ЗВОНИМИР ИВАНОВИЋ*
ОЛИВЕР ЛАЈИЋ
Криминалистичко полицијски универзитет
Земун

УДК 343:004.7
Прегледни рад
Примљен: 12.11.2019
Одобрен: 21.01.2020
Страна: 323-342

ПРЕТРЕСАЊЕ И ОДУЗИМАЊЕ ПРЕДМЕТА У ВЕЗИ СА АУТОМАТСКОМ ОБРАДОМ ПОДАТАКА

Сажетак: Аутори у раду приказују статус радњи претресања и одузимања предмета у погледу уређаја за аутоматску обраду података као и њихових носилаца. Ово чине кроз илустрирање различитих мера и радњи које су по својој природи и смислу сличне описаним, али и кроз статус и услове које законодавац прописује за ове радње. У том смислу аутори указују и на нелогичности на које се у оваквом приказивању наилази. Радње се покушавају приказати и у светлу истраживања које је спроведено у оквирима архиве Посебног тужилаштва за високотехнолошки криминал Републике Србије уз анализу одузетих предмета у случајевима кривичног дела из чл.185 КЗ РС

Кључне речи: високотехнолошки криминал, претресање рачунара, одузимање предмета, полицијско поступање, криминалистичка форензика

Увод

Претресање и привремено одузимање предмета, али и мера безбедности одузимања предмета у електронском окружењу изискује другачија правила у односу на класично поступање. Нова правила поступања у оваквом окружењу условљена су карактеристикама окружења, предмета који се одузимају, средствима на располагању органима поступка, али и самим предметом, који се има одузети. У оваквом светлу неопходно је поступати према правилима које диктира струка – леге артис. Поступање према правилима изискује и познавање карактеристика дигиталних доказа, процеса и дешавања у рачунарском и електронском окружењу. У том смислу правни прописи, којима се уређује поступање овлашћених лица, морају пратити стручне инструкције и смернице. Правне норме не могу у сваком тренутку и увек у право време обухватити све од значаја за поступање, у ситуацијама и околностима које прете да такве дигиталне трагове униште, оштете или измене. У овом смислу постоји кашњење правних норми за стручним упутствима и правилима. Рад обухвата у овом смислу како опис актуелног стања у вези са претресањем и (привременим)

* zvonko31@gmail.com

одузимањем уређаја за аутоматску обраду података – УОАП, као и њихових носилаца, (према правилима одузимања редмета) тако и могуће критике актуелних решења у прописима, те и давање предлога *de lege ferenda*.

Актуелно законско окружење и правила

У оквирима правног система Републике Србије, у кривичном праву[1], позната су два метода депривације лица државине над одређеним стварима, прибављеним на противправан начин. Они своје манифестације имају у привременом одузимању предмета и одузимању предмета у некој од мера одређених пресудом према чл. 424 ст. (5) ЗКП, а то подразумева: одлуку о мери безбедности, о одузимању имовинске користи или о одузимању имовине проистекле из кривичног дела. Као доказна радња, привремено одузимање предмета представља Закоником о кривичном поступку утврђени начин на који органи поступка обезбеђују материјалне доказе који могу послужити за успешно вођење кривичног поступка. Међутим, циљ није само доказивање кривичног дела у мери привременог одузимања предмета, већ и као мера – привременог карактера, како друга, неовлашћена, лица не би располагала оваквим предметима, евентуално, и због забрањености законом[2]. Иако је привремено одузимање предмета издвојио као посебну доказну радњу и одредбама чл. 147 до 151 ЗКП регулисао кључне елементе њеног вршења, законодавац је претпоставке и поступак вршења регулисао и бројним другим одредбама законика, али и у другим законима, а надлежни државни органи и појединим подзаконским актима.

Проналажење предмета који могу послужити као доказ за успешно вођење кривичног поступка од стране органа поступка остварује се вршењем појединих оперативно-тактичких мера и радњи које полиција предузима у случају постојања основа сумње да је извршено кривично дело за које се гони по службеној дужности (чл. 286 ст. 1, у вези са чл. 282 ст. 2 ЗКП), али и током и, у склопу, предузетих доказних радњи, на које су, као изузетак од правила (обзиром да је основни титулар предузимања доказних радњи Јавни тужилац), овлашћени припадници полиције, припадници пореске полиције, царински службеници.

Криминалистичке мере и радње којима се ови циљеви остварују су, пре свих, преглед превозних средстава, путника и пртљага, расписивање потрага за стварима за којима се трага, преглед одређених објеката и просторија државних органа, предузећа, радњи и других правних лица, и остваривање увида у њихову документацију, а, у случају потребе, и њено одузимање, привремено ограничење кретања.

---

[1] У грађанско – правном оквиру постоје и самопомоћ, привремене мере изречене од стране суда, али оне нису за нас у овом раду од неког посебног значаја, већ ћемо се фокусирати на кривично – правне мере.

[2] Нпр. чл.87. тач.1, 3. Кривичног Законика Републике Србије (КЗ РС), као општа одредба али и као мера безбедности чл.79. тач.7. КЗ РС, али и као прописана обавезна мера приликом утврђивања одговорности за извршење кривичног дела (нпр. чл.246. ст.7 или 246 а, ст.3. КЗ РС), у ком случају већ код постојања основа сумње за постојење кривичног дела и учиниоца, обавезно привремено одузимање предмета, а суд је тада обавезан да изрекне меру безбедности.

Као оперативно-тактичка мера која се састоји у прегледу докумената, пословних књига и евиденција, увид у документацију се предузима у случају постојања основа сумње да је извршено кривично дело које се гони по службеној дужности и када се претпоставља да се у документацији државних органа, предузећа, радњи и других правних лица могу пронаћи подаци о извршеном кривичном делу (чл.286. ЗКП), односно када се сумња да та документација представља предмет кривичног дела. Преглед документације врши се у присуству одговорног лица. То може бити учињено и у његовом одсуству уколико се оно није одазвало позиву да присуствује прегледу, или очигледно избегава да буде присутно. Ако се приликом прегледа документације утврде неправилности (нпр. нетачни подаци, трагови фалсификовања), она ће се привремено одузети од корисника (од стране органа поступка) у оригиналној форми и стању у коме је затечена. Изузетно се може узети препис или фотокопија. О предузетој радњи се сачињава записник. Приликом привременог одузимања списа, који могу да послуже као доказ они се пописују. У случају да то није могуће, списи се морају ставити у омот и запечатити, при чему власник списа може на омот ставити и свој печат. Лице од кога су списи одузети позваће се да присуствује отварању омота. Уколико се оно не одазове позиву, или је одсутно, омот ће се отворити, а списи прегледати и пописати у његовом одсуству. При прегледању списа мора се водити рачуна да њихов садржај не сазнају неовлашћена лица (чл. 150 ЗКП).

