v1.9.pdf;

40. Good Practice Guide for Computer-Based Electronic Evidence, http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

41. Guidelines for Evidence Collection and Archiving, http://www.faqs.org/rfcs/rfc3227.html;

42. Guidelines for the coopeation between law enforcement and Internet servise providers against cybercrime, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf;

43. Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, Study for the European Commission Directorate-General Information Society (2002), http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf;

44. ICAPO, Computer Usage For Child Abuse Investigators, http://www.vrhome.com/icapo/pedo/webax/index.htm.

45. ILAC-G19 "Guidelines for Forensic Science Laboratories", http://ilac.org/news/ilac-g19082014-published/;

46. International Organization on Computer Evidence, Guidelines for Best Practice in the Forensic Examination of Digital Technology, Digital Evidence Standards Working Group, 2002, http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf;

47. Interparliamentary Committee Meeting, "The reform of the EU Data Protection framework – Building trust in a digital and global world, 2012, http://www.europarl.europa.eu/document/activities/cont/201210/20121003ATT52831/20121003ATT52831EN.pdf;

48. ISO/IEC 17025 :2005, https://www.iso.org/obp/ui/#!iso:std:39883:en,

49. ISO/IEC 27035 "Information security incident management", http://www.iso27001security.com/html/27035.html;

50. ISO/IEC 27037 "Guidelines for identification, collection, acquisition, and preservation of digital evidence", http://www.iso.org/iso/catalogue_detail?csnumber=44381;

51. ISO/IEC 27041 „Guidelines on assuring suitability and adequacy of incident investigative methods", http://www.iso27001security.com/html/27041.html);

52. ISO/IEC 27042 „Guidelines for the analysis and interpretation of digital evidence", http://www.iso27001security.com/html/27042.html;

53. ISO/IEC 27043 „Incident investigation principles and processes", http://www.iso27001security.com/html/27043.html;

54. ISO/IEC 27050 „Electronic discovery“, http://www.iso27001security.com/html/27050.html;

55. ITU, Toolkit For Cybercrime Legislation, 2011, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf;

56. ITU, Understanding cybercrime: phenomena , challenges and legal response, 2012, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf;

57. Kaspersen H., Cybercrime and jurisdiction, 2009, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/IF_2009_presentations/default_en.asp;

58. Law enforcement challenges in transborder acquisition of electronic evidence from "cloud computing providers" (prepared for the Council of Europe/Global Project on Cybercrime), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp;

59. Maxwell W., Wolf C. Lovells White Paper: A Global Reality: Governmental Access to Data in the Cloud, 2012, http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf;

60. Mutual Legal Assistance in Computer-Related Cases, http://www.coe.int/tcj/;

61. National Center for Justice and the Rule of Law, Combating cyber crime: essential tools and effective organizational structures a guide for policy makers and managers, 2007, http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf;

62. National High Tech Crime Unit, Good Practice for Computer Based Electronic Evidence, Association of Chief Police Officers, London, United Kingdom, 2003, www.acpo.police.uk/asp/policies/Data/gpg computer based evidence v3.pdf .

63. Network Working Group, Guidelines for Evidence Collection and Archiving, 2002, http://www.faqs.org/rfcs/rfc3227.html;

64. Packaging, Transportation, and Storage of Digital Evidence, 2010, http://www.dfinews.com/article/packaging-transportation-and-storage-digital-evidence;

65. Packaging, Transportation, and Storage of Digital Evidence, http://www.dfinews.com/article/packaging-transportation-and-storage-digital-evidence;

66. Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE) - Technical Report Series, 2003, ftp://ftp.jrc.es/pub/EURdoc/eur2O823en.pdf;

67. Principles on Transborder Access to Stored Computer Data, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf;

68. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0010&from=en;

69. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=en;

70. Report: Recommendation R (87) 15 – Twenty–five years down the line, 2013, http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf;

71. Schwerha J., Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers, 2010, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf;

72. Specialised cybercrime units - Good practice study, CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe, European Union Cybercrime Task Force, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf;

73. The effectiveness of international cooperation against cybercrime: examples of good practice, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp;

74. U.S. Department of Justice, Office of Justice Programs National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf;

75. U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Washington, 2002, www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm;

76. U.S. Department of Justice, The Criminal Justice Resource Manual on Computer Crime, 1989, https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf;

77. Understanding Cybercrime:A Guide For Developing Countries, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf;

78. Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs, 2005, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf;

79. Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting CSIRTs, 2005, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf;

80. Working party on information security and privacy: the evolving privacy landscape: 30 years after the OECD privacy guidelines, 2011, http://www.oecd.org/internet/interneteconomy/47683378.pdf.

