МЕЂУНАРОДНА ПРАВНА РЕГУЛАТИВА ЗА СУПРОТСТАВЉАЊЕ ВИСОКОТЕХНОЛОШКОМ КРИМИНАЛИТЕТУ

Сандра Ковачевић[1]

Резиме: Високотехнолошки криминал је нови облик криминалитета који у себи има уграђен транснационални карактер. Међутим, законодавна регулатива, политика и методи криминалног прогона, као и међународна сарадња, нису ишли у корак са развојем информационих технологија. Убрзан развој компјутерских технологија захтева будност законодаваца и непрестано праћење промена које се дешавају, и подешавање позитивних законодавстава које би могло да одговори новим изазовима. У овом раду обрађује се међународни правни оквир за супротстављање високотехнолошком криминалитету кроз међународна документа, као и њихова усаглашеност са позитивним правима земаља света.

Кључне речи: високотехнолошки криминалитет, законодавна регулатива, информационе технологије, правни оквир, сузбијање високотехнолошког криминалитета

INTERNATIONAL LEGAL REGULATIONS AGAINST HIGH-TECH CRIME

Abstract: High-tech crime is a new form of crime that has a built-in transnational character. However, legislation, policies and methods of criminal prosecution, as well as international cooperation, have not kept pace with the development of information technology. The rapid development of computer technologies requires the vigilance of legislators and the constant monitoring of changes that are taking place, and the adjustment of positive legislation that could respond to new challenges. This paper deals with the international legal framework for combating high-tech crime through international documents, as well as their compliance with the positive law of the world.

Key words: high-tech crime, legislation, information technology, legal framework, combating high-tech crime

1. УВОД

Са развојем информационих технологија, мобилних телефона и других преносивих електронских уређаја за обраду и пренос података, омогућен је приступ подацима преко рачунарских мрежа са сваког места у сваком тренутку, и повећана свеопшта зависност од информационих технологија у свакодневном животу. Нажалост, свет информационих технологија, поред предности које су евидентне, поседује и негативну страну. Рачунарски системи и мреже пружају могућност за извршење неких традиционалних кривичних дела на сасвим нов и софистициран начин. Поред материјалне штете за појединце и правна лица, која може настати злоупотребом информатичких технологија и која свакако није занемарљива, опасности оваквих злоупотреба могу бити и много теже а последице далекосежније. Сходно томе, државе настоје да одрже корак са технолошким напретком и заштите физичка и правна лица од злоупотреба информационих система. Да би се одговорило на специфичну природу криминалних активности учињених коришћењем рачунарских система и мрежа, потребно је да државе прилагоде, односно употпуне постојеће кривичне законе новим одредбама и усагласе са међународном заједницом. За стварање одговарајућег правног оквира за супротстављање овој врсти криминала путем кривичног права, осим што се у прописима кривичног материјалног права одређена понашања инкриминишу, неопходно је да и прописи кривичног процесног права садрже одговарајућа овлашћења

[1] Академија струковних студија Шабац, Добропољска бр. 5, sandrakovacevic@gmail.com

надлежних органа у циљу откривања извора недозвољене радње, односно прикупљања података о учињеном кривичном делу и учиниоцу, водећи рачуна о специфичностима високотехнолошког криминала и окружења у ком се недозвољене активности предузимају, као и о усаглашености са међународним правом.

2. РЕАГОВАЊЕ ДРУШТВЕНЕ ЗАЈЕДНИЦЕ НА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛИТЕТ

Високотехнолошки криминалитет је нови облик криминалитета који у себи има уграђен транснационални карактер. Постоји више дефиниција појма високотехнолошког криминалитета [1] а заједничко им је поимање да у високотехнолошки криминалитет спадају кривична дела повезана на одређени начин са информационим технологијама. Тако, високотехнолошки криминалитет обухвата радње код којих је рачунарски систем/мрежа објект напада или средство извршења, односно незаконите/неовлашћене радње које се предузимају посредством рачунарске технологије (computer-mediated) у оквиру глобалне електронске мреже [2], односно кривична дела чије радње извршења су омогућене или извршене употребом рачунара, рачунарске мреже или хардверског уређаја [3]. Међутим, законодавна регулатива, политика и методи криминалног прогона, као и међународна сарадња, нису пратили темпо развоја информационих технологија. Само неколико земаља поседује законодавне инструменте који омогућавају ефикасан обрачун са високотехнолошким криминалом. Убрзан развој компјутерских технологија захтева будност законодаваца и непрестано праћење промена које се дешавају и подешавање позитивног законодавства које би могло да одговори новим изазовима.

Транснационални карактер ове врсте криминалитета захтева сарадњу између држава, која мора бити на високом нивоу и заснована на принципима који су обострано прихваћени. Основне проблеме који представљају препреку ефикасној међународној сарадњи и глобалним напорима да се сузбије високотехнолошки криминал можемо дефинисати на следећи начин: различито правно дефинисање радњи извршења и опсега ових радњи које представљају кривично дело високотехнолошког криминала; недовољна обученост полицијских службеника, тужилаца и судија који поступају у предметима високотехнолошког криминала; неусклађеност процесних правила у националним законодавствима у погледу истраге кривичних дела високотехнолошког криминала; неусклађеност или одсуство механизама међународне правне помоћи и споразума о екстрадицији. Глобални напори да се успостави ефикасна међународна сарадња у борби против високотехнолошког криминала засад су највише одмакли у земљама западне Европе и земљана чланицама ОЕБС-а. Иако резултати нису занемарљиви, неопходно је да се фронтови борбе против ове врсте криминалитета отворе у свим деловима света. Потребно је да учешће узму и земље које су у транзицији и развоју јер управо овим државама предстоји опсежна имплементација информационих технологијама са свим предностима али и опасностима које она доноси.

3. ПРАВНА РЕГУЛАТИВА ЗА СУЗБИЈАЊЕ ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛИТЕТА НА МЕЂУНАРОДНОМ НИВОУ

Потреба за инкриминисањем радњи извршених против, односно употребом рачунара настала током 60-их година прошлог века када су се појавили извештаји о манипулацијама рачунара, рачунарским саботажама и шпијунажама, и другим облицима незаконите употребе рачунарских система. Ти први појавни облици су се

односили на крађу телекомуникационих услуга и преваре у вези са трансфером електронских фондова [4]. Еволуција законодавних решења је сукцесивно пратила развој технологије, где је у почетку пажња била усмерена на инкриминисање неовлашћеног приступа приватним информацијама, али се временом појавила потреба за санкционисањем употребе рачунара за извршење кривичних дела против привреде. Током 1980-их година усвајају се први закони који су предвиђали посебне инкриминације: у америчкој држави Флориди 1978, Италији 1979, Аустралији 1981, Уједињеном Краљевству 1984, на нивоу САД 1985, Данској 1986, Немачкој и Шведској 1987, Аустрији и Норвешкој 1988, Француској 1990, Финској 1992, Холандији 1993, Шпанији 1995. године итд. [5].

Са развојем технологије рачунара, развијали су се и облици и начини злоупотреба, а као неопходност се појавила потреба за уношењем специфичних одредаба у кривично законодавство. Даљи технолошки развој условио је појаву нових облика угрожавања безбедности дигиталних садржаја – стална повезаност рачунара са Интернетом учинила је рачунаре рањивим у погледу спољних напада преко рачунарске мреже, а употребе peer-to-peer технологије омогућила је извршавање дистрибуираног напада ускраћивања услуга (Denial of Service:DoS) и ширења малициозних кодова [6].

Без одређених прилагођавања специфичностима високотехнолошког криминалитета, као појаве глобалних размера, откривање и доказивање ове врсте криминалитета готово да је немогуће. Стога је уочена потреба за стварањем правног оквира супротстављања високотехнолошком криминалитету, састављеног од материјалноправних и процесноправних правила прилагођених овој врсти криминалитета, као и за унапређењем међународне сарадње у оквиру глобалног и регионалног приступа борби против високотехнолошког криминалитета.