Већ је истакнуто да ЗКП садржи низ одредби које се тичу привременог одузмања предмета, па и ону којом предвиђа да се привремено одузимају предмети, који се по кривичном законику имају одузети и предмети који могу послужити као доказ у кривичном поступку (чл. 147 ст. 1 ЗКП). Предмети који су употребљени или су били намењени за извршење кривичног дела, или који су настали извршењем кривичног дела, могу одузети и кад нису својина учиниоца ако то захтевају интереси опште безбедности или разлози морала, или када и даље постоји опасност да ће бити употребљени за извршење кривичног дела (чл. 87 ст. 2 КЗ). Ова одредба ће бити веома значајна за наш предмет рада. Овим законником предвиђена је и могућност да се законом могу одредити услови за одузимање одређених предмета у појединим случајевима, односно обавезно одузимање предмета, као и њихово обавезно уништавање (чл. 87 ст. 3 КЗ), а кривичноправним одредбама, којима је предвиђено постојање појединих кривичних дела, оживотворена је одредба да се законом може одредити обавезно одузимање предмета[3]. У погледу оваквог одузимања предмета

[3] Тако се, нпр. наводи да ће бити одузети: новац, предмети од вредности и свака друга имовинска корист прибављена кривичним делом (чл. 92 ст. 1 КЗ), поклон или друга корист код давања и примања мита у вези са гласањем (чл. 156 ст. 4 КЗ), порнографски материјал (чл. 185 ст. 5 КЗ), ауторско дело код повреде моралних права аутора и интерпретатора (чл. 198 ст. 4 КЗ), производи неовлашћеног коришћења туђег дизајна (чл. 202 ст. 3 КЗ), лажан новац (чл. 223 ст. 5 КЗ), лажне хартије од вредности (чл. 224 ст. 4 КЗ), лажне платне картице (чл. 225 ст. 6 КЗ), лажни знакови за вредност (чл. 226 ст. 4 КЗ), средства за прављење лажног новца, лажних хартија од вредности, лажних платних картица или лажних знакова за вредност (чл. 227 ст. 3 КЗ), кријумчарена роба и превозно или друго средство чија су тајна или скровита места искоришћена за пренос робе (чл. 230 ст. 3 и 4 КЗ), новац и имовина који потичу из кривичног дела (чл. 231 ст. 7 КЗ), предмети

постоји значајна могућност злоупотребе овлашћења органа поступка, због специфичности електронских уређаја као и уређаја за електронску обраду података.

Код дефинисања предмета који се имају одузимату радњом привременог одузимања предмета у чл.147 ст. 3 ЗКП изричито се наводе уређаји за аутоматску обраду података и уређаји и опрема на којој се чувају или се могу чувати електронски записи (УАОП). Такође, и КЗ дефинише у чл.112. шта се под оваквим називом може сматрати, па тако тачка 33) каже да је рачунар сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке. Тачка 34) истог члана КЗ наводи да је рачунарски систем сваки уређај или група међусобно повезаних или зависних уређаја од којих један или више њих, на основу програма, врши аутоматску обраду података.

На овај начин законодавац децидно формулише да у предмете који се одузимају спадају и УАОП. Питања у погледу реализације доказне радње предвиђене Закоником о кривичном поступку (али и једног од полицијских овлашћења) усмерене на дигиталне трагове су бројна.[4] Прво питање везује се за начин и/или радњу којом се привремено одузимају предмети у оваквим случајевима. Када је у питању носилац дигиталних података (у оквиру УАОП), – то подразумева физичко одузимање носиоца. Овде се могу препознати и различите категорије носилаца – са аспекта могућности физичког одстрањивања забрањених материјала. Ту можемо разматрати оне са којих не могу трајно избрисати подаци, морају се категорисати другачије – овакви уређаји представљају циљ одредбе о одузимању, са намером уништавања истих (зато што се

обележени туђом фирмом, туђом географском ознаком порекла, туђим жигом или заштитним знаком (чл. 233 ст. 4 КЗ), роба и средства за производњу или прерађивање код недозвољене производње (чл. 242 ст. 3 КЗ), роба и предмети недозвољене трговине (чл. 243 ст. 5 КЗ), лажни знакови, мере и тегови (чл. 245 ст. 2 КЗ), опојне дроге и средства за њихову производњу и прераду (чл. 246 ст. 7 КЗ, 246а ст. 3 КЗ и 247 ст. 3 КЗ), шкодљиве животне намирнице, јело или пиће или други шкодљиви производи (чл. 256 ст. 4 КЗ), уловљена дивљач и средства за лов (чл. 276 ст. 5 КЗ), улов и средства за риболов (чл. 277 ст. 4 КЗ), уређаји и средства који су у својини учиниоца а којима је неовлашћено избрисан, измењен, оштећен, прикривен, или на други начин учињен неупотребљивим рачунарски податак или програм (чл. 298 ст. 4 КЗ), уређаји и средства којима је направљен или у туђ рачунар или рачунарску мрежу убачен рачунарски вирус (чл. 300 ст. 3 КЗ), средства немењена или коришћена при недозвољеном прелазу државне границе – кријумчарењу људи (чл. 350 ст. 5 КЗ), средства намењена или употребљена за извршење кривичног дела неовлашћеног организовања игара на срећу, као и новац и други предмети који служе у игри на срећу (чл. 352 ст. 3 КЗ), награда и имовинска корист код трговине утицајем (чл. 366 ст. 7 КЗ), примљени поклон и имовинска корист код примања мита (чл. 367 ст. 7 КЗ), средства намењена за финансирање вршења кривичног дела из чл. 312, 391 и 392 КЗ (чл. 393 ст. 3 КЗ).

[4] На уму треба имати и чињеницу да савремени живот брзих комуникација и постојања дигиталних продуката без којих је живот незамислив, условљавају посебна правила поступања са обезбеђењем места догађаја и носиоцима дигиталних информација и дигиталним траговима уопште. Нестручно поступање са материјалима, предметима и траговима са места догађаја може довести до њиховог уништења и измене, али и до погрешног усмерења активности полиције након обраде места догађаја. У том смислу и МУП РС је донео упутство о поступању са дигиталним траговима са места извршења кривичног дела. Иначе, ово упутство је после скоро шест година у примени, на ревизији.Такође, веома је значајно да овакви уређаји имају посебне карактеристике, те је њихово одузимање под упитником, најпре због могућности одстрањивања забрањених или недозвољених материјала, трајно и на сигуран начин.

не могу обрисати). Међутим, проблеми се јављају и у случајевима који су многобројни када су у питању дигитални подаци који се налазе у рачунару, паметном телефону, мрежној опреми корисника, серверима који нису у фактичком поседу – државини лица, од којег се одузимају (овде тек можемо правити различите категорије). Наше истраживање указује на велики број предмета који се одузимају са специфичним карактеристикама комуникационих уређаја. Начин прибављања дигиталних података, који се привремено одузимају у оваквим случајевима, најчешће се остварује кроз другу доказну радњу претресања УАОП (односно рачунара), у обзир долази и могућност примене радње вршења увиђаја на стварима, али до оне границе у којој би се разликовали затечен рачунар (телефон, мрежна опрема) - када би се такав рачунар (телефон, мрежна опрема) одузео и накнадно прибавила наредба за претресање УАОП. Описано је из разлога што је само радња претресања УАОП предвиђена ЗКП а не и увиђај, и само на основу наредбе суда (Упоредити са Писарић, М. 2015:215–238). Прегледање уређаја (ствари) би представљало потражну активност а која мора претходити сваком одузимању предмета. Међутим, законником је предвиђена радња привременог одузимања УАОП, те је тако дат простор за привремено одузимање, којим се онемогућава мењање и утицај на податке у уређају а, потом, може уследити претресање у просторијама органа поступка, на основу наредбе. У описаном случају није изричито предвиђено присуство два пунолетна сведока, мада је то општим правилима претресања прописано. Проблеми који произилазе из овакве ситуације, могу бити решени применом адекватних и унапред дефинисаних софтверских и хардверских решења, која фактички представљају и записнике, и облик надзора над вршењем радње претресања, јер верно евидентирају све активности стручних лица. Пратећи софтверски излази (у облику обавезног евидентирања активности стручних лица и интеракција софтвера) постоје и предвиђени су код свих стандардних софтвера (како комерцијалних тако и оних који су бесплатни – open source) за претресање. Теза по којој је ово једини пут (привременог) одузимања дигиталних података не може стајати. Веома је значајно у овом тренутку направити дистинкцију између одузимања носилаца дигитални података и одузимања самих дигиталних података. У сваком случају једна је активност неопходна пре друге, али и обавезна. Преглед ових уређаја, које претходи претресању обухвата физичко прегледање спољашности уређаја УАОП (и носилаца дигиталних података) у циљу прибављања њихових карактеристика и вршења увида, од стране стручних лица, у облике веза које ти УАОП имају са другим уређајима, и тада је, такође, могуће вршити привремено одузимање УАОП. У свим описаним случајевима привремено одузимање УАОП се јавља као радња физичког одузимања оваквог уређаја (укључујући и носиоце дигиталних података). У рачунарском свету и неким земљама чланицама ЕУ уређаји се из различитих разлога не морају увек одузимати, већ се применом форензичких мера могу направити њихове верне копије. Разлози за одузимање, наведени раније у тексту, нису у сваком од ових случајева испуњени, а, нарочито, ако посматрамо са аспекта људских потреба у савременом свету. Ово је посебно интересантно када се узме у обзир дефинисање дигиталних података као покретне ствари у чл.112, тач.16. Кривичног законика Републике Србије и тиме и као могућег

