Law and Internet Foundation

Criminal Justice 2007

ПРАВОСЪДИЕТО

В ДИГИТАЛНАТА ЕРА

Аналитичен доклад

Проектът се финансира от Програмата „Криминално правосъдие 2007” на Европейската комисия - Генерална дирекция “Правосъдие, свобода и сигурност”

С партньорството на

APTI Asociatia pentru Tehnologie si Internet

DFLabs Managing Infosecurity Risks

University of BRISTOL

Име на проекта	„Правосъдие в дигиталната ера: Укрепване на капацитета на магистратите на България и Румъния за провеждане на разследване, повдигане на обвинение и произнасяне на присъди в случаи, свързани с извършване на киберпрестъпления”
Проект No.	JLS/2007/JPEN/225, ABAC № 30-CE-0178633/00-29
Държава	Република България
Изпълнител	Фондация „Право и Интернет”
Адрес	Бул. “Патриарх Евтимий” 36 Б 1000 София, България
Телефон	+359 2 981 50 97
Факс	+359 2 981 50 97
Email:	george.dimitrov@dpc.bg
Лице за контакти	Георги Димитров

Дата на доклада:	6 ноември 2008
Версия	v0.2
Автори на доклада:	Д-р Георги Димитров, Председател на Центъра по право на ИКТ (България) Адв. Десислава Кръстева, Юрист (България) Димитър Марков, Център за изучаване на демокрацията (България) Богдан Маноля, ARTI Centre (Румъния) Д-р Максим Добриною (Румъния) ст.н.с. Андрю Чарлзуърт, Бристълски университет (Великобритания) Дарио Форте, CFE, CISM, Милански университет (Италия)
Начало на проекта:	31 декември 2007
Край на проекта:	30 април 2009
Срок на проекта:	16 месеца

СЪДЪРЖАНИЕ

I. ВЪВЕДЕНИЕ

1. ИНТЕРНЕТ: ИСТОРИЯ НА СЪЗДАВАНЕТО МУ, СТРУКТУРА И ВЪЗМОЖНОСТИ

Интернет, глобалното обединение на информационните мрежи и модел на „информационната супер-магистрала", курсът на създаването на която е бил определен от световните правителства, се създава от Министерството на отбраната на САЩ в края на 60-те години на 20-ти век, с цел гарантиране предаването на команди за изстрелване от командния център към пусковите ракетни установки, в случаите, когато всички други видове връзки са неизползваеми. За тази цел е била създадена Агенция за високоразвити проекти (ARPA). Впоследствие задачите й са били разширени до създаване на система, която да предоставя възможност за достъп до изчислителните ресурси на Съединените щати, които да са достъпни в един и същи момент за много ползватели едновременно. В резултат от дейността на Агенцията се създава мрежа, която се нарича ARPAnet.

Съществуването на тази мрежа, обединяваща главните изчислителни центрове на страната, и използването на технологии за предаване на информацията, разделена на автономни пакети, позволяват да се създаде гъвкава структура, в която да се включат компютри от всякакъв вид. Използването на техния „общ език" – протоколи TCP/IP, които бързо се възприемат от военните в техните отделни мрежи MILnet и университетите, се поддържа от Националния научен фонд (NSF) със създаването на пет големи изчислителни центрове. Те са оборудвани със супер-компютри и целта им е да се обезпечи достъпът на научната общественост на САЩ до информацията, която се съдържа в тези компютри. В последствие всички най-големи университетски изчислителни центрове в страната се включват в мрежата, създадена от NSF, която се превръща в „скелет" за всички по-малки мрежи. По това време става възможен достъпът до всяка точка на мрежата с помощта на всеки включен към нея компютър.

С цел поддържане работата на мрежата NSF и разширяването на възможностите й, през 1987 година правата за нейното управление са предоставени на частни инвеститори като Merit Network Inc., IBM и NCI. През 1992 година NSF изтегля своите инвестиции от „мрежата от мрежи", като по този начин дава възможност за финансирането й от други източници. От този момент количеството от съставни мрежи в Интернет постоянно се увеличава. През 1996 година обединява повече от 25 хил. мрежи и 40 млн. ползватели по целия свят.[1] През август 2008 г. в Интернет вече са включени повече от 176 млн. активни сайта.[2]

Днес Интернет е ежедневен способ за предаване на информация от всякакъв характер, достъпен до всеки, който има персонален компютър и благодарение на спътниковите връзки, до всяка точка на планетата.

Съществуването на такива услуги в Интернет като Email (електронна поща), The World Wide Web (WWW или Web), Telnet (дистанционен достъп), F. T. P. (протокол за предаване на файлове), Gopher, дискусионни групи (групи новини), Internet Relay Chat (IRC или просто чат) и регулярното появяване на нови хибриди (IP-телефония, например),

---

[1] Виж Olivier Hance, Business and Law on the Internet (Best Of Editions, 1996), p. 40

[2] Виж http://news.netcraft.com/archives/2008/08/29/august_2008_web_server_survey.html.

[3] Виж *US Retail E-Commerce Resilient*, eMarketer, Apr. 16, *at* http://www.emarketer.com/Article.aspx?id=1006171&src=article_head_sitesearch.

[4] Виж http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2005&RP_intLanguageID=1.

способства за повишаване на влиянието й във всички аспекти от ежедневието – образование, работа, здравеопазване, отдих.

Използването на Интернет в търговията, което е било забранено в началото на неговото съществуване, в последните години се развива с изключителна бързина. Все повече и повече предприятия използват Интернет с цел реклама, маркетинг, предоставяне на услуги, подписване на договори, извършване и получаване на плащания, вътрешна и външна връзка, пазарни изследвания, разработване на модели за собствено развитие, обмен на професионална информация, управление на персонал и наемането на работници и служители. Според някои оценки, само в САЩ през 2008 година чрез Интернет ще бъдат придобити стоки и услуги за сумата 204 трилиона долара.[3]

Съгласно данни на Международен комуникационен съюз, през 2005 година 964,2717 млн. души в света са имали достъп до Интернет.[4] Както съобщи Internet World Stats през декември 2007 год., 2.2 млн. или 30% от хората в България и 7 млн. или 31.4% от хората в Румъния ползват Интернет.[5] Според някои прогнози, през 2010 година общият брой на ползвателите на Интернет ще достигне 1,781 млрд.[6].

2. Правни проблеми, свързани появата на Интернет

Развивайки се с необичайно бързи темпове, Интернет променя познатите ни социално-икономически парадигми и правото не представлява изключение от това.
За съжаление, действащата правна рамка в тази област се основава на реалностите към момента на „цифровата революция" и в повечето случаи се оказва неспособна и неадекватна да реагира на измененията на обществените отношения, настъпили в резултат на появата на информационните технологии.

Ще изминат много години преди правото да „догони" съвременните технологии, ако въобще е възможно. Това създава редица проблеми за специалистите, занимаващи се с информационни технологии. На тях сега им е необходимо да са запознати с правните последствия от своите действия в Интернет. За тях се появява проблема да предвидят как с измененията на съвременното право ще бъдат решени въпросите, които са възникнали и продължават да възникват в процеса на функциониране на Интернет.

Гореспоменатите въпроси се отнасят не толкова до силно развитите страни като Съединените щати, където се намира „ядрото" на Интернет и специалистите, които се явяват световни „законодатели на модата" в областта на компютърните технологии, колкото до страните с по-ниско ниво на информатизация, в това число и България и Румъния. Въпреки че едва сега започва да се създава специално законодателство в тази сфера, на лице е всичко необходимо, за да дадат и двете страни значителен принос в развитието на „безкнижния" свят на информационните технологии.

[5] Виж http://www.internetworldstats.com/stats4.htm.

[6] Виж http://www.etforecasts.com/products/ES_intusersv2.htm#toc.

II. АНАЛИЗ

1. КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ – ПОНЯТИЕ И ИСТОРИЯ

Понятието „компютърни престъпления" се появява за първи път в специализираната научна литература през 60-те години на XX век във връзка със случаите на незаконно използване на компютърни системи, компютърен саботаж и компютърен шпионаж. Първите по-задълбочени изследвания в областта на компютърните престъпления са публикувани през 70-те години на XX век, провокирани от появата на няколко мащабни случая на злоупотреби, свързани с използването на информационни технологии. По същото време много държави приемат специализирано законодателство в областта на защитата на личните данни, в което включват разпоредби, санкциониращи посегателства срещу такива данни, събирани, съхранявани и предавани по електронен път. Исторически това са първите законови разпоредби в областта на компютърните престъпления.

В края на 70-те и началото на 80-те години въпросът за санкционирането на компютърните престъпления придобива все по-широко значение в резултат на драстично увеличилите се случаи на посегателства, извършени посредством използването на компютри и компютърни системи. Появяват се първите случаи на хакерство, компютърни вируси, компютърни измами, софтуерно пиратство и др. По отношение на много от тези прояви традиционното наказателно законодателство се оказва неприложимо, което принуждава много държави да приемат нови разпоредби, инкриминиращи различни видове компютърни престъпления, преди всичко в сферата на икономическите отношения.

През 90-те години на XX век компютърните престъпления надхвърлят границите на икономическата престъпност и започват да засягат все по-широк кръг обществени отношения в сферата на държавното управление, административните услуги, здравеопазването, транспорта и др. Бързото развитие на Интернет като глобална информационна и комуникационна среда също поставя редица сериозни проблеми пред наказателната политика на отделните държави. Информационните технологии се превръщат в средство за осъществяване на престъпна дейност от организирани групи и в сериозен фактор от гледна точка на националната и международната сигурност.

Всичко това води до непрекъснат стремеж на държавите към усъвършенстване на правната уредба на компютърните престъпления и дава нов тласък в развитието на международното сътрудничество в тази област. Приемат се множество нови разпоредби в националното законодателство на отделните държави и стартират редица международни инициативи, насочени към уеднаквяване на вътрешната уредба и създаването на механизми за ефективно международно сътрудничество в борбата с компютърните престъпления.

В Европа правна уредба на компютърните престъпления съществува във всички държави-членки на Европейския съюз, както и в Швейцария, Норвегия, Исландия и др. Компютърните престъпления са уредени още в САЩ, Канада, Русия, Украйна, Мексико, Австралия, Нова Зеландия, а също и в отделни държави от Азия (Япония, Сингапур, Китай, Малайзия, Индия), Южна Америка (Бразилия, Чили, Венецуела) и Африка (Южна Африка, Тунис).[1]

В повечето държави правната уредба на компютърните престъпления е включена в наказателните кодекси на съответните страни. От гледна точка на систематичното място на уредбата по-често съставите на компютърните престъпления са формулирани като квалифицирани състави на традиционни престъпления като кражба, измама, нарушаване на авторски права и др., които се отличават от основния състав по специалния начин на

[1] Виж по-подробно за нормативната уредба на компютърните престъпления в други държави: Законодателно проучване на тема „Компютърни престъпления", Програма „Студенти на стаж към парламента", София, юли 2001 г. Изследването обхваща вътрешното законодателство на всички държави-членки на Европейския съюз и правни актове на държави от Източна Европа, Азия, Северна и Южна Америка.

извършване на престъплението. По-рядко компютърните престъпления са обособени в самостоятелни раздели на наказателните закони (Бразилия, Естония). В сравнително малко страни компютърните престъпления са уредени в специални закони (Румъния, Китай, Индия), а в отделни държави съществува паралелна уредба в два нормативни акта (Япония, САЩ).

В част от държавите, предимно тези, в които компютърните престъпления са уредени със специален закон, правната уредба включва легални определения на основните понятия, използвани при формулирането на съставите (компютър, компютърна система, компютърна мрежа, компютърна програма, компютърни данни и др.).

Повечето държави предвиждат сходни санкции за компютърните престъпления. Най-често срещаното наказание е лишаване от свобода за различен срок (от 3 месеца до 12 години) в зависимост от характера на посегателството и размера на причинените вреди. Наред с лишаването от свобода като алтернативно или кумулативно наказание сравнително често е предвидена и глоба, като нейният размер обикновено зависи от размера на причинените вреди. В Китай като наказание е предвидено лишаването от право на достъп до Интернет за определен срок.

Според наказателните закони на повечето държави компютърните престъпления са от общ характер. Единствено в Германия и Полша са предвидени случаи на компютърни престъпления, които се преследват по инициатива на пострадалия.[2]

[2] Виж по-подробно за международното сътрудничество за противодействие на компютърните престъпления: The Legal Framework – Unauthorized Access to Computer Systems. Penal Regulation in 44 Countries (Updated April 7th, 2003) by Stein Schjolberg, Chief Judge, Moss Tingrett District Court, Norway.

2. Правна уредба на компютърните престъпления по българското наказателно право

2.1. Създаване и развитие на правната уредба – исторически бележки

Правната уредба на компютърните престъпления се съдържа в Наказателния кодекс на Република България (НК). Систематично основната част от съставите на престъпленията са обособени в новосъздадената глава девета „а", озаглавена „Компютърни престъпления". Единствено компютърната измама (чл. 212а НК) е уредена в главата за престъпленията против собствеността поради специфичния й предмет и близостта й с класическия състав на измамата по чл. 212 НК. Извън тези разпоредби, компютърните престъпления включват и някои състави на иначе традиционни престъпления, които по един или друг начин са свързани с използването на информационни технологии. Такива са нарушаването на тайната на кореспонденцията при съобщение, изпратено по електронен път (чл. 171, ал. 1, т. 3 и ал. 3 НК), унищожаване или повреждане на чуждо имущество чрез осъществяване на нерегламентиран достъп до компютър (чл. 216, ал. 3 НК), лъжливо документиране в съобщение, изпратено по електронен път (чл. 313, ал. 1 и 3 НК). Към компютърните престъпления могат да се причислят и съставите на престъпленията срещу интелектуалната собственост, които са свързани с използването на информационни технологии (чл. 172а НК), както и разпространението на порнографски материали, включително детска порнография, по електронен път (чл. 159 НК). На последно място в правната уредба на компютърните престъпления се включват и легалните определения на понятията, свързани с тези видове деяния, като „компютърна система" (чл. 93, т. 21 НК), „компютърни данни" (чл. 93, т. 22 НК), „доставчик на компютърно-информационни услуги" (чл. 93, т. 23 НК), „компютърна мрежа" (чл. 93, т. 25 НК), „компютърна програма" (чл. 93, т. 26 НК) и „компютърен вирус" (чл. 93, т. 27 НК).

Уредбата на компютърните престъпления беше въведена с измененията на НК от септември 2002 г.[3] На практика тя представляваше комбинация между внесените в парламента два законопроекта за изменение и допълнение на НК, предвиждащи текстове за компютърните престъпления. При формулирането на съставите на повечето престъпления беше отдадено предпочитание на законопроекта, внесен през юли 2001 г.[4] За легалните определения на основните понятия беше използван другият проект, внесен от Министерския съвет през април 2002 г.[5] Крайният резултат от този подход бе, че се създаде една вътрешно противоречива уредба и се получи нежелано разминаване между текстовете на престъпните състави от една страна и легалните дефиниции – от друга.

Терминологичното несъответствие между съставите на престъпленията и легалните определения, както и редица други слабости в уредбата, предизвикаха основателни критики в правната общност и още през януари 2005 г. правителството внесе в парламента проект на Закон за изменение и допълнение на НК, засягащ основно текстовете за компютърните престъпления.[6] Поради късното му внасяне (едва няколко месеца преди изтичането на мандата на парламента) този проект беше обсъден само в парламентарните комисии, но не стигна до гласуване в пленарна зала дори на първо четене.

Следващото правителство на свой ред подготви нов вариант за промени на правната уредба на компютърните престъпления, които, заедно с редица други предложения за

[3] Виж Закон за изменение и допълнение на Наказателния кодекс, приет от Тридесет и деветото Народно събрание на 13 септември 2002 г., обнародван в Държавен вестник, бр. 92 от 27 септември 2002 г.

[4] Виж проект на Закон за изменение и допълнение на Наказателния кодекс, внесен в Народното събрание от народния представител Михаил Миков на 19 юли 2001 г., № 154-01-24.

[5] Виж проект на Закон за изменение и допълнение на Наказателния кодекс, внесен в Народното събрание от Министерския съвет на 19 април 2002 г., № 202-01-22.

[6] Виж проект на Закон за изменение и допълнение на Наказателния кодекс, внесен в Народното събрание от Министерския съвет на 5 януари 2005 г., № 502-01-5.

изменения в наказателното законодателство, бяха внесени в парламента през март 2006 г.[7] Впоследствие, обаче, още преди да бъде гласуван на първо четене, законопроектът беше оттеглен от вносителя.

През август 2006 г. група народни представители внесоха третия поред законопроект, предвиждащ промени в разпоредбите за компютърните престъпления.[8] Този проект бе гласуван на първо четене през март 2007 г. и в последствие с някои промени стана основна част от измененията на НК, приети през април 2007 г.[9] С тези изменения беше направена съществена ревизия на повечето текстове, отнасящи се до компютърните престъпления, като редакцията им в повечето случаи бе значително подобрена. Голяма част от съществувалите до този момент несъответствия също бяха отстранени. Добавени бяха нови легални определения и бе постигната необходимата терминологична съгласуваност между легално дефинираните понятия и тези, използвани при формулирането на съставите на отделните престъпления.

За пълнота на изследването, при разглеждането на отделните престъпления, успоредно с анализа на действащите към момента разпоредби, ще бъдат отбелязани и старите редакции на текстовете, както и по-важните предложения за промени, включени в неприетите от парламента законопроекти.

2.2. Основни понятия

Чл. 93. Указаните по-долу думи и изрази са употребени в този кодекс в следния смисъл:

...

21. „Компютърна система" е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни.

22. „Компютърни данни" е всяко представяне на факти, информация или понятия във форма, поддаваща се на автоматична обработка, включително компютърни програми.

23. „Доставчик на компютърно-информационни услуги" е всяко юридическо или физическо лице, което предлага възможността за комуникация чрез компютърна система или което обработва или съхранява компютърни данни за тази комуникационна услуга или за нейните ползватели.

...

25. „Компютърна мрежа" е съвкупност от свързани помежду си компютърни системи или съоръжения, която дава възможност за обмен на компютърни данни.

26. „Компютърна програма" е поредица от машинни инструкции, които са в състояние да приведат компютърна система да осъществява определени функции.

27. „Компютърен вирус" е компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите компютърните системи лица и е предназначена за привеждане на компютърни системи или компютърни мрежи в нежелани от ползващите ги състояния или в осъществяване на нежелани резултати.

28. „Порнографски материал" е неприличен, неприемлив или несъвместим с обществения морал материал, който изобразява открито сексуално поведение. За такова се приема поведение, което изразява реални или симулирани полови сношения между лица от същия или различен пол, содомия, мастурбация, сексуален садизъм или мазохизъм, или похотливо показване на половите органи на лице.

[7] Виж проект на Закон за изменение и допълнение на Наказателния кодекс, внесен в Народното събрание от Министерския съвет на 22 март 2006 г., № 602-01-15.

[8] Виж проект на Закон за изменение и допълнение на Наказателния кодекс, внесен в Народното събрание от народните представители Светослав Спасов и Мария Ангелова - Колева на 9 август 2006 г., № 654-01-117.

[9] Виж Закон за изменение и допълнение на Наказателния кодекс, приет от Четиридесетото Народно събрание на 26 април 2007 г., обнародван в Държавен вестник, бр. 38 от 11 май 2007 г.

2.2.1. Общи бележки

При формулирането на съставите на компютърните престъпления НК използва множество специфични понятия, свързани с използването на информационните технологии. Прецизното определяне на съдържанието на тези понятия е от особено значение за ефективното приложение на разпоредбите. Приетата през 2002 г. правна уредба разкриваше известна непоследователност, дължаща се на недостатъчно доброто терминологично съгласуване между внесените в парламента проекти. Голяма част от предвидените в първоначалните варианти на проектите легални дефиниции не намериха място в приетия текст на закона и по този начин понятия като „компютър", „ресурси на компютъра", „информационна мрежа", „компютърна програма", „компютърен вирус" и др. останаха без легални определения, въпреки че бяха използвани при формулирането на отделните състави. Единствените понятия, за които бяха предвидени легални определения, бяха „компютърна информационна система", „компютърни информационни данни" и „доставчик на компютърно-информационни услуги". Освен това, повечето разпоредби от особената част на НК се разминаваха терминологично с легалните дефиниции по чл. 93 НК.

Подобна непоследователност създаваше предпоставки за трудности при тълкуването и прилагането на закона, особено предвид сложната и недостатъчно добре позната материя на компютърните престъпления. С измененията на НК от април 2007 г. голяма част от тези слабости бяха отстранени, като съществуващите определения бяха прецизирани, бяха добавени нови дефиниции и до голяма степен терминологията в общата и особената част беше уеднаквена.

В настоящата си редакция чл. 93 НК дава легални дефиниции на шест понятия, непосредствено свързани с компютърните престъпления – „компютърна система", „компютърни данни", „доставчик на компютърно-информационни услуги", „компютърна мрежа", „компютърна програма" и „компютърен вирус".

2.2.2. Компютърна система

Според чл. 93, т. 21 НК „компютърна система" е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което в изпълнение на определена програма осигурява или един от елементите на което осигурява автоматична обработка на данни. Определението повтаря дословно дефиницията на същото понятие по чл. 1 от Конвенцията за престъпленията в кибернетичното пространство.

Понятието „компютърна система" обхваща всички устройства, предназначени за автоматична обработка на данни в цифрова форма. Такова устройство може да включва хардуер и софтуер, както и устройства за въвеждане, извеждане и съхраняване на информация. „Автоматично" в случая означава без пряка човешка намеса, а под „обработка на данни" се разбира, че данните в системата се обработват посредством изпълнение на компютърна програма. Компютърната система обикновено се състои от процесор и различни устройства, които изпълняват определена специфична функция посредством взаимодействие с процесора, например принтер, монитор, устройство за четене и записване на компакт дискове и т.н.

С измененията на НК от април 2007 г. понятието „компютърна система" замени първоначално дефинираното понятие „компютърна информационна система", но самото определение беше запазено. Така терминологията, използвана от НК, беше приведена в съответствие с тази на Конвенцията за престъпленията в кибернетичното пространство, която също си служи с понятието „компютърна система" (*computer system*).

Със същите изменения бяха редактирани и повечето текстове от особената част на НК, отнасящи се до отделните компютърни престъпления. Преди промените, въпреки че бе легално определено, понятието „компютърна информационна система" не бе използвано в

нито един от текстовете в особената част на НК. Вместо него, при формулирането на съставите на престъпленията законодателят си служеше с понятията „ресурси на компютър" (чл. 319а, ал. 1 НК) и „компютър" (чл. 319б, ал. 1 и чл. 319г, ал. 1 НК), за които пък липсваха легални дефиниции. С измененията това несъответствие бе отстранено и понятията „ресурси на компютър" и „компютър" бяха заменени с „компютърна система". Единственото изключение остана пропуснатият от законодателя текст на чл. 216, ал. 3 НК, в който понятието „компютър" бе запазено.

2.2.3. Компютърни данни

Компютърните данни са определени в чл. 93, т. 22 НК като всяко представяне на факти, информация или понятия във форма, поддаваща се на автоматична обработка, включително компютърни програми. Определението се основава на дефиницията за данни на Международната организация по стандартизация (International Organization for Standardization – ISO). „Поддаващи се на обработка" означава, че данните са във форма, която позволява непосредственото им обработване от компютърна система. Терминът „компютърни" показва, че данните са в електронна или друга форма, позволяваща директна обработка. Компютърните данни са ресурсите на компютъра. Те могат да се намират в определена компютърна система или да се съхраняват на външен носител, например магнитен или оптичен диск, смарт-карта, чип и т.н.

С измененията на НК от април 2007 г. понятието „компютърни данни" замени първоначално използваното в закона понятие „компютърни информационни данни". По този начин, също както и при понятието „компютърна система", терминологията в НК беше уеднаквена с тази по чл. 1 от Конвенцията за престъпленията в кибернетичното пространство, която също си служи с понятието „компютърни данни" (*computer data*). За разлика от понятието „компютърна система" обаче, самата дефиниция на понятието „компютърни данни" също беше променена. Първоначалният вариант, който следваше дословно текста на конвенцията, обединяваше определенията на две понятия – компютърни данни и компютърна програма. Според този вариант данните се определяха като всяко представяне на факти, информации или понятия във форма, поддаваща се на автоматична обработка, *включително* такава програма, която е в състояние да направи така, че дадена компютърна система да изпълни определена функция. С цел въвеждане на по-кратки и ясни определения, с измененията българският законодател раздели двете дефиниции, като предвиди самостоятелно легално определение за „компютърна програма" и изключи от определението на понятието „компютърни данни" описанието на програмата като такава (програма, която е в състояние да направи така, че дадена компютърна система да изпълни определена функция), препращайки към новата дефиниция за „компютърна програма".[10] Последната като цяло следва смисъла на разпоредбите на конвенцията, въпреки че самата конвенция не предлага отделно определение на това понятие, а го описва в рамките на определението за „компютърни данни".[11]

Със същите изменения бяха редактирани и съставите на престъпленията, в които се използваше старото понятие „компютърни информационни данни". Преди промените в особената част на НК се използваха и двете понятия – „компютърни информационни данни" (212а, ал. 1 и 2 НК) и „компютърни данни" (чл. 319а, ал. 1 и чл. 319б, ал. 1 НК). След

[10] Предложения за разделяне на двете определения бяха дискутирани в правната литература още преди направените през 2007 г. промени. За повече аргументи в полза на разделянето на дефинициите виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 374.

[11] Измененията внесоха и любопитна, макар и незначителна от правна гледна точка, граматическа редакция в определението, като използваната в първоначалната дефиниция спорна от граматическа гледна точка форма за множествено число на думата „информация" – „информации" – беше заменена с формата за единствено число – „информация".

измененията това несъответствие вече е отстранено и навсякъде законът си служи с понятието „компютърни данни".

2.2.4. Доставчик на компютърно-информационни услуги

Според чл. 93, т. 23 НК „доставчик на компютърно-информационни услуги" е всяко юридическо или физическо лице, което предлага възможността за комуникация чрез компютърна система или което обработва или съхранява компютърни данни за тази комуникационна услуга или за нейните ползватели. Определението следва почти дословно дефиницията на понятието „доставчик на услуги" (*service provider*) по чл. 1 от Конвенцията за престъпленията в кибернетичното пространство. Така дефинираното понятие обхваща много широк кръг лица, които са свързани по някакъв начин с предаването или обработката на данни чрез компютърни системи. Тези лица могат да бъдат разделени на три основни групи. На първо място това са всички лица (публични или частни), които предоставят на потребителите възможността да комуникират помежду си. Няма значение дали потребителите представляват затворена група (например работещите в едно предприятие, на които услугата се предоставя чрез корпоративна мрежа) или доставчикът предлага своите услуги публично, както и дали това става срещу заплащане или безплатно. На второ място са лицата, които съхраняват или по друг начин обработват данни от името на лицата, предоставящи посочените услуги. На трето място са лицата, които съхраняват или по друг начин обработват данни от името на потребителите на услугите.

Понятието „доставчик на компютърно-информационни услуги" не се среща никъде в особената част на НК. Единствено при формулирането на разпоредбата на чл. 319е НК законът говори за „доставяне на информационни услуги". Доколкото обаче тази разпоредба препраща към задълженията на посредника при електронно изявление по чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронния подпис (ЗЕДЕП), приложение ще намери определението за посредник по чл. 6, ал. 1 ЗЕДЕП. Така на практика легалната дефиниция на понятието „доставчик на компютърно-информационни услуги" при сегашната редакция на съставите в особената част на НК е излишна.[12]

Логичното систематично място на определението на понятието „доставчик на компютърно-информационни услуги" е в Наказателно-процесуалния кодекс (НПК), тъй като именно той си служи с него. Според чл. 172, ал. 3 НПК доставчиците на компютърно-информационни услуги са длъжни да подпомагат съда и органите на досъдебното производство при събирането и записването на компютърни информационни данни чрез прилагане на специални технически средства, когато това се налага за разкриване на посочените в закона тежки умишлени престъпления.

