

СТАНДАРДИ У ПОСТУПАЊУ ТУЖИЛАЦА У БОРБИ ПРОТИВ КОМПЈУТЕРСКОГ КРИМИНАЛА

Јован Крстић
заменик Републичког јавног тужиоца
Правни саветник СЦГ при SECI

Увод

Тема међународних кривично-правних стандарда, није везана за било какав унапред прописан поступак стандардизације и лиценцирања, већ се ради о примени најбоље праксе у раду тужилаштва приликом поступања по појединим врстама криминалитета. За установљавање и дефинисање онога што се сматра најбољом праксом постоји уходана методологија која се заснива на проучавању правне праксе, образовању правника и вредновању поступања.

Претходно је потребно упознати се са неким значајним резултатима досадашње међународне активности Републичког јавног тужилаштва обављене у склопу дипломатске активности која је предузета са циљем да се Државна заједница Србија и Црна Гора прикључи пројектима регионалне сарадње тако што је преузела функцију координатора сарадње тужилаца земаља Југоисточне Европе у борби против прекограничног криминала.

Међународна иницијатива је започета септембра 2001. године, након првог контакта Окружног јавног тужилаштва у Београду са координатором међународне регионалне организације Иницијатива за сарадњу земаља Југоисточне Европе са седиштем у Букурешту (SECI), а лансирана је под окриљем Дирекције за економску међународну регионалну сарадњу и иницијативе при Министарству спољних послова СЦГ.

Након што је обезбеђено учешће представника јавног тужилаштва на састанку руководећег органа - Комитета за обједињену сарадњу (JCC) у SECI Центру за борбу против прекограничног криминала у Букурешту од 09. до 10. 10. 2003. године, делегација Србије и Црне Горе је ставила предлог за оснивање Саветодавне групе тужилаца земаља Југоисточне Европе. Иницијатива СЦГ је једногласно прихваћена од представника земаља чланица SECI.

Представници тужилаштва дванаест земаља су присуством на првом састанку Саветодавне групе земаља југоисточне Европе у Београду од 11. до 12.12.2003. године на делу показали одлучност држава Југоисточне Европе да се супротставе и боре против организованог криминала, свесни чињенице да, као што се активности разних криминалних група не прекидају на државним границама, тако се ни борба против криминала не може завршити на тим границама.

Ова сарадња је само почетак сложених напора у уједначавању кривичног гоњења на основу претходно установљене најбоље праксе, јер без прекограничне сарадње међу тужиоцима, хапшења не могу бити успешно изведена и следствено томе и кривични прогон, јер нема успешне борбе уколико се не циља и на руководство криминалних група за вршење организованог криминала, а које са

лакоћом прелази границе. Њихове софистициране операције остављају мало трагова на територијама разних држава, тако да се ови докази морају пажљиво сакупљати и употребити строго у складу са правилима кривичног поступка који треба да је пројектован тако да штити све што је вредно у нашем демократском друштву које се још увек развија.

Више се није могла игнорисати чињеница да развијајући средства да помогнемо суседној држави да започне кривични прогон против групе организованих криминалаца који су из разних разлога још нетакнути у нашој земљи, ако су тамо прикупљени докази и формиран предмет, у крајњем случају води ка започињању јединственог кривичног прогона и демонтирању злочиначке организације са више страна наших граница.

Схватајући то, државе Југоисточне Европе су још 1999. године закључиле Споразум о размењивању информација у циљу борбе против организованог криминала у земљама Југоисточне Европе (*The Agreement to Share Information to Combat Organized Crime - SECI Agreement*), како би не само успоставили Центар за борбу против прекограничног криминала у Букурешту, већ и како би се овај процес сарадње проширио и на тужилаштво и судство.

Отуда иницијатива Србије и Црне Горе за формирање Саветодавне групе земаља Југоисточне Европе (South Eastern European Prosecutor Advisory Group – SEEPAG) представља још један корак напред у остваривању и обнављању сарадње органа откривања и гоњења земаља овог региона. Овај напредак се остварио у развоју сарадње између Влада земаља чланица SECI Центра за борбу против прекограничног криминала који су заједно основале са седиштем у Букурешту.