4.2. Чланци и остали извори:

1. American Academy of Forensic Sciences (AAFS), http://www.aafs.org/;
2. Carter D.L, „Computer Crime Categories: How Techno-Criminals Operate“, FBI Law Enforcement Bulletin, 1995, http://www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf;
3. Cha A., E.Nakishima, “Google China Cyberattack Part of Vast Espionage Campaign, Experts Say,” The Washington Post, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html;
4. Cloud Services Users Will Hit 625 Million in 2013: IHS, http://slashdot.org/topic/cloud/cloud-services-users-will-hit-625-million-in-2013-ihs;
5. Computer Hacking Forensic Investigator, http://www.eccouncil.org/certification/computer-hacking-forensics-investigator);
6. Consortium of Digital Forensic Specialists (CDFS), http://www.cdfs.org/;
7. Cyber Security Institute’s Cyber Security Forensic Analyst: CSFA, http://www.cybersecurityforensicanalyst.com/;
8. Digital Forensic Certification Board (DFCB), http://www.dfcb.org/;
9. European Network of Forensic Science Institutes (ENFSI), http://www.enfsi.eu/;
10. Gareth S, Website Location: Cyberspace vs. Geographic Space, 2008, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/Gareth%20Samson%20Website%20Location.pdf;
11. Global Report on the Cost of Cyber Crime, 2014, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf
1. Google's Privacy Policy, http://www.google.com/privacypolicy.html;
12. Hale C., „Cybercrime: Facts & Figures Concerning this Global Dilemma“, Criminal Justice International 18/2002, http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37;

13. Harley, B ‘A global convention on cybercrime?’, Columbia Science and Technology Law Review, http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/;

14. Hawes J., “2013 An Epic Year For Data Breaches With Over 800 Million Records Lost,” Naked Security, February 19, 2014, http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-withover-800-million-records-lost/;

15. http://9to5mac.com/2014/08/26/seagate-announces-massive-8tb-hard-drive-for-bulk-data-storage/;

16. http://arhiva.mpravde.gov.rs/cr/articles/medjunarodne-aktivnosti-eu-integracije-i-projekti/medjunarodna-pravna-pomoc/medjunarodni-ugovori-o-pravnoj-pomoci-u-krivicnim-stvarima.html;

17. http://ceop.police.uk/Media-Centre/Press-releases/2011/HUNDREDS-OF-SUSPECTS-TRACKED-IN-INTERNATIONAL-CHILD-ABUSE-INVESTIGATION/;

18. http://ceop.police.uk/Media-Centre/Press-releases/2011/HUNDREDS-OF-SUSPECTS-TRACKED-IN-INTERNATIONAL-CHILD-ABUSE-INVESTIGATION/;

19. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG;

20. http://courses.southwales.ac.uk/courses;

21. http://ec.europa.eu/justice/criminal/recognition-decision/index_en.htm;

22. http://online-anonymizer.com/;

23. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp;

24. http://www.crimelibrary.com/forensics/dna/6.htm;

25. http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument;

26. http://www.encryptedcommunications.com/;

27. http://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence;

28. http://www.gddc.pt/codigos/code_criminal_procedure.html;