2.2.5. Компютърна мрежа

Легалното определение на понятието „компютърна мрежа" беше въведено с измененията на НК от април 2007 г. Преди това законът си служеше с две различни понятия – „информационна мрежа" (чл. 319г, ал. 1 НК) и „компютърна мрежа" (чл. 171, ал. 3 НК), като за нито едно от двете нямаше легално определение. С промените терминологията навсякъде беше уеднаквена и НК вече използва само термина „компютърна мрежа".

Според чл. 93, т. 25 НК компютърната мрежа представлява съвкупност от свързани помежду си компютърни системи или съоръжения, която дава възможност за обмен на компютърни данни. Връзките между отделните компоненти в мрежата могат да бъдат

[12] Предложение за отмяна на разпоредбата на чл. 93, т. 23 НК се съдържаше в два от законопроектите за изменение и допълнение на НК – от януари 2005 г. и от август 2006 г. И докато в първия случай целият законопроект не стигна до гласуване в пленарна зала поради изтичането на мандата на парламента, във втория случай предложението беше отхвърлено при обсъждането на проекта в парламентарните комисии.

наземни (например чрез кабел) и/или безжични (например чрез радио вълни, инфрачервени лъчи, сателит).

Съществуват различни класификации на видовете компютърни мрежи. Според собствеността мрежите могат да бъдат домашни (свързани в мрежа уреди с вградени компютри, които формират инфраструктурата на дома), корпоративни (затворени мрежи, които се ползват само от служители на определена корпорация) и обществени (открити за ползване от всички потребители мрежи, които могат да обхващат даден регион, държава или целия свят). Според географските ограничения мрежите могат да бъдат локални (обслужват малки територии, най-често отделни сгради), градски (обслужват отделни населени места или части от населени места) и регионални (свързват компютри, намиращи се в различни географски точки в определен регион). Отделните мрежи от своя страна също могат да се свързват помежду си. Интернет представлява глобална мрежа, състояща се от множество свързани помежду си мрежи, всички използващи едни и същи протоколи. Съществуват и други видове мрежи, свързани или не с Интернет, посредством които могат да обменят компютърни данни.[13]

Компютърните системи могат да бъдат свързани към мрежата като крайни точки или като средства за опосредяване на комуникацията по мрежата. От значение в случая е, че съвкупността от свързани компютърни системи осигурява възможност за обмен на данни, което отличава компютърната мрежа от отделните компютърни системи, свързани в нея.

В определението за компютърна мрежа освен взаимосвързаните компютърни системи са включени и т.нар. „съоръжения". Това са различните видове устройства, които не са компютърни системи, но участват в изграждането на мрежата и имат определена роля при обмена на данни. Такива устройства са: маршрутизаторите (*routers*), които изпращат пакетите информация по-възможно най-краткия път до тяхното местоназначение; комутаторите (*switches*), които предоставят на всеки мрежов компютър индивидуална връзка с друг компютър от мрежата; концентраторите (*hubs*), които копират информацията, постъпила от един порт, и я подготвят за изпращане през другите портове; и т.н.[14] Доколкото от текста на разпоредбата не става ясно колко широко следва да се тълкува понятието „съоръжение", отговор на този въпрос предстои да даде съдебната практика. От теоретична гледна точка и предвид това, че основната характеристика на компютърната мрежа е осигуряването на възможност за обмен на данни, възможен критерий при определянето на това кои устройства са част от мрежата би могла да бъде именно ролята им при обмена на данни.

2.2.6. Компютърна програма

Легалното определение на понятието „компютърна програма" също беше въведено с измененията на НК от април 2007 г. При приемането на първоначалната уредба през 2002 г. единият от предложените законопроекти предвиждаше легална дефиниция на понятието „компютърна програма", но тя не бе приета.[15]

Съгласно чл. 93, т. 26 НК компютърната програма е поредица от машинни инструкции, които са в състояние да приведат компютърна система да осъществява определени функции. Дефиницията до голяма степен се основава на описанието на компютърна програма, включено в определението за „компютърни данни" по чл. 1 от Конвенцията за престъпленията в кибернетичното пространство, където е посочено, че

[13] За повече информация относно видовете компютърни мрежи виж Тужаров, Хр., *Компютърни мрежи*. Изд. Пик. Велико Търново, 2002 г.

[14] За повече информация относно структурата и компонентите на компютърните мрежи виж Тужаров, Хр., *Компютърни мрежи*. Изд. Пик. Велико Търново, 2002 г.

[15] Тази дефиниция определяше компютърната програма като комбинация от команди и свързана информация, които когато са изпълнени в определена форма, карат компютър, компютърна система или компютърна мрежа да изпълнят зададени функции.

компютърните данни включват и всяка „програма, която е в състояние да направи така, че дадена компютърна система да изпълни определена функция".

Както Конвенцията за престъпленията в кибернетичното пространство, така и НК разглеждат компютърната програма като вид компютърни данни.[16] Това, което отличава програмата от останалите видове данни, е нейното свойство да приведе компютърната система в състояние да изпълни определени функции.

В продължение на няколко години българският НК неоснователно правеше разлика между понятията „компютърна програма" и „софтуер".[17] Този извод следваше от старата редакция на чл. 172а, ал. 2 НК, който определяше като престъпление против интелектуалната собственост незаконното използване на софтуер *или* компютърна програма. В теорията няма единно становище относно разликата между тези две понятия и много често те се използват като синоними. Основание за такова тълкуване дава и Законът за авторското право и сродните му права (ЗАПСП), който посочва като обект на авторското право само компютърните програми. С измененията на НК от август 2006 г. това несъответствие беше отстранено, като вместо изброяването на отделните обекти на авторското право беше въведено по-общото понятие „чужд обект на авторско или сродно на него право".[18]

2.2.7. Компютърен вирус

Легалното определение на понятието „компютърен вирус" бе въведено едва с измененията на НК от април 2007 г., близо пет години след инкриминирането на въвеждането на компютърен вирус. При създаването на правната уредба на компютърните престъпления през 2002 г. единият от обсъжданите законопроекти предлагаше легално определение за това понятие, но то не беше прието от парламента.[19]

Според чл. 93, т. 27 НК компютърният вирус представлява компютърна програма, която се разпространява автоматично и против волята или без знанието на ползващите компютърните системи лица и е предназначена за привеждане на компютърни системи или компютърни мрежи в нежелани от ползващите ги състояния или в осъществяване на нежелани резултати.

Според така формулираното определение компютърният вирус е компютърна програма, която се характеризира с две особености – начина, по който се разпространява, и въздействието, което е предназначена да оказва върху заразената компютърната система. Дефиницията като цяло следва преобладаващото в специализираната литература становище, че компютърният вирус е програма, която се саморазмножава и причинява нежелани за потребителите последици.

За да бъде квалифицирана като компютърен вирус, програмата трябва да се разпространява от една страна автоматично, т.е. без намесата на лицето, ползващо компютърната система, а от друга страна – против волята или без знанието на това лице. Определението в тази си част е излишно усложнено. Автоматичното разпространение, в комбинация с нежеланите последици, които причинява, би следвало да е напълно достатъчно за квалификацията на определена програма като вирус. Отношението на ползващото компютърната система лице не би следвало да има правно значение, тъй като от една страна то е трудно за доказване, а от друга – не променя обективните характеристики на съответната

---

[16] За обратното становище виж Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 38-39. Според автора определянето на компютърната програма като вид компютърни данни е неприемливо, с оглед различната същност на тези две понятия, които са двете основни категории на софтуера.

[17] Виж също Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 81. Според автора понятието „софтуер" е по-широко от „компютърна програма".

[18] Виж Закон за изменение и допълнение на Наказателния кодекс, приет от Четиридесетото Народно събрание на 30 август 2006 г., обнародван в Държавен вестник, бр. 75 от 12 септември 2006 г.

[19] Според това определение компютърният вирус беше дефиниран като група от компютърни инструкции, които се саморазмножават и са в състояние да заразят компютърни програми или компютърни данни, да погълнат компютърни ресурси, да променят, унищожат данни или по някакъв друг начин да попречат за нормалната работа на компютър, компютърна система или компютърна мрежа.

програма. Нещо повече, ако компютърната система разполага с надеждна антивирусна защита, тя ще уведоми ползващото я лице за наличието на вирус, т.е. вирусът вече няма да се разпространява без знанието на това лице.

Автоматичното разпространяване най-често се осъществява като създаденият компютърен вирус се прикрепя към съществуваща програма и след като тази програма бъде изпълнена той се активира, прикрепвайки свои копия към други програми в системата. Заразените програми на свой ред копират вируса върху други програми. Програмата, към която вирусът е прикрепен, трябва да бъде изпълнена, за да може вирусът да се активира. Това важи и за т. нар. „макро вируси", които, въпреки че са скрити в документи (компютърни данни), също имат подобно действие.

Другата характерна особеност на компютърните вируси са последиците, които те причиняват на заразените компютърни системи или мрежи. В НК тези последици са посочени като привеждане в нежелани от ползващите ги състояния или осъществяване на нежелани резултати. Нежеланите последици, причинявани от компютърните вируси, могат да бъдат най-разнообразни – от безобидната поява на съобщение на екрана на монитора, през блокиране на ресурси и забавяне на работата на компютъра, до унищожаването на програми или данни незабавно или в определен по-късен момент.

Според чл. 93, т. 27 НК за квалифицирането на една програма като вирус е необходимо тя да е предназначена за предизвикването на тези последици. Реалното настъпване на последиците е без значение. Това решение е обосновано, тъй като поставя ударението на свойствата на вируса, а не на действителните последици, които той причинява, които в някои случаи (например при наличието на надеждна антивирусна защита) може въобще да не настъпят.

С оглед на нежеланите последици, в обхвата на определението за компютърен вирус по чл. 93, т. 7 НК попадат и т. нар. „червеи" (*worms*), които според преобладаващото становище в специализираната компютърна литература не са вируси. Червеите са програми, които се саморазмножават, без да причиняват други вредни последици, освен претоварване на паметта вследствие на самото саморазмножаване. Претоварване на паметта само по себе си, обаче, е привеждане на системата в нежелано от ползващото я лице състояние, следователно червеите ще се квалифицират като компютърни вируси.

Всички останали програми, които, макар да причиняват определени нежелани последици, не отговарят на критериите на определението по чл. 93, т. 27 НК, няма да се квалифицират като компютърни вируси.

2.3. Копиране, използване и осъществяване на достъп до компютърни данни в компютърна система без разрешение

Чл. 319а. (1) Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.

(2) Ако деянието по ал. 1 е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние, наказанието е лишаване от свобода до една година или глоба до три хиляди лева.

(3) Ако деянието по ал. 1 е извършено повторно или по отношение на данни за създаване на електронен подпис, наказанието е лишаване от свобода до три години или глоба до пет хиляди лева.

(4) Ако деянията по ал. 1 – 3 са извършени по отношение на информация, представляваща държавна или друга защитена от закон тайна, наказанието е от една до три години лишаване от свобода, ако не подлежи на по-тежко наказание.

(5) Ако от деянието по ал. 4 са настъпили тежки последици, наказанието е от една до осем години.

2.3.1. Основни състави

Чл. 319а, ал. 1 НК регламентира три основни състава, които се различават по формата на изпълнителното деяние: осъществяване на достъп, копиране и използване на компютърни данни без разрешение.

Текстът беше значително подобрен с измененията от април 2007 г. Старата редакция (който осъществи нерегламентиран достъп до ресурсите на компютър, копира или използва компютърни данни без разрешение, когато се изисква такова) беше неясна и създаваше проблеми при тълкуването, особено по отношение на понятието „ресурси на компютъра".[20]

Непосредствен обект на престъплението са обществените отношения, осигуряващи неприкосновеността на различните видове информация, представена в електронен вид, и защитата й срещу неправомерно узнаване, разпространяване или използване по друг начин.

От обективна страна престъплението се характеризира със специфичен предмет на посегателство – компютърни данни по смисъла на чл. 93, т. 22 НК.[21] Приложното поле на разпоредбата е ограничено от добавеното в текста уточнение, че данните трябва да се намират в компютърна система.[22] По този начин неоснователно се изключват всички хипотези, при които данните не се намират в определена компютърна система, а се съхраняват извън нея на друг носител. Така например, една смарт-карта не е компютърна система по смисъла на чл. 93, т. 21 НК и достъпът до съдържащите се в нея данни, например данни за създаване на електронен подпис, няма да е съставомерно деяние по чл. 319а, ал. 1 НК. Действително, в повечето случаи достъпът до компютърни данни, съхранявани на друг носител, може да бъде осъществен само след като този носител бъде поставен в компютърна система, следователно в момента на посегателството данните ще се намират в системата. За да се избегнат обаче трудности при тълкуването и прилагането, изискването данните да се намират в компютърна система следва да отпадне и деянието да бъде съставомерно без оглед на това къде и по какъв начин тези данни се съхраняват.

Изпълнителното деяние на престъплението е определено като копиране, използване или осъществяване на достъп.

Копирането представлява създаването на копие (дубликат) на компютърните данни. Самото копиране по начало не накърнява целостта на данните. Особеното при него се състои в това, че всички копия са идентични както помежду си, така и по отношение на оригинала (доколкото при компютърните данни изобщо може да се говори за оригинал в класическия смисъл на това понятие). Единствената разлика между тях е времето на създаването им. Освен това всяко копие на компютърни данни е годно да бъде копирано и от него да бъдат произведени нови идентични копия на данните. Всичко това обуславя високата степен на обществена опасност на това деяние и нуждата от неговото инкриминиране.

Използването означава употреба на вече съществуващи данни. Примери за използване на данни са въвеждането им в компютърна система, изпращането им до друг компютър, прехвърлянето им върху различни преносими носители, разпечатването им на хартиен носител и т.н.

Осъществяването на достъп според обяснителния доклад към Конвенцията за престъпленията в кибернетичното пространство означава проникване в определена компютърна система или част от нея, включително чрез друга компютърна система, когато двете системи са свързани помежду си посредством публични телекомуникационни мрежи

---

[20] Предложение за замяна на понятието „ресурси на компютър" с „компютърни информационни данни" се съдържаше още в Законопроекта за изменение и допълнение на НК, внесен през януари 2005 г., който обаче не беше гласуван от парламента. За подробен анализ на предишния вариант на разпоредбата, включително предложения за нейното прецизиране, виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 375-380.

[21] По-подробно за определението на понятието „компютърни данни" виж анализа на чл. 93, т. 22 НК (т. 2.2.3 по-горе).

[22] По-подробно за определението на понятието „компютърна система" виж анализа на чл. 93, т. 21 НК (т. 2.2.2 по-горе).

или се намират в обща мрежа (например локална мрежа или Интранет). За да е налице съставомерно деяние по чл. 319а, ал. 1 НК, обаче, не е достатъчно да е осъществен достъп до определена компютърна система. Достъпът до системата е по-широкото понятие и означава наличие на определена информация в чужда система. Този достъп не е инкриминиран от закона и затова простото изпращане на съобщение или файл посредством електронна поща от една компютърна система до друга, както и на SMS до мобилен телефон, не може да се квалифицира като престъпление по чл. 319а, ал. 1 НК. Изпълнителното деяние на достъпа без разрешение се изразява в достъп до компютърни данни, т. е. наличие на такава информация в чужда компютърна система, която позволява на дееца да узнае или да повлияе по определен начин на съдържащите се в нея данни. Достъп до определени данни е всяко създаване на възможност за узнаване, копиране, променяне или въздействие по какъвто и да е друг начин върху тези данни. Често достъпът без разрешение е в основата и на други компютърни престъпления с по-висока степен на обществена опасност.

Инкриминирането на достъпа без разрешение като самостоятелно престъпление е в съответствие с разпоредбата на чл. 2 от Конвенцията за престъпленията в кибернетичното пространство, който позволява на страните да обявят за престъпление по вътрешното си право самия незаконен достъп до цялата или до част от определена компютърна система, без да е необходимо настъпването на друг престъпен резултат.

Чл. 319а, ал. 1 НК определя сравнително широк обхват на престъплението осъществяване на достъп. В тази насока Конвенцията за престъпленията в кибернетичното пространство изрично предвижда възможност страните да ограничат приложното поле на наказателната репресия, като предвидят допълнителни изисквания за съставомерността на деянието, например правонарушението да е извършено в нарушение на мерките за сигурност, с намерение да се получат компютърни данни или с друго престъпно намерение, както и във връзка с компютърна система, която е свързана с друга компютърна система. Българският закон възприема максимално широк подход и не предвижда подобни ограничения, с което значително разширява приложното поле на разпоредбата. Това е разумно, тъй като по този начин компютърните данни се защитават срещу възможно най-широк кръг посегателства. Изключение от приложното поле на текста остават единствено случаите по чл. 9, ал. 2 НК, когато поради своята малозначителност деянието не е обществено опасно или неговата обществена опасност е явно незначителна.

И по трите основни състава изпълнителното деяние може да бъде осъществено единствено чрез действие.

От обективна страна и в трите хипотези е необходимо изпълнителното деяние да е било осъществено без разрешение, когато такова се изисква. Старата редакция на текста използваше понятието „нерегламентиран достъп", което беше по-близо до използвания от Конвенцията за престъпленията в кибернетичното пространство термин „незаконен достъп" (*illegal access*), определен в обяснителния доклад към нея като „неправомерен достъп" (*access without right*).

Необходимостта от разрешение може да произтича както от разпоредбата на нормативен акт, така и по силата на други приложими правила и процедури. Деянието, обаче, ще бъде съставомерно, когато по силата на нормативен акт лицето, дало разрешението, няма право да предоставя достъп до компютъра на трети лица, например поради завишени изисквания за сигурност по отношение на конкретния компютър. Пример за такива завишени изисквания за сигурност са системите за издаване и управление на удостоверенията за усъвършенстван електронен подпис. Едно от изискванията по отношение на доставчиците на удостоверителни услуги, които издават удостоверения за усъвършенствани електронни подписи, е да осигурят надеждна защита на системите за издаване и управление на удостоверенията. Съгласно чл. 9 от Наредбата за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги системите за издаване и управление на удостоверенията трябва да се намират в специално защитени помещения, до които достъп

имат само надлежно овластени служители в съответствие с техните функционални задължения. Достъпът до тези системи на лица, които не са служители на доставчика на удостоверителни услуги, ще бъде във всички случаи нерегламентиран, дори когато те са получили разрешение от такъв служител.

Деянието няма да бъде съставомерно, когато става въпрос за отворени системи, предназначени за свободен (неограничен) достъп. Такива са например страниците в Интернет. Самото поддържане на обществено достъпна страница в Интернет съдържа в себе си съгласието на нейния собственик до тази страница да имат достъп неограничен кръг потребители на глобалната мрежа. Когато едно лице поддържа страница в Интернет, то разполага с различни технически средства, чрез които осъществява на практика достъп до системите на потребителите, които посещават неговата страница. Най-разпространеното такова средство са т.нар. „кукита" (*cookies*) – съобщения, които сървърът, на който се намира определена страница в Интернет, изпраща до браузъра на потребителя, посещаващ тази страница. Тези съобщения се съхраняват в системата на потребителя и се изпращат обратно до сървъра всеки път, когато потребителят посещава същата страница. Основната цел на кукитата е идентифициране на потребителите и евентуално подготвяне на специален вид на страницата в зависимост от получената информация (например вместо стандартната заглавна страница потребителят получава заглавна страница с изписано неговото име). Според обяснителния доклад към Конвенцията за престъпленията в кибернетичното пространство приложението на такива стандартни средства, инкорпорирани в масово използвани протоколи и програми, само по себе си не може да се квалифицира като незаконен достъп, защото обстоятелството, че потребителят е решил да използва тези протоколи и програми, означава, че мълчаливо се е съгласил с приложението на тези средства. В случая с кукитата това мълчаливо съгласие следва и от факта, че потребителят не е отказал изрично първоначалното им инсталиране, нито в последствие ги е премахнал от системата.

Няма да е налице престъпление и когато деянието е осъществено от лице, което изпълнява свои законово регламентирани правомощия, например при извършване на проверка от компетентен контролен орган. В този случай деянието е законосъобразно, независимо от наличието или липсата на разрешение или съгласие от страна на лицето, което администрира или ползва компютъра.

Моментът, към който съдът ще преценява наличието или липсата на разрешение, е моментът на осъществяване на изпълнителното деяние. Последващото получаване на разрешение няма отношение към съставомерността на деянието, но може да се преценява като смекчаващо вината обстоятелство, а в определени случаи – и като обстоятелство, изключващо наказателната отговорност поради малозначителност на деянието по смисъла на чл. 9, ал. 2 НК.

В хипотезата на копиране на компютърни данни престъплението е резултатно, като резултатът е новосъздаденото копие от съответните данни. В хипотезата на използване на данните престъплението е формално (престъпление на просто извършване) – достатъчно е да е осъществено определено действие със съответните данни, което може да бъде квалифицирано като използване. Осъществяването на достъп също е уредено като формално престъпление. За съставомерността на деянието е достатъчно лицето да е осъществило достъп до определени данни. Престъплението е довършено със самото осъществяване на изпълнителното деяние, без да се изисква настъпването на друг резултат.[23]

Субект на престъплението може да бъде всяко наказателно отговорно лице. От субективна страна е налице умисъл. Деецът съзнава, че за извършване на съответните действия е необходимо разрешение и че не е получил такова, но въпреки това целенасочено копира, използва или осъществява достъп до компютърните данни.

[23] Виж също Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г. Според автора престъплението е резултатно, като резултатът се състои в достигане, узнаване на съдържащата се в компютъра информация.

Наказанието и по трите основни състава е глоба до 3.000 лв.[24]

2.3.2. Квалифицирани състави

НК регламентира няколко квалифицирани състава на копирането, използването и осъществяването на достъп до компютърни данни без разрешение. Квалифициращи обстоятелства са предметът на престъплението (данни за създаване на електронен подпис, информация представляваща държавна или друга защитена от закон тайна), субектът (две или повече лица или едно лице при условията на повторност) и престъпният резултат (настъпване на тежки последици).

При формулирането на квалифицираните състави НК използва само класически квалифициращи обстоятелства, без да държи сметка за специфичния характер на компютърните престъпления. Не са взети предвид предложените от Конвенцията за престъпленията в кибернетичното пространство примерни квалифициращи обстоятелства, като нарушаване на мерките за сигурност, престъпно намерение или нарушение във връзка с компютърна система, свързана с друга компютърна система. Безспорно е, че тези обстоятелства също повишават степента на обществена опасност на деянието, като едновременно с това отразяват някои специфични особености на този вид деяния. Така например, обществената опасност на деяние, извършено чрез преодоляване на специални мерки за сигурност, много често ще е еднаква или дори по-висока от тази на деяние, извършено повторно. За значението на тези обстоятелства може да се съди и по предоставената в чл. 2 от Конвенцията за престъпленията в кибернетичното пространство възможност страните да не инкриминират във вътрешното си законодателство случаите на незаконен достъп въобще, а *само* тези, при които са налице посочените квалифициращи обстоятелства. При сегашната редакция на чл. 319а НК, обаче, наличието на някое от тези обстоятелства ще може да се преценява единствено при индивидуализацията на наказанието, което, обаче, по основния състав е само глоба и то в сравнително нисък размер.

2.3.2.1. Квалифицирани състави във връзка със субекта на престъплението

НК предвижда два квалифицирани състава с оглед субекта на престъплението – когато деянието е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние (чл. 319а, ал. 2 НК), и когато е извършено повторно (чл. 319а, ал. 3 НК).

Чл. 319а, ал. 2 НК предвижда по-тежко наказание (лишаване от свобода до една година или глоба до 3.000 лв.) за случаите, когато престъплението е извършено от две или повече лица, сговорили се предварително за извършване на такова деяние.[25]

Според чл. 93, т. 12 НК едно престъпление е извършено от две или повече лица, когато в самото изпълнение са участвали най-малко две лица. Това означава, че най-малко две лица осъществяват елементи на изпълнителното деяние. Ако едното лице само улеснява извършването на престъплението, без да осъществява елемент от изпълнителното деяние (например предоставя дискета, на която извършителят копира данните), ще е налице помагачество.

Необходимо е освен това съизвършителите да са действали при предварителен сговор за осъществяване на такова деяние. Сговорът е предварителен, когато лицата са взели решението за извършване на престъплението и са съгласували престъпната си воля известно време преди деянието, в сравнително спокойно състояние и с обсъждане на мотивите „за" и

[24] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше максималният размер на глобата да отпадне, но проектът беше оттеглен от вносителя и максималният размер беше запазен.

[25] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше глобата да бъде заменена с пробация, но проектът беше оттеглен и глобата беше запазена.

„против".[26] Предварителният сговор трябва да има за предмет копирането, използването или осъществяването на достъп до компютърни данни, без значение дали лицата са конкретизирали предварително предмета на посегателството (точно определена компютърна система или данни).

Чл. 319а, ал. 3 НК предвижда квалифициран състав, ако деянието е извършено повторно. Предвиденото наказание е лишаване от свобода до три години или глоба до 5.000 лв. По смисъла на чл. 28, ал. 1 НК престъплението е извършено повторно, ако деецът го е извършил, след като е бил осъден с влязла в сила присъда за друго такова престъпление. Според съдебната практика „еднакви по вид престъпления по смисъла на чл. 28 НК са тези, с които се осъществяват едни и същи или различни състави на едно и също престъпление, включително когато то е квалифицирано или привилегировано".[27] Това означава, че повторност ще е налице, когато деецът извърши престъпление по който и да е от съставите на чл. 319а НК, ако преди това е бил осъден с влязла в сила присъда за каквото и да е друго престъпление по същия член.

2.3.2.2. Квалифицирани състави във връзка с предмета на престъплението

Квалифицираните състави във връзка с предмета на престъплението са уредени в чл. 319а, ал. 3 и 4 НК.

По чл. 319а, ал. 3 НК особеният предмет на престъплението са данни за създаване на електронен подпис, а предвиденото наказание е лишаване от свобода до три години или глоба до 5.000 лв.[28]

Според § 1, т. 7 от Допълнителната разпоредба на ЗЕДЕП данните за създаване на подписа представляват уникална информация, като кодове или криптографски ключове, използвани от подписващото лице за създаване на електронен подпис. В зависимост от вида електронен подпис данните за неговото създаване са различни. При обикновените електронни подписи това е всяка информация (симетрични или асиметрични ключове, псевдослучайни числа, уникални информационни обекти и др.), която се използва за създаването на подписа. При усъвършенстваните и универсалните електронни подписи данните за създаване на подписа представляват т.нар. "частен ключ" – единият от двойка ключове, използван в асиметрична криптосистема за създаване на електронен подпис (§ 1, т. 5 от Допълнителната разпоредба на ЗЕДЕП). Тайната на данните за създаване на обикновен електронен подпис е защитена от нормата на чл. 14 ЗЕДЕП, според който никой освен автора няма право на достъп до данните за създаване на електронен подпис. Тайната на частния ключ при усъвършенствания и универсалния електронен подпис е защитена от нормата на чл. 18 ЗЕДЕП, според който никой освен автора няма право на достъп до частния ключ.[29]

Квалифицираният състав на престъплението с предмет данни за създаване на електронен подпис беше въведен с измененията на НК от април 2007 г. Промяната беше наложена с оглед все по-широкото използване на електронни подписи в различни сфери на обществения живот и оттам – високата степен на обществена опасност на посегателствата срещу тайната на тези данни, която не съответстваше на предвиденото по основния състав наказание глоба до 3.000 лв.

