Прегледни чланак 343.533:004]:061.1EU

Милана Писарић, асистент
Правног факултета у Новом Саду

СТАЊЕ И ТЕНДЕНЦИЈЕ У СУПРОТСТАВЉАЊУ КОМПЈУТЕРСКОМ КРИМИНАЛУ НА ЕВРОПСКОМ НИВОУ[1]

***Сажетак**: Интеграција телекомуникационих и информационих система у савременом друштву омогућава складиштење и пренос података о свим врстама комуникација чиме је створен низ нових могућности за злоупотребе у оквиру сајбер простора. Те злоупотребе се односе на угрожавање интегритета, доступности или поверљивости рачунарских мрежа и телекомуникационих система и са њима повезаних података или се односе на употребу таквих мрежа и система за извршавање «традиционалних» кривичних дела. Све ове злоупотребе могу се заједничким именом означити као компјутерски криминал. Без одређених прилагођавања специфичностима компјутерског криминала, као појаве глобалних размера, откривање, доказивање, истраживање и кривично гоњење ове врсте криминала готово да је немогуће. Стога је уочена потреба за постављањем правног оквира супротстављања компјутерском криминалу, који би чинила материјалноправна и процесноправна правила прилагођена овој врсти криминала као и за унапређењем међународне сарадње, у оквиру глобалне и регионалне борбе против сајбер криминала. У раду ће бити представљено тренутно стање стратешких и правних оквира супротстављања компјутерском криминалу на нивоу Савета Европе и Европске уније, као и тенденције у развоју планског супротстављања поменутим злоупотребама у оквиру ових регионалних организација.*

---

[1] Рад је резултат рада на Пројекту: "***Теоријски и практични проблеми стварања и примене права (ЕУ и Србија)***" чији носилац је Правни факултет Универзитета у Новом Саду

Кључне речи: *компјутерски криминал, правни оквири, Савет Европе, Европска унија.*

1. САВЕТ ЕВРОПЕ

Прва међународна иницијатива која се односила на компјутерски криминал потекла је са Конференције Савета Европе о криминолошким аспектима привредног криминала 1976. године[2], и већ тада је препознато неколико облика злоупотреба рачунара. Након тога, Савет Европе је донео две препоруке у вези са компјутерским криминалом, а 2001. године у оквиру ове организације усвојена је Конвенција о компјутерском криминалу.

1.1. Препоруке Савета Европе

Савет Европе именовао је 1985. год. стручну комисију ради разматрања правних питања у вези са компјутерским криминалом. Резиме смерница националним законодавствима представљен је у предлогу *Препоруке бр. (89) 9 од 13.септембра 1989. године која се односи на са компјутерима повезана кривична дела*[3]. У овој препоруци су просте наведени и описани поједини облици компјутерских кривичних дела, као смерница државама у регилисању ових појава на националном ниову. Занимљиво је да је још тада утврђен минимални списак компјутерских кривичних дела које би требало предвидети у кривичноматеријалним прописима, а на који су уврштени рачунарска превара, компјутерски фалсификат, оштећење компјутерских података или компјутерских програма, рачунарска саботажа, неовлашћени приступ, неовлашћено прислушкивање, неовлашћено умножавање заштићеног компјутерског програма и неовлашћено умножавање топографије[4].

Што се тиче процедуралних питања, значајна је *Препорука СЕ бр. (95) 13 од 11. септембра 1995. године која де односи на проблеме кривич-*

[2] 12th Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 15–18 November 1976.

[3] *Computer-related crime: Recommendation No. R. (89) 9,* Препорука је доступна на интернет страници: *https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2* (20.12.2010).

[4] Уз овај списак, представљена је опциона листа, на којој су измена компјутерских података и компјутерских програма, компјутерска шпијунажа, неовлашћена употреба компјутера, неовлашћена употреба заштићених компјутерских програма, а која као кривична дела могу предвидети земље приликом разматрања регулисања кривичних дела у вези са компјутерима у националним законодавствима.

ној процесној права у вези са информационом технологијом[5]. Препорука поставља 18 принципа који се односе на претрес и заплена; технички надзор; обавезу сарадње са истражним органима; електронске доказе; коришћење кодирања; истраживање, статистику и обуку и међународну сарадњу, а који су касније разрађени и инкорпорисани у Конвенцију СЕ.

1.2. Конвенција о компјутерском криминалу [6]

Европски комитет за проблеме криминала (*European Committee on Crime Problems (CDPC))* је у новембру 1996. године донео одлуку да образује комисију састављену од стручњака за компјутерски криминал која би саставила нацрт будуће конвенције[7]. Конвенција је усвојена и била је отворена за потпис на Конференцији Савета Европе 23. новемра 2001. године, а на снагу је ступила 1. јула 2004. године[8]. До јануара 2011. године Конвенцији су приступиле следеће земље чланице Савета Европе: Азербејџан, Албанија, Аустрија, Белгија, Босна и Херцеговина, Бугарска, Грчка, Грузија, Данска, Естонија, Ирска, Исланд, Италија, Јерменија, Кипар, Летонија, Лихтенштајн, Луксембург, Македонија, Малта, Мађарска, Молдавија, Немачка, Норвешка, Пољска, Португалија, Румунија, Словачка, Словенија, Србија[9], Турска, Уједињено Краљевство Велике Британије и Северне Ирске, Украјина, Финска, Француска, Холандија, Хрватска, Црна Гора, Чешка, Швајцарска, Шведска, Шпанија. Ако се узма у разматрање листа потписница, може се уочити следеће: Андора, Монако, Русија и Сан Марино су једине земље чланице Савета Европе које нису потписнице Конвенције, док су Конвенцију са друге стране потписале и земље ван Европе, чиме је превазишла регионални значај и стекла универзални карактер[10]. Ако се даље анализира листа потписница у погледу корака које су предузеле ка имплементацији Конвенције, уочава се да су четрнаест земаља чла-

---

[5] *Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on 11 September 1995, https://wcd.coe.int/wcd/com.instranet.InstraServlet? command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2* (20.12.2010).