предмета привременог одузимања. Одузети трајно некоме рачунар лишава га могућности да исти користи и приступа Интернету, такође и у случају одузимања мобилног телефона, (или других уређаја путем којих се обавља комуникација), онемогућава се комуникација са блиским и другим лицима предвиђене чл.41. Устава Србије[5]. У питању су и одредбе чл. 46. Устава Србије које гарантују слободу мишљења и изражавања[6], чиме се угрожава њихова примена. Сврха прибављања дигиталних трагова везаних за извршење кривичног дела испуњава се и прављењем верне копије оваквог уређаја у датом тренутку у времену[7] у комбинацији са привременим одузимањем (праћено претресањем као и трајним брисањем материјала са тог УАОП). Са друге стране овакво копирање стања (меморија) уређаја са собом носи и конотацију претресања рачунара - УАОП, обзиром да се тиме целокупан садржај уређаја клонира, те је након тога могуће претраживање уређаја различитим софтверским алаткама, а за шта је потребна наредба суда.

У сваком случају претресање УАОП се може спровести само на основу наредбе суда а која се издаје на образложен предлог Јавног тужиоца. Садржај таквог предлога или захтева за издавање наредбе мора одражавати смисао и потребе издавања исте, те је у њему значајно одредити уређаје који се имају претресати са свим индивидуалним и групним карактеристикама, из којих разлога се очекује да се оваквом радњом могу прибавити докази и чињенице везане за извршење кривичног дела (основни услов за претресање у чл.152. ЗКП јесте вероватноћа да се претресањем могу пронаћи предмети и трагови односно одређена лица), шта се тражи, органе који ће у претресању учествовати и у ком својству.

Прецизно дефинисање предмета и трагова који се могу пронаћи приликом оваквог претресања није могуће у сваком случају (на пример, уколико се траже подаци у облику датотека у формату докумената MS worda или неког другог текстуалног процесора а осумњичени је променио тип датотеке може настати проблем приликом претраживања). Ипак, овакво прецизно дефинисање могуће је оквирно одредити на такав начин, тако да претресањем не би дошло превеликог задирања у приватност лица применом ове радње. Недостатак

---

[5] Тајност писама и других средстава општења. Одступања су дозвољена само на одређено време и на основу одлуке суда, ако су неопходна ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом. У овом смислу поставља се питање неопходности ради вођења поступка.

[6] Јемчи се слобода мишљења и изражавања, као и слобода да се говором, писањем, сликом или на други начин траже, примају и шире обавештења и идеје. Слобода изражавања може се законом ограничити, ако је то неопходно ради заштите права и угледа других, чувања ауторитета и непристрасности суда и заштите јавног здравља, морала демократског друштва и националне безбедности Републике Србије.

[7] Оваква активност може се подвести под појам увиђаја, обзиром да представља по својој природи и представља констатовање и конзервацију тренутног стања затеченог на месту догађаја, и еквивалентно је аудио визуелном снимању вршења увиђаја, фотодокументацијом, графичком и записничком фиксирању ове радње. Шта више уређаји и софтверски пакети у савременој форензици омогућавају да се приликом прављења овакве копије не утиче уређајем и средствима којима се уређај копира на стање и процесе у том уређају. Оваквим активностима се омогућава и касније упоређивање стања и статуса процеса у уређају који је копиран (клониран) и констатовање промена протеком времена.

који се у теорији наводи у погледу недефинисања или неадекватног дефинисања законом услова и околности у погледу предузимања радње претресања УАОП и без наредбе (Писарић, М. 2015:215–238) веома је тешко надокнадити, а околности које се у животним ситуацијама могу створити, апсолутно указују на могуће значајне случајеве у којима би, тако нешто, и више него добро дошло. Нарочито забрињава ситуација у којој Уставом загарантована неповредивост стана у чл. 40. има своје изузетке у случајевима претресања без наредбе (чл.158. ЗКП) а да то претресање рачунара (УАОП) нема, што, само за себе, представља парадокс. Значајно је напоменути да би у погледу оперативнијег поступања овако нешто требало предвидети ЗКП-ом, чак и без присуства сведока уз обавезно евидентирање свих активности и њихово фиксирање кроз неки облик записника, аудио визуелног снимања или примену адекватног софтвера који све ово обухвата и сл. Дакле, могуће је предвидети да у склопу увиђаја на УАОП (рачунару, телефону или др.) обавезно мора бити направљена верна копија свих расположивих меморија, а да, касније, исти може бити анализиран различитим радњама, уз додатне облике сигурносног приступа таквој копији. У том смислу постоје могућности да се оваквим активностима мапирају и недозвољени објекти – предмети који се имају одузети, чиме се могу обезбедити даље активности којима се не би могло доћи до угрожавања описаних одредаба Устава РС. Или ако је претпоставка да је предмет привремено одузет па на њему примењена радња која има конотацију претресања и буде пронађен објекат који се тражи, он се може трајно обрисати са рачунара, чиме бива испуњен неопходно потребан услов предвиђен законом, а предмет ослобођен оваквог објекта може бити враћен држаоцу. (Ово такође подразумева да се након изрицања мере безбедности одузимања предмета, ове датотеке могу избрисати – уклонити са УАОП, и потом вратити држаоцу, без њих.) Наредбом за претресање УАОП дефинишу се задаци и субјекти који у истом учествују, уз предмете ка којима је радња претресања усмерена. Приликом примене софтвера за претресање УАОП могуће је поменутим софтвером предвидети да се приликом одузимања обришу или означе, ради каснијег брисања, (ово је вероватније, обзиром да се претресање врши на форензичкој копији) подаци који су недозвољени. Такође, уколико постоји сумња у вези предмета за одузимање (да није одузет укупан материјал или да постоји скривени који се тек има пронаћи), онда може уследити привремено одузимање а исто је касније, као мера безбедности могуће управо са дефинисањем и реализацијом у оквиру домашаја овог софтвера.