---

[26] По-подробно относно предварителния сговор виж Стойнов, Ал., *Наказателно право. Особена част. Престъпления против собствеността.* Изд. Сиела. София, 1997 г., стр. 34-35.

[27] Виж Пост. 2-70-Пл., т. 1.

[28] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше глобата да бъде заменена с пробация, но проектът беше оттеглен и глобата беше запазена.

[29] По-подробно за тайната на данните за създаване на електронен подпис виж Калайджиев, А., Белазелков, Б., Станчева, В., Димитров, Г., Марков, Д., Йорданова, М., *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 73-75 и стр. 99-103.

По чл. 319а, ал. 4 НК особеният предмет на престъплението е информация, представляваща държавна или друга защитена от закон тайна, а наказанието е от една до три години лишаване от свобода, ако деецът не подлежи на по-тежко наказание.[30]

Държавната тайна е легално дефинирана в Закона за защита на класифицираната информация (ЗЗКИ), който определя и реда за достъп до такава информация. Според чл. 25 ЗККИ държавна тайна е информацията, определена в списъка по приложение № 1, нерегламентираният достъп до която би създал опасност за или би увредил интересите на Република България, свързани с националната сигурност, отбраната, външната политика или защитата на конституционно установения ред.

Известно време дефиниция на държавната тайна даваше и чл. 104, ал. 3 НК, който определяше държавната тайна като факти, сведения и предмети от военно, политическо, стопанско или друго естество, узнаването на които от друга държава или чужда организация може да увреди интересите на републиката и особено нейната безопасност; списъкът на фактите, сведенията и предметите, които съставляват държавна тайна, се приема от Народното събрание и се обнародва в Държавен вестник. Въпреки че с приемането на ЗЗКИ текстът на чл. 104, ал. 3 НК не беше отменен, нито беше актуализиран в съответствие с новата уредба на държавната тайна, това несъответствие беше отстранено по-късно с промените на НК от март 2004 г.[31] В сегашната си редакция текстът на чл. 104, ал. 3 НК гласи, че информацията, представляваща държавна тайна, се определя със закон.

В наказателно-правната доктрина се приема, че определението на държавната тайна включва два кумулативно дадени белега – формален и материален. Формалният белег е, че информацията, представляваща държавна тайна, трябва да бъде включена в списък под формата на приложение към закона. Материалният белег се изразява в обстоятелството, че нерегламентираният достъп до съответната информация би създал опасност за или би увредил интересите на Република България. За да бъдат квалифицирани определени данни държавна тайна, трябва да бъдат налице и двата белега. Информация, която е включена в специалния списък, но нерегламентираният достъп до нея не би създал опасност, нито би увредил интересите на страната, не е държавна тайна. Същото важи и за информация, чието узнаване би създало опасност или би увредило интересите на държавата, но която не е включена в специалния списък към закона.

В предмета на престъплението по чл. 319а, ал. 4 НК се включва и всяка друга информация, която представлява защитена от закон тайна. Приложното поле на разпоредбата беше разширено с измененията от април 2007 г. Старата редакция предвиждаше като предмет на престъплението само сведения, съставляващи държавна тайна.[32]

Българското законодателство регламентира редица случаи на информация, чиято поверителност е защитена от закона. По-важните от тях включват: застрахователната тайна по чл. 93-94 от Кодекса за застраховането (КЗ); осигурителната тайна по чл. 109, ал. 2 от Кодекса за социално осигуряване (КСО); тайната на осиновяването по чл. 67а от Семейния кодекс (СК); служебната тайна по чл. 26, ал. 1 ЗЗКИ; производствената и търговската тайна по § 1, т. 7 от Допълнителните разпоредби на Закона за защита на конкуренцията (ЗЗК); банковата тайна по чл. 62, ал. 2 от Закона за кредитните институции (ЗКИ); различните видове професионална тайна по чл. 20 от Закона за частните съдебни изпълнители (ЗЧСИ), чл. 26 от Закона за нотариусите и нотариалната дейност (ЗННД), чл. 35ж от Закона за независимия финансов одит (ЗНФО) и др.

---

[30] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше увеличаване на лишаването от свобода на до пет години, но проектът впоследствие беше оттеглен и максималният размер на наказанието остана непроменен.

[31] Виж Закон за изменение и допълнение на Наказателния кодекс, приет от Тридесет и деветото Народно събрание на 16 март 2004 г., обнародван в Държавен вестник, бр. 26 от 30 март 2004 г.

[32] За повече аргументи в подкрепа на тази промяна виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 384.

От субективна страна за квалифицирания състав по чл. 319а, ал. 4 НК е характерно, че деецът съзнава, че сведенията, по отношение на които извършва съответните действия, са поверителни.

Квалифицираният състав по чл. 319а, ал. 4 НК има субсидиарен характер. Той се прилага единствено в случаите, когато деецът не подлежи на по-тежко наказание. По-тежки наказания са предвидени например за шпионство (издаване или събиране с цел издаване на чужда държава или чужда организация на информация, представляваща държавна тайна) по чл. 104, ал. 1 НК, за разгласяване на информация, представляваща държавна тайна, по чл. 357, ал. 1 и 2 НК и за разгласяване на информация от военен характер, представляваща държавна тайна, по чл. 393 НК.

Начинът, по който са формулирани двата квалифицирани състава с оглед предмета на престъплението, създава объркване, което може да породи затруднения в практиката. Проблемът произтича от това, че посегателството срещу информация, представляваща защитена от закон тайна, е уредено в различна алинея от това срещу данните за създаване на електронен подпис. На практика, обаче, данните за създаване на електронен подпис също са информация, чиято тайна е защитена от закона. Това на свой ред поставя въпроса по кой текст от НК ще се квалифицира престъпното копиране, използване или осъществяване на достъп до данни за създаване на електронен подпис. При буквално тълкуване се стига до извода, че при посегателства срещу данните за създаване на електронен подпис ще се приложи чл. 319а, ал. 3 НК, а при посегателства срещу всяка друга защитена от закон тайна – чл. 319а, ал. 4 НК.

Проблемът, обаче, не спира дотук, тъй като разпоредбата на чл. 319а, ал. 4 НК се прилага и по отношение на чл. 319а, ал. 3 НК (текстът буквално гласи: „ако деянията по *ал. 1 – 3* са извършени по отношение на...”). Така се стига до абсурдната ситуация винаги, когато предмет на посегателството са данни за създаване на електронен подпис, задължително да се прилага чл. 319а, ал. 4 НК, тъй като формално ще е осъществен и този състав – ще е налице деяние по ал. 3, извършено по отношение на информация, представляваща защитена от закон тайна (в случая – данни за създаване на електронен подпис).

Дори да се приеме, че законодателят целенасочено е разграничил данните за създаване на електронен подпис от останалата информация, представляваща защитена тайна, и е предвидил различен режим по отношение на престъпленията срещу тях, остава проблемът с разпоредбата на чл. 319а, ал. 5 НК, която предвижда още по-тежки наказания, когато от деянието са настъпили тежки последици. Тази разпоредба се прилага само по отношение на деянията по чл. 319а, ал. 4 НК, т.е. при посегателства срещу информация, представляваща държавна или друга защитена от закон тайна, и няма да може да се приложи, когато предмет на престъплението са данни за създаване на електронен подпис, въпреки че от копирането или използването на данни за създаване на подпис могат да настъпят значително по-тежки последици, отколкото от аналогични деяния срещу друга защитена тайна, например тайната на осиновяването.

Възможните решения за избягване на тези противоречия са две: отпадане на данните за създаване на електронен подпис от чл. 319а, ал. 3 НК (и автоматично прилагане на чл. 319а, ал. 4 НК на основание, че става въпрос за информация, представляваща защитена от закон тайна) или преместването им чл. 319а, ал. 4 НК, където да бъдат посочени като частен случай на защитена тайна (и където и без това е логичното им от систематична гледна точка място, тъй като именно там са уредени квалифицираните състави с оглед на предмета на престъплението).[33]

[33] За аргументи в полза на подобно предложение виж също Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в Калайджиев, А., Белазелков, Б., Димитров, Г., Йорданова, М., Марков, Д., Станчева, В., *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 383-384. Статията, която анализира старата редакция на текста на чл. 319а, ал. 4 НК (предвиждаща по-тежко наказание само ако предметът на престъплението е информация, представляваща държавна тайна), застъпва тезата, че именно с оглед въвеждане на по-тежки наказания за посегателства срещу

2.3.2.3. Квалифицирани състави във връзка с престъпния резултат

Престъпният резултат е квалифициращо обстоятелство по чл. 319а, ал. 5 НК. Това е единственият състав по глава девета „а" от НК, по който е налице тежко престъпление по смисъла на чл. 93, т. 7 НК, като предвиденото наказание е лишаване от свобода от една до осем години.

Особеното в този случай е наличието на две квалифициращи обстоятелства. Едното квалифициращо обстоятелство е престъпният резултат, който в закона е определен като настъпване на тежки последици. Освен това, обаче, разпоредбата изрично посочва, че се прилага само по отношение на деяния по чл. 319а, ал. 4 НК, т.е. необходимо е наличието и на особения предмет – информация, представляваща държавна или друга защитена от закон тайна.

Остава спорен въпросът дали чл. 319а, ал. 5 НК ще се приложи, когато тежките последици са настъпили от посегателство срещу данни за създаване на електронен подпис. Доколкото престъпленията с предмет такива данни са регламентирани в чл. 319а, ал. 3 НК, приложението на чл. 319а, ал. 5 НК изглежда недопустимо. Ако, обаче, се приеме, че данните за създаване на подпис са информация, представляваща защитена от закон тайна (каквито те в действителност са), то тогава, ако от деянието са настъпили тежки последици, ще е налице основание за прилагането на чл. 319а, ал. 5 НК.

Проблемът произтича от промяната, извършена в оригиналния текст на законопроекта преди гласуването му на второ четене. В първоначалния си вариант проектът предвиждаше отделен квалифициран състав за посегателства срещу данни за създаване на електронен подпис (чрез създаване на нова ал. 4, според която ако деянията по ал. 1 – 3 са извършени по отношение на данни за създаване на електронен подпис, наказанието е лишаване от свобода до три години или глоба до 5.000 лв.) и приложение на разпоредбата за тежките последици както по отношение на деянията срещу информация, представляваща държавна или друга защитена от закон тайна, така и спрямо престъпленията с предмет данни за създаване на подпис.[34]

От обективна страна настъпването на тежките последици трябва да е пряк и непосредствен резултат от изпълнителното деяние. Квалификацията на настъпилите последици като тежки ще се извършва от съда във всеки конкретен случай. Доколкото квалифицираният състав визира единствено посегателства срещу информация, представляваща държавна или друга защитена от закон тайна, при определянето на тежестта на последиците съдът следва да се ръководи от степента на застрашаване или увреждане на интереса, свързан със съответната тайна.

2.4. Престъпни посегателства срещу компютърни програми или данни

Чл. 319б. (1) Който без разрешение на лицето, което администрира или ползва компютърна система, добави, промени, изтрие или унищожи компютърна програма или компютърни данни, в немаловажни случаи, се наказва с лишаване от свобода до една година или глоба до две хиляди лева.

(2) Ако с деянието по ал. 1 са причинени значителни вреди или са настъпили други тежки последици, наказанието е лишаване от свобода до две години и глоба до три хиляди лева.

данни за създаване на електронен подпис е необходимо разширяване на приложното поле на разпоредбата по отношение на всяка информация, съставляваща защитена от закон тайна.

[34] Аналогично решение беше предложено преди това и в Законопроекта за изменение и допълнение на НК, внесен през януари 2005 г., като в този проект към данните за създаване на електронен подпис беше добавен и частният ключ.

(3) Ако деянието по ал. 1 е извършено с цел имотна облага, наказанието е лишаване от свобода от една до три години и глоба до пет хиляди лева.

Чл. 319в. (1) Който извърши деяние по чл. 319б по отношение на данни, които се дават по силата на закон, по електронен път или на магнитен, електронен, оптичен или друг носител, се наказва с лишаване от свобода до две години и с глоба до три хиляди лева.

(2) Ако деянието по ал. 1 е с цел да се осуети изпълнение на задължение, наказанието е лишаване от свобода до три години и глоба до пет хиляди лева.

2.4.1. Основни състави

Непосредствен обект на престъпните посегателства срещу компютърни програми и компютърни данни са обществените отношения, осигуряващи неприкосновеността на тези програми и данни и тяхната защита срещу неправомерно увреждане.

От обективна страна престъплението се характеризира с особен предмет – компютърна програма по смисъла на чл. 93, т. 22 НК или компютърни данни по смисъла на чл. 93, т. 26 НК.[35]

Изпълнителното деяние е посочено в четири различни форми – добавяне, променяне, изтриване и унищожаване. И при четирите форми деянието може да бъде осъществено само чрез действие.[36]

Добавяне на компютърна програма или компютърни данни е въвеждане на нова програма или данни в компютърна система. Въвеждането на програмата или данните може да стане както посредством периферните устройства на компютъра (например чрез клавиатурата), така и посредством прехвърлянето им от преносим носител на информация (компакт диск, дискета) или дистанционно чрез използването на друга компютърна система. Само по себе си добавянето на компютърна програма или данни не увреждa вече съществуващите в компютърната система програми и данни. В някои случаи, обаче, такова увреждане е възможно, например, когато чрез добавената програма или данни се нарушава нормалното функциониране на останалите програми или се накърнява целостта на други данни, намиращи се в системата. Типичен случай на добавяне на програма, която нарушава нормалното функциониране на системата, е въвеждането на компютърен вирус, което обаче е обособено като самостоятелно престъпление по чл. 319г НК.

Променяне на компютърна програма или данни означава качествено или количествено изменение на вече съществуващи програми или данни. Изменението обикновено води до промяна във функционирането на програмата и до изменение в съдържанието на данните.

Изтриването представлява прекратяване на достъпа на потребителите до съответната програма или данни. В повечето случаи изтриването не означава цялостно заличаване на програмата или данните от компютърната система. Когато една програма или данни бъдат изтрити, компютърът унищожава информацията, указваща тяхното местоположение върху твърдия диск. Тази информация се използва от операционната система за изграждането на структурата на директориите в компютъра. Когато тази информация е унищожена, съответната програма или данни стават невидими за операционната система. Те съществуват, но операционната система не знае как да достигне до тях. С възстановяването на тази информация, което може да стане с помощта на специални програми, могат да се възстановяват и изтритите програми или данни.

Унищожаването означава окончателно заличаване на програмата или данните от компютърната система или мрежа. При унищожаването се заличава цялата информация и

[35] По-подробно за определенията на понятията „компютърни данни” и „компютърна програма” виж анализа на чл. 93, т. 22 и 26 НК (т. 2.2.3 и т. 2.2.6 по-горе).

[36] По-подробно за изпълнителните деяния и отношението между тях виж Дончева, Д., *Компютърни престъпления по глава девета “а” от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г.

съответната програма или данни не могат по никакъв начин да бъдат възстановени. На практика единственият начин за пълно унищожаване на определена информация от компютъра е записването на нови данни върху съществуващите такива. Операционната система периодично записва нова информация върху данните, за които информацията къде се намират е унищожена. Това означава, че колкото повече време е изминало от изтриването на определени данни (от заличаването на информацията за тяхното местоположение), толкова по-голяма е вероятността операционната система да запише други данни върху тях и те да бъдат окончателно унищожени.[37]

Престъплението е резултатно. При отделните форми на изпълнителното деяние резултатът е съответно новопоявилата се в системата програма или данни (при добавянето), промяната в съществуваща програма или данни (при променянето), отсъствието на съществуваща програма или данни (при изтриването и унищожаването).[38]

От обективна страна е необходимо изпълнителното деяние да е осъществено без разрешението на лицето, което ползва или администрира компютърната система. Лицето, което администрира системата, е това, на което е поверена нейната поддръжка, а лицето, което ползва компютърната система, на практика осъществява определени действия с нея.

С измененията от април 2007 г. текстът на чл. 319б, ал. 1 НК беше прецизиран от терминологична гледна точка, като използваното в старата редакция понятие „компютър", за което липсваше легално определение, беше заменено с легално дефинирания термин „компютърна система".[39]

От обективна страна е необходимо случаят да е немаловажен. Според чл. 93, т. 9 НК маловажен случай е този, при който извършеното престъпление с оглед на липсата или незначителността на вредните последици или с оглед на други смекчаващи обстоятелства представлява по-ниска степен на обществена опасност в сравнение с обикновените случаи на престъпление от съответния вид. Дали случаят е маловажен подлежи на преценка от съда във всеки конкретен случай.

Субект на престъплението може да бъде всяко наказателно отговорно лице с изключение на лицата, които администрират или ползват компютърната система. От субективна страна престъплението е умишлено. Деецът съзнава, че няма необходимото разрешение, но въпреки това добавя, променя, изтрива или унищожава програмата или данните.

Предвиденото наказание по основния състав е лишаване от свобода до една година или глоба до 2.000 лв.[40]

2.4.2. Квалифицирани състави

---

[37] В проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., се предлагаше изпълнителните деяния „изтрие или унищожи" да се заменят с „премахне или временно заличи". Предложението имаше за цел да подчертае разликата между случаите, когато данните могат да бъдат възстановени, и тези, при които те са безвъзвратно унищожени.

[38] В проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше като елемент от обективната страна да се добави и специфичен резултат – с извършеното деяние да се „смущава работата на компютърна система". Това предложение отпадна още при обсъждането на законопроекта в парламента и не попадна в текста, предложен за гласуване на второ четене. Решението на законодателя е обосновано, тъй като добавянето на още един елемент щеше излишно да усложни редакцията на текста, да утежни процеса по доказването (смущаването на работата на компютърната система щеше да подлежи на доказване като елемент, определящ съставомерността на деянието) и да затрудни тълкуването кога е налице „смущаване" на работата на системата. Настъпването на специфични последици, включително „смущаване" на работата на системата, ще могат да се вземат предвид от съда при преценката дали случаят е маловажен, при индивидуализацията на наказанието и при прилагането на квалифицираният състав по чл. 319б, ал. 2 НК.

[39] Аналогично предложение се съдържаше още в проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., който не беше приет поради изтичането на мандата на парламента.

[40] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше замяна на глобата с пробация, но поради оттеглянето на проекта от вносителя наказанието не беше променено.

НК регламентира няколко квалифицирани състава на престъплението по чл. 319б, ал. 1 НК. Квалифициращи обстоятелства са престъпният резултат (причиняване на значителни вреди или настъпване на други тежки последици), престъпната цел (користна цел или осуетяване изпълнението на задължение) и предмета на престъплението (данни, които се дават по силата на закон, по електронен път или на магнитен, електронен, оптичен или друг носител).

2.4.2.1. Квалифицирани състави във връзка с престъпния резултат

Престъпният резултат е квалифициращо обстоятелство по чл. 319б, ал. 2 НК. Законът посочва два възможни резултата – причиняване на значителни вреди или настъпване на други тежки последици. Предвиденото по-тежко наказание е лишаване от свобода до две години и глоба до 3.000 лв.[41]

Според съдебната практика значителните вреди обхващат само имуществените вреди. Те се изразяват в намаляване на имуществото (намаляване на активите или увеличаване на пасивите) на определено лице. Дали вредите са обикновени или значителни се определя въз основа на два критерия – абсолютната стойност на вредата и нейната относителна стойност в сравнение със стойността на цялото имущество. Според съдебната практика, ако относителната стойност на вредата е голяма, а по абсолютния си размер е незначителна, няма да има значителна вреда по смисъла на закона. Обратно, когато абсолютният размер на вредата е значителен, но в сравнение със стойността на ощетения патримониум тя е незначителна, ще е налице значителна вреда.[42] Значителни имуществени вреди означава преди всичко, че вредите са такива по абсолютния си размер, т.е. паричният еквивалент на причинените вреди е значителен.[43]

Що се отнася до настъпването на други тежки последици, те следва да се тълкуват като причиняване на неимуществени вреди, защото имуществените вреди се обхващат от понятието значителни вреди. Кога тези последици са тежки е фактически въпрос и ще подлежи не преценка от съда във всеки конкретен случай.

Двата възможни резултата са посочени алтернативно.[44] При всички случаи е необходимо наличието на причинно-следствена връзка между престъпния резултат и изпълнителното деяние.

2.4.2.2. Квалифицирани състави във връзка с предмета на престъплението

Предметът на престъплението е квалифициращо обстоятелство по чл. 319в, ал. 1 НК и е определен като данни, които се дават по силата на закон, по електронен път или на магнитен, електронен, оптичен или друг носител. Предвиденото по-тежко наказание е лишаване от свобода до две години и глоба до 3.000 лв.[45]

От обективна страна е достатъчно изрична законова разпоредба да предвижда задължение за предоставяне на определени данни, както и възможност тези данни да бъдат предоставени по електронен път или на магнитен, електронен, оптичен или друг носител.

---

[41] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше максималният размер на глобата да отпадне, но в крайна сметка наказанието не беше променено.

[42] Виж ТР № 6 от 15.11.1973 г. на ОСНК по н.д. № 2 от 1973 г.

[43] Виж ТР № 2 от 09.08.1993 г. на ОСНК по н.д. № 2 от 1993 г.

[44] В първоначалния вариант на проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше двата резултата – причиняване на значителни вреди или настъпване на други тежки последици – да бъдат обединени под общата формулировка причиняване на „значителни тежки последици". Предложението отпадна при обсъждането на проекта в парламента, макар че евентуалното му приемане щеше да премахне неоснователното разделяне на имуществените от неимуществените последици и да направи редакцията на разпоредбата по-прецизна.

[45] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше максималният размер на глобата да отпадне, но поради оттеглянето на проекта това предложение не беше доразвито.

Приложното поле на разпоредбата обхваща две групи случаи. На първо място са хипотезите, в които законът предвижда *задължение* данните да се предоставят само по електронен път или на специален носител. На второ място са случаите, когато законът предвижда задължение данните да се предоставят и *възможност* това да стане по електронен път или на такъв носител (като алтернатива на предоставянето на хартиен носител). Тълкуването на разпоредбата в смисъл, че данните се предоставят задължително само в електронна форма или на специален носител, неоснователно би стеснило нейното приложно поле.

При тълкуването на понятието „електронен път" могат да се използват съществуващите легалните определения в други закони. Според § 1, т. 1 от Допълнителните разпоредби на Закона за търговския регистър (ЗТР) „електронен път" е предаване на данни в цифрова форма, при което се използват устройства за електронна обработка, включително цифрово компресиране и съхраняване на информацията, като преносът се осъществява чрез използването на проводник, радиовълни, оптически, електромагнитни или други средства. Според § 1, т. 20 от Допълнителните разпоредби на Данъчно-осигурителния процесуален кодекс (ДОПК) „предаване по електронен път" е предаването чрез електронно оборудване за обработка (включително цифрово компресиране) на данни и чрез използване на кабел, радиопредаване, оптични технологии или всякакви други електромагнетични средства. На практика предоставянето на данни по електронен път може да включва най-разнообразни хипотези като изпращане чрез електронна поща, предоставяне чрез Интернет, чрез факс-модем и др.

Що се отнася до различните видове носители, изброяването в чл. 319в, ал. 1 НК е примерно, а не изчерпателно. Посочени са три вида носители (магнитен, електронен и оптичен), като изрично е добавено, че разпоредбата ще се прилага и за данни, предоставяни на други носители.

Единственото легално определение на понятието „електронен носител" в българското законодателство се съдържа в § 1, т. 5 от Допълнителните разпоредби на Закона за националната стандартизация (ЗНС), според който „електронен носител" е техническо средство, което съхранява или предава информация в цифров вид.

Магнитните носители могат да бъдат гъвкави магнитни дискове (дискети), твърди магнитни дискове, магнитни ленти и др. Общото между тях е, че носителят на информацията е тънко покритие, като за четене на данните се използват физичните свойства на електромагнитното въздействие. За да могат да се използват, магнитните носители трябва да се поставят в специално устройство за запис и/или четене, което е снабдено със съответната магнитна глава.

Оптичните носители са най-често под формата на оптични дискове. Те се характеризират с това, че са със специално покритие, като записването и четенето на информацията стават посредством лазерен или друг високочестотен лъч. В сравнение с магнитните носители, оптичните носители имат по-голям капацитет за съхраняване на информация и са по-надеждни, поради което и придобиват все по-широко разпространение.

При определянето на различните видове носители разпоредбата на чл. 319в, ал. 1 НК не е прецизна, тъй като смесва различни категории понятия. Понятието „електронен носител" е родово понятие и включва в себе си видовите понятия „магнитен носител" и „оптичен носител". Объркването е резултат от промяната в текста на чл. 319в, ал. 1 НК, извършена с измененията на НК от август 2007 г. Старата редакция на текста използваше само понятието „магнитен носител" и беше остро критикувана поради неоснователното стесняване на приложното й поле и изключването на другите видове носители, включително оптичните.[46]

[46] В първоначалния си вариант проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., предвиждаше само замяна на понятието „магнитен носител" с „електронен носител", но при обсъждането на промените в парламента се стигна до идеята към магнитните носители да бъдат добавени оптичните и електронните, а освен това приложното поле на разпоредбата да се разшири още повече с добавянето и на „други" носители. Аналогично предложение се съдържаше и в проекта на Закон за изменение и допълнение на

Макар и с определени слабости в терминологично отношение, така променената разпоредба е сравнително ясна и за разлика от старата редакция приложното й поле отговаря адекватно на действителните обществени отношения, за които се отнася. Въпреки това, за да бъде напълно прецизна, в нея следва да остане само родовото понятие „електронен носител", което е технологично неутрално и включва не само всички познати към момента носители (включително магнитните и оптичните), но и всички нови видове, които биха се появили в бъдеще.

Чл. 319в, ал. 1 НК не съдържа ограничения относно това кой и на кого предоставя съответните данни. По-специално, няма изискване тези данни да се предоставят от или на държавен орган. От обективна страна е достатъчно единствено съществуването на законова разпоредба, регламентираща задължение за предоставяне на определена информация.

Понастоящем няколко закона предвиждат възможност за предоставяне на информация по електронен път или на електронен носител.

Такава възможност е предвидена в данъчното законодателство. ДОПК предоставя възможност за подаване по електронен път на искания за издаване на документи от значение за признаване, упражняване или погасяване на права и задължения (чл. 89, ал. 2 ДОПК) и на декларации и други подлежащи на подаване документи и данни (чл. 99, ал. 1 ДОПК). Според Закона за данъка върху добавената стойност (ЗДДС) по електронен път могат да се подават заявленията за регистрация (чл. 101, ал. 3 ЗДДС), а справките-декларации, VIES-декларациите и отчетните регистри могат да се подават както по електронен път (чл. 125, ал. 7 ЗДДС), така и на магнитен или оптичен носител (чл. 125, ал. 6 ЗДДС).

Възможност за подаване на информация по електронен път е предвидена и в митническото законодателство. Законът за митниците (ЗМ) предвижда, че декларирането пред митническите учреждения може да се осъществява по електронен път (чл. 67, ал. 1, т. 2 ЗМ), като в Правилника за приложение на Закона за митниците (ППЗМ) са уредени условията и редът за такова деклариране (чл. 134 – 136а ППЗМ).

Информация по електронен път или на електронен носител може да се предоставя и според законите, уреждащи правото на достъп до информация. Законът за достъп до обществена информация (ЗДОИ) предоставя възможност на лицата да подават заявления за предоставяне на достъп до обществена информация по електронен път (чл. 24, ал. 2 ЗДОИ) и да получават такава информация под формата на копие на технически носител (чл. 26, ал. 1, т. 4 ЗДОИ). Законът за защита на личните данни (ЗЗЛД) също предвижда възможност за подаване на заявления за предоставяне на достъп до лични данни по електронен път (чл. 29, ал. 2 ЗЗЛД) и за предоставяне на самите данни също по електронен път (чл. 31, ал. 2 ЗЗЛД).