Прихватајући предлог Комитет за обједињену сарадњу у SECI Центру изразио је очекивање да Саветодавна група тужилаца земаља Југоисточне Европе својом динамичном активношћу и по самом имену припадати свим тужилаштвима и да ће служити да унесе нову радну енергију и повећа коришћење јединствених ресурса које су створиле земље овог региона. То ће се омогућити путем сарадње са полицијским снагама стационираним у Центру за борбу против организованог криминала у Букурешту, са стварањем протокола за размену података у складу са европским конвенцијама и сарадњом са регионалним и националним Јединицама за борбу против трговине дрогом, трговине људским бићима, трговине оружјем малог калибра, кријумчарења, прања новца, повреда права интелектуалне својине и компјутерског криминала. Очекује се да се јединице за борбу против прекограничног криминала све више обраћају члановима SEEPAG. На њима је задатак и одговорност да користе ресурсе како SECI организације, тако и Пакта за стабилност земаља Југоисточне Европе и других регионалних и међународних организација које буду на располагању, све у склопу настојања да грађани добију стандардно квалитетну кривично-правну заштиту.

Примену међународних стандарда на националном и међународном плану илустроваћемо примерима поступасња против неких сродних врста криминала. Законодавна реформа у Србији је донела нове инкриминације за које још није остварена најбоља домаћа пракса, па је неопходно да се ослонимо на препоруке садржане у међународним правним актима и стројној пракси.

Инвестиционе преваре

Организатори и потенцијални извршиоци ове врсте преварне сплетке (fraud scheme) по договору на Internet-у оснивају лажне банке, штедионице, брокерске фирме, чак и земљорадничке задруге и сличне финансијске организације и започињу рад на разним инвестиционим пословима и ако не испуњавају законом прописане услове за пословање. Инвеститоре позивју преко разних медија и привлаче их да улажу уштеђевину или купују акције, тако што у пословању планирају и обећавају добит са високим каматним стопама на ангажована средства. Тако да стварају својеврсну финансијску пирамиду у којој је пројектовани прилив на основу пласмана средстава у таквој несразмери са преузетим обавезама да таква финансијска организација не може плаћати обавезе према улагачима и другим повериоцима. Ради избегавања плаћања обавеза организатори проузрокују стечај и наступање материјалне штете за улагаче.

За извршење ове врсте инвестиционе преваре потенцијални извршилац користи посебан информациони систем - упрошћен рачунарски програмски пакет.

У законодавству земаља Југоисточне Европе је у току обимна реформа кривичног права у које је уведено кривично дело рачунаске преваре. Дело је применљиво и у односу на извршиоце који употребљавају компјутере и комуникацију са инвеститорима и банкама преко LAN и WAN мреже и WWW (Интернета) и тако контактирају са потенцијалним жртвама или међусобно. Као резултат мониторинга на Интернету, смањен је број оваквих понуда у виду писама и ланаца среће, али се повећао број разних тражења да корисници дају своје личне податке како би добили обавештења о одређеним пословима за које су заинтересовани, што се користи за тзв. крађу идентитета на Интернету. То је увод за друге преваре са заменом идентитета или коришћењем финансијских података о корисницима.

МУП Србије оснива посебна одељења или јединице за борбу против компјутерског криминала и за борбу против повреде права интелектуалне својине. Очекује се да располажу са посебним програмом који може да пресретне, сакупља и одгонетне електронске поруке чији је садржај такав да је подобан да се у законитој процедури код суда добије одобрење за његово сазнавање путем праћења и прислушкивања. Републичка управа прихода у Одељењу за спречавање прања новца оснива Финансијску обавештајну службу (ФОВ). Тужилаштво мора да познаје све врсте компјутерског криминала и предлаже специјалне истражне технике и методе за прикупљање доказа у свакој области, почев од дела против уставног уређења и безбедности државе, где се као пратећа дела јављају финансирање тероризма путем прања новца, злоупотребе прилога разних интересних група, НВО и фондова за помоћ, све до криминала на Интернету, где је потребно знати како се врши идентификација сумњивих понуда, порука, трансакција, откривање идентитета извршиоца, заплена компјутера и обнављање обрисаног електронског садржаја порука и др. При томе трба имати у виду да се овим истражним радњама не повреде основна људска права и слободе. Мора се испоштовати основни стандард уставом гарнговане заштите од незаконитог претресања (пресретања порука и анализа порука) и заплена (скупљање порука, програма и рачунара) тако да у поступању постоји равнотежа између интереса заштите приватности и друштвеног интереса за кривични погон.