29. http://www.gpo.gov/fdsys/pkg/BILLS-113s607rs/pdf/BILLS-113s607rs.pdf;
30. http://www.htcia.org/history/;
31. http://www.iacis.com/;
32. http://www.internetworldstats.com/stats.htm;
33. http://www.internetworldstats.com/stats.htm;
34. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime;
35. http://www.mpravde.gov.rs/court-experts.php;
36. http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm;
37. https://dre.pt/application/dir/pdf1sdip/2009/09/17900/0631906325.pdf;
38. https://www.europol.europa.eu/sites/default/files/flags/interpol_.pdf;
39. https://www.swgde.org/;
40. International Electrotechnical Commission (IEC), http://www.iec.ch/;
41. International Laboratory Accreditation Cooperation (ILAC), http://ilac.org/;
42. International Organisation on Computer Evidence http://www.ioce.org;
43. International Organization for Standardization (IOS), http://www.iso.org/iso/home.html;
44. International Society of Forensic Examiners Certified Computer Examiner, https://www.isfce.com/certification.htm;
45. Internet Corporation for Assigned Names and Numbers: ICANN, http://www.icann.org;
46. INTERPOL Global Complex for Innovation (IGCI), http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation;
47. ISM Projected To Cost U.S. Cloud Computing Industry $35B, http://www.forbes.com/sites/louiscolumbus/2013/08/08/prism-projected-to-cost-u-s-cloud-computing-industry-35b/;
48. Kraft W., Ideas on the Establishment of an International Court for Cyber Crime, 2011, http://www.wclf.de/cybercrime_court_en.html?file=tl_files/Media/Download/FINAL-CYBER-COURT-ENGLISH.pdf;

49. McCombie S, Warren M, „Computer forensic: An issue of definition“, Proceedings of the First Australian Computer, Network and Information Forensics Conference, 2003, http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2003/forensics/;

50. McKemmish R., „What is forensic computing?“, Trends and Issues in Crime and Criminal Justice 118/2002, www.aic.gov.au/publications/tandi/ti118.pdf;

51. Moore's Law at 50: Its past and its future, http://www.extremetech.com/extreme/203031-moores-law-at-50-its-past-and-its-future;

52. Net Losses: Estimating the Global Cost of Cybercrime, 2014, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf;

53. Oxford English Dictionary, http://www.oed.com/;

54. Robertson J., "Why Are Hackers Flooding Into Brazil?" Bloomberg, September 13, 2013, http://www.bloomberg.com/news/2013-09-13/why-are-hackers-flooding-into-brazil-.html;

55. SANS Institute GIAC Certified Forensics Analyst, http://www.giac.org/certification/certified-forensic-analyst-gcfa;

56. Schjolberg S., Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace, 2014, http://www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf;

57. Scientific Working Group on Digital Evidence (SWGDE), https://www.swgde.org/;

58. Shelton E. The 'CSI Effect': does it really exist? NIJ J March 2008; 259, http://www.ojp.usdoj.gov/nij/journals/259/csieffect.htm;

59. Six Arrested Over 45 Million Cyber Heist on Middle East Banks," Al Arabiya, November 19, 2013, http://english.alarabiya.net/en/business/banking-and-finance/2013/11/19/Sixarrested-over-45-million-cyber-heist-on-Middle-East-banks.html;

60. Srivastava A., 2 Billion Smartphone Users By 2015 : 83% of Internet Usage From Mobiles, http://dazeinfo.com/2014/01/23/smartphone-users-growth-mobile-internet-2014-2017/#ixzz2rcbChM tk;

61. The Digital Forensics Research Workshop: DFRWS , http://www.dfrws.org/;

62. United Kingdom Accreditation Service (UKAS), http://www.ukas.com/;

63. www.williamgibsonbooks.com;

ПРИЛОЗИ

Прилог 1:

Упитник на основу ког је обављен стручни интервју са представником Одељења за борбу против високотехнолошког криминала Службе за борбу против организованог криминала у оквиру Дирекције полиције Министарства унутрашњих послова Републике Србије

УПИТНИК

(питања се односе на искуства у борби против кривичних дела
из надлежности Одељења)

Надлежност Одељења

1. Организација и надлежност државних органа за борбу против високотехнолошког криминала у Републици Србији регулисани су на одговарајући начин.

а) тачно;

б) делимично тачно;

в) нетачно.