Други закони, които предвиждат възможност за предаване на данни по електронен път, са Законът за здравното осигуряване (ЗЗО) относно задължението на изпълнителите на медицинска помощ да предоставят на районните здравно-осигурителни каси определени данни и документация само на електронен или магнитен носител в съгласуван с Националната здравно-осигурителна каса формат (чл. 66, ал. 3 ЗЗО), Законът за Сметната палата (ЗСП) относно правото на органите на Сметната палата да изискват справки и друга информация на електронен носител във връзка с извършваните от тях предварителни проучвания или одити (чл. 31, ал. 1, т. 2 ЗСП) и др.

2.4.2.3. Квалифицирани състави във връзка с особената цел на дееца

НК, внесен през януари 2005 г., но то не беше прието, тъй като парламентът не успя да гласува проекта преди изтичането на своя мандат. За подробен анализ на предишния вариант на разпоредбата, включително предложения за нейното прецизиране, виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 389.

НК регламентира два квалифицирани състава с оглед особената цел на дееца – когато престъплението е извършено с цел имотна облага (чл. 319б, ал. 3 НК) и когато е извършено с цел да се осуети изпълнение на задължение (чл. 319в, ал. 2 НК).

По чл. 319б, ал. 3 НК особената цел на дееца е посочена в закона като имотна облага, като предвиденото наказание е лишаване от свобода от една до три години и глоба до 5.000 лв.[47] Това е т.нар. „користна цел". Деецът цели настъпването на благоприятни изменения в своето имущество или в имуществото на трето лице. Действителното постигане на целта е без значение за съставомерността на деянието, но ще може да се преценява при индивидуализацията на наказанието.

По чл. 319в, ал. 2 НК особената цел на дееца се изразява в осуетяване изпълнението на задължение, а предвиденото наказание е лишаване от свобода до три години и глоба до 5.000 лв.[48]

Текстът на чл. 319в, ал. 2 НК се прилага само по отношение на деяния по чл. 319в, ал. 1 НК, т.е. необходимо е кумулативно да е налице и особеният предмет на престъплението – данни, които се дават по силата на закон, по електронен път или на магнитен, електронен, оптичен или друг носител. Най-често това ще бъдат данни, чието предоставяне е свързано с пораждането на задължение за определено лице. Такива са например справките и декларациите по данъчното и митническото законодателство, които са предпоставка за възникването на определени данъчни или митнически задължения.

Осуетяването означава създаване на пречки за изпълнението на задължението. Не е необходимо деецът да е длъжник по задължението, чието изпълнение се стреми да осуети.[49] Видът и размерът на задължението са без значение. Квалифициращото обстоятелство е единствено намерението на дееца да осуети изпълнението на задължението. Реализацията на тази цел е без значение за съставомерността на деянието. Действителното осуетяване на изпълнението на задължението, обаче, може да се преценява от съда при индивидуализацията на наказанието.

2.5. Въвеждане на компютърни вируси и други злонамерени програми

Чл. 319г. (1) Който въведе компютърен вирус в компютърна система или компютърна мрежа, се наказва с глоба до три хиляди лева.

(2) Наказанието по ал. 1 се налага и на онзи, който въведе друга компютърна програма, която е предназначена за нарушаване на дейността на компютърна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква, доколкото извършеното не съставлява по-тежко престъпление.

(3) Ако от деянието по ал. 1 са настъпили значителни вреди или е извършено повторно, наказанието е лишаване от свобода до три години и глоба до хиляда лева.

2.5.1. Основни състави

Чл. 319г НК урежда два основни състава, които се различават по средството за извършване на престъплението – компютърен вирус по чл. 319г, ал. 1 НК и компютърна програма, която е предназначена за нарушаване на дейността на компютърна система или

[47] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше минималният размер на лишаването от свобода и максималният размер на глобата да отпаднат, но предложението не беше доразвито поради оттеглянето на проекта от вносителя.

[48] В проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше максималният размер на глобата да отпадне, но поради оттеглянето на проекта той беше запазен.

[49] Виж също Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 95. Според автора задължението е чуждо, т.е. не е ва извършителя на престъплението.

компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква, по чл. 319г, ал. 2 НК.
Непосредствен обект на престъплението са обществените отношения осигуряващи нормалното функциониране на компютърните системи и мрежи и неприкосновеността на компютърните данни.

От обективна страна престъплението се характеризира с особено средство. В първия случай става въпрос за компютърен вирус по смисъла на чл. 93, т. 27 НК.[50] Във втория случай средството на престъплението е определено като компютърна програма, която е предназначена за нарушаване на дейността на компютърна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква. В специализираната литература тези програми са известни с общото наименование „злонамерени програми".

Въвеждането на злонамерена програма, която не е вирус, в компютърна система или мрежа беше инкриминирано с измененията на НК от април 2007 г. Новият текст на чл. 319г, ал. 2 НК е в отговор на критиките, породени от предишната правна уредба, която изключваше от приложното си поле различните вредни или злонамерени програми, които не са компютърни вируси. В мотивите към предложените изменения дори беше посочено, че в сравнение с въвеждането на компютърни вируси, въвеждането на други злонамерени програми разкрива „същата, даже още по-висока степен на обществена опасност".[51]

Според чл. 319г, ал. 2 НК става въпрос за компютърна програма, която е предназначена за нарушаване на дейността на компютърна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква. Преди всичко това са програми, които не се разпространяват автоматично (не се саморазмножават). Всички програми, които се разпространяват автоматично и имат посоченото предназначение, попадат в обхвата на определението за компютърен вирус по чл. 93, т. 27 НК и тяхното въвеждане ще се квалифицира като въвеждане на компютърен вирус по чл. 319г, ал. 1 НК.

Самото предназначение на компютърната програма е формулирано като „нарушаване на дейността на компютърна система или компютърна мрежа" или „узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква". Нарушаването на дейността на компютърна система или мрежа означава негативна промяна във функционирането на системата или мрежата, като забавяне на скоростта, спиране на една или повече програми и т.н. Узнаването на компютърни данни без разрешение е достигането на определени данни до знанието на лице, което няма право на достъп до тях. Заличаването е пълното премахване на определени данни от компютърната система или мрежа. Изтриването представлява унищожаване на информацията, указваща местонахождението на тези данни. За разлика от заличените данни, изтритите данни в определени случаи могат да бъдат възстановени. Изменението на компютърни данни означава внасяне на промяна във вече съществуващи данни. Копирането е свързано със създаването на едно или повече копия на данните.

---

[50] По-подробно за определението на понятието „компютърен вирус" виж анализа на чл. 93, т. 27 НК (т. 2.2.7 по-горе).

[51] Опит да се инкриминира въвеждането на злонамерени програми беше направен още с проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., но негласуван от парламента. В проекта се предлагаше замяна на понятието „компютърен вирус" с по описателното „вредоносен програмен продукт (софтуер) с цел да бъде използван за разстройване на компютърни информационни данни или дейността на компютърна информационна система". Внесеният през август 2006 г. законопроект за изменение и допълнение на НК следваше по-различен подход и предлагаше първоначалният текст на чл. 319г, ал. 1 НК да бъде допълнен, като към компютърните вируси като средство на престъплението бъде добавена и „друга компютърна програма с цел да смути дейността или да осъществи (да извърши) неразрешено въздействие върху компютърна система или компютърна мрежа, или с цел неразрешено узнаване, заличаване, изтриване, изменение или копиране на компютърни данни". В последна сметка обаче законодателят прие различно решение, като инкриминира въвеждането на злонамерена програма като отделен основен състав.

Съществуват много и различни видове злонамерени програми, известни още като малуер (*malware*). Такива са например различните видове шпионски софтуер (*spyware*), които събират информация за потребителя на компютърната система (например навици за търсене в мрежата, посещавани сайтове и т.н.), показват нежелани реклами, променят съдържанието на браузъра, пренасочват резултатите от търсенето към платени обяви и т.н. Друга злонамарена програма е т.нар. е „логър" (*logger*), който копира всяко натискане на клавиатурата при въвеждане на пароли, номера на кредитни карти, регистрационни кодове на програмни продукти, пароли и т.н. Злонамерена програма е и т.нар. „дайлър" (*dialer*) – приложение, което контролира модема на компютъра и посредством него набира телефонни номера с добавена стойност. Едни от най-разпространените злонамерени програми са т.нар. „троянски коне" (*Trojan horses*), които приканват потребителя да ги инсталира, но в същото време имат опасно съдържание и могат веднага да въздействат върху системата и да доведат до нежелани последствия, включително инсталиране на други злонамерени продукти.

Изпълнителното деяние е определено в закона като въвеждане.[52] Въвеждането представлява инкорпориране на вируса или другата злонамерена програма в определена компютърна система или мрежа. С измененията от април 2007 г. текстът на чл. 319г, ал. 1 НК беше прецизиран от терминологична гледна точка, като използваните в старата редакция понятия „компютър" и „информационна мрежа", за които нямаше легални определения, бяха заменени съответно с „компютърна система" и „компютърна мрежа", които са легално дефинирани.[53]

Въвеждането на вируса може да стане по всички начини, по които в компютъра могат да бъдат въведени компютърни данни – от директно въвеждане чрез периферните устройства на системата (устройствата за четене на информация, съхранявана на външни носители) до въвеждане от разстояние (чрез електронна поща, чат, програми за размяна на съобщения и дори SMS). Законът не изисква вирусът да бъде въведен в чужда система или мрежа. Подобно решение има основание, тъй като поради специфичните особености на компютърните вируси, много често въвеждането им в който и да е компютър създава сериозна опасност за разпространението им и в други компютри и мрежи.

Престъплението е резултатно. Резултатът е присъствието на вируса или злонамерената програма в определена компютърна система или мрежа.[54]

За разлика от чл. 319г, ал. 1 НК, инкриминиращ въвеждането на компютърен вирус, чл. 319г, ал. 2 НК, отнасящ се до другите злонамерени програми, има субсидиарен характер и се прилага само ако деянието не съставлява по-тежко престъпление. Така например, ако чрез въведената програма деецът е копирал данни за създаване на електронен подпис или информация, представляваща държавна тайна, деянието ще се квалифицира по чл. 319а, ал. 3 НК или съответно по чл. 319а, ал. 4 НК.

Субект на престъплението и по двата основни състава може да бъде всяко наказателно отговорно лице. От субективна страна е налице умисъл. Деецът цели да въведе компютърния

---

[52] Още при приемането на разпоредбата на чл. 319г НК през 2002 г. първоначалният вариант на проекта предвиждаше наказателна отговорност за по-широк кръг деяния, свързани с разпространението на компютърни вируси, включително за тяхното създаване. Разширяване на кръга от изпълнителни деяния беше предложено и в Законопроектите за изменение и допълнение на НК, внесени през януари 2005 г. и през август 2006 г. И двата законопроекта предвиждаха добавяне на деянията създаване, предаване и разпространяване. В последна сметка обаче в закона като единствена форма на изпълнителното деяние остана въвеждането. Когато обаче компютърният вирус или другата злонамерена програма е създадена от едно лице, а въведена в компютърната система или мрежа от друго лице, създателят на вируса ще носи наказателна отговорност като съучастник (помагач).

[53] За подробен анализ на предишния вариант на разпоредбата, включително предложения за нейното прецизиране, виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 392.

[54] Виж Дончева, Д., *Компютърни престъпления по глава девета "а" от Наказателния кодекс*, Правна мисъл, кн. 2, 2003 г. Престъплението е довършено с достигането на вируса до определен компютър или информационна мрежа, без значение дали се е активирал или е бил неутрализиран от специална антивирусна програма.

вирус или другата злонамерена програма в определена компютърна система или мрежа. Вината като елемент от субективната страна на престъплението е от особено значение при въвеждането на компютърни вируси поради специфичната характеристика на тези програми да се саморазмножават. Съставомерно ще е единствено деянието, при което деецът съзнава, че инструкциите, които въвежда в компютъра, представляват компютърен вирус и въпреки това цели тяхното въвеждане. Няма да е налице престъпление, ако лицето не знае, че програмата или данните, които въвежда в компютъра, съдържат вирус или друга злонамерена програма. Същото важи и за случаите, когато поради самото активиране на вируса системата автоматично въвежда вируса в други компютърни системи или мрежи или го изпраща по електронна поща.

Наказанието, което НК предвижда за въвеждането на компютърен вирус или друга злонамерена програма, е глоба в размер до 3.000 лв.

2.5.2. Квалифицирани състави

Чл. 319г, ал. 3 НК регламентира два квалифицирани състава на въвеждането на компютърен вирус или друга злонамерена програма. В първия случай деянието е квалифицирано с оглед на обективната страна, като квалифициращ признак е престъпният резултат, посочен в закона като настъпване на значителни вреди.[55] Пропуск на законодателя е изключването от престъпния резултат на настъпването на други тежки последици. По този начин неимуществените вреди неоснователно са изключени от квалифициращите обстоятелства.

Във втория случай деянието е квалифицирано, когато е извършено повторно. Квалифициращо обстоятелство е особеното качество на субекта на престъплението. По смисъла на чл. 28, ал. 1 НК престъплението е извършено повторно, ако деецът го е извършил, след като е бил осъден с влязла в сила присъда за друго такова престъпление. Предвид съдебната практика, според която еднакви по вид престъпления по са „тези, с които се осъществяват едни и същи или различни състави на едно и също престъпление, включително когато то е квалифицирано или привилегировано", повторност ще е налице и когато деецът въведе компютърен вирус, след като е бил осъден с влязла в сила присъда за въвеждане на друга злонамерена компютърна програма и обратното.[56]

И по двата квалифицирани състава предвиденото наказание е лишаване от свобода до три години и глоба до 1.000 лв.

2.6. Разпространяване на пароли и кодове за достъп до компютърна система или компютърни данни

> *Чл. 319д. (1) Който разпространи пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна, се наказва с лишаване от свобода до една година.*
>
> *(2) За деяние по ал. 1, извършено с користна цел, или ако с него са причинени значителни вреди или са настъпили други тежки последици, наказанието е лишаване от свобода до три години.*

2.6.1. Основен състав

[55] Виж по-подробно за причиняването на значителни вреди анализа на чл. 319б, ал. 2 НК (т. 2.4.2.1 по-горе).

[56] По-подробно за деянията, извършени при условията на повторност, виж анализа на чл. 319а, ал. 3 НК (т. 2.3.2.1 по-горе).

Непосредствен обект на престъплението са обществените отношения, осигуряващи поверителността и неприкосновеността на информацията в електронна форма, представляваща лични данни или защитена от закон тайна.

От обективна страна престъплението се характеризира с особен предмет – пароли или кодове за достъп до компютърна система или данни. С измененията от април 2007 г. разпоредбата на чл. 319д, ал. 1 НК беше променена от терминологична гледна точка. По старата редакция предметът на престъплението беше определен като „компютърни или системни пароли".[57]

Паролата представлява поредица от символи, която позволява на определен потребител да има достъп до определена компютърна система или данни. Кодът за достъп също представлява поредица от символи, които потребителят въвежда за получаване на достъп до определена компютърна система или данни. Тъй като в закона липсват легални определения на понятията „парола" и „код за достъп", е трудно да бъде точно определена разликата между тях. В специализираната литература най-често застъпваното становище е, че кодът за достъп (*passcode*) се състои само от цифри, докато паролата (*password*) може да включва различни символи (букви, цифри, знаци и т.н.).

Паролите и кодовете за достъп са най-често срещаните средства за защита на компютърните системи и данни срещу неправомерен достъп. Те се прилагат за автентификация на различните потребители, ползващи едновременно или последователно една и съща компютърна система или мрежа. Пароли и кодове се използват за осигуряване на достъп на потребителите до електронна поща, средства за онлайн комуникация (ICQ, Skype), Интернет страници за електронна търговия, електронни бази данни и т.н. С парола или код могат да се защитават и компютърни данни, когато се изпращат между две компютърни системи, съхраняват се на външен носител или се намират в компютър, до който достъп имат различни потребители.

От обективна страна изпълнителното деяние на престъплението се изразява в разпространяване. Разпространяването означава довеждане на определена информация, в случая на съответните пароли или кодове, до знанието на трети лица. Изпълнителното деяние може да бъде извършено само чрез действие. Паролите могат да бъдат разпространени както по електронен път, така и по друг начин, включително на хартиен носител. Дали разпространяването е извършено безвъзмездно или срещу заплащане е без значение за съставомерността на деянието.[58]

От обективна страна престъплението е резултатно. Резултатът е посочен като разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.[59] Разкриването на друга защитена от закон тайна беше добавено с

---

[57] Промяна на чл. 319д, ал. 1 НК се предлагаше още в Законопроекта за изменение и допълнение на НК, внесен през януари 2005 г., който предвиждаше предметът на престъплението да бъде променен от „компютърни или системни пароли" на „пароли за достъп до компютърна информационна система или компютърни информационни данни". За подробен анализ на предишния вариант на разпоредбата, включително предложения за нейното прецизиране, виж Марков, Д., *Правна уредба на компютърните престъпления по българското наказателно право*, в: *Електронният документ и електронният подпис. Правен режим*. Изд. Сиела. София, 2004 г., стр. 394-395.

[58] Виж също Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 64. Според автора чл. 319д, ал. 1 НК се отнася само за безвъздмездното разпространяване, тъй като законът предвижда квалифициран състав, когато деянието е извършео с користна цел (чл. 319д, ал. 2 НК). Възможно е, обаче, деецът да е получил някаква облага без да е имал користна цел в момента на извършване на деянието, както и да е имал за цел да получи облга, но тази цел да се е реализирала.

[59] С проекта на Закон за изменение и допълнение на НК, внесен през март 2006 г., се предлагаше деянието да е съставомерно дори когато от него може да последва разкриване на лични данни или държавна тайна. Проектът беше оттеглен от вносителя и предложението не беше доразвито. Запазването на варианта, при който престъпление е налице само при действителното разкриване на лични данни или защитена от закон тайна, е обосновано, тъй като доказването на потенциалната възможност за разкриване би създало затруднения в практиката.

измененията на НК от април 2007 г. Преди промените престъпният резултат по чл. 319д, ал. 1 НК включваше само личните данни и държавната тайна.[60]

Разкриването означава довеждане на определена информация до знанието на лице или лица, които нямат право на достъп до такава информация.

Личните данни са определени в ЗЗЛД, който урежда и правилата за работа с такива данни и реда за достъп до тях. Според чл. 2, ал. 1 ЗЗЛД лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци. Според Закона за българските документи за самоличност (ЗБДС) лични данни са имената, датата на раждане, единният граждански номер (или личен номер за чужденец), полът и гражданството на лицето (чл. 16, ал. 1 ЗБДС).

Останалите видове данни, включени в престъпния резултат, са тези, представляващи държавна или друга защитена от закон тайна.[61]

За да е налице съставомерно деяние по чл. 319д, ал. 1 НК, е необходимо наличието на причинна връзка между изпълнителното деяние и престъпния резултат. Причинната връзка също е елемент от обективната страна на престъплението и означава, че разкриването на личните данни или информацията, представляваща държавна или друга защитена от закон тайна, трябва да е пряка и непосредствена последица от разпространяването на паролите или кодовете за достъп.

Субект на престъплението може да бъде всяко наказателно отговорно лице. За съставомерността на деянието няма значение дали деецът е знаел съответните пароли или кодове правомерно. От субективна страна е налице умисъл, който обхваща както изпълнителното деяние (разпространяването), така и престъпния резултат (разкриването на личните данни или информацията, представляваща държавна или друга тайна, защитена от закон).

Предвиденото наказание по основния състав е лишаване от свобода до една година.

2.6.2. Квалифицирани състави

Чл. 319д, ал. 2 НК регламентира два квалифицирани състава. Първата хипотеза е, когато деянието е извършено с користна цел. Това е квалифициран състав с оглед на субективната страна, като квалифициращо обстоятелство се явява особената цел на дееца. Деянието е извършено с користна цел, когато деецът желае чрез него да набави за себе си или за другиго имотна облага.[62]

Втората хипотеза е, когато с деянието са причинени значителни вреди или са настъпили други тежки последици.[63] Другите тежки последици бяха добавени като резултат от престъплението с измененията на НК от април 2007 г. По този начин съставомерен резултат вече са както имуществените, така и неимуществените вреди. Промяната беше наложителна, тъй като в много случаи, особено при разкриването на лични данни, причинените вреди могат да имат неимуществен характер.[64]

---

[60] Добавянето на другите защитени от закон тайни беше предложено още в проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., но впоследствие негласуван от парламента.

[61] Виж по-подробно за информацията, представляваща държавна или друга защитена от закон тайна, анализа на чл. 319а, ал. 4 НК (т. 2.3.2.2 по-горе).

[62] Виж по-подробно за користната цел анализа на чл. 319б, ал. 3 НК (т. 2.4.2.3 по-горе).

[63] Виж по-подробно за причиняването на значителни вреди и настъпването на други тежки последици анализа на чл. 319б, ал. 2 НК (т. 2.4.2.1 по-горе).

[64] В проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше имуществените и неимуществените вреди да бъдат обединени под общата формулировка „значителни тежки последици". При обсъждането на проекта в парламента, обаче, се достигна до решението двата вида вреди да бъдат посочени алтернативно.

2.7. Престъпления във връзка със Закона за електронния документ и електронния подпис

Чл. 319е. Който при доставяне на информационни услуги наруши разпоредбите на чл. 6, ал. 2, т. 5 от Закона за електронния документ и електронния подпис, се наказва с глоба до пет хиляди лева, ако не подлежи на по-тежко наказание.

Непосредствен обект на престъплението по чл. 319е НК са обществените отношения, осигуряващи нормалното изпращане, получаване, записване и съхраняване на електронни изявления. Тези обществени отношения са регламентирани в ЗЕДЕП.

Нормата на чл. 319е НК е бланкетна норма, защото препраща за един от елементите на престъплението (изпълнителното деяние) към друг нормативен акт – ЗЕДЕП.

От обективна страна изпълнителното деяние се изразява в нарушаване на задължението за съхраняване на информацията за времето и източника на предаваните електронни изявления за срок от две години. Срокът от две години беше въведен със Закона за изменение и допълнение на НК, приет през април 2007 г. Преди промяната този срок беше шест месеца. Предложението за увеличаване на срока беше мотивирано с аргумента, че по този начин той се съобразява с необходимото време за провеждане на разследвания на извършени компютърни престъпления.

Изпълнителното деяние може да бъде осъществено както чрез действие (унищожаване на съответната информация), така и чрез бездействие (непредприемане на необходимите действия за запазване на информацията). Престъплението е формално – достатъчно е да е било осъществено изпълнителното деяние.

Престъплението по чл. 319е НК се характеризира с особен субект. Това е лице, което има качеството посредник при електронно изявление по смисъла на чл. 6, ал. 1 ЗЕДЕП. Изискването субектът на престъплението да има такова качество произтича от препращането към нормата на чл. 6, ал. 2, т. 5 ЗЕДЕП, която се прилага само по отношение на посредниците при електронни изявления. Понятието „посредник при електронното изявление" е легално дефинирано в чл. 6, ал. 1 ЗЕДЕП като лице, което по възлагане от титуляра изпраща, получава, записва или съхранява електронно изявление или извършва други услуги, свързани с него.

При определянето на субекта на престъплението по чл. 319е НК следва да се има предвид основният наказателно-правен принцип, че наказателната отговорност е лична и наказателно отговорни могат да бъдат само физически лица. Следователно субект на престъплението по чл. 319е НК ще бъде посредникът – физическо лице. Когато посредникът при електронното изявление е юридическо лице (например доставчик на Интернет услуги), субект на престъплението ще бъде физическото лице – служител на доставчика, което съгласно вътрешните правила на доставчика е задължено да съхранява посочената информация.

От обективна страна законът изисква изпълнителното деяние да е осъществено при доставяне на информационни услуги. НК не дава легално определение на дейността по доставяне на информационни услуги. При приемането на текста през 2002 г. в единия от първоначалните варианти на проекта беше предвидено легално определение на понятието „доставящ информационни услуги" (всяко лице, което обработва или съхранява компютърни данни в полза на услуги, даващи възможност за осъществяване на комуникация чрез компютърна система), което обаче не беше прието. Съдържанието на дейността по доставяне на информационни услуги може да бъде определено въз основа на легалната дефиниция на понятието „доставчик на компютърно-информационни услуги", дадена в чл. 93, т. 23 НК. По смисъла на това определение доставянето на информационни услуги ще представлява предлагане на възможност за комуникация чрез компютърна система или обработване или

съхраняване на компютърни данни за тази комуникационна услуга или за нейните ползватели.[65]

Изискването изпълнителното деяние да е осъществено при доставяне на информационни услуги е излишно. Напълно достатъчно за съставомерността на деянието е лицето да има качеството посредник при електронно изявление и да не е изпълнило задължението си да съхранява посочената информация в законово определения срок.[66]

От субективна страна престъплението е умишлено. Деецът съзнава, че е длъжен да съхранява посочената информация за определения срок, но въпреки това нарушава това свое задължение.

Разпоредбата на чл. 319е НК има субсидиарен характер. Тя се прилага само в случаите, когато деецът не подлежи на по-тежко наказание.

Предвиденото наказание е глоба до 5.000 лв. Освен това чл. 6, ал. 3 ЗЕДЕП предвижда и отговорност за вреди от неизпълнението на задължението за съхраняване на информацията.[67]

2.8. Компютърна измама

Чл. 212а. (1) Който с цел да набави за себе си или за другиго облага възбуди или поддържа заблуждение у някого, като внесе, измени, изтрие или заличи компютърни данни или използва чужд електронен подпис и с това причини на него или на другиго вреда, се наказва за компютърна измама с лишаване от свобода от една до шест години и глоба до шест хиляди лева.

(2) Същото наказание се налага и на този, който, без да има право, внесе, измени, изтрие или заличи компютърни данни, за да получи нещо, което не му се следва.

2.8.1. Основен състав по чл. 212а, ал. 1 НК

Компютърната измама е уредена като престъпление против собствеността. Нейното систематично място е в раздел четвърти „Измама" на глава пета „Престъпления против собствеността" от особената част на НК.

Непосредствен обект на престъплението са от една страна обществените отношения, осигуряващи неприкосновеността и нормалното упражняване на правото на собственост, а от друга – тези, гарантиращи сигурността на компютърните данни и осигуряващи правомерното създаване и използване на електронни подписи.

От обективна страна компютърната измама по чл. 212а, ал. 1 НК се характеризира с особен предмет на посегателство. Това са компютърни данни по смисъла на чл. 93, т. 21 НК.[68] Текстът на разпоредбата беше прецизиран с измененията на НК от април 2007 г., като и в двете алинеи старото понятие „компютърни информационни данни" беше заменено с новото „компютърни данни". Предмет на престъплението в хипотезата на компютърна измама чрез използване на чужд електронен подпис също са компютърни данни, защото електронният подпис по смисъла на ЗЕДЕП представлява именно такива данни. Предмет на

[65] По-подробно за определението на понятието „доставчик на компютърно-информационни услуги" виж анализа на чл. 93, т. 23 НК (т. 2.2.4 по-горе).

[66] Със Законопроекта за изменение и допълнение на НК, внесен през януари 2005 г., се предлагаше изразът „при доставяне на информационни услуги" да отпадне, но проектът така и не беше гласуван в пленарна зала.

[67] В Законопроектите за изменение и допълнение на НК, внесени през март и август 2006 г., се предлагаше чл. 319е НК да бъде отменен поради „липсата на висока обществена опасност, налагаща криминализиране на виновното неизпълнение на задължения от страна на посредниците при електронни изявления по чл. 6, ал. 1, т. 5 от ЗЕДЕП". В последна сметка, обаче, текстът беше запазен.