У аналогији са претресањем лица и ствари, присуство браниоца би требало да буде обезбеђено, али треба напоменути да је, управо ово случај, када ће одбрана ангажовати стручног саветника, ради контроле законитости и поштовања правила поступања lege artis органа гоњења у случајевима оваквог претресања. Ово се може омогућити и у приказаном случају прављења верне копије или клона уређаја (хард диска – физичке меморије, али и RAM меморије као и кеша) уз помоћ софтверских и хардверских решења, која стандардизовано онемогућавају поступање изван форензичких стандарда предвиђених, у смислу обавезног евидентирања активности приликом предузимања овакве радње (аудио-визуелног снимања, израда извештаја и службених белешки од

стране органа руководиоца претресања и израда извештаја од стране самог програма за претресање). Шта више, управо у оваквим случајевима се може предвидети уз разлоге хитности могућност спровођења претресања, без наредбе суда у будућим решењима ЗКП, као законским изузецима уз услове испуњавања предвиђених претпоставки. Рок за започињање спровођења ове наредбе је исти као и у случају сваког претресања 8 дана од издавања (чл.155 ЗКП), уколико се не почне спроводити, орган поступка је дужан да је врати суду и тада се претресање не може предузети. Активност радње претресања подразумева претраживање рачунара уз помоћ различитих софтверских (програмских) пакета (комерцијални у виду N-case, ФТК, али и некомерцијални као што су бивши Backtrack Linux, Kali linux, Sumuri Paladin или уз помоћ разних других облика команди у оквирима OS Linux), који користе претраге датотека у виртуелном окружењу оперативног система рачунара (УАОП), као и другим расположивим меморијама уређаја. Дакле, за разлику од прегледа, претресање представља радњу којом се констатују и проналазе одређене датотеке, сви дигитални елементи виртуелног окружења као и (приступи) остварене или, до тада, успостављене везе на уређају, постојање и облици шифрованих делова рачунара и њихова величина и сл. Према томе, преглед рачунара би представљао спољашње прегледање уређаја и фиксирање стања на радној површини уређаја, констатовање постојећих веза на уређају (физичких) и активних бежичних успостављених између веза у окружењу и самог уређаја као и окружење радног простора око уређаја. Оно што представља разлику јесте улазак у радно окружење рачунара, оперативни систем и претраживање садржаја, примену метода декрипције садржаја и анализе комуникационих активности на уређају, без остављања трагова на рачунару (УАОП) и уношења нових података у рачунар (дакле уз искључивање Локардовог принципа).

Описане активности врше се путем хардверски подешених уређаја и софтверски прилагођених програмских пакета у виду ливе forensics алата. Што се увиђаја тиче, он би обухватио преглед рачунара, али уколико се нека врста комуникације на рачунару одвија, неки подзаконски акти (обавезна инструкција МУП о поступању и обезбеђењу дигиталних доказа, која у овом тренутку пролази кроз процес ревизије) указују на могућност одржавања такве комуникације и упуштање у одвијање комуникације са потенцијалним извршиоцима, нпр. у случајевима отмице, чиме би се интервенција органа гоњења могла спровести у циљу спасавања живота и спречавања вршења кривичних дела, а са друге стране документовања кривичног дела и активности извршилаца. Према мишљењу дела теорије оваква активност је изводљива по нашем законодавству, а према одређеном делу теорије није. Аргументи који иду у прилог изводљивости јесте да се приликом вршења увиђаја могу примењивати одредбе ЗКП о увиђају над стварима из чл.135. Свако је дужан да органу поступка омогући приступ стварима и пружи потребна обавештења. Под условима из члана 147. ЗКП, покретне ствари се могу привремено одузети[8]. У овом смислу

[8] Привремено одузимање УАОП и дигиталних података, као и код претресања са собом носи обавезу предаје таквих предемета од стране лица која их имају у државини, одређена лица су изузета од ове обавезе: осумњичени и лица одређена чл.93 и 94. ЗКП као манифестација привилегије несамоинкриминисања. Ово представља посебан проблем, сам за себе обзиром да се у

могуће је замислити и физичко одузимање и виртуелно копирање стања и статуса уређаја. Ако је ради предузимања увиђаја потребно ући у зграде, станове и друге просторије, примењују се одредбе члана 155. (претресање стана и осталих просторија са наредбом) и члана 158. став 1. тачка 1 (без наредбе) ЗКП. На основу тумачења ове последње одредбе могуће би било улажење у стан ради вршења увиђаја на покретним стварима осумњиченог али наравно не и претресање, без наредбе суда, уколико су испуњени услови из чл.158 ЗКП, након овога ради претресања рачунара или других УАОП морали би прибавити наредбу. Поставља се питање да ли је за претходно описано копирање стања и статуса уређаја неопходна наредба, наше је становиште да она, у том случају, није неопходна, а као аргументе за то можемо навести строга правила поступања и обезбеђења дигиталних трагова у обавезној инструкцији МУП РС и обезбеђење ланца доказивања.

Лицу од кога су предмети одузети, издаје се потврда у којој ће се они описати, навести где су пронађени, подаци о лицу од кога се предмети одузимају, као и својство и потпис лица које радњу спроводи. Сачињена потврда треба да садржи оне идентификационе податке о одузетом предмету који ће омогућити како његово везивање за ситуацију и дуге околности проналажења и одузимања, тако и његову каснију поуздану идентификацију, очување и гарантовање интегритета и везивање за конкретну кривичну ствар у којој се поступа. Поред тога, детаљним описом се предупређују случајне или злонамерне замене предмета веће вредности предметом мање вредности, у циљу стицања користи, а стварају се и претпоставке за евентуалну процену и накнаду штете лицу од кога је предмет одузет, а за који је донета одлука да се мора вратити власнику (у случају оштећења или губитка предмета). Оваква ситуација такође иде у прилог нашем тумачењу које има логику у санирању последица могућег кривичног дела – брисањем датотека и враћањем привремено одузетог уређаја. Оно што у таквом моменту може бити проблем јесте да када се одузима предмет носилац дигиталних података – УАОП, јесте да се у потврди не може навести потпун садржај његових дигиталних података које носи. Наиме, чак и када би се предузела активност којом би се прелиминарно констатовао садржај, није могуће апсолутно бити сигуран да је садржај верно приказан, обзиром да је могуће намерно мењање наслова и екстензија података, како би личили на неке друге. У таквим случајевима за откривање оваквих активности неопходно је темељно и дубинско претраживање података, које подразумева претресање. Тада се привременим одузимањем решава позиција да се мења садржај уређаја, посебним придржавањем правила везаних за паковање и обезбеђење уређаја предвиђеним поменутом инструкцијом МУП –а.

У функцији обезбеђења и очувања доказног кредибилитета одузетих предмета је и систем њиховог чувања и контроле манипулисања. Систем под-

---

последње време у пракси појединих земаља налазе тумачења која иду у прилог приморавању у одређеном смислу и ових лица на предају или чињење доступним дигиталних података, на пример последња одлука суда у САД да примора осумњиченог да путем свог отисака папиларних линија прста откључа Iphone или Наредбе Врховног суда САД да примора Аппле да откључа Iphone 5c.