2. Да ли је постојање Одељења које је надлежно за територију целе Републике адекватно решење или би било целисходније да поред Одељења, као централне јединице полиције, постоји и више подручних једница чијим радом би се координирало из Одељења?

3. Да ли је потребно проширити круг кривичних дела за која је надлежно Одељење?

4. На који начин је, осим наведеног, могуће унапредити решења у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала?

Састав, унутрашња организација и услови рада у Одељењу:

1. У функционисању Одељења постоје организациони недостаци.

а) нетачно;

б) делимично тачно;

в) тачно, уочени су следећи недостаци:

2. Колико је запослених у Одељењу?

3. Који услови у погледу знања, вештина и искуства се захтевају за запослење/ распоређење у оквиру Одељења?

4. Да ли је квантитавни (број запослених) и квалитативни (структура запослених) састав Одељања одговарајући?

5. На који начин је извршена организација послова у надлежности и делокругу рада Одељења: да ли у оквиру Одељења постоје групе (јединице) које су посебно задужене за предузимање одређених задатака: а) оперативне и процесне радње; б) анализа података и информација; в) рачунарска форензика?

6. Да ли постоје интерна правила поступања у вези са предузимањем оперативних и процесних радњи? Ако постоје, која су то правила? Шта је њима уређено? Да ли су та правила поступања једнообразна или су она прилагођена специфичностима појединих кривичних дела?

7. У функционисању Одељења постоје технички недостаци.

а) нетачно;

б) делимично тачно;

в) тачно - уочени следећи недостаци:

8. Којом техничком опремом располаже Одељење?

9. Који форензички алати се користе приликом предузимања активности везаних за обезбеђење електронских доказа?

10. На који начин се остварује перманентна обука заполених у оквиру Одељења?

Предузимање оперативних и процесних радњи

1. Са којим проблемима се запослени у Одељењу суочавају приликом предузимања оперативних радњи и мера за кривична дела из своје надлежности, и на који начин се ти проблеми могу превазићи?

2. Са којим проблемима се запослени у Одељењу суочавају приликом предузимања увиђаја места за кривична дела из њихове надлежности, и на који начин се ти проблеми могу превазићи?

3. Са којим проблемима се запослени у Одељењу суочавају приликом предузимања увиђаја над уређајима за аутоматску обраду података и уређајима и опремом на којој се чувају или се могу чувати електронски записи, и на који начин се ти проблеми могу превазићи?

4. Са којим проблемима се запослени у Одељењу суочавају приликом прикупљања података о саобраћају комуникација (извор и одредиште комуникације) које се остварују у реалном времену, и на који начин се ти проблеми могу превазићи?

5. Са којим проблемима се запослени у Одељењу суочавају приликом прикупљања података о садржају комуникација (пресретање комуникације) у реалном времену, односно приликом предузимања радње тајног надзора комуникација, и на који начин се ти проблеми могу превазићи?

6. На који начин се обезбеђује прикупљање података о саобраћају остварених комуникација/података о садржају комуникација, а који су ускладиштени у рачунару/рачунарској мрежи којим је могуће приступити преко рачунара који је предмет увиђаја/претреса?

7. На који начин се води рачуна о поштовању приватности трећих лица укључених у комуникацију са осумњиченим лицима, а које се не односе на кривично дело?

8. Које радње и мере (и којим редоследом) се предузимају у ситуацији уколико су потребни подаци ускладиштени у рачунару/рачунарској мрежи који су лоцирани у иностранству, а којим је могуће приступити преко рачунара који је предмет увиђаја/претреса?

9. Које радње и мере (и којим редоследом) се предузимају у ситуацији уколико постоје основи сумње да је учинилац кривичног дела лице чија ИП адреса је у иностранству?

10. Да ли се запослени у Одељењу суочавају са проблемима приликом испитивања у својству сведока/ вештака у кривичном поступку на околности прикупљања електронских доказа?

Сарадња Одељења са другим органима и институцијама

1. Да ли постоје проблеми у сарадњи Одељења за надлежним тужилаштвом: ако постоје? Ако постоје, који су и на који начин се превазилазе?

2. На који начин се остварује сарадања Одељења са другим јединицама у оквиру Министарства?