[68] По-подробно за определението на понятието „компютърни данни" виж анализа на чл. 93, т. 21 НК (т. 2.2.2 по-горе).

компютърната измама могат да бъдат и материалните носители, върху които тези данни се съхраняват. Това могат да бъдат магнитни и оптични носители, компютърни системи и т.н.[69]

Изпълнителното деяние на престъплението включва два взаимно свързани елемента. Първият елемент е посочен в закона като възбуждане или поддържане на заблуждение у друго лице.[70] Заблуждението представлява неправилна представа за факти и обстоятелства от обективната действителност. При компютърната измама, както и при обикновената измама по чл. 212 НК, това са факти и обстоятелства, свързани по определен начин с правното действие, което измаменото лице предприема или не предприема. Възбуждането на заблуждение представлява първоначално създаване у лицето на неправилна представа за определени факти и обстоятелства, докато поддържането на заблуждение се изразява в утвърждаване на вече формирана без участието на дееца неправилна представа.

Вторият елемент на изпълнителното деяние е посочен в закона като внасяне, изменение, изтриване или заличаване на компютърни данни или използване на чужд електронен подпис.

Внасянето, изменението, изтриването и заличаването на компютърни данни са същите изпълнителни деяния, както и при престъпните посегателства срещу компютърни програми и данни по чл. 319б НК, независимо от терминологичното разминаване между двете разпоредби (в чл. 212, ал. 1 НК са използвани понятията „внесе", „измени" и „заличи", докато чл. 319б, ал. 1 НК си служи с термините „добави", „промени" и „унищожи").[71]

Използването на чужд електронен подпис означава използване на определен електронен подпис от всяко лице, различно от неговия автор. Самото използване се изразява в създаване на подпис чрез използване на данните за неговото създаване, до които съгласно чл. 14 ЗЕДЕП достъп може да има само авторът.[72]

Вторият елемент на изпълнителното деяние се явява начин или средство за осъществяване на първия елемент – възбуждане или поддържане на заблуждение.
Компютърната измама по чл. 212а, ал. 1 НК е резултатно престъпление. Престъпните резултати са два – на първо място резултат е настъпилата промяна в компютърните данни, а на второ място – настъпването на вреди за измаменото или за друго лице.[73]

Субект на компютърната измама по чл. 212а, ал. 1 НК може да бъде всяко наказателно отговорно лице. В хипотезата на компютърна измама чрез използване на чужд електронен подпис субект на престъплението не може да бъде авторът на подписа, тъй като за него подписът не е чужд.

От субективна страна престъплението е умишлено. Деецът извършва посегателството като съзнава, че възбужда или поддържа заблуждение у измаменото лице. Освен това

---

[69] Виж Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г. Според автора компютърната измама има за предмет още физическото лице, върху което деецът въздейства, както и имуществото, намиращо се във фактическа власт на измаменото лице.

[70] В проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., като алтернатива на възбуждането и поддържането на заблуждение се предлагаше още едно изпълнително деяние – причиняване на смущения във функционирането на компютърна система. Предложението, обаче, не получи достатъчно подкрепа при обсъждането в парламента и не попадна в текста, предложен за гласуване на второ четене.

[71] Виж по-подробно за изпълнителните деяния анализа на чл. 319б, ал. 1 НК (т. 2.4.1 по-горе). С проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., беше предложено изпълнителните деяния „изтрие или заличи" в двете алинеи на чл. 212а НК да бъдат променени на „премахне или временно заличи", но тъй като парламентът не успя да гласува този проект, формулировката на деянията остана непроменена.

[72] В проекта на Закон за изменение и допълнение на НК, внесен през януари 2005 г., се предлагаше използването на чужд електронен подпис да отпадне като изпълнително деяние по основния състав на чл. 212а, ал. 1 НК. Парламентът обаче не успя да гласува проекта и това предложение не беше доразвито. Предложение за подобна промяна се съдържаше и в проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г. В него се предлагаше използването на чужд електронен подпис да бъде заменено от използване на чужди данни за създаване на електронен подпис или чужди лични данни без разрешение. При обсъждането на проекта в парламента обаче това предложение не беше прието и отпадна от варианта на текста, предложен за гласуване на второ четене.

[73] Виж Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г. Според автора вредата от компютърната измама може да бъде или само имуществена, или съчетание от имуществени и морални увреждания.

законът изисква и наличието на особена цел. Става дума за користна цел – деецът цели да набави облага за себе си или за другиго.[74]

Предвиденото наказание по основния състав на компютърната измама по чл. 212а, ал. 1 НК е лишаване от свобода от една до шест години и глоба до 6.000 лв.[75]

2.8.2. Основен състав по чл. 212а, ал. 2 НК

Компютърната измама по чл. 212а, ал. 2 НК се различава от престъплението по чл. 212а, ал. 1 НК по няколко белега.[76]

На първо място, разлика има в изпълнителното деяние. По чл. 212а, ал. 2 НК изпълнителното деяние е посочено само като неправомерно внасяне, изменение, изтриване или заличаване на компютърни данни. Липсва възбуждането или поддържането на заблуждение у друго лице.

От обективна страна при компютърната измама по чл. 212а, ал. 2 НК законът изрично изисква деянието по отношение на компютърните данни да е извършено без деецът да има съответното право за това.

Престъплението по чл. 212а, ал. 2 НК също е резултатно, но резултатът обхваща единствено настъпилата промяна в компютърните данни. Съставомерността на деянието не зависи от настъпването на вреди за измаменото лице или за други лица.

Субект на престъплението по чл. 212а, ал. 2 НК може да бъде всяко наказателно отговорно лице с изключение на лицата, които имат право да извършват посочените действия спрямо конкретните компютърни данни.

От субективна страна престъплението по чл. 212а, ал. 2 НК също е умишлено престъпление, но се характеризира с различна цел – получаване от самия деец на нещо, което не му се следва. Ако деецът цели не той, а трето лице да получи в резултат на деянието нещо, което не му се следва, деянието няма да е съставомерно по чл. 212а, ал. 2 НК.[77]

Предвиденото наказание по основния състав на компютърната измама по чл. 212а, ал. 2 НК е същото, както и по чл. 212а, ал. 1 НК – лишаване от свобода от една до шест години и глоба до 6.000 лв.

2.9. Престъпления против интелектуалната собственост

Чл. 172а. (1) Който записва, възпроизвежда, разпространява, излъчва или предава или използва по друг начин чужд обект на авторско или сродно на него право или екземпляри от него без необходимото по закон съгласие на носителя на съответното право, се наказва с лишаване от свобода до пет години и глоба до пет хиляди лева.

(2) Който без необходимото по закон съгласие държи материални носители, съдържащи чужд обект на авторско или сродно на него право на стойност в големи размери или държи матрица за възпроизвеждане на такива носители, се наказва с лишаване от свобода от две до пет години и глоба от две хиляди лева до пет хиляди лева.

(3) Ако деянието по ал. 1 и 2 е извършено повторно или са причинени значителни вредни последици, наказанието е лишаване от свобода от една до шест години и глоба от три хиляди лева до десет хиляди лева.

---

[74] Виж по-подробно за користната цел анализа на чл. 319б, ал. 3 НК (т. 2.4.2.3 по-горе).

[75] Проектът на Закон за изменение и допълнение на НК, внесен през март 2006 г., предлагаше цялостна редакция на чл. 212а, ал. 1 НК. Той предвиждаше възбуждането и поддържането на заблуждение да отпадне, изпълнителни деяния да останат само внасянето, изменянето, изтриването и унищожаването (вместо заличаването) на компютърни данни и използването на чужд електронен подпис, да се добави уточнението, че както облагата, така и настъпилата вреда са „имотни", т.е. имат имуществен характер, и да се премахне максималният размер на глобата. Проектът обаче беше оттеглен от вносителя и предложените промени не се осъществиха.

[76] Виж по-подробно за отношението между съставите на чл. 212а, ал. 1 и 2 НК, както и за отношението между компютърната измама и другите видове измама Стойнов, Ал., *Компютърната измама*, Съвременно право, кн. 4, 2002 г.

[77] Проектът на Закон за изменение и допълнение на НК, внесен през март 2006 г., предвиждаше чл. 212а, ал. 2 НК да бъде отменен, но разпоредбата беше запазена.

(4) Когато деянието по ал. 2 е в особено големи размери, наказанието е лишаване от свобода от две до осем години и глоба от десет хиляди лева до петдесет хиляди лева.

(5) За маловажни случаи деецът се наказва по административен ред по Закона за авторското право и сродните му права.

(6) Предметът на престъплението се отнема в полза на държавата, независимо чия собственост е, и се унищожава.

Посегателствата срещу правата на интелектуална собственост бяха инкриминирани за първи път в българското законодателство с измененията на НК от 1995 г.[78] Тези текстове останаха почти непроменени до 2006 г., когато с поредните промени в НК правната уредба на престъпленията против интелектуалната собственост беше съществено изменена.[79]

Престъпленията против интелектуалната собственост включват различни видове престъпни деяния, от които само някои са свързани с информационните технологии. Поради бързото развитие на тези технологии през последните години, обаче, те постепенно се превърнаха в основен предмет и средство за извършване на престъпления срещу интелектуалната собственост. Понастоящем, основният проблем, пред който е изправена защитата на авторските права, е именно незаконното разпространение на обекти на интелектуална собственост посредством съвременните информационни технологии.

Основната разпоредба, която има отношение към престъпленията против интелектуалната собственост, които могат да бъдат определени като компютърни престъпления, е чл. 172а НК.

2.9.1. Основен състав по чл. 172а, ал. 1 НК

Чл. 172а, ал. 1 НК инкриминира нерегламентираното използване на чужд обект на авторското право или екземпляри от него.

Непосредствен обект на това престъпление са обществените отношения, свързани с нормалното осъществяване на авторското и сродните му права, както и установените от държавата условия и ред за упражняването на тези права.

От обективна страна предметът на престъплението е определен като „обект на авторско право или сродно на него право, включително екземпляр от него". Преди промените от 2006 г. НК предвиждаше два отделни основни състава с едно и също изпълнително деяние (записване, възпроизвеждане, разпространяване, излъчване или предаване чрез техническо средство или използване по друг начин без необходимото по закон съгласие на носителя на съответното право) и една и също санкция (лишаване от свобода до три години и глоба от 1.000 до 3.000 лв.), но различен предмет. По единия основен състав ставаше въпрос за чуждо произведение на науката, литературата или изкуството, а по другия – за звукозапис, видеозапис или радиопрограма, телевизионна програма, софтуер или компютърна програма. С измененията двата състава бяха обединени в един, а предметът на престъплението беше определен с общото понятие „чужд обект на авторско право или сродно на него право, или екземпляр от него". Със същото изменение беше увеличен и размерът на наказанието, който сега е лишаване от свобода до пет години и глоба до 5.000 лв.[80]

Обектите на авторското право са легално дефинирани в ЗАПСП. Според чл. 3, ал. 1 ЗАПСП обект на авторското право е всяко произведение на литературата, изкуството и науката, което е резултат на творческа дейност и е изразено по какъвто и да е начин и в

[78] Виж Закон за изменение и допълнение на Наказателния кодекс, обнародван в Държавен вестник, бр. 50 от 1 юни 1995 г.

[79] Виж Закон за изменение и допълнение на Наказателния кодекс, приет от Четиридесетото Народно събрание на 30 август 2006 г., обнародван в Държавен вестник, бр. 75 от 12 септември 2006 г., в сила от 13 октомври 2006 г.

[80] В проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше екземплярите от обекти на авторското право да отпаднат като отделен предмет на престъплението и наказанията да бъдат намалени: лишаването от свобода – на до три години, а глобата – на от 1.000 до 3.000 лв. Предложението обаче не беше прието.

каквато и да е обективна форма. В допълнение към определението, примерно са изброени най-разпространените обекти на авторското право, като литературни произведения, включително произведения на научната и техническата литература, музикални и сценични произведения, филми, произведения на изобразителното изкуство и т.н.

Според чл. 72 ЗАПСП правата, сродни на авторското, включват правата на артистите-изпълнители върху техните изпълнения, на продуцентите на звукозаписи върху техните звукозаписи, на продуцентите на първоначалния запис на филм или друго аудиовизуално произведение върху оригинала и копията, получени в резултат на този запис, и на радио- и телевизионните организации върху техните програми.

Екземпляр от обект на авторското право е всяка самостоятелна бройка от него. Екземпляри са както оригиналите, така и копията на съответния обект на авторско или сродно на него право.

Характерно за предмета на престъплението е, че става дума за чужд обект на авторско или сродно на него право, т.е. деецът не е носител на съответното право.

Носителите на авторското право и на сродните му права са подробно регламентирани в ЗАПСП. По начало, носител на авторското право е авторът на произведението. В определени от ЗАПСП случаи носители на авторско право могат да бъдат и други лица. Така например авторското право върху филм или друго аудиовизуално произведение принадлежи на режисьора, сценариста и оператора, докато авторите на музиката, на диалога, на вече съществуващата литературна творба, по която е създадено произведението, на сценографията, на костюмите, както и на други произведения, включени в него, запазват авторското си право върху своите произведения.

Що се отнася до сродните на авторското права, техни носители са артистите-изпълнители (върху своите изпълнения), продуцентите на звукозаписи (върху своите звукозаписи), продуцентите на първоначалния запис на филм или друго аудиовизуално произведение (върху оригинала и копията, получени в резултат на този запис), и радио- и телевизионните организации (върху своите програми).

За всички останали лица съответното произведение е чужд обект на авторско или сродно на него право.

Изпълнителното деяние на престъплението е определено изключително широко, като са изброени примерно няколко деяния, които според преценката на законодателя са най-често срещаните случаи на такива посегателства (записване, възпроизвеждане, разпространяване, излъчване и предаване), към които е добавено и всяко използване по друг начин.[81]

Възпроизвеждането и разпространението са легално определени в ЗАПСП. Според § 3 от Допълнителните разпоредби на ЗАПСП „възпроизвеждане на произведение" е прякото или непрякото размножаване в един или повече екземпляри на произведението или на част от него, по какъвто и да е начин и под каквато и да е форма, постоянна или временна, включително запаметяването му под цифрова форма в електронен носител. Според § 4 от Допълнителните разпоредби на ЗАПСП „разпространение на произведение" е продажбата, замяната, дарението, даването под наем, както и съхраняването в търговски количества, а също и предложението за продажба или даване под наем на оригинали или екземпляри от произведението.

Легалните определения по ЗАПСП могат да се използват за изясняване на съдържанието и на останалите изпълнителни деяния на престъплението по чл. 172а, ал. 1 НК. Така например на основата на § 7 от Допълнителните разпоредби на ЗАПСП, който дава определение на понятието „звукозаписване", съдържанието на изпълнителното деяние записване може да се определи като фиксиране върху траен материален носител на обект на авторско право, по

[81] При приемането на промените в НК се обсъждаше добавянето и на още две деяния (внасяне и изнасяне) към примерното изброяване, но в последствие това предложение беше отхвърлено.

начин, позволяващ неговото възприемане, възпроизвеждане, презаписване, излъчване по безжичен път или предаване чрез кабел или друго техническо средство.

Понятието „излъчване на произведение по безжичен път", определено в § 5 от Допълнителните разпоредби на ЗАПСП, може пък да се приеме за равнозначно на изпълнителното деяние излъчване, още повече че преди последните изменения на НК от 2006 г. чл. 172а НК също говореше за излъчване по безжичен път. Излъчването обхваща всяко излъчване по радио или телевизия по наземен път, както и включването му в непрекъсната съобщителна верига, водеща до спътник и оттам обратно до Земята чрез сигнали, носещи програми, под контрола и на отговорност на излъчващата организация с оглед да бъде то прието, било пряко и индивидуално от публиката, било чрез посредничеството на организация, различна от излъчващата.

Що се отнася до последната посочена форма на изпълнителното деяние – предаването – тя има съдържание близко до излъчването, като за разлика него вместо по безжичен път предаването става чрез кабел.[82]

Освен тези изрично изброени случаи изпълнително деяние на престъплението по чл. 172а, ал. 1 НК е налице и при всяко „използване по друг начин" на съответния обект на авторското право. По този начин законодателят се стреми да обхване максимално широк кръг случаи на посегателства срещу обекти на авторското право и сродните му права. От една страна това е оправдано с оглед бързото развитие на информационните технологии и опасността изброените форми на изпълнителното деяние да се окажат недостатъчни за санкциониране на всички общественоопасни посегателства в тази сфера. От друга страна, обаче, прекалено широкият кръг деяния, които биха могли да се квалифицират като престъпления по чл. 172а, ал. 1 НК, може да породи необоснована строгост от страна на компетентните органи по отношение на нарушения, които не разкриват степента на обществена опасност, необходима за ангажиране на тежката процедура на наказателния процес. Наистина, НК съдържа известни гаранции, че по наказателен ред ще се преследват само действително сериозните случаи на посегателства срещу авторското и сродните му права. Такива гаранции са както общата разпоредба на чл. 9, ал. 2 НК, според която деянието няма да се квалифицира като престъпление, ако е малозначително, така е разпоредбата на чл. 172а, ал. 5 НК, предвиждаща налагане на административно наказание за маловажните случаи. Независимо от това, широката формулировка на изпълнителното деяние на практика оставя преценката за това дали деецът подлежи на наказателна отговорност изцяло в ръцете на прокуратурата и съда.

Важен елемент от обективната страна на престъплението е липсата на необходимото по закон съгласие на носителя на съответното право. Случаите, когато такова съгласие се изисква, редът за неговото получаване и срокът на действието му са уредени подробно в ЗАПСП.

Субект на престъплението е всяко наказателно отговорно лице с изключение на самите носители на авторското или сродното на него право. От субективна страна престъплението е умишлено. Деецът съзнава, че не е носител на авторско или сродно на него право върху съответния обект, както и че не е получил съгласието на носителя на правото.

Предвиденото наказание за деянията по чл. 172а, ал. 1 НК е лишаване от свобода до пет години и глоба до 5.000 лв.

2.9.2. Основен състав по чл. 172а, ал. 2 НК

Чл. 172а, ал. 2 НК инкриминира неправомерното държане на носители, съдържащи чужд обект на авторско или сродно на него право, или на матрица за възпроизвеждане на

[82] Със Законопроекта за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше към изпълнителните деяния „излъчва" и „предава" да бъде добавено уточнението „чрез техническо средство", но предложението не беше прието.

такива носители. Това деяние беше криминализирано за първи път с измененията на НК от 2006 г.[83]

Непосредствен обект на престъплението, освен обществените отношения, свързани с нормалното осъществяване на авторското и сродните му права, и установените от държавата условия и ред за упражняването на тези права, са също и обществените отношения, свързани с реда за производство и разпространение на материалните носители, съдържащи обекти на авторското право и сродните му права, както и на матрици за тяхното възпроизвеждане.

Материалните носители, съдържащи обекти на авторското право и сродните му права, и матриците за възпроизвеждане на такива носители са и предмет на престъплението по чл. 172а, ал. 2 НК. При определянето на тези понятия могат да се използват легалните определения, посочени в приетия през 2005 г. Закон за административното регулиране на производството и търговията с оптични дискове, матрици и други носители, съдържащи обекти на авторското право и сродните му права. Според допълнителните разпоредби на този закон „други носители" (освен оптичните дискове) са всички трайни материални носители, върху които са фиксирани обекти на авторското право и сродните му права по начин, даващ възможност тези обекти с помощта на подходящи устройства да бъдат доведени до знанието на публиката. „Оптични дискове" пък са носители, върху които е фиксирана и съхранена или може да бъде фиксирана и съхранена информация в цифрова форма, четима с помощта на оптичен механизъм, използващ лазер или друг високочестотен светлинен източник, като в тази категория се включват CD, CD-DA, CD-I, CD-P, CD-ROM, CD-R, CD-RW, CD-WO, DVD, DVD-RAM, DVD-ROM, LD, MD, VCD, CVD, SVCD, SACD. На практика материалните носители, които биха могли да съдържат обекти на авторското право или сродно на него право, са много широк кръг. Тук се включват както преносимите носители, като магнитни дискове и дискети, оптични дискове, външна памет (флаш памет), различните видове карти с памет за мобилни телефони и т.н., така и носители, които са практически част от други устройства, като твърдия диск на компютъра, вградената памет на мобилните телефони и др.

Законът за административното регулиране на производството и търговията с оптични дискове, матрици и други носители, съдържащи обекти на авторското право и сродните му права, определя понятието „матрица" като първообраз на оптичен диск, съдържащ информация, от който по специална технология могат да се произвеждат ограничен брой екземпляри оптични дискове.

Изпълнителното деяние е посочено в закона като държане, което означава упражняване на фактическа власт върху съответните материални носители или матриците за тяхното възпроизвеждане.

От обективна страна е необходимо държането да се извършва при липсата на необходимото по закон съгласие. В тази си част редакцията на разпоредбата не е напълно прецизна, тъй като не посочва от кого следва да изхожда това съгласие. Чл. 172а, ал. 1 НК говори изрично за съгласието на носителя на съответното право. По ал. 2 обаче носителят на авторското или сродното на него право не е изрично споменат, което дава възможност и за по широко тълкуване при определяне на съгласието.

Във всички случаи, ако липсва необходимото по закон съгласие на носителя на съответното право, деянието ще се квалифицира като престъпление по чл. 172а, ал. 2 НК. Спорният въпрос в случая е, дали ако липсва друго необходимо по закон съгласие, разпоредбата на чл. 172а, ал. 2 НК отново ще бъде приложима.

Тълкуването от тази гледна точка има важно значение дотолкова, доколкото производството и търговията с оптични дискове, матрици и други носители е предмет на специална законодателна уредба и се подчинява на различни режими (регистрационен, когато става дума за възпроизвеждане на обекти на авторското право върху оптични дискове и други носители без запис, лицензионен за производството на оптични дискове и матрици,

[83] С проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., се предлагаше чл. 172а, ал. 2 НК да бъде отменен, но предложението беше отхвърлено.

уведомителен за вноса и износа на матрици, суровини и оборудване за производството на оптични дискове и т.н.). В настоящата си редакция разпоредбата на чл. 172а, ал. 2 НК следва да се прилага и в тези случаи, тъй като на практика става въпрос за държане на материален носител или матрица без да е получено необходимото съгласие на компетентния държавен орган. Подобно тълкуване, обаче, може да създаде известни затруднения в практиката. Така например, за производството на оптични дискове и матрици за тяхното производство е необходим лиценз. Липсата на такъв лиценз, следователно, би могло да се приеме за липса на необходимото по закон съгласие. Вносът на дискове и матрици, от друга страна, се подчинява на уведомителен режим, при който на практика няма акт на съответния държавен орган, който да може да се приеме за равностоен на съгласие. Единствената последица от уведомяването е вписването му в специален регистър, което обаче едва ли може да се квалифицира като съгласие.

Когато предмет на престъплението са материални носители, законът изисква наличието и на още един елемент от обективна страна. Става въпрос за стойността на тези носители, която НК определя като „стойност в големи размери". Според съдебната практика големи размери са налице, когато паричната равностойност на предмета на престъплението надхвърля седемдесет пъти установената в страната минимална работна заплата.[84] От 1 януари 2008 г. минималната работна заплата за страната е 220 лв.[85] Това означава, че за да бъде в големи размери, стойността на предмета на престъплението трябва да надвишава сумата от 15.400 лв.

Редакцията на текста налага извода, че при квалификацията на деянието трябва да се държи сметка само и единствено за стойността на самите носители, независимо от съдържащата се на тях информация, а тази стойност при някои носители (оптични дискове, дискети) е изключително ниска. По този начин, за да е налице престъпление, извършителят ще трябва да държи значително количество такива носители. Така например, ако предмет на престъплението са оптични дискове, съдът ще трябва да вземе предвид единствено стойността на самите дискове, абстрахирайки се от тяхното съдържание. Като се има предвид, че цената на тези дискове е около 50 ст. на диск, деянието ще се квалифицира като престъпление, ако е налице държане на над 30.000 диска, съдържащи чужди обекти на авторското право. Нормалният капацитет на един такъв оптичен диск, обаче, е 650 MB, което означава, че 30.000 диска ще се равняват на близо 20 терабайта информация. За да бъде прецизен, законът следва да отчита и други признаци при квалифицирането на деянието като престъпление, като например обема на информацията, съдържаща се върху съответните носители, пазарната стойност на съответния обект на авторското право, размера на причинените с деянието вреди (който е предвиден единствено като квалифициращо обстоятелство по чл. 172а, ал. 3 НК) и т.н.

Субект на престъплението е всяко наказателно отговорно лице с изключение на носителя на авторското право или сродното на него право, за когото предметът на престъплението няма характера на чужд обект на авторското право.

От субективна страна е налице умисъл – деецът съзнава, че не разполага с изискващото се по закон съгласие за държането на съответния материален носител или матрица.[86]

Наказанието, предвидено за извършване на престъпление по чл. 172а, ал. 2 НК, е лишаване от свобода от две до пет години и глоба от 2.000 до 5.000 лв.

2.9.3. Квалифицирани състави

[84] Виж ТР № 1 от 30.10.1998 г. на ОСНК по тълк. н. д. № 1/98 г.

[85] Виж Постановление № 1 на МС от 11.01.2008 г. за определяне на нов размер на минималната работна заплата за страната, обнародвано в Държавен вестник, бр. 6 от 18 януари 208 г.

[86] При приемането на промените в НК се обсъждаше като елемент от субективната страна на престъплението по чл. 172а, ал. 2 НК да бъде добавена и особена цел на дееца, определена като „търговска". Подобна цел не присъства в нито една друга разпоредба от НК и закономерно отпадна от окончателния вариант на приетите от парламента промени. За анализ и критика на това предложение виж *Е-България 2006*, Фондация „Приложни изследвания и комуникации", София, 2006 г., стр. 82.

Квалифицираните състави на престъпленията срещу интелектуалната собственост са уредени в чл. 172а, ал. 3 и 4 НК. Квалифициращи обстоятелства са субектът на престъплението и престъпният резултат, а за деянието по чл. 172а, ал. 2 НК – и размерът на деянието. След промените от 2006 г. всички квалифицирани състави на посегателствата срещу авторското право и сродните му права вече са тежки престъпления по смисъла на чл. 93, т. 7 НК.

2.9.3.1. Квалифицирани състави във връзка със субекта

НК предвижда само един квалифициран състав на престъпленията по чл. 172а, ал. 1 и 2 НК от гледна точка на субекта и това са случаите, когато деянието е извършено повторно (чл. 172а, ал. 3 НК).[87] Предвиденото наказание е лишаване от свобода от една до шест години и глоба от 3.000 до 10.000 лв.

Повторност ще бъде налице винаги, когато деецът извърши престъпление по една от първите две алинеи на чл. 172а НК, след като е бил осъден с влязла в сила присъда за друго престъпление по същата алинея, без значение от самото изпълнително деяние. Така например, ако едно лице е осъдено с влязла в сила присъда за неправомерно записване на чужд обект на авторското право, а в последствие бъде обвинено за разпространение на екземпляри от такъв, деянието ще се квалифицира като извършено при условията на повторност.

Възниква обаче въпросът дали този принцип ще важи за деяния, попадащи в приложното поле на двете различни алинеи. Такъв ще бъде, например, случаят, когато лице, осъдено за неправомерно записване, впоследствие бъде обвинено за държане на матрица. Отговорът на този въпрос зависи преди всичко от съдебната практика и от това дали тя ще тълкува ал. 1 и 2 като „различни състави на едно и също престъпление" или като състави на различни престъпления. В първия случай лицето ще носи отговорност по квалифицирания състав за повторност, а във втория – по основния състав.