Као основне препреке ефикасном међународном деловању на сузбијању високотехнолошког криминалитета као глобалној појави, могу се означити следећи фактори: различито правно дефинисање радњи извршења појединих кривичних дела; неусклађеност процесних правила у националном законодавству у погледу истраге кривичних дела високотехнолошког криминала и неусклађеност или одсуство механизама међународне правне помоћи [7]. Остваривање ефективне међународне сарадње у супротстављању високотехнолошком криминалитету представља регулатива усвојена у оквиру Савета Европе, Уједињених нација и Европске уније.

3.1. Савет Европе

Прва међународна иницијатива која се односила на рачунарски криминалитет потекла је са Конференције Савета Европе о криминолошким аспектима привредног криминала одржане 1976. године у Стразбуру и већ тада је препознато неколико облика злоупотреба рачунара [8]. Након тога, 1985. године формирана је стручна комисија са циљем разматрања правних питања у вези са рачунарским криминалитетом. Као резултат рада ове комисије, резиме смерница националним законодавствима представљен је у Препоруци која се односи на кривична дела повезана са компјутерима, усвојеној 1989. Године [9]. У овој препоруци су наведене две листе кривичних дела, као смерница државама у регулисању ових појава на националном нивоу: обавезујућа листа минималних захтева у погледу кривичних дела које би државе требало да предвиде у кривичноматеријалним прописима (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) и опциона листа кривичних дела чије предвиђање је

препуштено диспозицији држава (измена компјутерских података и компјутерских програма, компјутерска шпијунажа, неовлашћена употреба компјутера, неовлашћена употреба заштићених компјутерских програма). Што се тиче процедуралних питања, значајна је Препорука која се односи на проблеме кривичног процесног права у вези са информационом технологијом, усвојена 1995. године [10]. Препорука садржи 18 принципа, категоризованих у 7 поглавља (претрес и заплена; технички надзор; обавеза сарадње са истражним органима; електронски докази; коришћење кодирања; истраживање, статистика и обука; међународна сарадња), а који су касније разрађени и инкорпорисани у Конвенцију.

3.1.1. Конвенција о високотехнолошком криминалу

Конвенција о високотехнолошком криминалу (удаљем тексту: КВК) је усвојена на Конференцији Савета Европе 23. новембра 2001. године у Будимпешти, а на снагу је ступила 1. јула 2004. године [11]. У питању је најзначајнији подухват хармонизације националних законодавстава у борби против високотехнолошког криминалитета, а колики је значај ове конвенције и колико су универзални и прихватљиви установљени принципи и решења можда најбоље говори чињеница да су Конвенцији приступиле и државе које нису чланице Савета Европе. Правни акти, резолуције, препоруке и одлуке осталих међудржавних организација редовно се позивају на одредбе Конвенције Савета Европе, па се сматра да је ово правни акт који је најзначајнији легислативни искорак на међународном плану у оквиру сузбијања високотехнолошког криминалитета.

Циљеви Конвенције су, пре свега, хармонизација између националних законодавстава када је реч о материјалноправним одредбама у области високотехнолошког криминала; увођење адекватних инструмената у национална законодавства када је реч о процесним одредбама, како би се створила основа за истраживање и процесуирање ових кривичних дела; установљавање брзих и ефикасних институција и процедура међународне сарадње.