[6] *Convention on cyber crime CETS No. 185*, *http://conventions.coe.int* (20.12.2010).

[7] Наведено према: *Explanatory Report of the Convention on Cybercrime (185), No. 10, http://conventions.coe.int* (20.12.2010).

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

[9] Конвенција потписана 7/4/2005, ратификована 14/4/2009, ступила на правну снагу 1/8/2009.

[10] Ради се о следећим земљама: Канада, Јапан, Јужноафричка република, Сједињене Америчке државе (у САД Конвенција не само да је потписана 23/11/2001, него је и ратификована 29/9/2006 а на правну снагу ступила је 1/1/2007).

ница Савета Европе потписале Конвенцију али у тим земљама овај међународноправни инструмент није ни ратификован, па самим тим није ни ступио на правну снагу – осам од тих земаља су истовремено чланице Европске уније.[11]

Ратификовањем или приступањем Конвенцији, држава се обавезује да имплементацијом обезбеди да у домаћем законодавству буду као кривична дела предвиђена одређена понашања описана у материјалним одредбама Конвенције и да успостави поступке неопходне за истрагу и кривично гоњење таквих кривичних дела, а који су описани у процесним одредбама Конвенције.

Што се тиче структуре, Конвенција садржи четири поглавља.

У *првом поглављу* дефинисани су основни појмови (рачунарски систем, рачунарски подаци, провајдери услуга, проток података).

Друго поглавље садржи легислативне мере које треба предузети на националном нивоу, а односе се на кривично материјално право и кривично процесно право. У оквиру одељка 1. постављена је типологија кривичних дела, која је од изузетног значаја јер је усвајају међународни и национални прописи који уређују компјутерски криминал (иста је преузета и у актима ЕУ). Конвенција наиме разликује четири типа кривичних дела:

– прву групу чине кривична дела усмерена против поверљивости, интегритета и доступности података и информационих система;

– другу групу чине кривична дела која су повезана са компјутерима (*computer-related crimes*) у извршењу којих се компјутер појављује као средство (као што су фалсификовање и превара);

– трећу групу чине кривична дела у вези са садржајем (као што је дечја порнографија);

– четврту групу чине повреде ауторских и сродних права[12].

Конвенција пред потписнице поставља захтев за увођењем истражних овлашћења, а ради модернизације «алата» који стоје на располагању органима истраге и гоњења у вези са са компјутерским криминалом. Наиме, у оквиру одељка 2. (чланови 14–21.) су одредбе које се односе на процесно право, а садрже одређене смернице за поступак, који се води у вези са кривичним делом које извршено путем компјутерских система, и смернице за

[11] Листа потписница (стање на дан 3.3.2011.године) може се пронаћи на интернет страници: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

[12] Државе могу искључити безначајна или ситна дела из импленетације. Дела морају да буду намерно почињена да би постојала кривична одговорност. Дело мора бити почињено без правног основа, што може да се односи на то да су радње предузете без овлашћења или уз овлашћење, које не покрива законске одбране, изговор, оправдања или релевантне принципе по домаћем закону.

прикупљање доказа у електронском облику о извршеном кривичном делу (чак и о кривичном делу које не спада у компјутерски криминал у смислу Конвенције). Овај део Конвенције садржи одредбе које се односе на:

– захтев за убрзаном процедуром чувања ускладиштених компјутерских података – органи гоњења треба да буду овлашћени да издају наредбу да се сачувају похрањени подаци, и до 90 дана, за податке од могућег значаја за кривични поступак, како би се избегло уништење или оштећење ових података – треба омогућити и тражење и чувања података о комуникационом саобраћају (*traffic data*) од провајдера телекомуникационих услуга;

– наредбу за издавање (*production order*) – којом се може тражити издавање података о кориснику од лица које такве податке има у поседу, односно од провајдера телекомуникационих услуга;

– претрагу и заплену података похрањених у рачунару који се претреса као и рачунара ком се преко прегледаног може приступити;

– прикупљање рачунарских података у реалном времену – како података о комуникационом саобраћају (*traffic data*), тако и података о садржају комуникација (*content data*) – прикупљање могу вршити органи гоњења или провајдери услуга по њиховом налогу.

Успостављање, спровођење и примена овлашћења и поступака наведених у делу који се односи на процесно право захтева од државе да обезбеди адекватну заштиту људских права и слобода – првенствено права на приватност. При том треба да се поштују уобичајени стандарди, тј. минималне мере заштите, укључујући међународне инструменте о људским правима[13].

Треће поглавље односи се на међународну сарадњу, те поставља принципе у вези са надлежношћу, екстрадицијом и међународном помоћи (процедуре које се односе на међусобне захтеве за помоћ у недостатку важећих међународних споразума, узајамну помоћ у вези са привременим мерама, те узајамну помоћ у вези са истрагом). Што се тиче надлежности, у члану 22. Конвенције предвиђена су три критеријума за њено одређивање – место извршења кривичног дела, држављанство извршиоца и место лишења слободе извршиоца, а у случају сукоба надлежности између две државе потписнице, као метод решавања сукоба предвиђа се договор између пот-

[13] Принцип пропорционалности треба да буде укључен. Свако овлашћење или поступак ће се применити/спроводити сразмерно природи и околностима извршења кривичног дела. Свака држава трба да размотри утицај овлашћења и поступака из овог одељка на права, одговорности и легитимне интересе трећих лица, укључујући и пружаоце услуга и интересе јавности и жртава. Такође, државе могу обезбедити у својим законодавтсвима додатну заштиту права и слобода, предвиђајући судску или другу независну контролу основа за одређивање таквих мера, трајања итд.