2.9.3.2. Квалифицирани състави във връзка с престъпния резултат

Престъпленията по чл. 172а, ал. 1 и 2 НК са по-тежко наказуеми (лишаване от свобода от една до шест години и глоба от 3.000 до 10.000 лв.), когато с деянието са причинени значителни вредни последици. Вредните последици обхващат както имуществените, така и неимуществените вреди. Последиците трябва да са пряк и непосредствен резултат от деянието. Дали те са значителни ще се преценява във всеки конкретен случай от съда, който следва да се ръководи преди всичко от размера на вредите, претърпени от носителя на съответното авторско или сродно на него право.

2.9.3.3. Други квалифицирани състави

С измененията на НК от 2006 г. беше добавен още един квалифициран състав, само за престъплението по чл. 172а, ал. 2 НК. Според чл. 172а, ал. 4 НК престъплението е по-тежко наказуемо (лишаване от свобода от две до осем години и глоба от 10.000 до 15.000 лв.), когато „деянието по ал. 2 е в особено големи размери". Според съдебната практика особено големи размери са налице, когато паричната равностойност на предмета на престъплението надхвърля сто и четиридесет пъти установената за страната минимална работна заплата.[88] При минимална работна заплата от 220 лв. това означава, че особено големи размери ще са налице при стойност не по-малка от 30.800 лв.

[87] По-подробно за деянията, извършени при условията на повторност, виж анализа на чл. 319а, ал. 3 НК (т. 2.3.2.1 по-горе).
[88] Виж ТР № 1 от 30.10.1998 г. на ОСНК по тълк. н. д. № 1/98 г.

Редакцията на текста не е прецизна и може да създаде затруднения в практиката. Очевидно е, че самото деяние няма стойност, следователно няма как то да бъде „в особено големи размери". В особено големи размери могат да бъдат отделни негови елементи, като причинените вреди, облагата, предметът и т.н. Ако текстът се тълкува само във връзка с основния състав по чл. 172а, ал. 2 НК, се налага изводът, че става въпрос за стойността на предмета на престъплението. По основния състав се изисква предметът на престъплението, когато това са материални носители, да е на стойност в големи размери. Когато тези носители са в особено големи размери деянието ще се квалифицира като по-тежко наказуемо. Логично е същият подход да се приложи и когато предмет на престъплението са матрици за възпроизвеждане на материални носители, въпреки че по основния състав за тях не се изисква да са на стойност в големи размери. Що се отнася до причинените с деянието вреди, въпросът остава открит и ще бъде решен от съдебната практика. Следва да се има предвид и разпоредбата на чл. 172а, ал. 3 НК, която предвижда квалифициран състав в случай на значителни вредни последици. От една страна тази разпоредба като че ли изключва вредите като критерий при квалифицирането на деянието като по-тежко наказуемо поради особено големи размери. От друга страна, наказанията по чл. 172а, ал. 4 НК са значително по-тежки от тези по чл. 172а, ал. 3 НК и ако се приеме че „особено големите размери" надвишават „значителните вредни последици" приложението на чл. 172, ал. 4 НК не изглежда неоправдано.

Така формулиран, текстът на чл. 172а, ал. 4 НК не изключва и съобразяването на други обстоятелства за определяне на особено големите размери на деянието, като например извлечената от престъплението облага. При тази категория престъпления облагата в много случаи е значителна и може да надвишава многократно стойността на предмета на престъплението. Така например, печалбата от продажбата на един оптичен диск със софтуер в нарушение на авторското право е далеч по-голяма от стойността на самия диск.

Във всички случаи редакцията на чл. 172а, ал. 4 НК трябва да бъде прецизирана, за да се избегне появата на противоречива съдебна практика.

2.9.4. Маловажни случаи

Според чл. 172а, ал. 5 НК за маловажни случаи деецът се наказва по административен ред по ЗАПСП. Административните наказания, предвидени в ЗАПСП, са глоби, чийто размер варира между 300 и 5.000 лв.

Според чл. 93, т. 9 НК маловажен случай е този, при който извършеното престъпление с оглед на липсата или незначителността на вредните последици или с оглед на други смекчаващи обстоятелства представлява по-ниска степен на обществена опасност в сравнение с обикновените случаи на престъпление от съответния вид. Разпоредбата, предвиждаща административно наказание за маловажните случаи на посегателства срещу интелектуалната собственост, е от особено значение предвид нарастващите случаи на неправомерно разпространение на обекти на авторското право и сродните му права през Интернет.[89] В много от тези случаи става въпрос за размяна на отделни произведения между ограничен кръг лица, на което може ефективно да се противодейства и със средствата на административно-наказателната отговорност. На практика е невъзможно, а и ненужно, всяко едно нарушение на авторско или сродно на него право да се санкционира посредством бавния, тежък и скъп механизъм за реализиране на наказателната отговорност. Остава, обаче, открит въпросът дали не е по-целесъобразно самите състави на престъпленията против

[89] Въпреки първоначалните идеи, измененията на НК от 2006 г. не засегнаха разпоредбата, предвиждаща налагане на административно наказание за маловажните случаи на посегателства срещу авторското право и сродните му права. Приетият на първо четене първоначален вариант на проекта, предвиждаше този текст да бъде отменен. Подобна промяна щеше да остави като единствена алтернатива на наказателната отговорност липсата на престъпно деяние поради неговата малозначителност по чл. 9, ал. 2 НК. За критика на подобна промяна виж *Е-България 2006*, Фондация „Приложни изследвания и комуникации", София, 2006 г. стр. 83.

интелектуалната собственост да бъдат по-прецизно формулирани, така че да обхващат само наистина сериозните посегателства, разкриващи висока степен на обществена опасност и поради това изискващи по-тежка санкция от страна на държавата. При сегашната редакция на текстовете преценката за маловажността на всяко едно деяние остава в компетентността на съдебните органи, което от една страна излишно ги обременява, а от друга страна може да доведе до неоправдано завишаване или занижаване на критериите за маловажност на деянието.

2.9.5. Отнемане на предмета на престъплението в полза на държавата

Чл. 172а, ал. 6 НК предвижда като принудителна административна мярка отнемане в полза на държавата и унищожаване на предмета на престъплението, независимо чия собственост е. Преди измененията на НК от 2006 г. същата разпоредба предвиждаше, че предметът на престъплението се отнема в полза на държавата само когато принадлежи на виновния и не уреждаше изрично въпроса за унищожаването.

В новата си редакция разпоредбата относно отнемането в полза на държавата на предмета на престъплението поражда някои спорни въпроси, най-важният от които се отнася до обхвата на понятието „предмет на престъплението".

Предмет на престъплението по чл. 172а, ал. 1 НК е чужд обект на авторско или сродно на него право или екземпляри от него. За да бъде отнет, чуждият обект на авторското право трябва да е материализиран върху определен носител. На практика това, което може да бъде отнето, е самият носител – магнитен или оптичен диск, дискета, магнитна лента и т.н. Същото важи и за екземплярите от чуждия обект на авторското право.

Предмет на престъплението по чл. 172а, ал. 2 НК са материални носители, съдържащи чужд обект на авторско или сродно на него право, както и матрици за възпроизвеждане на такива носители. Материалните носители могат да бъдат най-различни – оптични дискове, магнитни дискети, външна памет и т.н. Когато материалният носител е част от по-голямо устройство, например твърд диск на компютър или карта с памет за мобилен телефон, на отнемане и унищожаване следва да подлежи самият носител, а не цялото устройство. Спорен остава въпросът как следва да се процедира, когато материалният носител не може да бъде физически отделен от съответното устройство без последното да бъде повредено. Такъв би бил случаят, например, с някои устройства с вградена памет, като мобилни телефони, MP3 плеъри и др.

Що се отнася до отнемането на матрици за възпроизвеждане на такива носители, стриктното тълкуване на текста на закона изисква в полза на държавата да се отнема единствено самата матрица (първообраза на оптичния диск), но не и самата технология за възпроизвеждане. Самата технология ще може евентуално да бъде отнета в полза на държавата на основание чл. 53, ал. 1, б. „а" НК, ако принадлежи на виновния и е била предназначена или е послужила за извършване на престъплението. На същото основание ще могат да бъдат отнети и други устройства, които принадлежат на виновния и са били предназначени или са послужили за извършване на диянието (компютри, сървъри, модеми, принтери и т.н.).

Спорен е въпросът доколко е обосновано отнемането и унищожаването на предмета на престъплението, когато той не е собственост на виновния. Това нововъведение от 2006 г. беше посрещнато с противоречиви реакции. От една страна, разбираем е стремежът на законодателя да предотврати последващи посегателства с използването на същия предмет на престъплението, независимо на кого принадлежи той. От друга страна, обаче, непрецизното дефиниране на предмета на престъплението може да доведе до отнемане в полза на държавата на вещи на значителна стойност, които не принадлежат на извършителя на престъплението, което създава опасност от неоправдано накърняване на правата на трети добросъвестни лица.

Определени въпроси поставя и задължителното изискване предметът на престъплението да бъде унищожен. По-целесъобразното решение би било заличаване на чуждия обект на авторското право от материалния носител и едва като крайна мярка, ако заличаването е технически невъзможно, да се прибягва към унищожаване на самия материален носител. Такова решение беше възприето с промените на ЗАПСП от 2005 г., когато предмет на нарушението са компютърни програми. Така според § 1а, ал. 3 от Допълнителните разпоредби на ЗАПСП отнемане в полза на държавата на предмета на нарушението, когато той представлява компютърна програма, е и неговото заличаване от електронния носител, на който е бил възпроизведен.

2.10. Престъпления, свързани с порнографски материали

Чл. 159. (1) Който създава, излага, представя, излъчва, предлага, продава, дава под наем или по друг начин разпространява порнографски материал, се наказва с лишаване от свобода до една година и глоба от хиляда до три хиляди лева.

(2) Който разпространява чрез Интернет порнографски материал, се наказва с лишаване от свобода до две години и глоба от хиляда до три хиляди лева.

(3) Който излага, представя, предлага, продава, дава под наем или по друг начин разпространява порнографски материал на лице, ненавършило 16 години, се наказва с лишаване от свобода до три години и глоба до пет хиляди лева.

(4) За деянията по ал. 1 - 3 наказанието е лишаване от свобода до шест години и глоба до осем хиляди лева, ако за създаването на порнографския материал е използвано лице, ненавършило 18 години, или лице, което изглежда като такова.

(5) Когато деянието по ал. 1 - 4 е извършено по поръчение или в изпълнение на решение на организирана престъпна група, наказанието е лишаване от свобода от две до осем години и глоба до десет хиляди лева, като съдът може да постанови и конфискация на част или на цялото имущество на дееца.

(6) Който държи или набавя за себе си или за другиго чрез компютърна система или по друг начин порнографски материал, за създаването на който е използвано лице, ненавършило 18 години, или лице, което изглежда като такова, се наказва с лишаване от свобода до една година или глоба до две хиляди лева.

(7) Предметът на престъплението се отнема в полза на държавата, а ако липсва или е отчужден, се присъжда неговата равностойност.

Престъпленията, свързани с порнографски материали, също както престъпленията срещу интелектуалната собственост, не са типични компютърни престъпления. Поради широкото разпространение на информационните технологии, обаче, разпространението на такива материали по електронен път става все по-често срещано явление. Тази форма на разпространение разкрива и много висока степен на обществена опасност, тъй като за разлика от разпространението на хартиен носител, използването на новите технологии дава възможност материалите да достигнат до на практика неограничен кръг лица. Поради тази причина с измененията на НК от април 2007 г. старата уредба на престъпленията, свързани с порнографски материали, беше променена, като бяха въведени нови, по-тежко наказуеми състави, свързани с разпространението на такива материали чрез Интернет.

2.10.1. Основни състави

НК регламентира два основни състава на престъпления, свързани с порнографски материали. И по двата основни състава, обаче, законът не прави разлика дали при осъществяване на деянието са използвани компютри или други информационни технологии или не.

Първият основен състав включва създаването, излагането, представянето, излъчването, предлагането, продаването, даването под наем или разпространяването по друг начин на порнографски материал (чл. 159, ал. 1 НК).[90]

С измененията на НК от април 2007 г. за първи път в българското законодателство беше въведено легално определение на понятието „порнографски материал" (чл. 93, т. 28 НК). Според това определение „порнографски материал" е неприличен, неприемлив или несъвместим с обществения морал материал, който изобразява открито сексуално поведение. Определението се състои от два елемента. На първо място става въпрос за материал, който изобразява открито сексуално поведение. Самият чл. 93, т. 28 НК дава примери кога едно действие може да се приеме за открито сексуално поведение. Това са случаите, когато поведението изразява реални или симулирани полови сношения между лица от същия или различен пол, содомия, мастурбация, сексуален садизъм или мазохизъм, или похотливо показване на половите органи на лице.[91] Изброяването е примерно и във всеки конкретен случай съдът ще трябва да преценява дали определено действие представлява или не открито сексуално поведение. Вторият елемент на дефиницията отразява обществената оценка за този материал, а именно, че той е неприличен, неприемлив или несъвместим с обществения морал. Кога определен материал е неприличен, неприемлив или несъвместим с обществения морал ще определи съдебната практика. От значение в случая е, че двата елемента на определението трябва да са налице едновременно, за да може определен материал да се квалифицира като порнографски. Ако определен материал изобразява открито сексуално поведение, но по своя характер не е неприличен, неприемлив или несъвместим с обществения морал, той няма да има качеството порнографски материал. Примери за такива материали са различните материали с учебна или образователна цел, научната литература, произведения на изкуството, и т.н. Когато един материал е неприличен, неприемлив или несъвместим с обществения морал, но не изобразява открито сексуално поведение, той също няма да може да се квалифицира като порнографски.

Основният състав на престъплението по чл. 159, ал. 1 НК е формулиран по технологично неутрален начин и обхваща създаването и разпространяването на порнографски материали по всякакъв начин. Изброяването на различните начини на разпространяване е примерно и разпоредбата ще се приложи по отношение на всяко друго деяние, което може да се квалифицира като разпространяване, т.е. като довеждане на съдържанието на съответните материали до знанието на трети лица. В приложното поле на разпоредбата попадат както разпространението на порнографски материали на хартиен носител (вестници, списания, плакати, календари и т.н.), така и на електронен носител (компакт дискове, видеокасети, DVD и т.н.) или по електронен път (електронна поща, мултимедийни съобщения през мобилни телефони и т.н.). Нито материалният носител, нито начинът на разпространяване на материалите имат значение за съставомерността на деянието. Предвиденото наказание е лишаване от свобода до една година и глоба от 1.000 до 3.000 лв.

Вторият основен състав включва деянията държане или набавяне за себе си или за другиго чрез компютърна система или по друг начин на порнографски материал, за създаването на който е използвано лице, ненавършило 18 години, или лице, което изглежда като такова (чл. 159, ал. 6 НК).[92] И този основен състав, въпреки изричното посочване на компютърната система като възможно средство на престъплението, обхваща всички

---

[90] По-подробно за основния състав по чл. 159, ал. 1 НК виж Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 120-123.

[91] В първоначалния текст на проекта на Закон за изменение и допълнение на НК, внесен през август 2006 г., към примерните хипотези на открито сексуално поведение бяха добавени и действия за възбуждане или удовлетворяване на полово желание. При обсъждането на проекта в парламента тази хипотеза отпадна от определението.

[92] Проектът на Закон за изменение и допълнение на НК, внесен през август 2006 г., предлагаше да се въведе легално определение и на понятието „материали с детска порнография" (порнографски материали, които изобразяват или описват открито сексуално поведение на малолетно или непълнолетно лице или на лице, което изглежда като такова). При обсъждането на проекта в парламента това предложение беше отхвърлено.

възможни деяния, които могат да се квалифицират като държане или набавяне.[93] Държането означава упражняване на фактическа власт върху съответния порнографски материал, докато набавянето означава придобиване на материала. За съставомерността на деянието е без значение дали деецът държи или набавя порнографския материал за себе си или за другиго. Деянието е съставомерно само когато за създаването на порнографския материал е използвано лице, ненавършило 18 години, или лице, което изглежда като такова. Меродавен е моментът на създаването на материала. Кога едно лице изглежда като непълнолетно (ненавършило 18 години) е фактически въпрос и ще се преценява от съда във всеки конкретен случай. Носителят, върху който са обективирани порнографските материали, е без значение за съставомерността на деянието. Изричното посочване на компютърната система като примерен носител е по-скоро стремеж да се подчертае обществената опасност на деянието, когато за извършването му е използвана такава система. Деянието ще е престъпление при държането или придобиването на посочените порнографски материали на какъвто и да е материален носител (хартиен носител, друг електронен носител различен от компютърната система и т.н.). Наказанието, предвидено за това престъпление, е лишаване от свобода до една година или глоба до 2.000 лв.

2.10.2. Квалифицирани състави

НК предвижда квалифицирани състави само по отношение на престъплението по чл. 159, ал. 1 НК. Квалифициращи обстоятелства са специфичният начин за извършване на престъплението (разпространяване чрез Интернет), предметът на престъплението (лице, ненавършило 16 години), средството на престъплението (порнографски материал, за чието създаване е използвано лице, ненавършило 18 години, или лице, което изглежда като такова) и други елементи от обективната страна (деяние, извършено по поръчение или в изпълнение на решение на организирана престъпна група).

Квалифицираният състав, който е най-тясно свързан с компютърните престъпления, е разпространяването на порнографски материали чрез Интернет (чл. 159, ал. 2 НК). Предвиденото по-тежко наказание за това престъпление е лишаване от свобода до две години и глоба от 1.000 до 3.000 лв. Разпоредбата беше въведена с измененията на НК от април 2007 г.

Начинът на разпространение на порнографските материали е определен с израза „чрез Интернет". В тази си част редакцията на разпоредбата не е прецизна и може да доведе до неоснователно разширяване на приложното поле на по-тежко наказуемия състав по отношение на деяния, чиято степен на обществена опасност не е толкова висока. Смисълът на текста е да санкционира тези деяния, които се изразяват в разпространяването на порнографски материали до неограничен кръг лица. Такова разпространяване е преди всичко публикуването на материалите в общодостъпна страница в Интернет. Сравнително висока степен на обществена опасност би имала и хипотезата, когато порнографските материали се съхраняват в компютърната система на дееца, но посредством т.нар. *peer-to-peer* технологии (които са базирани на Интернет), той предлага достъп до тях за неограничен кръг лица. Глобалната мрежа, обаче, позволява обмен на информация и между отделни лица, например чрез електронна поща, ICQ, Skype и др. базирани на Интернет средства за комуникация. Използването на тези средства за обмен на порнографски материали не разкрива по-висока степен на обществена опасност в сравнение с деянията по основния състав на чл. 159, ал. 1 НК и не обосновава налагането на по-тежко наказание. В този смисъл, разпоредбата на чл. 159, ал. 2 НК следва да бъде променена и изпълнителното деяние да бъде по-конкретно дефинирано.[94]

---

[93] По-подробно за определението на понятието „компютърна система" виж анализа на чл. 93, т. 21 НК (т. 2.2.2 по-горе).

[94] Проектът на Закон за изменение и допълнение на НК, внесен през август 2006 г., предлагаше различно решение. Той предвиждаше по-тежкото наказание да се прилага само за публично разпространяване чрез Интернет страница на произведения с порнографско съдържание. Тази редакция на текста беше по-удачна, тъй като по-ясно разграничаваше

От особено значение при това престъпление е субективната страна на деянието. Престъплението е умишлено, следователно деецът трябва да съзнава, че материалът е порнографски, и целенасочено да го разпространява. Това означава, че лицето знае или би трябвало да знае съдържанието на материала. Когато едно лице публикува порнографски материал на страница в Интернет, наказателна отговорност ще носи самото лице. Служителите на доставчика на Интернет услуги, които само осигуряват на лицето възможност да поддържа своя Интернет страница, нямат задължение да проверяват публикуваната информация и ще носят отговорност само ако са знаели за нейното съдържание, например ако са били уведомени за това съдържание, и не са предприели необходимите мерки за неговото премахване.

Съставът по чл. 159, ал. 3 НК е квалифициран с оглед на предмета на престъплението и обхваща хипотезите, когато порнографският материал се излага, представя, предлага, продава, дава под наем или по друг начин разпространява на лице, ненавършило 16 години. Предвиденото наказание е лишаване от свобода до три години и глоба до 5.000 лв. Съставът не разкрива специфични особености с оглед използването на компютри или други информационни технологии. Изпълнителните деяния са същите, както по основния състав по чл. 159, ал. 1 НК, и обхващат както разпространение на електронен носител или по електронен път, така и всяка друга форма на разпространение.

По чл. 159, ал. 4 НК квалифициращо обстоятелство е средството на престъплението (порнографски материал, за чието създаване е използвано лице, ненавършило 18 години, или лице, което изглежда като такова), а наказанието е лишаване от свобода до шест години и глоба до 8.000 лв. По чл. 159, ал. 5 НК деянието е по-тежко наказуемо, когато е извършено по поръчение или в изпълнение на решение на организирана престъпна група, като наказанието е лишаване от свобода от две до осем години и глоба до 10.000, а съдът може да постанови и конфискация на част или на цялото имущество на дееца. И двата квалифицирани състава не разкриват специфични особености, които да ги причислят към компютърните престъпления, освен че се прилагат и по отношение на случаите, когато порнографските материали са разпространени чрез Интернет.

2.10.3. Отнемане на предмета на престъплението в полза на държавата

Според чл. 159, ал. 7 НК предметът на престъплението се отнема в полза на държавата, а ако липсва или е отчужден, се присъжда неговата равностойност. Правилното определяне на предмета на престъплението е от особено значение за законосъобразното прилагане на разпоредбата. Предмет на престъплението е самият порнографски материал и само той подлежи на отнемане, съответно на възстановяване като парична равностойност. Материалният носител, на който той е възпроизведен, не подлежи на отнемане, ако самият порнографски материал може да бъде премахнат от него. В този случай отнемането трябва да се изразява в премахването на материала от носителя.

2.11. Компютърни престъпления срещу неприкосновеността на кореспонденцията

Чл. 171. (1) Който противозаконно:

1. отвори, подправи, скрие или унищожи чуждо писмо, телеграма, запечатани книжа, пакет или други подобни;

2. вземе чуждо, макар и отворено, писмо или телеграма с цел да узнае тяхното съдържание или пък със същата цел предаде другиму чуждо писмо или телеграма;

3. узнае неадресирано до него съобщение, изпратено по електронен път, или отклони от адресата му такова съобщение,

---

деянията с по-висока степен на обществена опасност, а именно – случаите, когато разпространяването е публично чрез Интернет страница. Парламентът обаче отхвърли това предложение и прие по-общата формулировка разпространяване чрез Интернет.

се наказва с лишаване от свобода до една година или с глоба от сто до триста лева.

(2) Ако деянието е извършено от длъжностно лице, което се е възползувало от служебното си положение, наказанието е лишаване от свобода до две години, като съдът може да постанови и лишаване от право по чл. 37, ал. 1, точка 6.

(3) Който чрез използуване на специални технически средства противозаконно узнае неадресирано до него съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство, се наказва с лишаване от свобода до две години.

(4) Когато деянието по ал. 3 е извършено с користна цел или са причинени значителни вреди, наказанието е лишаване от свобода до три години и глоба до пет хиляди лева.

С измененията на НК от 2002 г. беше допълнена правната уредба на престъпленията против неприкосновеността на кореспонденцията, което беше продиктувано от все по-широкото използване на новите технологии за обмен на информация. Непосредствен обект на тези престъпления са обществените отношения, които осигуряват неприкосновеността и тайната на кореспонденцията въобще и в частност на тази, която се предава по електронен път.[95]

2.11.1. Основни състави

Чл. 171, ал. 1, т. 3 НК инкриминира два основни състава, които се различават по изпълнителното деяние. В първия случай става въпрос за неправомерното узнаване на съдържанието на чуждо съобщение, изпратено по електронен път, а във втория – за отклоняване на такова съобщение от неговия адресат.

Непосредствен обект на престъплението са обществените отношения, гарантиращи тайната на кореспонденцията и сигурността на нейното предаване от изпращача на адресата.

От обективна страна предмет на престъплението е съобщение, изпратено по електронен път.[96] Съобщението представлява определена информация. За разлика от традиционните престъпления срещу неприкосновеността на кореспонденцията, които имат два предмета – от една страна самата информация, а от друга – носителят на тази информация (например писмо, телеграма и др.), при неправомерното узнаване на съобщение, изпратено по електронен път, е възможно деецът да узнае съдържанието на съобщението и без да е необходимо да има физически достъп до материалния носител на информацията. Такава ще бъде например хипотезата, когато едно лице проникне в електронната поща на друго лице през Интернет.

Изпълнителното деяние по първия основен състав е формулирано в закона като узнаване, т.е. достигане на съдържанието на съобщението до знанието на извършителя на деянието. Деецът може да узнае чуждото съобщение като осъществи достъп до компютърната система на изпращача или на получателя или до друга компютърна система, през която съобщението преминава или в която се съхранява. От обективна страна е необходимо съобщението да не е адресирано до дееца. При съобщение, изпратено по електронна поща, обаче, деянието ще се смята за адресирано до определено лице дори когато това лице е копирано (включително сляпо) от изпращача. Престъплението е резултатно – резултатът е новото познание у дееца за съдържанието на съобщението.[97]

По втория основен състав изпълнителното деяние се изразява в отклоняване на съобщението от неговия адресат. Отклоняването на съобщението означава възпрепятстване

---

[95] По-подробно относно престъпленията против неприкосновеността на кореспонденцията виж Стойнов, Ал. *Наказателно право. Особена част. Престъпления против правата на човека*. Изд. Сиела. София, 1997 г., стр. 205 и сл.

[96] По-подробно за определението на понятието „електронен път" виж анализа на чл. 319в, ал. 1 НК (т. 2.4.2.2 по-горе).

[97] За обратното становище виж Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 55. Според автора и по двата основни състава престъплението е формално.

на неговото получаване от адресата, за когото то е предназначено. Престъплението е резултатно, а резултатът се изразява в липсата на съобщението в съответното устройство за получаване на съобщения на адресата.

Субект на престъплението и по двата основни състава може да бъде всяко наказателно отговорно лице с изключение на титуляра, автора и адресата на съобщението, за които то не е чуждо. При отклоняването на съобщението от адресата, доколкото законът не квалифицира съобщението като „чуждо", теоретично е възможно субект на престъплението да бъде и титулярът или авторът на съобщението, когато той отклонява собственото си съобщение. Въпреки това, замисълът на законодателя едва ли е бил да санкционира точно тези хипотези, така че с оглед прецизирането на текста е препоръчително и по двата основни състава съобщението да бъде изрично определено като „чуждо".

От субективна страна е налице умисъл. Деецът съзнава, че съобщението е чуждо (че не е адресирано до него) и въпреки това узнава неговото съдържание или възпрепятства получаването му от адресата.

Предвиденото по чл. 171, ал. 1, т. 3 НК наказание е лишаване от свобода до една година или глоба от 100 до 300 лв.

2.11.2. Квалифицирани състави

НК предвижда четири квалифицирани състава на посегателствата срещу тайната на кореспонденцията, когато тя се осъществява по електронен път. Квалифициращи обстоятелства са субектът на престъплението (длъжностно лице), средството на престъплението (специални технически средства), престъпната цел (користна цел) и престъпния резултат (причиняване на значителни вреди).

2.11.2.1. Квалифицирани състави с оглед на субекта на престъплението

Деянието е квалифицирано с оглед на субекта на престъплението, когато е извършено от длъжностно лице, което се е възползувало от служебното си положение (чл. 171, ал. 2 НК). Предвиденото наказание е лишаване от свобода до две години, като съдът може да постанови и лишаване от право на заемане на определена държавна или обществена длъжност.

По смисъла на чл. 93, т. 1 НК длъжностно лице е това, на което е възложено да изпълнява със заплата или безплатно, временно или постоянно служба в държавно учреждение с изключение на извършващите дейност само на материално изпълнение или ръководна работа или работа, свързана с пазене или управление на чуждо имущество в държавно предприятие, кооперация, обществена организация, друго юридическо лице или при едноличен търговец, както и на частен нотариус и помощник-нотариус, частен съдебен изпълнител и помощник-частен съдебен изпълнител.