разумева означавање, категоризацију, фотографско и видео снимање, прикупљање и паковање материјалних доказа, али и постојање писаних података о службеним лицима која су поступала са њима. Уколико је квалитетно постављен, систем пружа гаранцију да су докази који се представљају на суду управо они који су, као такви, прикупљени на месту догађаја, односно пронађени претресањем или одузети од лица. У том контексту треба схватати и могући захтев да се сва службена лица, у чијој су држави били одређени докази, (нарочито отисци прстију, опојне дроге, видео-траке, фотографије, биолошки трагови итд.) појаве у својству сведока у кривичном поступку и дају исказ којим ће потврдити да докази нису замењени, контаминирани и покварени док су били под њиховим надзором и контролом. Због тога се сматра да је у случају доказа код којих се захтева *chain of custody*[9], односно ланац доказивања, најбоље да се докази налазе код малог броја људи.

Посебна брига мора бити посвећена одузимању и паковању оних предмета који су по својој природи извор опасности. Орган поступка ће обезбедити чување привремено одузетих предмета (чл. 147 ст. 1 ЗКП). За поједине предмете, уз обавезу одузимања, законодавац предвиђа и обавезу њиховог уништавања: предмети којима је неовлашћено искоришћавано ауторско дело или сродно право (чл. 199 ст. 5 КЗ), предмети којима је извршено неовлашћено уклањање или мењање електронске информације о ауторском и сродним правима (чл. 200 ст. 2 КЗ), предмети којима је извршена повреда проналазачког права (чл. 201 ст. 5 КЗ).

Предмети који су у току поступка привремено одузети, вратиће се држаоцу ако престану разлози због којих су предмети привремено одузети, а не постоје разлози за њихово трајно одузимање. Ако је предмет неопходно потребан држаоцу, он му се може вратити и пре престанка разлога због којег је одузет, уз обавезу да га на захтев органа поступка донесе (чл. 151 ст. 1 и 2 ЗКП). Поједини предмети ће се вратити и лицу које је учинило кривично дело (нпр. поклон, односно друга корист, који буду одузети од лица које је примило мито могу се вратити даваоцу мита у случају да је учинилац кривичног дела давања мита дао мито на захтев службеног лица и пријавио дело пре његовог откривања или сазнања да је дело откривено – чл. 368 ст. 6 КЗ).

Претресање уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи

Под аутоматском обрадом података подразумева се поступак обраде података аутоматским средствима, пре свега рачунарима. Унети подаци, као и подаци и информације добијени обрадом, похрањују се и чувају на меморијским јединицама. Када данас говоримо о уређајима за аутоматску обраду по-

[9] *Chain of custody* – ланац државине одузетих предмета за период између момента када је одређени предмет пронађен и одузет до момента његове презентације на суду. J. T. Gardner, M. T. Anderson, *Criminal Evidence, Principles and Cases, 5th edition,* Thomson/Wadsworth, Wadsworth, 2004, p. 330, 309, i 310.

датака (УАОП) и опреми на којој се чувају или се могу чувати електронски записи, под тим подразумевамо сваки производ који се користи за обраду и/или складиштење електронских (дигиталних) података: рачунари (десктоп, лаптоп, или сервери), мобилни уређаји (паметни телефони, *Personal Digital Assistant* - ПДА, таблети, уређаји за сателитску навигацију...), меморијски медијуми (ХД, ЦД/ДВД, УСБ дискови, СД картице, ...), одређена мрежна опрема (нпр. модеми, рутери, свичеви...), дигиталне камере, *Cloud Data* сервери и др (упоредти са Л. Комлен-Николић; и др, 2010).

Сврха претресања ових уређаја јесте проналажење електронских (дигиталних) доказа, што подразумева сваку информацију у електронском (дигиталном) облику која има доказну вредност, а која је или ускладиштена или пренесена у таквом облику [10].

Две основне категорије електронских (дигиталних) података могу чинити електронски (дигитални) доказ:

– Нестални (непостојани, Volatile) подаци: - они који се налазе у радној меморији (РАМ), или се налазе у преносу, а губе се након искључивања рачунара (нпр. мрежни статус и везе, активни процеси, кеш меморија...);
– Стални (али осетљиви) подаци ускладиштени на меморијском медијуму (нпр. на чврстом диску - ХД) и који су сачувани и након искључивања рачунара. Неки од тих података се могу лако изменити (нпр. последње време приступа), а некима је могуће само условно приступити (нпр. подаци на шифрованом диску који су привремено доступни само док је рачунар укључен, а где након искључења и поновног стартовања рачунара њихова доступност зависи од поседовања одговарајуће шифре).

Електронски докази су по својој природи осетљиви - могу се променити, оштетити или чак уништити услед неправилног руковања или испитивања. Како су, уз то, у неопипљивом облику и могу бити читани само уз употребу рачунарског софтвера, као основне препреке за њихову правосудну прихватљивост сматрају се осетљивост и променљивост као и инхерентна посредност електронских доказа. Зато је неопходно предузети посебене мере поступања како би доказ био прихватљив на суду, односно потребно је испоштовати 4 основна принципа поступања са електронским доказима[11]:

– Мора се поступати на начин којим се омогућава очување веродостојности доказа (акције предузете у току аквизиције, анализе и презентације не смеју проузроковати никакву измену тих доказа);
– Уколико је неопходно приступити оригиналном дигиталном доказу, особа која то ради мора бити компетентна и способна да на суду пружи доказе уз објашњење зашто је то било неопходно и који су резултати предузете акције;
– Све активности везане за прибављање, приступ, складиштење или трансфер дигиталног доказа морају бити потпуно документоване, сачуване и расположиве за ревизију - очуван ланац доказа (a chain of custody).

[10] Obavezna instrukcija o prikupljanju i obezbeđenju elektronskih dokaza MUP RS od 26.02.2013.god.,
[11] Водич најбоље праксе поступања са електронским доказима - Association of Chief Police Officers' (ACPO) publication - Good Practice Guide for Computer-Based Electronic Evidence - Official release version, dostupno na: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5B1%5D.pdf

– Овлашћено службено лице које задужено за поступање са предметима - је у потпуности одговорно да обезбеди да се закон, подзаконски акти и ови принципи поштују.

Имајући све горе наведено у виду, јасно је да претресање уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи, мора спровести компетентна особа која је оспособљена да исто може урадити:

– у форензичкој лабораторији уколико је извршено привремено одузимање наведених предмета, или ако то није могуће
– на лицу места на уређају који је укључен (тзв. ливе форензика), уколико у свом поседу има за то специјализоване алате, за то је оспособљен и стручан/а, као и овлашћен.

Доступни су многобројни алати (бесплатни и комерцијални) за обезбеђивање електронских доказа. Тако је ради очувања њиховог интегритета потребно, када је год то могуће, направити форензичку копију уређаја (тзв. клон) која подразумева верну копију постојећих меморијских јединица (копирање се ради бит по бит и прави се тзв. Имаге; могу се користити слободно доступни (*open source*) програми нпр. dd, или комерцијална решења EnCase, FTK, или нпр. UFED – када су у питању телефони и сл.). Све методе и алати за аквизицију и анализу електронских доказа примењују се онда на форензичкој копији, (*image clone*) а не на оригиналном уређају. Како би била обезбеђена проверљивост добијених резултата, по правилу се праве две форензичке копије - једна радна и једна резервна. Истоветност форензичке копије и оригинала потврђује се одређивањем њихових хеш[12] вредности које морају бити идентичне.

Обавезна опрема органа за претресање и одузимање предмета јесте: Фото апарат или видео камера, рукавице, налепнице, кесе за заштиту, провидне пластичне кесе и печати са воском, папирне кесе и селотејп, антистатичке кесе, фломастери у боји, кутије на склапање.