3. На који начин се остварује сарадања у оквиру Интерполовог центра за координацију активности у борби против високотехнолошког криминала?

4. У колико Интерполових заједничких акција је полиција Србије учествовала у вези са високотехнолошким криминалом?

5. Колико се молби за пружање међународне правне помоћи у кривичним стварима на годишњем нивоу упућује Одељењу/ Одељење шаље?

6. Које оперативне и процесне радње су најчешће предмет захтева за пружање помоћи?

7. У случају слања молбе за пружање међународне правне помоћи, колико се чека на поступање надлежних органа замољене државе?

8. На који начин се превазилазе проблеми дуготрајног процеса пружања међународне правне помоћи у кривичним стварима када је потребно обезбедити податке у што краћем временском периоду?

9. Који подаци и информације су најчешће предмет хитне размене са полицијом других држава?

10. Сарадња полиције са пружаоцима телекомуникационих услуга у Републици Србији је:

а) недовољно добра;

б) добра;

в) одлична.

Прилог број 2:

Упитник на основу ког је обављен стручни интервју са Тужиоцем за високотехнолошки криминал Републике Србије

УПИТНИК

(питања се односе на искуства у борби против кривичних дела
из надлежности Тужилаштва)

Надлежност Одељења

1. Организација и надлежност државних органа за борбу против високотехнолошког криминала у Републици Србији регулисани су на одговарајући начин.

а) тачно;

б) делимично тачно;

в) нетачно.

2. Да ли је постојање спцијализованог Тужилаштва које је надлежно за територију целе Републике адекватно решење?

3. Да ли је потребно проширити круг кривичних дела за која је надлежно Тужилаштво?

4. На који начин је, осим наведеног, могуће унапредити решења у Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала?

Састав, унутрашња организација и услови рада у Тужилаштву:

4. У функционисању Тужилаштва постоје организациони недостаци.

а) нетачно;

б) делимично тачно;

в) тачно, уочени су следећи недостаци:

5. Колико је запослених у Тужилаштву?

6. Који услови у погледу знања, вештина и искуства се захтевају за запослење/ распоређење у оквиру Тужилаштва?

7. Да ли је квантитавни (број запослених) и квалитативни (структура запослених) састав Тужилаштва одговарајући?

5. На који начин је извршена организација послова у надлежности и делокругу рада Одељења?

6. Да ли постоје интерна правила поступања у вези са предузимањем оперативних и процесних радњи? Ако постоје, која су то правила? Шта је њима уређено? Да ли су та правила поступања једнообразна или су она прилагођена специфичностима појединих кривичних дела?

7. У функционисању Тужилаштва постоје технички недостаци.

а) нетачно;

б) делимично тачно;

в) тачно - уочени следећи недостаци:

8. Којом техничком опремом располаже Тужилаштва?

9. Који форензички алати се користе приликом предузимања активности везаних за обезбеђење електронских доказа?

10. На који начин се остварује перманентна обука заполених у оквиру Одељења?

Предузимање оперативних и процесних радњи

1. На који начин Тужилаштво долази до сазнања да су учињена кривична дела из надлежнсти Тужилаштва?

2. Са којим проблемима се Тужилаштво суочава приликом предузимања увиђаја места за кривична дела из њихове надлежности, и на који начин се ти проблеми могу превазићи?

3. Са којим проблемима се Тужилаштво суочава приликом предузимања увиђаја над уређајима за аутоматску обраду података и уређајима и опремом на којој се чувају или се могу чувати електронски записи, и на који начин се ти проблеми могу превазићи?

4. Са којим проблемима се Тужилаштво суочава приликом прикупљања података о саобраћају комуникација (извор и одредиште комуникације) које се остварују у реалном времену, и на који начин се ти проблеми могу превазићи?

5. Са којим проблемима се Тужилаштво суочава приликом прикупљања података о садржају комуникација (пресретање комуникације) у реалном времену, односно приликом предузимања радње тајног надзора комуникација, и на који начин се ти проблеми могу превазићи?