Заштите права интелектуалне својине која се угрожавају преко преко рачунара

У области заштите права интелектуалне својине јавни тужиоци морају прво да увиде одређене глобалне економско-политичке аспекте заштите ове врсте друштвених вредности.

У двадестом веку технологија је омогућила да се створи глобална стратегија пословања. Међународни споразуми у трговини (GATT)¹ су показали колико би било успорено пословање без редукције царинских ограничења. Ово је утицало да се промени пословна политика предузећа, тако да се она све мање заснива на проценама и вештини руководиоца, већ се претвара у тзв. менаџмент знања ("Knowledge Management). У основи ове економске политике се ради о фрагментацији пословања фирми и привреде земаља.

Конкретни напредак у технологији довео је до повећања продуктивности (ефикасности) и то: 1) развој микропроцесора и 2) развој Интернета.

Произвођачи са најсавременијом технологијом у свету имају највећи број заштићених патената. То нису фирме за које бисмо могли претпоставити да им се производи не могу лако копирати, већ се ради о фабрикама чији је производе готово немогуће створити због недостатка скупocene опреме, а ипак заштићују проналаске.

Произвођачима компјутера је информациона технологија важнија од патентне заштите, пошто купцима омогућује брзо доношење одлука. Ипак им је патентна заштита неопходна, јер представља основ њихове међусобне сарадње. За финални производ виисоке технологије (рачунар) треба спојити разне компаније тако да се на тај начин стварају тзв. стратешке алијансе. У уговорима о пословној сарадњи се налазе одредба о деоби профита у складу са бројем патената сваке фирме који су примењени у производњи финалног производа. Такав производ често има технолошку иновацију и зато и у погледу своје заштите и у погледу регистравања врши одређен позитиван утицај на стварање све савршенијих производа и технологија убудуће². Треба имати у виду да и саме технолошке иновације омогућавају и повреде ауторских права.

Са друге стране, претерана заштита не доприноси напретку. Као што је штампарска преса била револуционарни производ који је довео до појефтинјења производње књига, тако се и данас применом револуционалне технологије, створа огроман број јефтиних производа. Ово је довело до револуције знања, тако да је ауторство постало још значајније и важније за економски развој. Уколико би се пак, ауторско право претерано штитило, то би довело до ограничавања приступа информацијама.

Нове пословне стратегије пословања фирми показују да су жигови сада важнији него икад. У глобалној економији државе и предузећа се глобално утркују тако што се развијају процеси тзв. »Building Brand« - а - стварање "Brand Name" производа.³ Оплеменењивање и жигосање производа од стране произвођача

¹ GATT – General Agreement on Tariffs and Trade

² Michael Rayan, исто стр. 27

³ TM (Trade Mark) је сваки знак који разликује један производ од другог по дефиницији из TRIPS-а. Оно што је битно за заштиту знака или жига јесте тзв. «brand awareness» (свест о постојању заштићеног знака). Елементи

постаје најважније у пословној стратегији. У технологији је ово битно због тога што се са именом продаје и производ.

Тако долазимо до сгледавања огромне штетности пиратерије интелектуалних добара. Потребно је обезбедити трансфер знања који поспешује развој привреда неразвијених земаља. Пиратерија не представља трансфер знања! Ако се пође од закључка да светску економију води знање, поставља се питање: да ли се може сматрати да пиратерија шири знање?

Према ставу светских економских стручњака пут до знања води кроз процесе лиценцирања. Аргумент да мања економија нема потребу за тим није логичан и оправдан изговор за прибегавање пиратерији.

Лиценцирање омогућава великим светским фирмама да у процесу производње проналазе локалне партнере који су значајни за развој у мањим земљама. Ово се односи на све врсте производа, па и оне најсавременије, као што су то софтверски производи. У овим процесима је значајна правна информисаност. Примена међународног и националних права у овој области доводи до тзв. праведне употребе («Fair Use») интелектуалних добара, на пример софтверских производа.