Традиционални приступ искључивања и одузимања уређаја ради његове форензичке анализе, превиђа велику количину несталних података који ће искључењем бити изгубљени. Зато се данас, пре искључења рачунара, неопходним сматра поступак чувања тренутног садржаја радне меморије (РАМ-у), као вредног извора краткотрајних и несталних информација које између осталих могу укључивати и: лозинке за шифроване партиције (TrueCrypt, BitLocker, PGP Disk), идентификационе податке за пријављивање на различите налоге и сервисе (Gmail, Yahoo Mail, Hotmail; Facebook, Twitter, Google Plus; Dropbox, Flickr, SkyDrive, i dr.), списак активних процеса у тренутку преузимања и сл. За ту сврху се могу искористити алати (који се као форензички тестирани и потврђени могу покренути са ДВД/ЦД-РОМ или УСБ уређаја) који

[12] Хеширање представља механизам којим се садржај било које дужине трансформише, помоћу одговарајућег алгоритма (најпознатији су из фамилија МД и СХА), у краћи запис (сажетак) – хеш (*hash*) фиксне дужине. Поступак је иреверзибилан, а свака промена у оригиналу резултоваће променом хеша, што овај поступак чини погодним за проверу интегритета садржаја.

омогућавају преузимање (тзв. дамповање) садржаја меморије без уношења било каквих промена у електронске податке посматраног уређаја (нпр. Helix, Belkasoft Live RAM Caputer, AccessData FTK Imager, PMDump, Paladin i dr.).

Уколико је из било којег разлога немогуће извршити привремено одузимање УАОП, онда компетентна особа може претресање обавити на лицу места, применом одговарајућих форензичких алата, у поступку који се назива ливе форенсицс. У овом случају, потрага за електронским доказима спроводи се у реалном времену, на уређају који ради. Претходно описан поступак чувања садржаја радне меморије укљученог рачунара део је *live forensic* postupka. Ту је међутим и испитивање осталих меморијских јединица уређаја, а у случају да је уређај у мрежном окружењу може се, након детектовања веза и конекција, извршити и испитивање удаљених складишта података[13].

Привремено одузимање УАОП

Упутства (најбоља пракса) за привремено одузимање уређаја за аутоматску обраду података и опреме на којој се чувају или се могу чувати електронски записи незнатно се разликују у зависности да је уређај укључен или искључен. Оно што је битно поштовати у вези поступања је да се искључени уређај не сме укључивати. У случају затвореног лаптоп рачунара потребно је прво посматрањем сигнала на рачунару –лампица које означавају стање спавања или сл, или подизањем поклопца утврдити његову активност (укључен или не), имајући у виду да се неки од њих подизањем поклопца и укључују. У наставку ћемо навести кораке и разлике у поступку одузимања укљученог и искљученог уређаја.

Поступак одузимања ИСКЉУЧЕНОГ уређаја (десктоп и лаптоп рачунари, мобилни телефони, ПДА)

1. Не укључивати уређај
2. Фотографисати место где се налази уређај, све каблове и околне уређаје.
3. Искључити кабл за напајање струјом из уређаја (не из зида), као и остале каблове и повезане уређаје. Сви уређаји, портови и каблови се морају прописно означити за касniју реконструкцију повезаних уређаја. У случају лаптоп рачунара извадити батерију, уколико је то могуће.
4. Потребно је потражити лозинке од лица, као и у његовим белешкама и дневницима. Такође је потребно потражити (и одузети) и све приручнике и упутства за коришћење софтвера.
5. Обавезно тражити информације од лица од којег се уређај привремено одузима да ли користи енкрипцију или неки од сервиса на интернету за складиштење по-

[13] Уколико се она физички налазе у јурисдикцији друге државе, потребно је придржавати се одговарајућих правних аката која регулишу ту материју, иако у оквиру ЦЕТС 185 (Конвенције о високотехнолошком криминалу Савета Европе,) постоје превиђени механизми за поступање и у таквим случајевима и олакшавање МЛАТА – Mutual legal assistance аката, односно захтева за пружање међународне правне помоћи у кривичним стварима али у области ВТК. кроз спровођење онлајн истрага. Ово посебно у чл.19-22. ЦЕТС.

датака и комуникацију. Ако је одговор потврдан, а уколико је то могуће, пре предузимања других радњи потребно је о томе обавестити стручно лице, које ће спровести поступак претресања и поступити по његовом упутству. У случају мобилног телефона питати власника о ПИН коду и лозинкама и исте забележити. Према обавезној инструкцији МУП – а то су припадници СБПОК Одељења за борбу против ВТК, односно припадици ССИМ

6. Поред рачунара и рачунарске опреме, одузимају се и сви уређаји за складиштење електронских података, приручници за употребу тих уређаја и белешке. Све одузете предмете потребно је обележити и спаковати на прописан начин и о томе направити службену белешку.
7. Све радње документовати кроз службену белешку и потврду о привремено одузетим предметима

Поступак одузимања УКLjУЧЕНОГ уређаја (десктоп и лаптоп рачунари, мобилни телефони, ПДА):

1. Укључени уређај се не сме претраживати и забрањено је користити тастатуру;
2. Фотографисати место где се налази уређај, све каблове и околне уређаје;
3. Фотографисати садржај екрана уређаја и описати га у службеној белешци. Уколико је потребно деактивирати сцреенсавер, то урадити употребом миша (само померањем истог никако притиском на тастер) а не тастатуре. Уколико је сцреенсавер заштићен лозинком не предузимати даље никакве акције са тим у вези. Обавезно документовати време и разлог употребе миша;
4. Уколико је могуће, форензичким алатом прикупити несталне податке који ће бити изгубљени након искључења рачунара (нпр. активни процеси и сл.);
5. Уколико је у току нека штампа, омогућити да се тај поступак заврши;
6. Искључити уређај:
   - **Десктоп рачунар**
   - Искључити кабл за напајање струјом из рачунара (не из зида), као и остале каблове и повезане уређаје;
   - **Лаптоп рачунар**
   - Извадити батерију (уколико је то могуће);
   - **Мобилни телефон**

- искључити, осим у посебним случајевима када мора остати укључен:
- када је заштићен лозинком, па му се без познавања исте неће моћи приступити након укључивања,
- хитним случајевима, односно уколико се очекује остварење комуникације која би помогла поступку истраге;

ПДА (Personal digital assistant/electronic organisers)

- потребно је оставити укљученим, пошто је велика вероватноћа да је заштићен лозинком и да му се без познавања исте неће моћи приступити након укључивања. Такође, уклањање батерије може резултовати губитком свих података, па је потребно обезбедити да оне буду пуњене све док компетентно лице не спроведе поступак претресања уређаја.
- Искључити све остале каблове и повезане уређаје. Сви уређаји, портови и каблови се морају прописно обележити у сврху касније реконструкцију повезаних уређаја.
- Спровести кораке 4, 5, 6 и 7 описане код поступка одузимања искљученог уређаја

Поступање у случају постојања кућног мрежног окружења и бежичне технологије

Препоруке за поступање у случају мрежног окружења и бежичних технологија укључују следеће кораке[14]:

- Идентификовати и проверити мрежне уређаје како би се утврдило постојање активности на Интернету (мрежног саобраћаја). Размотрити и употребу детектора бежичних мрежа, како би се утврдило да ли оне постоје и како би се лоцирали бежични уређаји.
- Искључити уређај са мреже, онда када смо сигурни да неће доћи до губитка података(искључивањем везе са телефоном, или једноставним искључивањем кабловских веза). Модеми и рутери треба да остану укључени пошто ће можда бити испитивани у циљу проналажења повезаних уређаја. Због природе везе, посебно је тешко утврдити шта је повезано на бежичну мрежу.
- Пратити сваку жицу из мрежног уређаја како би се пронашао рачунар на који је повезан. Ово, можда неће бити могуће у пословним просторијама, где се каблови налазе унутар зидова или посебних канала, па је у том случају потребно консултовати ИТ стручњака фирме (наравно, уколико он није осумњичени). Означити сваку везу и уређај на начин да се може обавити реконструкција мреже. Обратити пажњу да кабловски модеми могу да имају уграђену функцију бежичног повезивања.
- У случајевима када постоји сигурност да неће доћи до потенцијалног губитка доказа, могу се из идентификованих мрежних уређаја извући све конекције, што резултује изоловањем сваког рачунара са мреже.
- Фотографисати мрежни распоред и локације свих уређаја повезаних на њу, за потребе евентуалног захтева за реконструкцијом.
- Одузети и упаковати сав мрежни хардвер (под условом да је лако преносив)
- Сваки мрежни рачунар третирати на претходно описан начин (поступак одузимања десктоп и лаптоп рачунара).
- Никако не остављати ниједан мрежни рачунар, пошто се елекронски доказ може наћи на било којем од њих.

Имати у виду да се на мрежу могу повезати (преко WiFi или Bluetooth конекције) и други уређаји као што су мобилни телефони и ПДА. У том смислу говоримо и о онлајн корисничким налозима и онлајн просторима за складиштење података. Питање поступања са овако похрањеним подацима везује се за националне јурисдикције држава у областима кривично – правне материје, односно важење кривично – процесног права на територији државе на којој је неопходно поступање. Међународна правна регулатива у овој области везује се за ЦЕТС 185, конвенцију Савета Европе, али се она de facto своди на националну јурисдикцију. Посебно се може напоменути да се са неких сервиса (е-бау, ПауПал) који су глобално присутни могу прибавити подаци путем регистрације у том сервису као орган гоњења, чиме се чине доступни подаци везани за сервисе тог сервиса.

---

[14] Водич најбоље праксе поступања са електронским доказима - Association of Chief Police Officers' (ACPO) publication - Good Practice Guide for Computer-Based Electronic Evidence - Official release version, доступно на: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5B1%5D.pdf

Уколико се електронски докази налазе у великој пословној мрежи или на серверу сложене инфраструктуре, након обезбеђења места потребно је контактирасти стручно лице и поступити по препоруци.

Обележавање и паковање

Када су утврђени предмети који ће бити привремено одузети следи поступак њиховог обележавања и паковања. Сви одузети предмети описују се у потврди о привремено одузетим предметима, као и у записнику о претресању. Сваки одузети предмет се посебно означава и пакује, при чему се мора водити рачуна да се ознака не ставља на предмет већ на амбалажу у коју је упакован.

Све електронске уређаје је потребно упаковати у тзв. антистатичке кесе (ЕСД) чија је функција да спрече оштећења од електростатичког пражњења. За то се евентуално могу користити и чврсте картонске кутије, или комбинација паковања у папирну и пластичну амбалажу.

За заштититу од комбинованог деловања радио таласа, електромагнетног и електростатичког поља неопходно је користити кесе са ефектом тзв. Фарадејевог кавеза. Употреба ових кеса је неопходна како би се спречио бежични приступ (преко WiFi или Bluetooth конекције) укљученим уређајима - мобилним телефонима и ПДА.

На сваком запакованом одузетом предмету исписују се подаци о:

- лицу од кога је предмет одузет (са генералијама)
- датуму и времену одузимања уређаја као и ознаци органа коме се предмет предаје ради даљег чувања или поступања, а што се потврђује потписом овлашћеног лица.
- У случају даљег трансфера предмета другом органу и/или овлашћеном лицу, потребно је, без скидања старе налепнице, ставити нову на којој ће бити уписани нови подаци. На тај начин је обезбеђено очување тзв. 'ланца доказа' односно валидност самог електронског доказа.

Истраживање

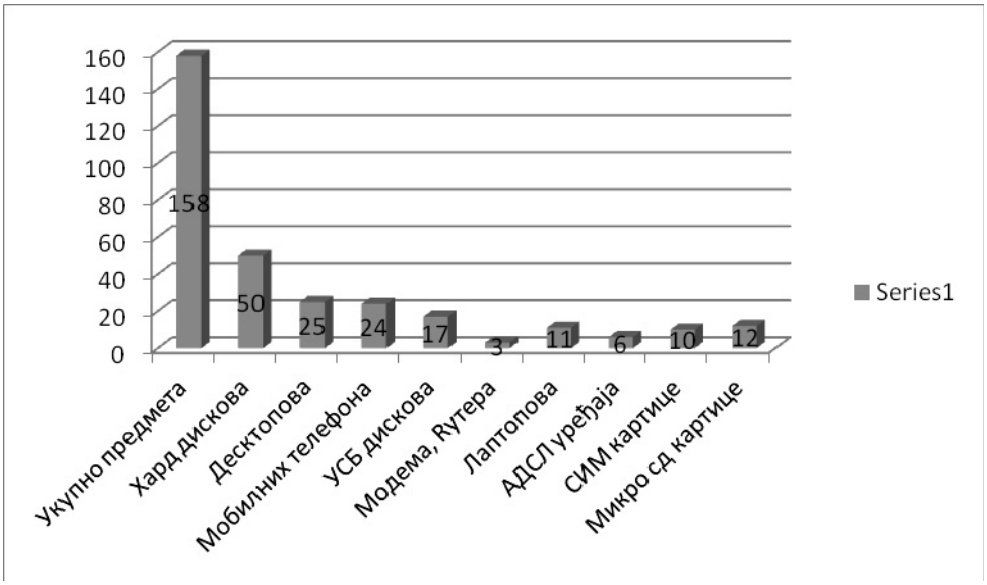
У циљу да што више илуструјемо проблематику привременог одузимања предмета приказаћемо и резултате дела истраживања спроведеног у просторијама Посебног Тужилаштва за ВТК. Временски период обухваћен овим истраживањем је од 2013. до 2017. године. Извршена је анализа евидентираних кривичних дела из облати високотехнолошког криминала територији Републике Србије, на основу изречених пресуда надлежних правосудних органа у вези са извршењем кривичног дела „Приказивање, прибављање и поседовање порнографског материјала и искоришћавање малолетног лица за порнографију“ из члана 185 КЗ РС. Став 6 овог члана регулише део који се односи на предмете порнографске садржине настале искоришћавањем малолетног лица (дечија

порнографија). Тако се под овим предметима сматрају материјали који визуелно приказују малолетно лице које се бави стварним или симулираним сексуално експлицитним понашањем, као и свако приказивање полних органа детета у сексуалне сврхе. Предмети у вези са овим кривичним делом се обавезно одузимају.