6. На који начин се обезбеђује прикупљање података о саобраћају остварених комуникација/података о садржају комуникација, а који су ускладиштени у рачунару/рачунарској мрежи којим је могуће приступити преко рачунара који је предмет увиђаја/претреса?

7. На који начин се води рачуна о поштовању приватности трећих лица укључених у комуникацију са осумњиченим лицима, а које се не односе на кривично дело?

8. Које радње и мере (и којим редоследом) се предузимају у ситуацији уколико су потребни подаци ускладиштени у рачунару/рачунарској мрежи који су лоцирани у иностранству, а којим је могуће приступити преко рачунара који је предмет увиђаја/претреса?

9. Које радње и мере (и којим редоследом) се предузимају у ситуацији уколико постоје основи сумње да је учинилац кривичног дела лице чија ИП адреса је у иностранству?

10. Са којим проблемима се Тужилаштво суочавају приликом презентовања електронских доказа у кривичном?

Сарадња са другим органима и институцијама

1. На који начин се остварује сарадња Тужилаштва за посебни одељењем полиције: ако постоје? Ако постоје проблеми, који су и на који начин се превазилазе?

2. На који начин се остварује сарадања Одељења са другим јединицама у оквиру Министарства?

3. На који начин се остварује сарадања у оквиру Интерполовог центра за координацију активности у борби против високотехнолошког криминала?

4. У колико Интерполових заједничких акција су надлежни органи учествовали у вези са високотехнолошким кримналом?

5. Колико се молби за пружање међународне правне помоћи у кривичним стварима на годишњем нивоу упућује/шаље?

6. Које оперативне и процесне радње су најчешће предмет захтева за пружање међународне правне помоћи?

7. У случају слања молбе за пружање међународне правне помоћи, колико се чека на поступање надлежних органа замољене државе?

8. На који начин се превазилазе проблеми дуготрајног процеса пружања међународне правне помоћи у кривичним стварима када је потребно обезбедити податке у што краћем временском периоду?

9. Који подаци и информације су најчешће предмет хитне размене са надлежним органима других држава?

10. На који начин се остварује сарадња са пружаоцима телекомуникационих услуга у Републици Србији?

БИОГРАФИЈА АУТОРА

Рођена је 1984. године у Новом Саду. Основне академске студије на Правном факултету у Новом Саду уписала је школске 2003/2004, а дипломирала школске 2006/2007. године. Школске 2008/2009 године уписала је дипломске академске студије права и одбранила дипломски рад с темом „Недозвољена доказна средства у кривичном поступку“, под менторством проф. др Татјане Бугарски.

Од октобра 2007. године до септембра 2009. године волонтирала у Општинском суду у Новом Саду у својству судијског приправника. Током 2008. године била запослена на Високој пословној школи струковних студија у Новом Саду у звању сарадника у настави, за предмет Пословно право.

На Правном факултету у Новом Саду изабрана је у звање сарадника у настави 2008. године, а у звање асистента 2010. Године. Изводи вежбе из предмета Кривично процесно право 1 и 2 (на 2. години основних академских студија), Криминалистичка техника и тактика и Криминалистичка методика (на 2. години основних академских студија Смера унутрашњих послова).

Учествовала је на неколико домаћих и међународних скупова.

Област њеног интересовања су: докази, кривични поступак за дела високотехнолошког криминалитета, међународна сарадња у кривичним стварима.

Говори енглески и немачки језик, а служи се италијанским и француским језиком.

Аутор је више научних радова.

Прилог 1.

Изјава о ауторству

Потписана **Милана Писарић**

број индекса **ДС 17/2010**

Изјављујем

да је докторска дисертација под насловом

ПОСЕБНОСТИ ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 01.04.2016.године

_____

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора **Милана Писарић**

Број индекса **ДС 17/2010**

Студијски програм Докторске студије

Наслов рада: ПОСЕБНОСТИ ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Ментор **проф. др Милан Шкулић, редовни професор Правног факултета Универзитета у Београду**

Потписана **Милана Писарић**

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 01.04.2016.године

_____

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

ПОСЕБНОСТИ ДОКАЗИВАЊА ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 01.04.2016.године

_____

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.