На светском плану заштите интелектуалне својине се приликом нормирања комбинују резултати научног истраживања која дају одговоре на два кључна питања: 1) Колико је довољно издвајати на плаћање права по основу интелектуалне својине да би се развили нови производи? Одговор на ово питање диктира јачину репресије у заштити права интелектуалне својине. 2) Колико треба издвојити за трансфер знања? Одговор на то питање диктира питање степен примене принципа опортунитета у заштити интелектуалне својине.

Од маја 2002.године, у процедури пред Савезном Владом усвојени су Закони о потврђивању следећих међународних конвенција: Уговора о ауторском праву WIPO (1996), Уговора о интерпретацијама и фонограмима WIPO (1996) Конвенције за заштиту права произвођача фонограма од неовлашћене употребе њихових фонограма (1971), Римске конвенције за заштиту извођача, произвођача фонограма и установа за радио-дифузију (1961).

Због потребе јачања заштите јавног интереса у овој области, ипак је извршена измена Кривичног закона Србије и уведено ново кривично дело неовлашћена употреба туђег ауторског права у чл. 183а. Ово дело има три квалификована облика где се у првом ставу санкционише употреба туђег ауторског права без елемената користољубља, затим у ставу два се санкционише повреда ауторског и сродног права уз прибављање противправне имовинске користи, а у трећем ставу се као квалификаторна околност санкционише организована пиратерија са запрећеном казном до 8 година затвора. Норме Закон о ауторском праву у односу на ову норму не представљају «lex specialis», већ је то, вољом законодавца, обрнуто. Другачији правни став заузимају они којима воља законодавца не одговара из политичких или криминалних разлога.

Међународне стандарде заштите од криминалитета у овој области дају прописи Светска трговинска организација (WTO), Светска организација за интелектуалну својину (WIPO) и мултилатерална конвенција Споразум о

трговинским аспектима заштите права интелектуалне својине (TRIPS).⁴ За кривичноправну заштиту на регионалном нивоу велику важност у овој области треба да има окупљање и сарадње земаља Југоисточне Европе ради уједначене примене норми за заштиту права интелектуалне својине и других облика транснационалног криминала.⁵ Тужилаштва земаља Југоисточне Европе морају у потпуности овладати стандардима нормирања (кодификација) и стандардима процесуирања (унификација поступања) кривичних дела неовлашћене употребе туђег ауторског права.

Компјутерски криминал

У области компјутерског криминала који је у вези са повредама права интелектуалне својине, поједине државе организују посебне институције које се баве нормирањем заштите и едукацијом у области заштите од компјутерског криминала и повреда интелектуалне својине и сродних права.⁶

Сматрамо да је потребно да прво анализирамо одређене карактеристике компјутерског криминала у овој области кршења одредби TRIPS конвенције, јер се мотивација извршилаца пре свега, састоји у користољубљу.

Проблем ефикасности кривичноправне заштите од компјутерског криминала неки стручњаци стављају у зависност од одговора на претходно морално питање. Уколико у некој средини не постоји одређени морални приступ овом проблему, тада нису испуњени сви неопходни предуслови за ефикасну заштиту наших података на рачунарима, нити других друштвених вредности!⁷

Највећи део права обезбеђује се путем грађанско правне заштите у оквиру које се процедурално покрећу поступци пред судом од стране оштећених компанија. Глобалне и регионалне слабости заштите се састоје у томе што:

1. Државни органи по службеној дужности ретко покрећу поступак,
2. Оштећени је по Закону често једини овлашћен да поднесе тужбу,
3. Држава реагује тек када је дошло до извршење кривичног дела,
4. Релативно висок сандард за покретање кривичног поступка (услов да постоји основана сумња да је извршено кривично дело).

Кад је у питању копирање и кријумчарење софтвера, као што је то био случај раније код копирања плоча и трака, ова појава представља својеврстан проблем за одређивање правне квалификације кривичног дела, с обзиром да је дошло до промена у технологији копирања. Разликујемо два технолошка периода: период пре-дигиталне револуције (B.D. – »Before Digital« као аналогија на ознаку историјског раздобља: »BC«) и период пост-дигиталне револуције (AD) у најновијем добу.