Што се тиче структуре, Конвенција поред Преамбуле, садржи четири поглавља: 1. основни појмови (рачунарски систем, рачунарски подаци, пружаоци услуга, проток података), 2. легислативне мере које треба предузети на националном нивоу, а односе се на кривично материјално право и кривично процесно право (кривична дела су категоризована у четири групе), а ова типологија је од изузетног значаја јер је усвајају међународни и национални прописи који уређују високотехнолошки криминал (иста је преузета и у актима ЕУ). У оквиру 2. одељка (чланови 14-21) су одредбе које се односе на процесно право. 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. Треће поглавље тиче се међународне сарадње и поставља принципе који се односе на надлежност, екстрадицију, основне принципе међународне помоћи – процедуре које се односе на међусобне захтеве за помоћ у недостатку важећих међународних споразума, узајамну помоћ у вези са привременим мерама, те узајамну помоћ у вези са истрагом. Четврто поглавље садржи завршне одредбе. Циљ Конвенције је хармонизација националних законодавстава држава потписница. Ратификовањем или приступањем Конвенцији, држава се обавезује да одговарајућим механизмима имплементације обезбеди да у домаћем законодавству буду као кривична дела предвиђена одређена понашања (наведена у материјалним одредбама Конвенције), те да предвиде одређена овлашћења надлежним органима ради откривања и доказивања дела високотехнолошког криминалитета и прикупљања електронских доказа (у смислу

процесних одредаба Конвенције). Конвенција представља свеобухватан оквир за прилагођавање кривичног, материјалног и процесног законодавства специфичностима високотехнолошког криминалитета, а с обзиром на неадекватност традиционалних истражних овлашћења и одсуство у већини земаља посебних процедуралних правила која су се примењивала у кибер простору. Конвенција има за циљ да се у домаћем кривичном процесном праву обезбеде овлашћења надлежним органима, која су неопходна за истрагу кривичних дела учињених у вези са рачунарским системима као и других кривичних дела за гоњење код којих је неопходно прикупити доказе у електронском облику [13]. Осим тога, предвиђене су значајне процедуралне гаранције, што представља један од главних доприноса Конвенције. До сада је Конвенција као узор за регулисање високотехнолошког криминалитета послужила законодавствима у преко 100 земаља. Свакако да би пун смисао Конвенције био постигнут када би је потписале и ратификовале, а тиме и имплементирале у своја законодавства све државе света, међутим, за сада, реалност је другачија. Ипак, Конвенција је значајна за европски простор јер је послужила као модел за састављање референтних правних аката ЕУ.

Уз Конвенцију је 2003. донет, а ступио је на снагу 2006. Године, Додатни протокол који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених употребом рачунарских система [12]. Основна сврха његовог доношења јесте да се инкриминишу понашања која нису обухваћена Конвенцијом, а која се тичу ширења мржње, нетолеранције и нетрпељивости према расним, националним, верским и другим групама и заједницама, коришћењем рачунара као средства комуникације и ширења пропаганде. И заиста, развој рачунарских мрежа, а нарочито пораст доступности и популарности Интернета и имејл сервиса, учинили су рачунар моћним средством ширења различитих идеја које могу бити корисне и едукативне, али исто тако могу бити, нпр. позив на величање нацистичких тековина, уперене на бојкотовање, или отворени позив на линч појединаца или група које се разликују по својим личним карактеристикама од других група у својој средини. Ови акти су веома опасни јер се њихово ширење не може адекватно контролисати, свако има право мишљења и изражавања мишљења, а када се то право злоупотреби на Интернету или некој другој мрежи, коришћењем рачунара, често се не може правовремено и адекватно реаговати како би се злоупотреба спречила. Отуда је Протокол пре свега усмерен на ретрибуцију, односно инкриминацију и кажњавање оваквих испада, без обзира на то да ли се њима шири мржња, или се историјске чињенице представљају на неистинит начин, или се неким другим средствима дискриминише или ниподаштава одређена етничка, расна, верска група или организација која их представља.

3.1.2. Остале Конвенције Савета Европе

Конвенција о заштити права појединца у вези са аутоматском обрадом личних података [13] ступила је на снагу 1. октобра 1985. године. Основни циљ усвајања ове Конвенције јесте јачање правне регулативе на пољу заштите података о личности у светлу драматичног пораста употребе рачунарске технологије у административне сврхе.