От обективна страна, за да е налице престъпление по квалифицирания състав на чл. 171, ал. 2 НК, е необходимо длъжностното лице да се е възползвало от служебното си положение, т.е. да е използвало служебните си функции за осъществяване на достъп до чуждото съобщение.[98]

2.11.2.2. Квалифицирани състави с оглед средството на престъплението

[98] По-подробно относно престъпленията, извършени от длъжностно лице, което се е възползвало от служебното си положение, виж Стойнов, Ал. *Наказателно право. Особена част. Престъпления против собствеността.* Изд. Сиела. София, 1997 г., стр. 36.

Престъплението е квалифицирано с оглед на използваното средство, когато е извършено чрез използване на специални технически средства (чл. 171, ал. 3 НК).[99] Предвиденото наказание е лишаване от свобода до две години. По-тежко наказуемият състав се прилага само по отношение на узнаването на чуждо съобщение, но не и по отношение на отклоняването на съобщение от неговия адресат.

От обективна страна е необходимо съобщението да е изпратено чрез компютърна мрежа или по друго далекосъобщително средство.[100] С оглед прецизиране на разпоредбата и уеднаквяване на терминологията с тази, използвана в основния състав, е препоръчително и в квалифицирания състав да бъде използван израза „съобщение, изпратено по електронен път".

От обективна страна престъплението трябва да е извършено чрез използване на специални технически средства.[101] Това са средства, които се използват за осъществяването на специфични технически дейности. За да бъде по-тежко наказуемо деянието, техническите средства трябва да са били използвани именно според специфичното си предназначение. Техническите средства са специални, когато за използването им се изискват специални познания. В хипотезата на съобщение, изпратено чрез компютърна мрежа, тези технически средства могат да бъдат специален хардуер или софтуер, позволяващ свързване към компютърна мрежа и осигуряващ достъп до информацията, обменяна по нея.

2.11.2.3. Квалифицирани състави с оглед престъпната цел и престъпния резултат

С измененията на НК от април 2007 г. бяха добавени още два квалифицирани състава на посегателствата срещу тайната на кореспонденцията. Квалифициращи обстоятелства са престъпната цел (користна цел) и престъпният резултат (причиняване на значителни вреди).[102] И двата състава са уредени в чл. 171, ал. 4 НК, като предвиденото наказание е лишаване от свобода до три години и глоба до 5.000 лв. Особеното на разпоредбата е, че се прилага само по отношение на чл. 171, ал. 3 НК, т.е. отнася се само за случаите на противозаконно узнаване чрез използване на специални технически средства на неадресирано до дееца съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство.[103]

2.12. Унищожаване и повреждане на чуждо имущество

Чл. 216. (1) Който унищожи или повреди противозаконно чужда движима или недвижима вещ, се наказва с лишаване от свобода до пет години.

(2) Който унищожи, разруши или повреди свое ипотекирано или заложено имущество, се наказва с лишаване от свобода до пет години и глоба до две хиляди лева.

(3) Който, като осъществи нерегламентиран достъп до компютър от значение за предприятие, учреждение, юридическо или физическо лице, и по този начин унищожи или

[99] Виж също Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 56-59. Според автора текстът на чл. 171, ал. 3 НК регламентира различен основен състав на престъпление срещу тайната на кореспонденцията.

[100] По-подробно за определението на понятието „компютърна мрежа" виж анализа на чл. 93, т. 25 НК (т. 2.2.5 по-горе).

[101] По-подробно относно използването на специални технически средства виж Стойнов, Ал. *Наказателно право. Особена част. Престъпления против собствеността*. Изд. Сиела. София, 1997 г., стр. 33.

[102] По-подробно относно причиняването на значителни вреди и користната цел виж анализа на чл. 319б, ал. 2 и 3 НК (т. 2.4.2.1 и т. 2.4.2.3 по-горе).

[103] Проектът на Закон за изменение и допълнение на НК, внесен през август 2006 г., предлагаше деянието неправомерно прихващане чрез технически средства на чуждо електронно съобщение или други неадресирани до дееца компютърни данни да бъде инкриминирано като отделно престъпление (наказуемо с лишаване от свобода до една година и глоба до 3.000 лв.), и квалифицираните състави при користна цел или причинени значителни вреди (наказуеми с лишаване от свобода до три години и глоба до 5.000 лв.) да се прилагат само по отношение на това престъпление. При обсъждането на проекта в парламента, обаче, въвеждането на нов основен състав не беше прието, а предлаганите квалифициран състави бяха добавени, но по отношение на вече съществуващия основен състав на противозаконното узнаване чрез използване на специални технически средства на неадресирано до дееца съобщение, предадено по телефон, телеграф, чрез компютърна мрежа или по друго далекосъобщително средство.

повреди чуждо имущество, се наказва с лишаване от свобода от една до шест години и глоба до десет хиляди лева.

(4) В маловажни случаи наказанието е лишаване от свобода до шест месеца или глоба от сто до триста лева.

(5) Ако са причинени значителни вреди или са настъпили други тежки последици или ако деянието е извършено от лице по чл. 142, ал. 2, точки 6 и 8, или ако деянието е свързано с унищожаване или повреждане на елементи от далекосъобщителната мрежа, наказанието е лишаване от свобода до десет години, като съдът може да постанови и лишаване от права по чл. 37, ал. 1, т. 6 и 7.

(6) Ако деянието по ал. 1, 2, 3 и 5 е извършено по непредпазливост, наказанието е лишаване от свобода до две години или глоба от сто до триста лева.

Унищожаването и повреждането на чуждо имущество посредством осъществяването на нерегламентиран достъп до компютър е уредено в чл. 216, ал. 3 НК.[104]

От обективна страна изпълнителното деяние на престъплението включва два елемента. Първият елемент е осъществяване на нерегламентиран достъп до компютър от значение за предприятие, учреждение, юридическо или физическо лице. Компютърът представлява компютърна система по смисъла на чл. 93, т. 21 НК.[105] Кога определен компютър е от значение за предприятие, учреждение, юридическо или физическо лице е фактически въпрос, който ще се преценява от съда във всеки конкретен случай. При тази преценка съдът следва да изхожда както от характеристиките на самия компютър, така и от информацията и данните, които се съхраняват в него. Нерегламентиран достъп ще бъде всеки достъп, за който няма правно основание (нормативен акт, разпоредба от вътрешни правила или процедури, частно-правна сделка и т.н.).

Вторият елемент на изпълнителното деяние е същият както по основния състав на унищожаването и повреждането по чл. 216, ал. 1 НК – унищожаване и повреждане на чуждо имущество.[106] Следва да се има предвид, че за да е налице престъпление по чл. 216, ал. 3 НК от обективна страна между двете деяния трябва да е налице функционална връзка – осъществяването на нерегламентирания достъп е начин, средство за унищожаването или повреждането на чуждото имущество.

Според чл. 216, ал. 5 НК деянието е по тежко наказуемо (лишаване от свобода до десет години, като съдът може да постанови и лишаване право да се заема определена държавна или обществена длъжност или да се упражнява определена професия или дейност), ако е налице специфичен престъпен резултат (причинени значителни вреди или настъпили други тежки последици), ако е извършено от особен субект (лице, което се занимава с охранителна дейност, служител в организация, която извършва охранителна или застрахователна дейност, лице, което действа по поръчка на такава организация или се представя, че действа по такава поръчка, лице от състава на Министерството на вътрешните работи или лице, което се представя за такова, лице, което действа по поръчение или в изпълнение на решение на организирана престъпна група или организация или група, която чрез използване сила или внушаване на страх сключва сделки или извлича облаги) или ако е със специфичен предмет (свързано с унищожаване или повреждане на елементи от далекосъобщителната мрежа).

Предвидени са и два привилегировани състава – когато деянието е маловажен случай наказанието е лишаване от свобода до шест месеца или глоба от 100 до 300 лв. (чл. 216, ал. 4

[104] Законопроектът за изменение и допълнение на НК, внесен през март 2006 г., предлагаше чл. 216, ал. 3 НК да бъде отменен, но поради оттеглянето на проекта разпоредбата беше запазена.

[105] При измененията на НК от април 2007 г. законодателят пропусна да коригира терминологията в текста на чл. 216, ал. 3 НК. Навсякъде другаде понятието „компютър" беше заменено с „компютърна система".

[106] По-подробно относно престъпленията против неприкосновеността на кореспонденцията виж Стойнов, Ал. *Наказателно право. Особена част. Престъпления против собствеността.* Изд. Сиела. София, 1997 г., стр. 115 и сл.

НК), а когато е извършено по непредпазливост, наказанието е лишаване от свобода до две години или глоба от 100 до 300 лв. (чл. 216, ал. 6 НК).

2.13. Лъжливо документиране

Чл. 313. (1) Който потвърди неистина или затаи истина в писмена декларация или съобщение, изпратено по електронен път, които по силата на закон, указ или постановление на Министерския съвет се дават пред орган на властта за удостоверяване истинността на някои обстоятелства, се наказва с лишаване от свобода до три години или с глоба от сто до триста лева.

(2) Когато деянието по ал. 1 е извършено с цел да се избегне заплащане на дължими данъци, наказанието е лишаване от свобода от една до шест години или глоба от сто до двеста и петдесет лева.

(3) Наказанието по ал. 1 се налага и на онзи, който потвърди неистина или затаи истина в частен документ или съобщение, изпратено по електронен път, в които по изрична разпоредба на закон, указ или постановление на Министерския съвет е специално задължен да удостовери истината, и употреби този документ като доказателство за невярно удостоверените обстоятелства или изявления.

(4) Който във връзка с публично предлагане на ценни книги в проспект или обзор за икономическо състояние използва неистински благоприятстващи данни или премълчава неблагоприятни такива, които са от съществено значение при вземане на решение за придобиване на ценни книги, се наказва с лишаване от свобода до три години и глоба до петстотин лева.

С измененията на НК от 2002 г. в съставите на лъжливото документиране по чл. 313, ал. 1 и 3 НК като предмет на престъплението беше добавено съобщението, изпратено по електронен път.[107] Самите състави инкриминират потвърждаването на неистина или затаяването на истина в различни видове документи и единствената връзка с компютърните престъпления е възможността тези документи да бъдат съобщения, изпратени по електронен път.[108]

Промените в съставите на лъжливото документиране са практически ненужни. Съобщението, изпратено по електронен път, ще бъде документ по смисъла на НК, единствено ако отговаря на изискванията за електронен документ по ЗЕДЕП. В този случай, обаче, по силата на чл. 3, ал. 2 ЗЕДЕП това съобщение ще бъде приравнено на писмен документ, с което попада в приложното поле на чл. 313 НК и преди промяната. От друга страна, ако съобщението, изпратено по електронен път, не отговаря на изискванията за електронен документ, то няма правно значение, защото не автентифицира изявлението.

[107] По-подробно за определението на понятието „електронен път" виж анализа на разпоредбата на чл. 319в, ал. 1 НК (т. 2.4.2.2 по-горе).

[108] По-подробно за лъжливото документиране виж Копчева, М., *Компютърни престъпления*. Изд. Сиби. София, 2006 г., стр. 125-127.

3. Правна уредба на компютърните престъпления в Румъния

3.1. Въведение

Според публикуваните данни на Националната агенция за регулиране на комуникациите и информационните технологии (ANRCTI) през последните години в Румъния достъпът до Интернет сред населението се е увеличил с 27%, като 10% от потребителите имат достъп до широколентови технологии.

Логично е това нарастване на достъпа до Интернет да се съпровожда от развитие на цяла национална индустрия, свързана с новата среда на комуникация, така че електронната търговия и рекламата в Интернет вече не представляват нещо необичайно. Местният пазар на електронната търговия се оценява на 120 милиона евро, макар че според статистиките EuroStat едва 3% от населението на Румъния пазарува в Интернет.

Системите за електронни разплащания навлязоха в ежедневна употреба, като вече са издадени над 10 милиона карти, а 29 банки разработват системи за онлайн банкиране. Въпреки това, голяма част от икономиката се базира на ликвидни средства, ако вземем предвид факта, че 78% от населението ползва картите само за теглене от банкомат (ATM).

За съжаление, се появиха и лица, които се опитват да се възползват от някои пропуски в сигурността на компютърните приложения или от новите методи за комуникация за извършване на традиционни престъпления. Нужно е да се подчертае, че заедно с наистина забележителното развитие на Интернет и приложенията му в последните 10 години се развиха и усъвършенстваха и закононарушенията, осъществявани посредством тях и особено компютърните измамите, както от гледна точка на извършители, така и с оглед на използваните технологии.

В този контекст, целта на този раздел е да разгледа накратко основните правни понятия, свързани с компютърните престъпления и начина им на уреждане в румънското законодателство. Тъй като става дума за непрекъснато променяща се среда, считаме че правната уредба трябва да бъде актуализирана периодично и точно заради това бе включен Раздел 4.

3.2. Правна уредба на новите технологии в Румъния

Трябва да признаем факта, че голяма част от румънското законодателство относно информационните технологии представлява прилагане на правото на Общността, а на практика – в по-голямата част от случаите, е превод на директивите. Положителната страна на този процес е сходството с европейските директиви и в последствие улеснение в тълкуването или сравняването им с нормативните актове в други държави. Отрицателният аспект на този процес, обаче, е липсата на съответствие между създадения нормативен акт и останалото румънско законодателство, което понякога поражда противоречия и неясноти между различните актове. Освен това, буквалният превод понякога затруднява практическото прилагане на разпоредбите, тъй като е трудно за един неспециалист да отнесе конкретен казус към определен законов член. Именно заради една от поставените цели да идентифицираме конкретни казуси, за които могат да се приложат определени разпоредби.

С оглед на по-голямата яснота на това изследване предлагаме разделяне на румънското законодателство на 3 категории:

А. Закони за прилагане на правото на Общността:

- Закон за електронната търговия – в сила (Закон 365/2002 и с внесените изменения от Закон 121/2006)

- Наредба за защита на потребителя при сключване и изпълнение на договори, сключени от разстояние – в сила (OG 130/2000 с внесените изменения от Закон 51/2003 и Закон 373/2007)

- Закон за електронния подпис - 455 / 2001

- Технически и методологически инструкции от 13 декември 2001 за прилагане на Закон 455/2001 за електронния подпис.

- Закон за защита на гражданите по отношение на обработването и свободния обмен на личните им данни - 677 / 2001

- Закон за защита на личните данни и на личния живот на гражданите в сектора на електронните съобщения - 506/2004

- *Нормативни актове за регламентиране на комуникациите*

  - Правителствена наредба 34/2002 за достъпа до обществените мрежи за електронни съобщения и прилежащата инфраструктура и връзката помежду им, обнародвана с допълнения и изменения от Закон 527/2002.

  - Извънредна правителствена наредба 79/2002 относно общата рамка за контрол на съобщенията, обнародвана от Закон 591/2002 за изменение и допълнение

  - Разпоредба на правителството 31/2002 относно пощенските услуги, обнародвана с изменения и допълнения чрез Закон 642/2002, с последвалите изменения

  - Закон 304/2003 за универсалните услуги и правата на потребителите по отношение на мрежите и услугите на електронните съобщения.

  - Закон 239/2005 за изменение и допълнение на някои нормативни актове в областта на съобщенията

- *Нормативни актове за внасяне на изменения в законовата рамка за авторското право*

  - Извънредна наредба 123 от 1 септември 2005 г. за изменение и допълнение на Закон 8/1996 за авторското право и сродните му права

  - Закон 285 от 23 юни 2004 г. за изменение и допълнение на Закон 8/1996 за авторското право и сродните му права

Б. Румънски закони, приети вследствие на присъединяване към Международната конвенция

В тази категория на първо място влизат:

- Разпоредби за предотвратяване и борба с компютърните престъпления (Глава III от Закон 161 от 19/04/2003 относно мерките за осигуряване на прозрачност при изпълнение на обществените функции и задължения в сферата на бизнеса, предотвратяване и борба с корупцията – Обнародван в Държавен вестник, Раздел I на бр. 279 от 21.04.2003 г).

- Закон 64 от 24.03.2004 г. за ратифициране на Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, приета в Будапеща на 23 ноември 2001 г.

В. Румънски закони, приети вследствие на национални инициативи

Тези нормативни актове имат по-слабо влияние от гледна точка на настоящото изследване:

- Закон за временната марка 451/2004. Обнародван е в Държавен вестник, Раздел I на бр. 1021 от 05/11/2004 г.

- Закон за правния режим на нотариалната дейност по електронен път - 589/2004, обнародван в Държавен вестник, брой 1227/20 декември 2004 г.

- Наредба на Министерство на съобщенията и информационните технологии номер 221/ 16 юни 2005 г. за одобряване на техническите и методологически норми за прилагане на Закон 589/2004 относно правния режим на нотариалната дейност по електронен път

- Закон за архивиране на електронните документи 135/2007 – обнародван в Държавен вестник, бр. 345 от 22.05.2007 г.

- Закон за регистриране на търговските операции чрез електронни средства 260/2007 - обнародван в Държавен вестник, Раздел I на бр. 506 от 27.07.2007 г.

- Закон за създаване, управление и функциониране на Националната агенция за контрол на работата с личните данни -102/2005 г.

- Закон за предотвратяване и борба с порнографията - 196/2003, обнародван в Държавен вестник, брой 342 / 20 май 2003 г.

3.3. Компютърни престъпления

В Раздел III на Закон 161/2003 са включени следните три категории престъпления, свързани с компютърните нарушения:

а) Престъпления срещу неприкосновеността на поверителния характер и целостта на компютърните системи

- Престъпления за незаконен достъп до информационна система;

- Престъпления за нелегално прихващане при предаване на компютърни данни;

- Престъпления за промяна на целостта на компютърните данни;

- Престъпления за смущаване на дейността на компютърните системи;

- Престъпления за извършване на нелегални операции чрез компютърни устройства и програми.

б) Компютърни престъпления

- Компютърно фалшифициране;

- Компютърна измама.

в) Детска порнография, осъществявана с помощта на компютърните системи

В настоящото изследване ще разгледаме подробно и престъпленията описани в Закон 365/2002, който се прилага често и в областта на компютърните престъпления:

- Фалшифициране на електронни платежни инструменти

- Чл. 25: Притежание на оборудване за фалшифициране на електронни платежни инструменти

- Чл. 26: Фалшифициране на данни при издаване или ползване на електронни платежни инструментите

- Чл. 27: Извършване на финансови операции чрез измама

- Чл. 28: Приемане на извършени чрез измама финансови операции

С оглед на по-ясното тълкуване и разбиране на тези разпоредби в следващата част на изследването ще преминем към подробен правен анализ на гореизброените престъпления.

3.3.1. Термини и дефиниции

В началото е необходимо да дефинираме инструментите и способите, които законодателят е избрал да ползва в тази сфера. Тези дефиниции са формулирани от самия законодател в чл. 35 на Закон 161/2003 по следния начин:

а) **компютърна система** *е всяко отделно устройство или съвкупност от взаимосвързани или сходни устройства, което осигурява или един от елементите на което осигуряват автоматично обработване на данните с помощта на компютърна програма.*

Пример: персонален компютър (PC), два или повече свързани с кабел или безжично (wireless) компютри, мрежа от компютри, съчетание от компютърен тип – периферни устройства (принтер, външно запаметяващо устройство, скенер, др.), банкомати и др.

б) под **автоматично обработване на данните** *се разбира процесът, чрез който данните от една компютърна система се обработват с помощта на компютърна система.*

Пример: следвайки логически алгоритъм, инструкциите за компютър са написани на някакъв език на програмиране на високо ниво (Pascal, C++, Visual Basic, Java и др.), набират се от клавиатурата и се интерпретират от централна обработваща единица, а по-късно се транслират на език код-машина и се предават за изпълнение на изпълняваща единица, като всеки компонент от компютърната система изпълнява определена операция.

в) под **компютърна програма** *се разбира набор от инструкции, които могат да бъдат изпълнени от една компютърна система с цел получаване на определен резултат.*

Пример за програми: операционни системи (MS-DOS, MS Windows, UNIX, Ubuntu, др.), пакети от стандартни приложения (напр. Microsoft Office , Open Office, Star Office – които по принцип съдържат текстови редактор, софтуер за управление на база данни, програма за изчисляване в таблица, програма за презентация и др.), пакети от специализирани приложения (ERP – Enterprise Resource Planning – за планиране на финансови, логистични резултати, както и резултатите постигнати от персонала в рамките на едно предприятие или институция, CRM – Customer Relationship Management – инструмент за управление на сделки и организиране на връзките с клиенти и др.), антивирусни програми (BitDefender, Norton System Works, др.), програми за ползване на Интернет (браузъри – Internet Explorer, Mozilla Firefox, Netscape и др., електронна поща – Outlook, Webmail, Eudora и др.), различни приложения с определена цел (вируси, троянски коне, логични бомби, следене на различни протоколи, шпионски софтуер и др.) и много други;

г) под **компютърни данни** *се разбира всяко представяне на факт, информация или понятие във форма, която може да бъде обработена чрез компютърна програма. В тази категория се включва и всяка компютърна програма, която може да определи реализирането на една функция от определена компютърна система.*

На ниво ползване данните са представени под буквено-цифрова форма - цифри, букви, специални символи, така както се изписват на екрана, а на нивото на компютърната система те са представени под форма на подредени редове от по 8, 16, 32, 64 или 128 бита (елементи „0” и „1”, които на нивото на електронните елементи на изчислителната система представляват еквиваленти с контролирани вариации на захранващото напрежение).

На практика, всички данни, които се намират в една компютърна система могат да съставляват компютърни данни. Например: текстови файлове, таблици, снимки, музика или видео материал в цифров формат.

д) под **доставчик на услуги** *се разбира следното:*

1. всяко физическо или юридическо лице, което предлага на потребителите възможност за комуникация чрез компютърни системи;

2. всяко физическо или юридическо лице, което обработва или съхранява компютърни данни за лицата, дефинирани в точка 1 и за потребителите на предлаганите от тях услуги.

Отбелязваме факта, че румънският законодател не е ограничил категорията на доставчици на услуги само до доставчици на Интернет услуги, тъй като дефиницията е достатъчно широка, за да включи, например, един доставчик на безплатен Интернет, едно Интернет кафе, собственика на заведение, което предлага достъп до Интернет чрез WiFi (радио вълни), доставчик на хостинг услуги, доставчик на услуги за електронно архивиране на документи и др.

е) под **данни за международен трафик** *се разбира всякакъв вид компютърни данни, отнасящи се до комуникация, реализирана чрез компютърна система и нейните производни продукти, които са част от мрежата на комуникация и показват произхода, посоката, пътя, часа, датата, големината, обема и продължителността на комуникацията, както и типа на ползваната услуга за комуникация.*

Например – съхраняваните данни от един сървър за достъп до FTP (log FTP)

Mon Feb 14 15:20:47 2000 1 mail2.iserv.net 1904 /usr/local/www/htdocs/iserv/slice b _ i r kevin ftp 0 * c

Mon Feb 14 15:23:47 2000 1 web2.iserv.net 985 /usr/local/www/htdocs/iserv/web-slice b _ i r kevin ftp 0 * c

ж) под **данни за потребителите** *се разбира всеки тип информация, с която може да се идентифицира един потребител, в това число начина на комуникация и използваната услуга, пощенски адрес, географски адрес, телефонен номер и други номера за достъп, начин на плащане на съответната услуга, както и всички други данни, посредством които може да се идентифицира потребителя.*

Отбелязваме подобния характер на дефиницията – с тази на личните данни съгласно Закон 677/2001, чл. 3а).

з) под **лични данни** *се разбира всеки тип информация, отнасяща се до идентифицирано физическо лице или такова, което може да бъде идентифицирано; лице, което може да бъде идентифицирано пряко или непряко по специфичен начин чрез съотнасяне към идентификационен номер или към един или повече специални фактори, касаещи процеса на физическа, физиологична, психическа, икономическа, културна и социална идентификация.*

Една от важните данни за потребителите, която има особено значение в процеса на компютърното разследване е IP адреса. Той представлява номер от 32 цифри, по принцип е създаден в десетичен формат с точки. Напр. 154.162.1.28 идентифицира (за ползване на Интернет протокол и на излъчваните или приеманите IP пакети) мрежовия интерфейс на един компютър. Този адрес, обаче, може да бъде разпределен статично или динамично от страна на Интернет доставчика и затова не е лесно да се установи връзка с едно физическо лице.

и) под **мерки за сигурност** *се разбира използването на процедури, устройства или специализирани компютърни програми, с помощта на които се ограничава или забранява достъпа до определена компютърна система на някои категории потребители.*

Пример: система за достъп (LOGIN), базирана на парола и потребителско име, инфраструктура на криптиране на комуникацията, инфраструктура с обществен ключ (PKI), приложения за електронен подпис, оборудване за достъп чрез смарт карти, четец за разпознаване на текст или на ириси.

к) под **порнографски материали с малолетни** *се разбира всеки материал, който представя малолетно лице с открито сексуално поведение или пълнолетно лице, което преторено се представя като малолетно с изявено сексуално поведение, или изображения, които макар и да представят реално съществуващо лице, по убедителен начин симулират и го представят като малолетно лице с открито сексуално поведение.*

За по-подробна интерпретация на тази дефиниция в сравнение с други законодателства препоръчваме да се запознаете с няколко цитирани в библиографията статии.

л) Също така, по смисъла на съществуващия закон, **действа без право** *лице, което се намира в следните ситуации:*

а) не е оторизирано, въз основа на закона или на някакъв договор;

б) надхвърля границите на оторизация;

в) няма разрешение от страна на компетентните физически или юридически лица, според закона, да предостави, да ползва, да управлява или контролира компютърна система, или да провежда научно изследване, да извършва всякаква друга операция в една определена компютърна система.

Пример: Не бихме могли да се озовем в ситуация на престъпление за незаконен достъп, ако самият достъп е оторизиран от легитимния потребител на съответната компютърна система (от собственика или законния титуляр). Още повече, че достъпът до една компютърна система, която е обща собственост на двама съпрузи, от страна на единия от тях не може да бъде считан за незаконен, в случай че тази система е ползвана и от двамата съпрузи (независимо от отпуснатия период на тази дейност), а съхраняваните компютърни данни не са персонализирани или определени като такива чрез криптиране или защитени срещу отваряне/надписване/промяна/забрана на достъпа и др.

Също така, не можем да считаме за престъпление нарушенията, извършвани с една компютърна система, която позволява свободен и безплатен обществен достъп.

Към обичайните, специализирани дефиниции относно компютърните престъпления трябва да добавим и предвидените в Закон 365/2002 за електронната търговия, Глава I, Основни положения, чл. 1, за да може да се представи целият спектър от специфични термини.