4 World trade Organisation (WTO) - СТО – Светск трговинска организација, World Intellectual Property Organisation (WIPO) Светска организација за интелектуалну својину; Trade Related Aspects of Intellectual Property Rights (TRIPS) - ТРИПС – Споразум о трговинским аспектима заштите права интелектуалне својине

5 Иницијатива за сарадњу земаља југоисточне Европе - SECI - Southeast European Cooperation Initiative

6 Програм развоја привредног права у САД - CLDP - Commercial Law Development Program

7 Jason Gull, Trial Attorney for Computer Crime and Intellectual Property Rights Регионална конференција земаља југоисточне Европе о питањима заштите права интелектуалне својине од 17. до 19. 10. 2001. године у Цавтату

У ери предигиталне револуције познати су бројни случаји копирања видео касета са филмовима и другим интелектуалним творевина.⁸ Начин откривања илегално копираних видео снимака је релативно једноставнији и обавља се класичним полицијским методама заплена робе у продавницама и поређењем са оригиналним касетма.

У постдигиталном периоду познато је да се копирање и неовлашћено корошћење права интелектуалне својине дешава на Интернету на тзв. «Warez» – чвориштима. На овим чвориштима сами корисници дају свој софтер или филмове који су претходно копирани и омогућавају да се и други корисници упознају са софтером и да га користе на својим компјутерима дакле, да пренесу и шире кршење права интелектуалне својине у недоглед. Но ни Интернет више није сигуран, па криминалци прибегавају коришћењу сателитске комуникације да се ексклузивно повежу.

За копирање кредитних картица извршиоци користе тзв. «скимере» који меморишу магнетни запис на картици, тако да је картица жртве ове врсте крађе идентитета «виђена» од момента када је провучена кроз апарат, до узимања отиска на «слипу» и враћања. У стању су да накаче лажан интерфејс (бројчаник) на банкомату који копира и меморише и број кредитне картице и «ПИН» код. Како доказати постојање кривичног дела, ако је садржај магнетног записа копиран и послат електронском поштом, а порука одмах затим избрисана са «палм-топ» компјутера?

У случајевима када се ради о неовлашћеном дигиталном копирању, тужилац може да наложи да се спроведе прикривена операција по одобрењу истражног судије. У суштини се ради о томе да се организује својеврстан мониторинг на Интернету или у информационим системима банака и на местима коришћења картица.

Кад је реч о појавама на Интернету, сумњичени обично користи један компјутер тако што на њему организује Интернет чвориште (преварни или пиратски сајт). Овакви пиратски сајтови обично се организују илегално у некој фирми која има много бржи приступ на Интернет са већим трансфером, што омогућава да и корисници на том пиратском сајту буду брже услужени, да се брже дистрибуира слање преварних порука, односно, да врше бржи downloads софтера са тако моћног сервера.

Посебна врста извршилаца ових кривичних дела представљају пирати на одређеном нивоу (**PWA**). Ради се уствари, о тајним групама извршилаца који имају својеврсну структуру. Комуницирају преко IRC где је приступ дозвољен члановима под шифром, где се нови чланови примају гласањем, а унапређују постојећи чланови. FTP чворишта користе да преносе или сторнирају библиотеке пиратизованог софтвера и ту је IP адреса позната само онима који су претходно установили свој ID & passwords. Најчешће се у пиратерији ангажују људи који су на законит начин набавили софтер, па га затим ставили на располагање хакерима који разбијају шифре (тзв. »крекери« и »рипери«). Након тога на сцену ступају тзв. «анонимни римејлери». Они користе главну карактеристику Интернета - анонимност, тако да се у пошти разних корисника може пронаћи илегално пиратизован софтер,

⁸ Случај у спору између Владе САД и Тан Тиен Гоа, који је настао тако што је именовани основао ланац видео продавница које су биле снабдеване са видео записима који су се по свом паковању и садржају згледали као оригинални производи а на којима је фасификовано и ТМ - Tai Seng, произвођача са Далеког Истока а који легално копира филмове са тог подручја

послан од стране анонимних “поштар”. На многим пиратским чвориштима се објављују оригинални серијски бројеви софтвера ⁹.

У међународној борби против компјутерског криминала запажени су и следећи видови криминалног понашања: објављивање генератора шифара разних система заштите, давање такозване шервер верзије софтера на пиратизовање, упознавање са системима заштите на шервер везији, Stasck верзије (разбијање шифре), давање на коришћење тако лажно регистрованог софтера, ктрађа идентитета итд.