Конвенција о заштити деце од сексуалне експлоатације и сексуалног злостављања [14] усвојена је 25. октобра 2007. године, и потписале су је земље чланице Савета Европе. У питању је врло важан међународни документ који ће, након што га земље потписнице ратификују, довести до тога да кривични поступци у којима се деца појављују као жртве сексуалне експлоатације и злостављања буду ефикаснији. Такође, са аспекта борбе против високотехнолошког криминалитета овај правни акт представља легислативни искорак ка хармонизацији националних законодавстава у

погледу материјалног кривичног законодавства у свим оним случајевима, нажалост бројним, у којима се рачунарске технологије и мреже користе у циљу дистрибуције, размене и складиштења недозвољених садржаја.

У вези са борбом против тероризма, Савет Европе је још 1977. године усвојио Конвенцију о сузбијању тероризма [15] која је 2005. године допуњена Конвенцијом о спречавању тероризма која је ступила на правну снагу 1. јуна 2007. године. Конвенција дефинише акте тероризма као акте наведене у 10 тематских конвенција.

3.2. Европска Унија

Први извор права који се односио на регулисање злоупотребе информационе технологије је Директива о правној заштити компјутерских програма усвојена 1991. године [16]. На почетку новог миленијума супротстављање високотехнолошком криминалитету уврштено је међу политичке приоритете Европске уније у неколико стратешких докумената, од којих су најзначајније Саопштење Комисије ЕУ Стварање безбеднијег информационог друштва кроз унапређење безбедности информационих инфраструктура и борбом против криминала повезаног са компјутерима из 2001. године, и Саопштење Комисије ЕУ Према заједиичкој политици у борби против компјутерског криминала из 2007. године. Осим поменутих стратешких докумената, супротстављање високотехнолошком криминалитету се манифестује и у донетим изворима права, од којих су најзначајнији: Директива о борби против сексуалне злоупотребе и искоришћавања деце и дечје порнографије [17] и Оквирна одлука о нападима на информационе системе [18]. На нивоу Европске уније је 2004. године усвојена Оквирна одлука о борби против сексуалног искоришћавања деце и дечје порнографије [19]. Децембра 2011. године усвојена је Директива о борби против сексуалне злоупотребе и искоришћавања деце и дечје порнографије. Директива има за циљ да створи правни оквир за заштиту деце од свих облика сексуалне злоупотребе и искоришћавања, унапређење међународне сарадње, те предузимање мера превенције и мера заштите деце жртава тих кривичних дела. Члан 5. Директиве обавезује државе да предузму потребне мере да се наведене радње у вези са онлајн дечјом порнографијом које су предузете с умишљајем и неовлашћено предвиде као кривично дело и за њих пропишу казне затвора у одређеном трајању. Осим тога, Директива од државе чланице тражи да би требало да успоставе, односно унапреде сарадњу и са трећим државама, како би заједничким напорима уклониле порнографске садржаје са сервера који се налазе ван територије ЕУ.

Савет ЕУ је 24. фебруара 2005. године усвојио Оквирну одлука о нападима на информационе системе. Сврха поменуте одлуке је приближавање националног законодавства и унапређење међународне полицијске и правосудне сарадње држава чланица у вези са најзначајнијим формама употребе информационих система у криминалне сврхе. Поменута Оквирна одлука заправо је први корак ка уређењу кривичних дела у вези са нападима на информационе системе у оквиру ЕУ.

3.3. Уједињене Нације

У светлу убрзаног и планетарног развоја информатичких технологија, специјализована тела УН предузела су напоре да се на глобалном нивоу испита значај и улога информатичких технологија, као и опасности које долазе из овог „виртуелног" простора, а које имају своје импликације како на живот и безбедност сваког појединца, тако и на односе међу сувереним државама и регионалним и међународним организацијама. Кроз делатност Комисије за превенцију криминалитета и кривично правосуђе учињени су напори да се промовише међународна сарадња у области хармонизације и примене кривичних закона у разним областима, па тако и у области

борбе против високотехнолошког криминалитета. Резултати ових напора опредмећени су у резолуцијама и телима УН (Резолуција бр. 55/63 о борби против информационих технологија, Резолуција бр. 56/121 Генералне скупштине УН, Економско социјални савет (ECOSOC) 2007/20 и Међународна телекомуникациона унија као водећа у поступку хармонизације националних законодавстава у области високотехнолошког криминалитета, као и генерално у материји безбедности у сајбер простору).