писница. У погледу међусобне помоћи, Конвенција успоставља процедуре, како у вези са истрагом и гоњењем извршиоца, тако и за прикупљање доказа у дигиталном облику, али има супсидијарни карактер, јер пружа правни оквир за међусобну помоћ када не постоји други основ (уговор) за пружање међународне помоћи између две државе.

Четврто поглавље садржи завршне одредбе. У складу са чланом 40., свака држава може изјавити да оставља могућност захтевања додатних елемената, како је предвиђено, по одређеним члановима. Слично је са стављањем резерви у складу са чланом 42. по ком свака држава може изјавити да ће искористи могућност стављања резерви како је то предвиђено у појединим члановима.

Што се тиче значаја Конвенције, неспорно је да представља први и за сада једини међународни уговор глобалног домета који се односи на компјутерски криминал, а који је императивног карактера. Наиме, када држава приступи Конвенцији или је потпише и ратификује, Конвенција постаје обавезујућа за државу у смислу што је неопходно у националном законодавству предузети неопходне законодавне мере у циљу имплементације одредба Конвенције у правни систем земље потписнице. Међутим, не само да Конвенција садржи минимална правила која треба да се угради у материјално и процесно законодавство држава потписница (директна имплементација – имплементација као обавеза), него и та иста правила могу да послуже као као модел за израду прописа међународним организацијама и државама које нису у обавези имплементације (индиректна имплементација – имплементација као модел).

Треба истаћи да је до сада Конвенција као узор за регулисање компјутерског криминала послужила законодавствима у преко 100 земаља[14], али пун смисао Конвенције био постигнут зек када би је потписале и ратификовале, а тиме и имплентирале у своја законодавства све државе света, међутим, за сада, реалност је другачија –неке од најзначајнијих земаља чланица СЕ нису је ни потписале (Русија, Турска), друге је нису ратификовале (Шпанија, УК, Пољска итд.), а од десет земаља које имају највећи број корисника интернета по становнику, само три су је ратификовале (САД, Немачка, Француска), док је Кина, Бразил, Индија и Русија нису чак ни потписале[15].

Ипак, Конвенција је од изузетног значаја за европски простор, јер је послужила као модел/ узор са састављање референтних правних аката ЕУ.

---

[14] Наведено према: *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Ws%203/cyber_octopus_WS_3_ alexander_CCC_global_frame.pdf* (20.12.2010).

[15] F. Calderoni, „The European legal framework on cybercrime: striving for an effective implementation“, *Crime, Law and Social Change*, 5/2010, 350.

2. ЕВРОПСКА УНИЈА

На почетку новог миленијума борба против високотехнолошог криминала уврштена је међу политичке приоритете Европске уније. Европска комисија је у априлу 1998. године представила Студију о правним аспектима компјутерског криминала у информационом друштву[16], у коме је указано на специфичне проблеме и опасности криминала повезаног са компјутерима. Маја 1999. године Комисија је заузела становиште у вези са преговорима око нацрта Конвенције СЕ о компјутерском криминалу, према ком земље чланице ЕУ у потпуности подржавају будућу Конвенцију[17]. Међутим, иако су до сада Конвенцију о компјутерском криминалу СЕ из 2001. године потписале све државе у оквиру ЕУ, иста до сада још увек није ратификована а тиме ни ступила на снагу у свим земљама чланицама.

На нивоу Европске уније препозната је опасност од компјутерског криминала и утврђена је јасна опредељност супротстављању овом облику криминала. Поред тога што постоји неколико стратешких докумената, који се односе превасходно на рачунарску безбедност, од релевантних правних извора најзначајнија је *Оквирна одлука о нападима на информационе системе*, а у току је припрема за поступак усвајања директиве која би на свеобухватан начин уредила питање компјутерског криминала. Такође, формиране су специјализоване агенције у циљу супротстављања кривичним делима у вези са компјутерима, а инситира се и на унапређењу прекограничне сарадње.

2.1. Стратешко опредељење ка борби против компјутерског криминала

Стратешко опредељење ЕУ ка борби против компјутерског криминала утврђено је у Саопштењу Комисије ЕУ *Стварање безбеднијег информационог друштва побољшањем безбедности информационих инфраструктура и борбом против са компјутерима повезаног криинала*[18] из 2001. године . У овом саопштењу указано је да на нивоу ЕУ не постоји ниједан извро права који се директно односи на компјутерски криминал, па је уочена потреба за стварањем одговарајућих правних инструмената.

---

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

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

[18] Communication *Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*, може се преузети на интернет страници: *http://www.justice.gov/criminal/cybercrime/intl/EUCommunication.0101.pdf* (20.12.2010).

С тим у вези Комисија је утврдила да ће предложити одређене легислативене мере са циљем приближавања националних материјалноправних и процесноправних прописа у вези са компјутерским криминалом. У погледу материјалноправних мера, изражена је намера да се следи типологија кривичних дела и стандарди које поставља Конвенција СЕ, док је у погледу процесноправних мера, утврђено је да је неопходно уређење следећих питања: пресретање комуникација, међусобно признавање судских наредби у вези са истрагама компјутерског криминала, задржавање информација о преносу података, анонимни приступ и употреба, практична сарадња на међународном нивоу, надлежност, доказна снага копмјутерских података, и сл.

Ово саоштење је заправо представљало иницијативу за касније усвајање Оквирне одлуке о нападима на информационе системе из 2005. године, као обавезујућег извора права у оквиру некадашњег трећег стуба ЕУ.