Анализирајући пресуде надлежног суда, укупно 55, узимајући у обзир период од 2013. до 2017. године, дошло се до закључка да кривично дело из члана 185 Кривичног Законика Републике Србије, извршавају лица мушког пола, средње животне доби (од 35 – 48 година живота, док су, у пар случајева, извршиоци овог кривичног дела имали су више од 60 година живота), нису у радном односу, место пребивалишта је градско насеље. У највећем броју случајева извршиоци су неожењени, са средњом стручном спремом. Ипак, ово није апсолутна одредница, па су се, међу извршиоцима, нашли и они, који имају завршену чак и вишу школу или факултет. Према извршиоцима овог кривичног дела, у највећем броју случајева, изрицана је казна затвора, условна осуда, обустава поступка, ослобођен, мера безбедности одузимање предмета. У погледу одузетих предмета, одузимани су хард дискови, мобилни телефони, лап топ рачунари, микро СД картице, АДСЛ уређај, СИМ картице, УСБ дискови. Процентуално исказано ови предмети чине следећу табелу:

Графикон :1 *Одузети предмети процентуално*

Графикон 2: *Одузети предмети*



Закључак

У вези са приказаним се може закључити да је област Високотехнолошког криминала и уређаја за аутоматску обраду података регулисана на потпунији начин у односу на друге, као на пример, област класичног криминала. Такође, треба указати на то да су директни актери у пољу примене закона имали интерес да сопственим подзаконским прописима допуне и конкретније регулишу материју, због сопствене сигурности али и правне сигурности, како њихови напори и стручна ангажовања не би били доведени у питање. Тенденција филигранског прописивања обавеза и дужности у области везаној за електронске доказе, која долази до изражаја због неколико значајних карактеристика исте – непознавање околности, правила и логике окружења од стране шире јавности, несигурности опште популације за поступање у специфичном окружењу, али и специјализованих стандардизованих поступака и мали број стучних организација оспособљених за стручно поступање. Наводи који се елаборирају на претходним странама указују на неколико значајних чињеница. Прва се везује за околност да у овој области није прописан увиђај, нити преглед дигиталних трагова. Веома је просто предвидети могућност да се приликом предузимања радње обезбеђења „лица места“ омогући и предузимање вршења увиђаја на уређајима за аутоматску обраду података, те њиховим носиоцима (електронским доказима), односно, њихову анализу. У овом раду је дат предлог како би требало регулисати ове радње, и указано је на постојање могућности за дефинисање оквира оваквог поступања. Шта више, приказано је

да се сличне активности већ предузимају од стране стручних лица у поступању на терену али да се такве активности не препознају у том смислу као засебне. Наиме прављење верне копије - *image*-а одређеног рачунара и дамп (*dump*) меморије и нису ништа друго до вршење увиђаја на одређеном УАОП. Претресање за које је неопходна наредба може уследити након прибављања наредбе на, овако креираним форензичким идеалним копијама УАОП – гоустовима или имиџима. Такође у раду је указано и на могуће постојање ситуација које изискују обавезно поступање припадника полиције, стручних лица у случајевима који би могли да представљају изузетке од правила обавезног претресања рачунара уз наредбу. У таквим случајевима неопходно би било и дефинисати слична правила за иазузетке као и код претресања стана и осталих просторија без наредбе. Услови су већ описани. Посебно се у овом раду указује на процедуре и правила у вези са привременим одузимањем предмета – конкретно, УАОП, њиховим обележавањем, паковањем и похрањивањем у безбедном окружењу. Невероватна количина енергије и стручних напора уложена је на прописивање правила поступања приликом привременог одузимања предмета а да се при том није водило много рачуна о сврси оваквог одузимања. Стручна јавност није разматрала о томе да се оваквим привременим и консеквентим трајним одузимањем и, евентуалним уништавањем, беспотребно ради нешто што представља додатну санкцију за лице које је одговорно за вршење дела које му се ставља на терет. Наиме, и поред објашњења које указује на уставне одредбе које пружају заштиту грађанима у погледу права на комуникацију, односно изражавања сопствене мисли, неопходно је размотрити и да у оваквим случајевима постојање могућности да се дело понови употребом таквог средства није довољно преклузивно да би се увек морало примењивати. Постоје аспекти овог и оваквог поступања органа гоњења који не указују на могућност и капацитет дискриминиативног понашања у оваквим случајевима. Наиме, могуће је да је извршилац дела (или чак само држалац предмета) за које се одузима електронски уређај лице које је тежак инвалид, непокретан и којем је овај уређај једини прозор у свет. Као што можемо видети из истраживања највећи број одузетих предмета представљају екстерни хард дискови и рачунари. Тиме се овом лицу, које има посебне потребе одузима могућност комуникације која му је неопходно потребна, могућност прибављања добара – доставним путем (доставе хране, одеће обуће и сл.), чиме угрожавамо и његову личност. Такође, савремен развој информатичких технологија пружа све доступније уређаје са ниским ценама, па се онда одузимањем уређаја извршилац не спречава у будућем вршењу дела, већ само лишава имовине, а за релативно ниско улагање, врло брзо, може доћи до другог уређаја. Треба размотрити примену селективног брисања на основу резултата претресања и такав уређај након процедуре брисања може се вратити окривљеном или оптуженом. Са друге стране могуће је овакве активности урачунати у трошкове поступка, те је могуће и на тај начин задовољити сврху кривичних санкција – а уједно и омогућити лицу да беспредметно не остане без уређаја. Тиме ће се задовољити и јавни и лични интерес лица.

Литература:

1. J. T. Gardner, M. T. Anderson(2004), Criminal Evidence, Principles and Cases, 5th edition, Thomson/Wadsworth, Wadsworth.
2. L. Komlen-Nikolić; R. Gvozdenović; S. Radulović; A. Milosavljević; R. Jeković,; V. Živković,; S. Živanović; M. Reljanović; I. Aleksić (2010): „Suzbijanje visokotehnološkog kriminala“, MUP RS, Beograd.
3. M. Pisarić (2015), Pretresanje računara radi pronalaska digitalnih dokaza (str. 215–238) Zbornik radova Pravnog fakulteta u Novom Sadu, 1/2015,
4. Obavezna instrukcija o prikupljanju i obezbeđenju elektronskih dokaza MUP RS (2013) od 26.02.2013.god.,
5. Vodič najbolje prakse postupanja sa elektronskim dokazima - Association of Chief Police Officers' (ACPO) publication - Good Practice Guide for Computer-Based Electronic Evidence - Official release () version, dostupno na: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence%5B1%5D.pdf
6. Broadhurst, R., Chang, Lennon Y.C. (2013). Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds). Asian Handbook of Criminology (pp. 49–64). New York: Springer.
7. Chang, Lennon, Y.C., & Grabosky, P. (2014). Cybercrime and establishing a secure cyber world. In M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.
8. Cherry, S. with Ralph Langner (2010). How Stuxnet Is Rewriting the Cyberterrorism Playbook. IEEE Spectrum.

SEARCH AND SEIZURE OF DEVICES IN RELATION TO THE AUTOMATIC PROCESSION OF DATA

Summary: The authors of the paper show the status of search and seizure of objects in relation to automatic data processing devices and their carriers. They do this by illustrating various measures and actions that are similar in nature and meaning to those described, but also through the status and conditions prescribed by the legislator for these actions. In this sense, the authors point out the illogicalities encountered in this presentation. The above mentioned actions are also being represented in the light of research conducted within the archives of the Special Prosecution Office for High-Tech Crime of the Republic of Serbia, with an analysis of seized objects in cases of criminal offenses under Article 185 of the RS Criminal Code.

Key words: high-tech crime, computer search, seizure of items, police conduct, criminal forensics