Околности које погодују настанку ове врсте криминалитета су:

1. Лакоћа комуникације на Интернету,
2. Последице могу бити велике због распрострањености ове светске мреже,
3. Постоји могућност наступања материјалне и моралне штете за жртве које су јако удаљене (доступност жртава),
4. Тешкоћа је забранити ове активности и гонити извршиоце због анонимности на Интернету и веома великих могућности у погледу скривања трагова.
5. Постоје тешкоће у спровођењу истрага на транснационалном нивоу (неопходна асистенција страног правосуђа). Ограничења у националном законодавству, као што је на пример: извршења кривичног дела коцке - хазардерства, где у неким земљама за коцкање или игре хазардним играма није предвиђен кривични прогон, па је због тога отежана асистенција која подразумева реципротитет. Затим “хаковање” страног софтера, у условима када није предвиђена заштита на националном нивоу, затим тешкоће у спречавању дистрибуције порнографије.

Намеће се закључак да глобална природа Интернета отежава примену сваког посебног националног законодавства. Многе земље, као и Република Србија имају модерно национално законодавство и предвиђају кривични прогон, али се кривични прогон не примењује са подједнаком ефикасношћу. У пракси је тешко издејствовати забрану односно, привремену меру безбедности забране растурања и стављања у промет неког садржаја или заплону кривотворене робе, а поготово тешкоће настају када треба спровести кривични прогон у целини.

Идентитет извршилаца је следећа критична тачка у истрази и представља тешкоћу у откривању из следећих разлога: кривично дело се врши са велике дистанце преко више чворишта, не постоје “биометрички” идентификациони знаци за извршиоца као што то постоји у реалном свету ван Cyberspace-а (нема отисака прстију), докази постојања електронских наредби, налога програма и другог се лако уништавају, идентитет извршиоца као учесника у комуникацији на мрежи је могуће открити, али је то отежано с обзиром на начин на који се извршиоци идентификују, адреса је или у виду E-mail address или постоји само IP адреса, а даља тешкоћа је што адреса, односно домен чворишта може бити лажан.

Потенцијални извршилац обезбеђује лажну адресу и идентитет на Интернету на следеће ачине:

1. Карађа адресе неког легалног корисника у E-mail –а који се користи тако да се пошта шаље са сервера неког другог провајдера, а не онога који је организовао чвориште - Интернет сајт оригиналне адресе, с тим што су адресе

⁹ Познат је случај заплена пиратског чворишта на серверу који је део Хрватског Телекома.

истоветне по свом називу Такође је могуће да се IP адреса којој се обраћа потенцијални корисник фалсификује и тада се ради о другом домену, а не само провајдеру.

2. Поступак којим се сакрива прави извор односно, право место компјутера са кога долази напад. При томе се, ради отежавања могућности откривања извора напада, врше скокови са једног сервера на други сервер – тзв «пресељавање» Интернет странице или сајта тако да се приметне траг. Ова појава се може приказати као више IP адреса на различитим клијентима које се размењују преко једног чворишта тако да долази до скокова на мрежи при чему се мењају и адресе.

Тужиоци морају да предлажу примену специјалне истражне технике трагања на мрежи (“Tracing”). Полази се од чињеница које детерминишу идентификацију. Најважнија је информација од провајдера који може саопштити телефонски борј или други прикључак са кога је дошла порука, међутим, тешкоћа је што у процесу трагања долази до протекла времена и до тога да потенцијални извршилац ово време користи за уништавање трагова свог присуства на мрежи. Због тога је трагање и кривични прогон на интернационалном плану неопходно организовати и координирати, јер се само на тај начин брзо може реаговати на ове појаве.

Постоји могућност тзв. “on-line истраге”, али је ова истрага веома отежана због недостатка адекватне комуникације и сарадње на кривичном прогону. За ову врсту истраге и кривичног прогона врше се одређене стручне припреме. Формиран је тим за борбу против компјутерског криминала у Окружном и Другом општинском јавном тужилаштву у Београду. Врши се стручно усавршавање на консултацијама у иностранству уз помоћ UNDP, CLDP, OESC, SPOC, SECI. Остварује се повезивање овог тима са одељењима МУП-а за борбу против компјутерског криминала и пиратерије.