Даље, Комисија утврђује да ће се заложити за предузимање негелислативних мера, с обзиром да прописи на националном и нивоу ЕУ јесу неопходни, али не и довољни за ефикасно супротстављање компјутерском криминалу. У том смислу, Комисија ће: промовисати формирање полицијских јединица на националном нивоу специјализованих за компјутерски криминал, подржати обуку полицијских службеника и подстицати сарадњу између органа гоњења, привреде, удружења потрошача и организација за заштиту података.

Овакво опредељење Комисије потврђено је и додатно учвршћено у неколико година касније усвојеном саопштењу *Према зејединчкој политици у борби против компјутерскоī криминала* из 2007. године. Након што су препознати основни трендови компјтерског криминала, Комисија је за основне правце даљег развоја политике супротстављања таквом облику криминала поставила: побољшање прекограничне сарадње између полицијских и судских органа држава чланица, између јавног и приватног сектора и међународне сарадње уопште[19]. Препознавање ових принципа, као неопходних, проистекло је из чињенице да компјутерски криминал карактерише повећање броја извршених кривичних дела чије радње су све префињеније са израженом прекограничном димензијом, да је при томе је у извршењу кривичних дела све више изражена заступљеност организованих криминалних група, а да се са друге стране број истрага таквих кривичних дела на принципу прекограничне сарадње не повећава. Због тога побољшање сарадње на националном, европском и међународном нивоу

[19] Towards a general policy on the fight against cyber crime, *http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF* (20.12.2010).

представља императив успешне борбе против компјутерског криминала.[20] У оквиру тога, једна од кључних активности би свакако требала да огледа у успостављању оперативне сарадње између националних органа гоњења и процедура размене података, стручности и примера добре праксе на свим нивоима, као и између јавног и приватног сектора (првенствено се мисли на провајдере интернет услуга). Такође, јасно је постало да је за постизање бољег разумевања феномена компјутерског криминала неопходно установити процедуре статистичког праћења размера компјутерског криминала и обезбедити подршку истраживањима у вези са специфичностима копмјутерског криминала, као и финансијаксу подршку програмима за обуку припадника органа гоњења[21].

Компјутерски криминал је препознат као значајан фактор угрожавања безбедности у оквиру ЕУ и у *Стокхолмском програмуиз 2010. години,* документу који представља политичку агенду ЕУ за период 2010–2014[22], у којој је Савет ЕУ одредио изазове које жели да превазиђе и циљеве које жели да постигне у оквиру простора слободе, безбедности и правде, те је поставио смернице за легислативне и оперативне планове упућене како Комисиј ЕУ тако и државам чланицама. При томе, Савет је указао да би државе чланице требало што је пре могуће да ратификују Конвенцију Савета Европе о компјутерском криминалу, с обзиром да би ова Конвенција требало да постане референтни правни оквир за борбу против високотехнолошког криминала на глобалном нивоу. Пред Комисију је Савет поставио захтев да даје предлоге за разраду правног оквира за истраживања у сајбер простору унутар Уније, те да предузима мере за унапређење/ побољшање партнерства јавног и приватног сектора. С тим у вези, унутар Уније би такође требало се да разјасне правила о надлежности и утврди законски оквир који се примењује на сајбер простора унутар Уније, укључујући уређење прибављања доказа у циљу промоције прекограничне истраге. Услед значаја прекограничне сарадње, Савет је позвао државе чланице да унапреде међусобну правосудну сарадњу у предметима високотехнолошког криминала, нагласивши потребу сарадње и са земљама ван Уније. Такође, Савет је позвао државе чланице да дају пуну подршку националним платформама за обавештавање задужене за борбу против високотех-

[20] Из тих разлога Комисија се и у овом саопштењу залаже за подстицање држава чланица да ратификују Конвенцију СЕ – чак се помиње разматрање могућности да Заједница постане потписница Конвенције (што се до сад није десило).

[21] Ову обуку спроводе у сарадњи *Europol, Eurojust, European Police College (CEPOL) u European Judicial Training Network (EJNT).*

[22] Official Journal of European Union C 115/1, 4.5.2010, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF* (20.12.2010).

нолошког криминала. Истакнуто је да би ЕУРОПОЛ могао да игра улогу ресурсног центра, стварањем Европске платформе за идентификацију дела која би требало да помогне националним платформама за упозоравање, те разменом релевантних података и најбоље праксе у вези са борбом против високотехнолошког криминала између држава чланица.

2.2. Правни оквири

Иако је претња од компјутерског криминала уочена на нивоу ЕУ још почетком новог миленијума и створено јасно опредељење супротстављању овом облику криминала, у погледу релевантних правних оквира, а пре свега услед структуре и надлежности ЕУ у оквиру некадашњег трећаг стуба, још увек не постоји обавезујући извор права који би се директно примењивао у државама чланицама.

Европска комисија је Савету ЕУ 2002. године упутила предлог да се регулише на одређени начин незаконит приступ и поступање у вези са информационим системима, да би Савет ЕУ 24. фебруара 2005. године усвојио Оквирну одлуку о нападима на информационе системе (*Framework Decision 2005/222/JHA on attacks against information systems*)[23]. Сврха поменуте одлуке била је приближавање националног законодавства и унапређење међународне полицијске и правосудне сарадње држава чланица у погледу предвиђања као кривичних дела одређених активности повезаних са информационим системима. Оквирна одлука је створила скуп правних дефиниција и одредила које су то противправне активности у вези са електронским мрежама, компјутерима и другим уређајима повезаним са мрежом (нпр. мобилни телефони), као и у вези са подацима и програмима у тим уређајима и мрежама. У типологији кривичних дела, Оквирна одлука се ослања на типологију утврђену Конвенцијом СЕ, па пред државе чланице поставља захтев да предузму мере да се као кривична дела предвиде и као такве санкционишу следеће активности:

– незаконит приступ информационим системима (чл. 2.);
– незаконито ометање система (чл. 3.), и
– незаконито ометање података (чл. 4.).