4. ЗАКЉУЧАК

Из наведених карактеристика високотехнолошког криминалитета, произлази недвосмислени закључак да је велики проблем уколико различити правни системи различито приступају регулисању одговора државе на поменуте изазове, и уколико не постоји јединствен став о томе које се то неовлашћене активности злоупотребом информационих технологија сматрају високотехнолошким криминалитетом и којим радњама и мерама превентивно и репресивно реаговати на њих. На основу изложеног, јасно је да се значајни напори предузимају како на међународном, тако и на националном нивоу, како би се установили законодавни оквири за ефикасну борбу против сајбер криминала: оквири који би били довољно флексибилни да буду примењиви у свим правним системима и довољно ефикасни да произведу резултате у виду повећане сигурности у сајбер простору. На основу досадашњих искустава, јасно је да развој рачунарских технологија намеће потребу константног ревидирања постојећих решења и њихово усклађивање са реалношћу која се мења из дана у дан. Због тога, када одговарамо на питање шта даље, у ствари, говоримо о различитим правцима деловања који би били: усклађивање материјалних кривичних законодавстава, ослањајући се првенствено на решења предвиђена Конвенцијом Савета Европе о високотехнолошком криминалу; усклађивање процесног права, нарочито у области истраге и кривичног прогона, где би се такође могли послужити решењима предвиђеним Конвенцијом Савета Европе, нарочито у области доступности електронских података које поседују интернет провајдери а који могу да служе као доказ у судском поступку.

5. ЛИТЕРАТУРА

[1] Jaishankar, K. (2007). *Establishing a Theory of Cyber Crimes*. International Journal of Cyber Criminology 2/2007, p.5.

[2] Hale, C. (2002). Cybercrime: Facts & Figures Concerning this Global Dilemma, Criminal Justice International 18/2002. Преузето 21. децембра 2020. године са http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

[3] Gordon S., Ford R. (2006). *On the definition and Classification of cybercimes*. Journal in Computer Virology1/2006, p.14.

[4] Goodman, B. (2002). *The emerging Consensus in on Criminal Conduct in Cyberspace*. International Journal of Law and Information Technology 2/2002.

[5] Schjolberg. The History of Cybercrime:1976-2014, p. 24-31.

[6] Taylor, M. (2011). *Digital evidence from peer-to-peer networks*. Computer law & security review 27/2011, p. 648.

[7] Николић К. (2010). *Сузбијање високотехнолошког криминала*. Удружење јавних тужилаца и заменика јавнх тужилаца Србије, Београд. стр. 31.

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

[9] Computer-related crime: Recommendation No. R. (89) 9. Преузето 23. децембра 2020. године са https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 .

[10] Council of Europe Convention No.185 on cybercrime. Преузето 23. децембра 2020. године са http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm .

[11] 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. Преузето 24. децембра 2020. године са https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=536686&SecMode=1&DocId=528034&Usage=2 .

[12] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Преузето 24. децембра са http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm .

[13] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, the 28 January 1981, Entry into force: 1. 10. 1985). Преузето 25. децембра 2020. године са https://rm.coe.int/1680078b37 .

[14] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Преузето 25. децембра 2020. године са https://rm.coe.int/1680084822

[15] Council of Europe Convention on the Prevention of Terrorism (CETS No. 196). Преузето 25. децембра 2020. године са https://rm.coe.int/16800d3811 .

[16] Council Directive 91/250/EEC on legal protection of computer programs,http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31991L0250. Преузето 26. децембра 2020. године са https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0024 .

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

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

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