За међународну сарадњу на кривичном прогону постоји нормативна основа јер је Европски Савет донео одређене документе у виду Конвенције за сузбијање компјутерског криминала. Истом је предвиђено да се врши кривични прогон за све врсте штетних понашања на Интернету као кривичних дела, што значи и обавезу земаља које буду приступиле да кривичне одредбе инкорпорирају у своје Кривичне законе те да предвиде одређени механизам за узајамну помоћ при откривању и у кривичном прогону.

У складу са овим европским нормативним решењима предвиђена је посебна група кривичних дела, која имају за групни заштитни објект безбедност рачунарских података. Законодавац је узео крајње уопштен појам – рачунарски податкк, као основни елемент богатог мозаика интелектуалних творевина Интернета и кибер-простора. Санкционисане су све најопасније радње: неовлашћен приступ, оштећење мреже или базе података, прикривено убацивање, уношење вируса, обмане из користољубља, крипто приступ и сметње приступу. При сакупљању доказа минимални стандард је да се докази законито прибаве и да су независно потврђени. Електронски податак је сам по себи безличан, као што је то и само наелектрисање које може бити само позитивно или негативно и на било ком медијуму, али уколико се електронски податак региструје од стране уређаја који је унапред припремљен да бележи тзв. дневник улаза (log entries) или тзв. дневник предмета (log files), тада тужилац располаже са независно потврђеним доказом подобним да се изведе пред судом (independently corroborative evidence). Ово потврђивање доказа може бити фактичко (снимање и конзервација порука –

архивираних или послатих и сакупљање порука издатих на захтев МУП-а) или може бити документално (докази прикупљени у тзв. регистарску замку или добијени трагањем на Интернету (tracing), документи државе издавања, државе транзита и државе пријема). У овој истрази тужиоци треба да разликују несадржајне податке који се релативно лако прибављају (подаци о промету, о подносиоцу итд.) и садржајне податке који се теже прибављају (наредбе, поруке и др). Потребно је правити разлику између података у реакном времену (real-time data), кој је теже прибавити путем мониторинга или пресретања и историјских података у информационом систему које је лакше прибавити.

Истрага на Интернету је стандардна као и механизам функционисања ове светске мреже. У истрази се полази од тога да сваки рачунар има своју «личну карту» (IP address). Најједноставније речено мрежни рачунари (рутери) као емисиони сецкају поруке у пакетиће, а одредишни рачунари склапају поруке. По једном протоколу рачунар сецка и пакује поруке по случајном редоследу (TCP), а по другом протоколу рачунар одрђује датаграме и додељује адресе (IP). Ако се на неком порталу на Интернету појави преварна порука, организује се мониторинг. Традиционалним истражним методама (утврђивање необичних послова, мотива користољубља, тражење провере од финансијске полиције) овде се ништа не постиже. Неопходна је примена тзв. кибер-метода (cyber-methods). Прво се употребљавају тзв. јавно доступни алати за проверу IP адресе (програмски алати који обезбеђују независно потврђивање резултата, могу се добити преко на пример: ARIN, samspade.org, geekotools.org). Када се одреди ком web сервису (hosting service) припада нека Интернет страница, тужилац може предложити истражном судији да затражи од сервисера податке о идентитету лица које је послало поруку, ако је истрага започета или да наложи примену прислушкивања и мониторинга, ако се то утврђује у преткривичном поступку. Први подаци могу бити са листе корисника из јавне базе на web претраживачу «Yahoo». Обично су први добијени подаци лажни, јер се ради о јавном приступу, али се испоставља да је E-mail адреса иста као и алтернативна адреса корисника под неким именом које користи осумњичени. Сервисер има листу корисника који креирају или едитују Интернет страницу. Истражном судији се обично предлаже да тражи и ту листу или је прибави путем узајамне правне помоћи из иностранства. Из ових листа се може утврђивати веза између IP адреса код разних сервис провајдера где се појављује осумњичени. Затим се утврђује одакле се шаљу поруке сервис провајдерима. Овде се одгонета да ли је порука послата из неког предузећа и да ли је то правно лице умешано у превару или се неко крије иза тога. Да би се на крају истраге или провера утврдило и ко шаље поруке. Анализирају се дневници мониторинга добијени по налогу истражног судије (у дневницима се бележе историјски подаци по времену коришћења и по IP адресама). Дневници показују ко плаћа чвориште на Интернету. Прибављају се и рачуни којима је плаћено чвориште. Но то није све, рачун за услуге може бити «хакован». Тада се за утврђивање идентитета иде другим путем. Ако су дневници приступа (radius log entries) обезбеђени за приступ од стране НН корисника, тада се записују идентификациони подаци (ID) позивара интернет сервис провајеру (ISP). Након тога се сазнаје телефонски број осумњиченог. Али тужилац не располаже са довољно доказа док се не спроведе заплена рачунара у стану осумњиченог. Подаци на рачунару откривају везу осумњиченог са провајдером. Због изненадног упада у стан осумњичени не може или нема довољно знања да обриш податке са рачунара, а могу постојати и разне белешке. За тужиоце је довољно да знају да могу дати налог да се са специјалним алатим испијају дискови на рачунару и утврди садржај «обрисаних» порука.