Државе чланице се обавезују да за ова кривична дела предвиде максималне казне између 1 и 3 године затвора (чл.6.), односно између 2 и 5 година затвора, уколико су кривична дела почињена у оквиру криминалне организације, што је предвиђено као отежавајућа околност (чл.7.). За кри-

[23] Оквирна одлука објављена је у: Official Journal of the European Union, L 69/67, 16.3.2005., а доступна је на интернет страници: *http://eurlex.europa.eu/LexUriServ/ LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF* (20.12.2010).

вичну одговорност за ова дела неопходно је утврдити постојање умишљаја код учиниоца, а подстицање, помагање, подржавање као и покушај извршења тих дела такође ће би требало да буду кажњени (чл.5.).

Што се тиче надлежности, преузета су правила из Конвенције СЕ, па је држава надлежна за кривично дело извршено на њеној територији[24], критеријум држављанаства се предвиђа као алтернативни за одређивање надлежности, док ће се случају сукоба, надлежност одредити споразумевањем између држава чланица да се централни поступак води у једној од држава које конкуришу на јурисдикцију (чл.10)[25]. У вези са унапређењем међусобне сарадње, у циљу побољшања размене података, од држава чланица се тражи да успоставе мрежу на принципу "24/ 7 " у оквиру које је 24 сата дневно, 7 дана у недељи, могућа размена информација о нападима на информационе системе (чл.11.). Остали аспекти процесног права нису преузети из Конвенције СЕ[26].

Поменута оквирна одлука заправо је први корак ка уређењу компјутерских кривичних дела у оквиру ЕУ. Оквирна одлука није извор права који се непосредно примењује у државама чланицама, него је неопходна имплементација у национална законодавства. Рок за имплементацију ове оквирне одлуке био је 16. март 2007. године (чл.12.), а Комисија је завршила процену нивоа имплементације у јулу 2008. године, и то само за 20 земаља чланица које су доставиле документацију. У извештају је наведено да није извршена потпуна имплементација нити једне одредбе у свих 20 држава, те је процењено да је било потребно 50% више времена за имплементацију Оквирне одлуке него што је државама првобитно остављено.

Због незадовољавајућег успеха у имплементацији Оквирне одлуке, а услед технолошког напретка и појаве нових облика извршавања компјутерских кривичних дела, уочена је потреба за изменом постојећих и стварањем таквих правила и механизама који би заиста допринели откривању и доказивању тих кривичних дела. Могућност за постизање таквог циља ствара тзв. „комунитаризација“ Трећег стуба ЕУ[27]. Наиме, правила ЕУ која

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

[25] То ће бити држава на чијој територији је кривично дело извршено, или држава чији је држављанин извршилац или држава у којој је извршилац пронађен.

[26] M. Gercke, „Europe's legal approaches to cybercrime“, *ERA Forum*, 10/2009, 412.

[27] Дакле, право које је извирало из делокруга трећег стуба Уније није имало дејства комунитарног права, као што су непосредна примењивост и принцип првенства,а са друге стране, комунитарно право има директно дејство и примат у односу на национално право и оно је једино подлегало контроли Европског суда правде.

се односе на уређење одређених области у оквиру бившег Трећег стуба ЕУ пре Лисабонског уговора доношена су у форми оквирних одлука које немају директно дејство у државама чланицама, него је потребна њихова имплементација у национална законодавства. При том Комсија има само могућност надгледања нивоа имплементације правила из оквирних одлука, без могућности да изрекне било какву санкцију држави чланици која не приказује задовољавајући ниво импленетације или да држава одговара због неиспуњења обавеза из оквирне одлуке пред Европским судом правде. Ступањем на снагу Лисабонског уговора 1. децембра 2009. године створене су могућности за олакшано усвајање нових легислативних мера у области правосудне и полицијске сарадње (квалификованом већином чланова Савета ЕУ уз учешће Парламента) и то у форми директиве (која има директно дејство), док је Комисији дато овлашћење да надгледа да ли се земља чланица придржава директиве, те уколико не поступа у складу са директивом, Комисија може да се обрати Европском суду правде[28] .

У вези са потребом за новим правилима у области напада на информационе системе, а на основу нових легислативних могућности, 30. септембра 2010. године Комисија је Савету упутила предлог директиве о нападима на информационе системе, која би требало да замени постојећу Оквирну одлуку[29]. У односу на Оквирну одлуку, предложена директива:

1. поред незаконитог приступа информационим системима, незаконитог ометања система и незаконитог ометања података, предвиђа инкриминацију употребе одређених алата (као што су малициозни софтвери – нпр. ботнет – или незаконито прибављање компјутерских лозинки) за извршавање кривичних дела;

2. уводи незаконито ометање информационог система као кривично дело;

3. предвиђа подизање минимума затворске казне на 2 године;

4. подиже висину максималне казне затвора за кривична дела извршена под отежавајућим околностима на најмање пет година (уместо на две године, како је предвиђено у Оквирној одлуци) уколико је кривично дело извршено: (а) у оквиру криминалне организације; (б) употребом алата који могу да изазову било нападе на велики број информационих система, било нападе који са собом повлаче знатна оштећења, у смислу поремећаја системских услуга, финансијских трошкова или губитка личних података (отежавајућа околност која није била предвиђена у Оквирној одлуци);

[28] E. Kerlin- Karnell, „The Treaty of Lisbon and the Criminal Law: Anything New Under the Sun?“, *European Journal of Law Reform*, 3/2008, 328.

[29] Наведено према: *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1239* (20.12.2010).

(в) прикривањем правог идентитета извршиоца и изазивањем штете законитом власнику идентитета (отежавајућа околност која није била предвиђена у Оквирној одлуци);

5. предвиђа побољшањање полицијске/судске сарадње јачањем постојећег система размене података на принципу 24/7, укључујући обавезу одговора на хитан захтев најкасније у року од 8 сати од постављања захтева;

6. уводи обавезу прикупљања статистичких података о компјутерском криминалу[30].

Иако ће у прелазном периоду до 1. децембра 2014. године Комсија моћи још увек само да надгледа и подржава ефективну имплементацију правила из оквирних одлука у државама чланицама, предвиђено је да ће моћи државу која не спроводи правила да тужи пред Европским судом.

3. ТЕНДЕНЦИЈЕ У СУПРОТСТАВЉАЊУ КОМПЈУТЕРСКОМ КРИМИНАЛУ

За успешно супротстављање компјутерском криминалу није било довољно препознати опасности, креирати одређена правила и успоставити сарадњу на институционалном нивоу. Имајући у виду да ће развој информационих и комуникационих технологија стварати стално нове могућности извршења кривичних дела и онемогућавати њихово откривање, да ће се број корисника поменутих технологија ширити а тиме и размере и распрострањеност компјутерског криминла, као неопходност намеће се константна будност, оспособљеност и спремност на реакцију органа гоњења.

Што се тиче активности **у *оквиру Савета Европе***, од значаја је имплементација друге фазе Пројекта СЕ посвећеном компјутерском криминалу која ће трајати од 1. марта 2009. до 30. јуна 2011. године[31]. Овај Пројекат има за приоритетни циљ промоцију и подршку државама у имплементацији Конвенције и пратећих међународних стандарда, што ће се остварири кроз резултате у следећим областима:

– подстицање националног законодавства и политике држава потписница и могућих потписница на усаглашавање са стандардима постављеним у Конвенцији;

---

[30] Предлог Комисије доступан је јавности преко интернет странице - *http://europa.eu/rapid/ pressReleasesAction.do?reference=MEMO/10/463&format=HTML&aged=0&language=EN&guiLanguage=en* (20.12.2010).

[31] О томе више видети на интернет страници: *http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/projectcyber_en.asp* (20.12.2010).

– подстицање унапређења међународне сарадње – постављањем и јачањем улоге мрежа на принципу 24/7 и специјализованих јединица за компјутерски криминал у оквиру постојећих органа гоњења као и одређивање органа надлежних за пружање међународне правне помоћи;

– подстицање унапређења сарадње органа гоњења и провајдера интернет услуга у истрази компјутерског криминала, у складу са смерницама издатим априла 2008. године[32];

– подстицање стварања институционалне обуке судија и тужилаца у вези са компјутерским криминалом;

– обезбеђење заштите података и приватности у вези са компјутерским криминалом, а у складу са правилима СЕ и другим релевантним међународним стандардима.

На нивоу Европске уније у погледу будућег планског супротстављања компјутерском криминалу постоји неколико стратешких докумената у којима се ова борба поставља као приоритет.

Савет министара ЕУ је новембра 2008. године усвојио *Стратегију за јачање борбе против сајбер криминала* у којој је предложено увођење читавог низа оперативних активности, као што су сајбер патроле, заједнички истражни тимови и даљинска претрага компјутера, који би требало да постану део борбе против компјутерског криминала у будућности. Истовремено у Стратегији су предвиђени конкретени кораци које треба предузети ради успостављања ближе сарадње и размене података између органа гоњења и приватног сектора о истражним техникама заснованим на знању и трендовима копјутерског криминала[33]. На састанку министара ЕУ у априлу 2010. године Савет је у *Акционом плану за спровођење Стратегије за јачање борбе против сајбер криминала*[34] поставио за циљ да се у средњем року оствари напредак у вези са следећим акцијама:

– подстицање држава чланица које су потписале Конвенцију Савета Европе на ратификацију;

– разматрање подизања стандарда у специјализацији полиције, судија, тужилаца и форензичког особље до одговарајућег нивоа за потребе спровођења истрага о компјутерском криминалу (кроз сарадњу држава чланица са ЕУРОПОЛ-ом и Европском групом за обуку и образовање у вези са компјутерским криминалом[35]);

---

[32] Guidelines for the cooperation between law enforcement and internet service providers against cybercrime, доступно на: *http://www.ifap.ru/library/book294.pdf* (20.12.2010).

[33] Наведено према: *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827* (20.12.2010).

[34] Наведено према: *http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/114028.pdf* (20.12.2010).

[35] Европска група за обуку и образовање у вези са компјутерским криминалом, односно *European Cybercrime Training and Education Group (*ECTEG*)* је радна група формирана

– подстицање размене информација између држава чланица (нарочито преко базе података у оквиру ИНТЕРПОЛ-а које садрже слике у вези са дечјом порнографијом);

– промовисање развоја односа између европских агенција (ЕУРОПОЛ[36], ЕНИСА[37] итд.), сличних агенција у трећим земљама и међународних организација (нпр. ИНТЕРПОЛ) ради потпуније процене ситуације у вези са борбом против кибернетичког криминала, сагледавања трендова и нових облика *modus operandi* копмјутерских кривичних дела;

– промовисање хармонизације различитих мрежа на принципу 24/7 (уз избегавање могућег дуплирања у односу на постјеће система у оквиру Г-8 и ИНТЕРПОЛ -а);

– усвајање заједничког приступа у борби против кибернетичког криминала на међународном плану, посебно у односу на одузимање домена и ИП адреса.

Такође, Европској комисији је упућена иницијатива да размотри могућност формирања јединствене и централизоване агенције чији би се задатак огледао у превенцији компјутерског криминала, првенствено онлајн превара и дечје порнографије, кроз подстицање размене информација између надлежних органа држава чланица. Та агенција би требало да има задатак да постави стандарде за обуку полиције, суда, тужилаштва и

у оквиру ЕУРОПОЛ-а која координира хармонизацију иницијатива за обуку органа надлежних за борбу против компјутерског криминала, у заједници са академским институцијама, привредним сектором и представницима цивилног друштва. О томе више видети на интернет страници: *http://www.ecteg.eu/*.