У складу са европским нормативним решењима и према Нацрту Кривичног законика СРЈ, извршена је измена Кривичног закона Србије, па је тако предвиђена посебна група кривичних дела, која имају за групни заштитни објект безбедност рачунарских података. Законодавац је узео крајње уопштен појам – рачунарски податк као основни елемент богатог мозаика Интернета и кибер-простора.

У суштини ових промена закона је намера законодавца да инкриминише сва до сада регистрована штетна понашања и злоупотребе извршене уз употребу рачунара и рачунарске технологије. Овај напор законодавца треба подржати јер сматрамо да се ради о специфичној врсти кривичних дела и по начину извршења и по средствима (објектима) радње извршења и по последицама. Овај приступ је у складу са до сада објављеним научним радовима у којим су дате дефиниције компјутерског криминала и оцењено да се ради о специфичној области.

Нова кривична дела су: Неовлашћено коришћење рачунара и рачунарске мреже, Оштећење рачунарских података, Рачунарска саботажа, Прављење и уношење рачунарских вируса, Рачунарска превара, Ометање функционисања електронске обраде података и рачунарске мреже, Неовлашћен приступ заштићеном рачунару и рачунарској мрежи, Спречавање и ограничавање приступа рачунарској мрежи и др, конструисана су на основу постојећих, да тако кажемо «класичних кривичних дела». Та кривична дела су: Оштећење туђе ствари, Уништење или оштећење јавних уређаја, Саботажа, Шпијунажа, Крађа, Превара, Повреда тајности писама или других пошиљки, Неовлашћено откривање тајне, Одавање пословне тајне, Одавање и коришћење берзанске тајне, Одавање службене тајне и др.

**Jovan Krstić, Deputy Prosecutor General of Serbia
Legal Advisor of SCG in SECI**

Standards of Conduct for the Prosecutors in Combat to Cybercrime

Summary

Prosecutor representatives of Albania, Bosnia and Herzegovina, Bulgaria, Croatia, Greece, Hungary, FYR of Macedonia, Moldova, Romania, Serbia and Montenegro, Slovenia and Turkey, convened in Beograd, decided on December 11-12, 2003, to constitute the Southeastern European Prosecutors Advisory Group (SEEPAG). That is the unique international body with the professional independence and self-managed position, and it has the common characteristic of the position of prosecutors of the region in the framework of their national legal systems. It is expected that the members of the SEEPAG can be responsible for developing and coordinating transnational prosecutions.

Contact Persons were appointed in each of the above mentioned states. Close cooperation will be ensured with all the relevant regional institution and initiatives, in

order to provide necessary assistance to the Task Forces functioning under the SECI Regional Center for Combating Trans-border Crime.

National Parliament of Serbia adopted the changes of the Criminal Law by introducing new criminal offense: Unauthorized use of another man right of the author and related rights (Article 183-a). In the Esential Criminal Code we have another legal tool for combat IPR infringements: Unauthorized use of another man's firm (Article 165)

There are numerous differences between Cyber-crimes and Classic crimes because the previous one is happening mostly in specific surrounding known as Cyberspace which itself consists of many intellectual creations. Computer pogroms are often created, used and abused for various fraudulent schemes. The most dangerous one is the Pyramid Scheme, and the theft of identitiy on the Internet. All of the regional countries experienced the investigations in subjects on legal prosecution for investment frauds and some concrete measures in law enforcement should be standardized.

Key words: SEEPAG – Standards - IPR – Cyber-crime - Fraud