[36] Европска полиција или *Europol* је битан актер борбе против компјутерског криминала који је до сада усавршио алате информационе технологије и формирао тим професионалних аналитичара и стручњака за ИКТ како би био у стању да пружи подршку органима гоњења на нивоу ЕУ. С тим у вези, у оквиру Еуропол-а формиран је *Центар за високотехнолошки криминал* (High Tech Crime Centre at Europol). Новине је то што је у *Стратегији Европола за период* 2010–2014 (из фебруара 2010. године) јасно постављен план да се ојачају способности супротстављања компјутерском криминалу, стварањем *Европског центра за компјутерски криминал у оквиру Европола*.

[37] Поред Еуропола, значајну улогу би требало да оствари *Европска агенција за мрежну и информациону безбедност* (*European Network and Information Security Agency* (ENISA)). ЕНИСА је независна агенција ЕУ, са седиштем у Хераклиноу (Грчка), за коју је предвиђено да ће постојати деловати од 14.марта 2004. до 13.марта 2012. Године и за то врееме допринети повећању мрежне и информативне безедности., схваћене као способност мреже/информационог система да одолева случајним догађајима или малициозним активностима које имају за циљ угрожавање доступности, изворности, целовитости и поверљивости потхрањених или преношених података. Задатак ове агенције је, између осталог, да прикупља и обрађује податке у вези са мрежним и информационом безбедносним ризицима. У односу на компјтерски криминал, ЕНИСА би могла да има улогу пружања саветодавне помоћи Комсији у вези са развојем и унапређењем легислативних аката ЕУ. О томе више видети на интернет страници*: http://www.enisa.europa.eu/*.

форензичког особља у стандарде најбоље праксе а у циљу спровођења технолошке истраге, те да саставља годишње извештаје о феномену компјутерског криминала на европском нивоу и појава у вези са новим технологијама полазећи од националних статистичких података, те да буде саветодавно телу Комисији и Савету у стварању правила и препорука у вези за бробром против компјутерског криминала. Европска комисија ће до краја 2011. године окончати студију у којој ће размотрити потребу за стварањем једне такве агенције, њеним циљевима, задацима, седишту и начину финансирања[38].

Планско супротстављање компјутерском криминалу је одређено као приоритет и у *Стратегији унутрашње безбедности ЕУ* коју је усвојио Савет ЕУ 23. фебрауара 2010. године[39]. У Стратегији је компјутерски криминал оцењен као глобална, техничка, прекогранична и анонимна претња безбедности информационих система ЕУ[40]. У саопштењу Европске комисије *Спровођење Стратегије унутрашње безбедности ЕУ: пет корака ка сигурнијој Европи* од 26. новембра 2010. године, Комисија је одредила компјутерски криминал, нарочито с обзиром на прекогранични карактер, као један од битних чинилаца који угрожавају безбедност ЕУ, па је међу пет стратешких циљева за период 2011–2014. године уврстила подизање нивоа безбедности грађана и пословања у оквиру сајбер простора. За спровођење таквог циља, Комисија је предвидела предузимање следећих активности у оквиру ЕУ:

– до 2013. године биће формиран Центар за компјутерски криминал, у оквиру ког ће се вршити надзор и процена постојећих превентивних и истражних мера, као и тренинг и подизање свести међу извршним и правосудним органима о специфичностима компјутерског криминала. Предвиђено је да будући центар постане кључна тачка у борби против компјутерског криминала, у оквиру ког ће бити обезбеђена централизована координација прикупљања и анализе података, обуке и сарадње држава чланица са институцијама ЕУ;

– Сарадња са приватним сектором ради побољшања заштите грађана – сарадња је значајна не само ради размене информација и доказа, него и

---

[38] Наведено према: *http://www.eubusiness.com/news-eu/action-plan-cybercrime/* (20.12.2010).

[39] Наведено према: *http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf* (20.12.2010).

[40] Према најновијим подацима ЕУРОПОЛ-а штета коју Европској унији на годишњем нивоу причини компјутерски криминал износи 750 милијарди еура, што превазилази штету од трговине наркотицима, а представља 1% БДП у ЕУ. С обзиром да је више од 150 000 вируса и других малициозних кодова је у оптицају, док се око 148.000 хиљада компјутера на дан зарази, државе чланице ЕУ се убрајају међу најугроженије државе; наведено према: *http://www.europol.europa.eu/index.asp?page=news&news=pr110103.htm* (20.12.2010).

ради развоја техничких алата и мера за спречавање компјутерског криминала; државе чланице треба да створе могућност за грађане да пријаве извршење компјутерских кривичних дела, да сачине и учине доступним смернице за рачунарску безбедност, те да подстакну академске институције да се укључе у истраживање специфичности компјутерског криминала[41];

– Унапређење способности реаговања на сајбер нападе – до 2012. године свака држава чланица и све институције ЕУ треба да успоставе функциомалне тимове за рачунарску безбедност *(Computer Emergency Response Team CERT)* који ће бити умрежени на нивоу ЕУ и сарађивати са извршним органима у превенцији и одговору на безбедносне инциденте, уз подршку ЕНИСА-е.

– У току је постављање Европске платформе за обуку у вези са истрагом компјутерског криминала. Ову активност спроводи Комисија у сарадњи са државама чланицама, ЕУРОПОЛ-ом, универзитетима и приватним сектором[42].

4. ЗАКЉУЧАК

Приликом креирања правних оквира за борбу против високотехнолошког криминала, неколико питања се намеће као изазов који треба превазићи:

1. питање одређивања шта се под компјутерским криминалом подразумева;

---

[41] ЕУРОПОЛ тренутно у сарадњи са Комисијом ради на постављању платформе за пријављивање кривичних дела учињених на интернету која би требало да омогући бољу координацију истрага копмјутерског криминала. План је да се до 2012. године успостави и постане функционална тзв. Европска платформа за кривична дела у вези са интернетом - (*European alert platform for Internet-related offences*), у оквиру које би постојале три структурне целине: (1) онлајн систем за пријављивање кривичних дела извршених на интернету (*Internet Crime Reporting Online System (I-CROS)*); (2) Радна јединица за анализу (*Analysis - Work File (Cyborg*)) која би активно пратила деловање криминалних група на Интернету; (3) Форум за интернет форензичаре (*Internet & Forensic Expert Forum (IFOREX))* на ком би се размењивали подаци између стручњака за компјутерски криминал. Такође, у ову платформу државе чланице ЕУРОПОЛ-а би уносиле податке који се односена примере најбоље праксе и обуке; наведено према: *http://register.consilium.europa.eu/pdf/en/10/st06/st06517.en10.pdf.* (20.12.2010).

[42] Ујуну 2010. године на нивоу ЕУ формирана је Радна група за компјутерски криминал (*European Union Cybercrime Task Force*) као група састављена од стручњака, представника Европола, Еуројаста и Комисије, који ће заједно са представницима националних - јединица за борбу против компјутерског криминала радити на постизању стратешког циља, а то је унапређење и олакшавање вођења истрага и поступака у вези са компјутерским криминалом на нивоу ЕУ и унапређење прекограничне сарадње у вези са супротсваљањем овој врсти криминала. Наведено према: *http://www.europol.europa.eu/ index.asp?page=news&news=pr100622.htm* (20.12.2010).

2. чињеница да се компјутерска кривична дела извршавају у виртуелном окружењу, где су готово неприменљива традиционална правила о надлежности и правила за откривање и доказивање;

3. чињеница да информационе и комуникационе технологије нису сродне и у довољној мери познате припадницима органа гоњења и правосуђа.

Према томе, у правним оквирима за борбу против високотехнолошког криминала неопходно је:

а) дефинисати које се то активности у вези са информационим системима сматрају компјутерским криминалом;

б) одредити специфична процедурална правила, да би се могло приступити истраживању и процесуирању компјутерског криминала,

в) омогућити оспособљавање и константно обучавање припадника институција надлежних за супротстављање овом облику криминала.

На европском нивоу, правни оквир за борбу против рачунарског криминала постављен је у Конвенцији СЕ о компјутерском криминалу и Оквирној одлуци Савета ЕУ о нападима на информационе системе. У низу докумената органа ЕУ изражена је стратешка подршка Конвенцији СЕ и настојање да се државе чланице подстакну на ратификацију Конвенције. Осим тога, на Конвенцију се ослања и поменута Оквирна одлука као извор права на нивоу ЕУ, тако да је веза између акта Савета Европе и правних оквира ЕУ супротстављању компјутерском криминалу недвосмислена. Ова два правна инструмента имају исти циљ – ублажавање разлика између националних законодавстава, увођење нових овлашћења у откривању и доказивању компјутерског криминала и побољшање међународне сарадње у борби против високотехнолошког криминала. Иако се њихова правна природа и домет разликују, поменути циљ ће се остварити тек ако се правила постављена у правним оквирима ових аката буду спроводила.

Без обзира на данашње стање у броју потписа и ратификација и нивоа имплементације Конвенције СЕ уопште, она је одиграла значајну улогу као први инструмент који је уредио основна питања у вези са компјутерским кримналом и тиме послужио као путоказ националним законодавтсвима великог броја земаља у Европи и у свету. Ипак, да би Конвенција као међународни уговор постала обавезујућа за државу потписницу, неопходна је њена ратификација и имплементирање њених одредби у национална законодавства. Исто тако, ни Оквирна одлука Савета ЕУ нема директно дејство у земљама чланицама ЕУ, те је потребна је имплементација њених правила. Из свега овога може се закључити да супротстављање компјутерком криминалу на европском нивоу и поред постојања правних оквира утврђених у поментим инструментима и стратешког опредељења држава неће бити ефикасно, док год не буде спроведена стварна и ефективна имплементација ових правних правила.

Milana Pisarić, Assistant
Faculty of Law Novi Sad

Status and Tendencies in Combating Computer Crime at European Level

Abstract

Without certain adjustments to specifics of computer crime, as to a phenomenon of global proportions, detection, investigation and prosecution of this type of crime is almost impossible. Therefore, the need for setting up a legal framework for combating cyber crime has been identified, in order to define which activities related to information systems are considered computer crime; to determine the specific procedural rules, which would enable the access to data, computer and networks during investigating and prosecuting computer crime and to provide continuous training of members of the institutions responsible for countering this form of crime.

This legal framework should consist of substantive and procedural rules adapted to this type of crime due its aim is the improvement of international cooperation in the framework of global and regional approach to combating cyber crime.

In this this paper the current situation of strategic and legal framework of countering cyber crime is presented (at the level of the Council of Europe and of the European Union) as well as trends in the development of systematic approach towards countering the mentioned abuses within these regional organizations. At the European level, the legal framework to combat cyber crime is set in the Council of Europe Convention on cyber crime and the Council of EU Framework Decision on attacks against information systems. In a series of documents organs of EU confirmed the strategic support of COE Convention and the encouragement of Member States to ratify the Convention. In addition, the Convention represent the base of the said Framework Decision. These two legal instruments have the same goal - removing the differences between national legislation, the introduction of new powers in the discovery and evidence of computer crime and improvement of the international cooperation in combating cyber crime. Although their legal nature and scope vary, its objectives will be achieved only if the rules laid down in the legal framework are enforced.

Key words: cybercrime. – legal framework. – Council of Europe. – European Union.