Услуга на информационното общество – *всяка услуга, която се извършва с помощта на електронни средства и има следните характеристики:*

- *Извършва се заради общо благо, доставено на предлагащия по нормален начин към получателя;*
- *Не е нужно оферираща та страна и получателя да са представени по едно и също време на едно и също място;*
- *Извършва се посредством изпращане на информация при индивидуална заявка от страна на получателя.*

Тази дефиниция породи дискусии в практиката. Ние сме на мнение, че тълкуването на дефиницията трябва да бъде съгласувано с мнението на законодателя. В конкретния случай Закон 365/2002 имплементира европейската директива за електронна търговия, поради което считаме за важно да се вземе предвид обяснението на точка (18) на Директива 2000/31/ЕО с оглед на включеното в услугите на информационното общество:

Услугите на информационното общество обхващат голяма гама от икономически дейности, развивани по електронен път. Тези дейности се заключават изключително в продажба на продукти по електронен път. Дейности като доставката на продуктите

като такива или доставката на неелектронни услуги не са включени. Услугите на информационното общество не се ограничават само до услуги, вследствие на които се сключват договори по електронен път, а и доколкото те представляват някаква икономическа дейност, се разпростират и до услуги, които не се заплащат от потребителите, както са услугите за доставяне на информация по електронен път или търговски съобщения, или тези които доставят инструменти за търсене, достъп и възстановяване на данни. Услугите на информационното общество предполагат също така и услуги, които са свързани с предаване на информация в комуникационна мрежа, предоставяне на достъп до такава мрежа и с хостинг на доставените информации от потребител на услугата. Телевизионните услуги по смисъла на Директива CEE/89/552 и услугите по радио разпръскване не са услуги на информационното общество, тъй като не са доставяни по индивидуална заявка. От друга страна, услугите, които не са предавани от точка по точка, както например видео по поискване или доставка на търговски съобщения по електронна поща, представляват услуги на информационното общество. Използването на електронната поща или на други индивидуални средства за комуникация, от физически лица, които не действат със служебни и търговски цели, включително ползването на други средства за сключване на договори между такива лица, не представлява услуга на информационното общество. Договорните отношения между служител и работодател също не представляват услуга на информационното общество. Дейностите, които заради естеството им не могат да бъдат осъществявани от разстояние чрез електронни средства, каквито са например оторизираният одит на счетоводството на едно дружество или медицинската консултация, която налага физически преглед на пациента, не представляват услуга на информационното общество.

Електронни средства – *електронно оборудване и мрежи от кабели, оптичен кабел, радио, сателит и други подобни, които се използват за обработване, съхраняване или предаване на информация.*

Домейн – *зона в компютърната система, притежавана като такава от физическо или юридическо лице, или от група физически/юридически лица с цел преработка, съхраняване или предаване на данни.*

Например: в случая на уеб страницата, хоствана на адрес http://www.legi-internet.ro, домейнът е “legi-internet.ro”.

Търговско съобщение – *всяко съобщение с предназначение да предлага, директно или косвено, продуктите, услугите, имиджа, името или наименованието, формата или емблемата на един търговец или член на определена професионална сфера; Сами по себе си следните не са търговски съобщения: съобщения, позволяващи прекия достъп до дейността на едно физическо/юридическо лице, и по-специално на името на домейна или електронен адрес; съобщенията, свързани с продуктите, услугите, имиджа или марките на едно физическо или юридическо лице, извършвани от трета независима от съответното лице страна, особено когато са реализирани безплатно.*

Инструмент за електронно разплащане – *инструмент, които позволява на титуляра да извършва следните операции:*

- *Трансфер на парични средства, различни от наредените и извършени от финансовите институции;*

- *Теглене на пари в брой, както и захранване и изпразване на определен инструмент с електронна валута.*

Титуляр – *лице, което е притежател на инструмент за електронно разплащане въз основа на договор, сключен с издаваща институция в предвидените от закона условия.*

Идентификационни данни – *всяка информация, която може да позволи или спомогне извършването на различните видове операции, споменати в т. 10, както и един идентификационен код, име и наименование, адрес по местожителство или адрес на фирмено седалище, телефонен или факс номер, електронен адрес, регистрационен номер*

или други подобни средства за идентификация, данъчен номер, единен граждански номер и др.

Нужно е да отбележим, че понастоящем наказателното право в Румъния се намира в период на преход. Подготвя се широкообхватна наказателна реформа, която предполага промени в структурата на Наказателния кодекс на Румъния. По отношение на компютърните престъпления, в Наказателния кодекс е възможно да бъде въведен самостоятелен раздел, Раздел X, наречен "Нарушения спрямо компютърните данни и системи", в който да бъдат изменени и допълнени престъпленията от Закон 161/2003.

3.3.2 Незаконен достъп до компютърна система

Чл. 42 на Закон 161/2003

(1) Достъпът, без право на такъв, до една компютърна система представлява престъпление и се наказва със затвор от 3 месеца до 3 години или с глоба.

(2) Деянието по алинея (1), извършено с цел получаване на компютърни данни се наказва със затвор от 6 месеца до 5 години.

(3) Ако предвиденото в алинея (1) или (2) деяние е извършено чрез нарушаване на мерките за сигурност, наказанието със затвор е в рамките от 3 до 12 години.

Защитен правен интерес

Представлява стойността на една *компютърна система* за една фирма и отношенията между фирмите, които се пораждат във връзка с ползването на автоматичните системи за обработване на данни. В същото време, стойността се измерва и в ненарушимостта на "компютърното пространство". Други изследователи говорят дори за съхраняване на "компютърния дом". Разбира се, в термина "компютърно пространство" влизат и компютърните данни, така както ще бъдат дефинирани по-късно.

Защитеният правен интерес е този на собственика, на титуляра или на законния потребител на компютърната система, но и на собственика, на титуляра или на законния потребител на компютърните данни, съхранени или активни в съответната компютърна система.

Тук е редно да спомена и факта, че компютърните престъпления са престъпления, които по отношение на законовото предвиждане за вина, се характеризира с това, че засягат най-малко 2 страни/единици (понякога и повече), заради което можем да твърдим, че имат две (понякога и повече) юридически обекта, като единият от тях е главен, а другият – второстепенен (или прилежащ).

Участници в престъплението

Активен извършител

Може да бъде всяко наказателно-отговорно лице, като за него не се предвиждат специални способности в законовите текстове.

Юридическата практика е показала, че в повечето случаи тези лица имат познания в областта на компютърните технологии. Голям процент от тях са експерти в изчислителните системи и компютърните мрежи, като са запознати и с 'разбиване' на мерките за сигурност на компютрите или на компютърните мрежи.

Криминологичните изследвания са показали, че най-напреднали са "вътрешните врагове", т. е. както лицата, които нямат познания или способности да работят с изчислителна техника и по този начин са заплаха за компютърните системи, така и членовете на организации и институции (служители, наемен персонал, сътрудници и др.), които притежавайки компютърни познания, поради определени причини избират да отговорят по неподходящ начин на дадени решения на мениджмънта, като насочват вниманието си към компютърните системи или ги използват по време на извършване на някои незаконни действия.

Участието е възможно под всички форми: съучастие, помагачество или укривателство.

Пострадал

Това е физическо или юридическо лице, което е собственик или притежава право над компютърната система, до която има незаконен достъп или такъв до съответните компютърни данни. Може да има и колективен пасивен извършител, съставен от група физически или юридически лица, тогава когато достъпът до компютърната система се генерира по незаконен и автоматичен начин в други подобни системи, взаимно свързани с първата.

Съществува и вторичен пасивен извършител, в случая когато компютърните данни за незаконен достъп се отнасят до физическо или юридическо лице, различно от собственика или притежателя на право над съответната компютърна система. Например, извършителят нелегално осъществява достъп до система за компютърна отчетност на лицето и присвоява личните данни, принадлежащи на определен индивид (очевидно с цел след това те да бъдат използвани).

Обективен елемент

Компютърните престъпления се осъществяват по правило чрез достъп без право на такъв до определена компютърна система (работна станция, сървър или компютърна система).

Достъпът съгласно легалната му дефиниция означава влизане в цялата или част от компютърната система. Начинът на комуникация – от разстояние, включително и чрез сателит или без, или директно, не е от значение.

В най-опростената форма **достъпът без право до една компютърна система** изисква взаимодействие на *извършителя със съответната изчислителна техника,* посредством оборудването или различните компоненти на тази система (източник на захранване, бутони за стартиране, клавиатура, мишка, джойстик).

Съществува незаконен достъп в опростена форма и в случая, когато чрез манипулиране на собствените периферни устройства лицето открива и използва външен път за достъп в друга изчислителна система. Това е типичният случай на влизане в чужда работна станция в LAN, MAN, WAN и т.н.

За да си осигури достъп, извършителят опитва цяла гама от технически способи, като например атака *чрез парола, атака със свободен достъп, атака за използване на технологичните пропуски, атака за експлоатиране на разделените библиотеки, IP атака* или *атака с увреждане на TCP сесията и др.*

Интересен тип незаконен достъп, който бива все по-често използван в днешно време и в Румъния, са **атаките чрез обществено инженерство.** Тези случай значително зачестяват, като стават все по-опасни, тъй като повече потребители се включват в Интернет и във вътрешни мрежи. Разпространен пример за обществено инженерство е, когато един хакер изпраща електронни съобщения до потребителите (или просто използва телефон) и ги информира, че той е администраторът на системата. Много често в тези съобщения се изисква потребителите да изпратят паролата си на администратора по имейл, тъй като се системата е повредена или че ще бъде временно деактивирана. Атаките от типа обществено инженерство се основават най-вече върху незнанието на потребителите в областта на компютрите и мрежите. Затова, най-добрата рецепта срещу този род атаки е образоване на потребителите.

Достъп до електронната поща на друго лице

3.3.2.1 По отношение на достъпа до електронната поща, съществуват повече варианти (ситуации) за извършване на престъпления, за които считаме за правилни същите варианти на действия, а именно:

- достъпът до електронната поща може да бъде осъществен през изчислителната система, която потърпевшата страна притежава, независимо от името или просто ползва законосъобразно въз основа на договор, според характеристиките на услугата или основавайки се на законова предпоставка. При тези условия, всеки достъп до системата от страна на друго лице, което не притежава същите права се счита за незаконен и може да бъде подведено под законовите мерки на чл. 42, алинея 1.

- обикновено, достъпът до електронната поща се осъществява чрез специален интерфейс, наречен **имейл клиент.** Тази програма обслужва собственика на имейл акаунт във връзка с изпращане, получаване и/или съхраняване на съобщения (под формата на компютърни данни). По принцип, след обмена на данни между имейл сървърите, както получените, така и изпратените съобщения, чрез тази програма биват съхранявани на хард диска на компютъра (в зоната на памет на приложението на електронната поща).

  3.3.2.1.1 Приложението на електронната поща (имейл клиент) не е защитено(а) срещу неоторизиран достъп чрез мерки за сигурност. При влизане на лице в това приложение не можем повече да бъдем в условията на незаконен достъп до една компютърна система, тъй като според дефинициите в чл. 35 компютърната система представлява устройство или комбинация от устройства, а не компютърна система или приложение. Просто достъпът до програмата на електронната поща не може да бъде обхванат от действащите законови разпоредби.

Ако извършителят влезе в приложението на електронната поща с цел получаване на вече получени, изпратени или съхранени съобщения от засегнатата страна, тогава правилното определение е - **незаконен достъп до компютърна система, с цел получаване на компютърна информация (чл. 42, ал. 2)** (като това се отнася само до достъпа без право в предвидената в т. 1 система) и **нарушаване на тайната на кореспонденцията (чл. 195, ал. 1 от Наказателния кодекс).**
Мнението, според което след като се използва имейл клиент е налице незаконен достъп до сървъра с електронните съобщения не е вярно, защото при отваряне на приложението, то съобщава автоматично и независимо от потребителя на сървъра за съобщенията и съхранява на съответното място (за прочит) новите съобщения. С други думи, липсва форма на вина, която е абсолютно необходима за наличие на престъпление.

3.3.2.1.2 Приложението за електронна поща е защитено от различни мерки за сигурност, а извършителят действа за тяхното отстраняване. В тази ситуация се запаметява само **нелегалният достъп до компютърната система, евентуално и целта на получаване на компютърните данни (чл. 42, ал. 2), както и нарушаването на тайната на кореспонденцията (чл. 195, ал. 1. от НК), като всеки друг извод за наличие на връзка с чл. 42, алинея 3 от Закон 161/2003 (незаконен достъп до компютърна система чрез нарушаване на мерките за сигурност) е погрешен.**

3.3.2.2 В електронната поща се влиза директно от сървъра на имейл доставчика на компютърни услуги (provider, ISP), посредством обслужване от WEBMAIL (достъп до имейл акаунта от разстояние), което е възможно чрез помощното средство на оперативната система на компютъра, наречено браузър.

Когато става дума за външен ресурс и като се има предвид фактът, че сървърът представлява електронно устройство (взаимно свързан с други такива), е ясно, че се намираме в условия за **достъп/влизане в компютърна система.**

Задължително е влизането на потребителя в системата чрез потребителско име (идентификатор) и асоциирана с него парола.

3.3.2.2.1 Влизане в акаунта на електронната поща чрез Webmail става от страна на потребителя след правилно регистриране в системата чрез използване на потребителското име (идентификатор) и вярна парола.

В този момент, правилното тълкуване на този акт е: **престъпление на незаконен достъп до компютърна система в прост вариант (чл. 42, ал. 1)** – във връзка с проникването без право в информационната система, която е собственост или е ползвана от засегнатата страна, **престъпление за незаконен достъп до компютърна система с цел получаване на компютърни данни (чл. 42, ал. 1)** – във връзка с проникването в сървъра на имейла от разстояние, **и нарушаване тайната на кореспонденцията (чл. 195, ал. 1 от НК), като последните са в идеална съвкупност,** тъй като извършителят не е бил в качеството на собственик или не е имал право на достъп до съответния имейл акаунт, създаден и ползван от засегнатата страна.

Прилагането на нормата на чл. 42, ал. 3 (незаконен достъп до компютърна система чрез нарушаване на мерките за сигурност) би било погрешно, защото от техническа гледна точка (на компютърната система) влизането в акаунта (дори и с цел измама) е извършено правилно, след правилно въвеждане на данните за идентификация, които са били разпознати. Приемайки само тези два елемента за сигурност (потребителско име и парола), няма да се разполага с други възможности за проверка самоличността на потребителя по право и не може да се прецени, че всъщност са били нарушени мерките за сигурност.

Влизането в акаунта на електронната поща чрез Webmail става от страна на извършителя с нарушаване на мерките за сигурност. За получаване на достъп, той опитва различни технически методи, като например: атака с парола, атака за свободен достъп, атака, ползваща слабите технологични места, атака чрез използване на разделените библиотеки, IP атака или атакуване чрез изкривяване на TCP системата и др.

В този случай, правилната квалификация би била **незаконен достъп до компютърна система в прост вариант (чл. 42, ал. 1)** – т. е. неоторизиран достъп до компютърната система, която принадлежи или е ползвана законно от засегнатата страна, **незаконен достъп до компютърна система с цел получаване на компютърни данни чрез нарушаване на мерките за сигурност (чл. 42, ал. 3) –** във връзка с интервенция спрямо имейл сървъра от разстояние, **и нарушаване тайната на кореспонденцията (чл. 195, ал. 1 от НК) като двете деяния са в идеална съвкупност.**

3.3.3 Електронната поща се администрира от друг компютър със свободен достъп или с обществен и неограничен достъп. Достъпът до електронната поща е посредством имейл клиента.

3.3.3.1 Достъпът до електронната поща става през незащитен от мерки за сигурност имейл клиент. При тези условия тълкуването може да бъде само **нарушаване тайната на кореспонденцията (според чл. 195, ал. 1 от НК)**.

3.3.3.2 Достъпът до електронната поща се осъществява чрез защитен имейл клиент, а извършителят действа за премахване на мерките за сигурност. Тук отново единствената възможна квалификация е **нарушаване тайната на кореспонденцията (според чл. 195, ал. 1 от НК)**.

3.3.4 **Достъпът до електронната поща става посредством** WEBMAIL с достъп от разстояние в имейл сървъра, като съответно това е влизане в компютърната система по смисъла на Закон 161/2003.

Извършителят успява на проникне в имейл сървъра след въвеждане на правилното потребителско име (идентификатор) и парола. В този случай правилното законово определение е **незаконен достъп до компютърна система с цел получаване на компютърни данни (чл. 42, ал. 2) и нарушаване тайната на кореспонденцията (според чл. 195, ал. 1 от НК), които са в идеална съвкупност.**

Извършителят успява на проникне в имейл сървъра след деактивиране на мерките за сигурност. В този случай правилното законово определение е **незаконен достъп до компютърна система чрез нарушаване на мерките за сигурност (чл. 42, ал. 3) и нарушаване тайната на кореспонденцията (според чл. 195, ал. 1 от НК)**, **които са в идеална съвкупност.**

Във всички тези случаи дискутирахме престъпление от рода на нарушаване тайната на кореспонденцията, предвидено и наказвано съгласно чл. 195 от НК. Макар че при първоначален преглед може да се стори достатъчно квалифицирането на действията съгласно законовите норми, предвидени от чл. 42, ал. 1-3 на Закон 161/2003, все пак трябва да отбележим, че вниманието на извършителя се насочва към една отделна категория от компютърните данни, и по-конкретно – към съобщенията в електронната поща.

Практиката показва, че в голяма степен при неоторизиран достъп, извършителят цели **получаване на компютърни данни,** което може да означава:

- Визуално пренасяне на тези данни;
- Присвояване чрез отпечатване (хартиен документ);
- Задействане на програми и приложения за управление на компютърните данни (напр. програми за управление на базите данни на една организация, програми за електронна поща и др.).

Под получаване на компютърни данни се разбира включително и тяхното копиране върху външни носители за съхранение (флопи диск, компакт диск, преносима памет, карта и др.). Ако става дума само за копиране на данни, тогава действието се определя според разпоредбата на чл. 42, ал. 2. Ако, обаче, извършителят прехвърли данните върху външен носител (при пренос или прехвърляне на данни върху устройство), тогава се прилагат разпоредбите на чл. 44 от закона, които се отнасят за „нарушаване целостта на компютърните данни". Простото копиране на компютърни данни от хард диска на един компютър или от друго средство за съхранение, върху външен запаметяващ носител, принципно не засяга по някакъв начин целостта на съответните компютърни данни, но техния трансфер може да породи изтриването им от първоначалното им местонахождение.

По принцип, собствениците, притежателите или законните потребителите избират да защитават компютърните си системи чрез **стандартни мерки за сигурност.**

Защитата може да бъде *физическа* (изолиране на изчислителната техника в обезопасена каса, осигуряване с механични устройства с ключ или метално заключване с шифър, ръчен контрол на текущия източник и др.) или *логическа* (чрез пароли, кодове за достъп или с кодиране).

По смисъла на ал. 3 извършителят действа срещу дадена компютърна система чрез *разрушаване на тази защита.*

На физическо ниво разрушаването предполага деактивиране на механичните устройства за сигурност чрез различни механични или електро-химически средства. На логическо ниво, обаче, става дума за атакуване на паролите.

Атаките с парола от историческа гледна точка са сред най-предпочитаните от хакерите за превземане на електронните мрежи. В началото хакерите се опитвали да проникнат в мрежите чрез въвеждане на идентификатор и парола за достъп в системата. Опитва се парола след парола, докато не се намери правилната. В крайна сметка хакерите си дали сметка, че има възможност за съставяне на прости програми за тестване на паролите. Като цяло тези елементарни програми пробват последователно всички думи от речника в опита да открият вярната парола. По този начин атакуването с автоматични пароли бързо станало известно под наименованието *атаки с речник* (*dictionary-based attacks*). Оперативните системи Unix са изключително уязвими на тези атаки с речник, тъй като Unix не изключва автоматично потребителя след определен брой влизания в мрежата, за разлика от други оперативни системи, които деактивират потребителското име след като се въведат

определен брой грешни пароли. С други думи един хакер може да опита хиляди пъти да се свърже към една система Unix без тя да прекъсне връзката, да алармира автоматично или да информира администратора на системата.

В местната юридическата практика има достатъчно много примери за това как хакери са успявали да получат достъп до файловете с пароли (от обществено достъпни места в системата) при ползването на услуги Unix като *Telnet* или *FTP*. Оперативната система кодира паролите в подобни файлове. Тъй като системата Unix кодира паролите в тези файлове, използвайки същия алгоритъм (математическа функция) един хакер може да игнорира кодирането на този файл като ползва наличен в Интернет алгоритъм. Този алгоритъм е инкорпориран в повечето от инструментите за "разбиване" на системите, които често се ползват в общността на хакерите.

Изискване за наличие на престъпление е извършителят да е действал **без право** (виж дефиницията и асоциираните обяснения по-горе).

Субективна страна

Престъплението за незаконен достъп се извършва с ***пряко*** или ***косвено умисъл***. В случай на получаване на компютърен достъп (ал. 2), ***намерението е изяснено като цел.***

Форми

Подготвителните действия, макар и възможни, не се тълкуват като престъпление и като такива, не са наказуеми. Определени подготвителни действия са инкриминирани сами по себе си, както в случая на чл. 46 "Незаконни операции с компютърни устройства и програми".

Опитът за извършване на такива деяния се наказва според разпоредбите на чл. 47 от закона.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.4. Незаконно прихващане на компютърни данни

Чл. 43 от Закон 161/2003

(1) Незаконното прихващане, без право на пренос, на компютърни данни, които не са от публичен характер, предназначени за дадена компютърна система и произхождащи от подобна система или в рамките на компютърна система, представлява престъпление и се наказва с лишаване от свобода от 2 до 7 години.

(2) Със същото наказание се санкционира и прихващането без право на пренос на електромагнитна емисия от една компютърна система, която съдържа непублични компютърни данни.

Защитен юридически интерес

Представен е от социални отношения, отнасящи се до телекомуникации и компютърни комуникации, като цяло, и към съобщаването на данни (компютърни), които не са публични.

Извършител на престъплението

Активен извършител може да бъде всяко отговорно пред закона лице. По принцип той е общ за всички компютърни престъпления. В настоящия случай извършителят трябва непременно да използва (по директен начин) определени електронни устройства,

предназначени за прихващане в ИТ среда, без познанията в тази област да имат значение. С други думи може да бъде държавен служител, който има за задача да прихване определено предаване на данни, използвайки специално приложение (компютърна система), което му позволява да прихване и състави отново пакетите от данни, но (от техническа гледна точка) той не трябва да има ИТ познания.
Участието е възможно във всичките му форми: извършителство, подбудителство или съучастие.

Пострадал

Това е физическо или юридическо лице, което притежава права над компютърна система, или над свързващите компоненти (елементи на трансмисията), между две или повече компютърни системи.

По сходен начин пострадал е и притежателят на права върху прихванатите компютърни данни или лицето, което е пряко засегнато от автоматичното преработване на тези данни.

Обект на престъплението

Под **прихващане** (в техническия смисъл) се разбира прихващане с помощта на специално разработено за тази цел електронно устройство или компютър, на електрическите импулси, промени в напрежението или електромагнитните излъчвания, които преминават през една компютърна система или се проявява като негов функционален ефект, или се намира на трасето за връзка между две или повече компютърни системи, които комуникират помежду си.

Прихващането на пакетите представлява едно от най-трудните за откриване действия и в същото време е сериозна заплаха за комуникациите в мрежа (Интернет, LAN). Всеки пакет от изпратени данни в мрежата може да премине през голям брой компютри и мрежи преди да стигне до крайната дестинация. С помощта на *прихващателно устройство на пакети* хакерите могат да уловят пакетите с данни (включително и съобщенията за влизане/log-in, предаване на цифровите идентификатори на кредитни карти, имейл пакети и др.), които се намират на различни места в Интернет. След прихващането на един такъв пакет хакерът може да открадне името на хоста, потребителското име, както и асоцииранта с пакета парола. Експерти в областта на сигурността са нарекли прихващането на пакети *шпионаж в мрежа (network snooping)* или *скрито наблюдение (promiscous monitoring).*

Компютърно прихващане може да се осъществява по няколко начина.

По пряк начин, чрез взаимодействие на извършителя с външните компоненти на компютърната система (кабели, превключватели/суичове, рутъри, компютри и др.). Например, комуникацията между два компютъра в една локална LAN мрежа (Local Area Network) на дадена институция се свързва физически към кабелното трасе на съответната мрежа посредством разделянето на кабелите и тяхното събиране (паралелно) с кабела, който е свързан със собствения компютър, където ще прихваща трафика компютърни данни.

Косвено или от разстояние прихващането може да приеме формата на едно специализирано приложение (така наречените **sniffers/снифъри – от глагола "подушвам"),** които могат да следят трафика на пакетите в една мрежа и да запаметяват данни, представляващи интерес, в рамките на файл от типа **log**. Като цяло снифърите се използват от администраторите на мрежи или от Интернет доставчиците (ISP) с цел осъществяване анализ на трафика в рамките на мрежата с техническа цел за оптимална поддръжка. Също така снифърите се използват от администраторите на мрежи в една институция за следене на комуникацията (вътрешна и външна) между служителите, както и за предотвратяване на изтичане на информации, разпадане на целостта на дейността в рамките на системата (напр.

сваляне на програми под режим на защита на авторските права, излагане на показ на порнографски материали с непълнолетни и др.), а дори и за изготвяне на обстоен доклад за мениджмънта относно това как служителите прекарват времето си в локалната мрежа или в Интернет.

Напоследък предпочитаните цели на хакерите са безжичните мрежи (wireless) (или точките за достъп hot-spot), които най-често са незащитени с код (макар и рутърите, които предлагат услугата access point фабрично да съдържат такива решения или кодирани пакети).

За да открият какво съдържа една компютърна система заинтересованите лица вече разполагат с нов метод, на който не издържа нито една защита от тип firewall, антивирусна програма или която и да е друга програма за компютърна защита. Накратко, могат да се декодират издаваните звуци от бутоните на клавиатурата. Досега в Румъния не е констатиран подобен случай.

Друг метод за косвено прихващане или прихващане от разстояние представлява използването на програми от типа **keylogger, adware, spyware**. Програмите от типа Adware и Spyware автоматично се свалят в персоналният компютър, когато се посещава една Интернет страница. Целта тук е да се запише „електронното трасе" и да се предадат обратно на изпращачите (по принцип става дума за компании, които се занимават с електронна търговия, маркетинг и реклама) данни и информации за предпочитанията на потребителя в областта на Интернет страницата, съдържанието, тематиката и др.

Програмата Keylogger е специализирано приложение, което регистрира всеки бутон от клавиатурата, който се натиска от потребителя, като изпраща изключително полезни информации за всеки хакер, като например номер на кредитна карта, фирмени доклади, секретна информация в една институция или данни от финансов характер. Този тип прихващане съществува и в Румъния, като е доста разпространен както на индивидуално ниво, така и на организационно.

Отново в същата гама съществуват и програми за наблюдение на имейлите (Websense, MIMEsweeper, FastTrack etc.).

В ал. 2 е предвиден подобен начин на извършване на престъпление, съответно на прихващане, без право, на електромагнитно излъчване, изхождащо от компютърна система, която съдържа лични компютърни данни. Това предполага прихващане на паразитните емисии или на съществуващите електромагнитни полета (на едно определено от науката разстояние) около всяко устройство за пренос на електрически или електромагнитни импулси. В наши дни лоша репутация има модерният метод, чрез които заинтересовани лица могат да улавят със специални устройства съществуващи електромагнитни излъчвания в непосредствена близост до монитора на компютъра-цел, които след се това "превеждат" трансформирани в електрически импулси и накрая в буквено-цифрови символи. (Терминологията за защита на изчислителните системи срещу прихващане на излъчванията се нарича TEMPEST – Transient ElectroMagnetic Pulse Emanation Standardizing и е в период на въвеждане в гражданските и военните институции, в които има движение на класифицирана информация от национално и от ЕС/НАТО ниво).

Изискване за наличие на престъпление е извършителят да е действал ***без право***. Практиката показва, че действието ще е законосъобразно, ако лицето, което извършва прихващане:

- има право да разполага с данните от предаваните пакети (това е случаят на собственик или притежател на права върху компютърните системи);

- ако действа на базата на договор, по поръчка или посредством упълномощяване от участниците в процеса на комуникация (какъвто е случаят на администратора на мрежата, на Интернет доставчиците – ISP);

- ако данните са предназначени за собствено ползване;

- ако въз основа на законовите разпоредби електронното наблюдение е оторизирано в интерес на националната сигурност или за да разреши на службите за сигурност, агенциите по прилагане на закона или прокурорите да извършват закононарушения (това е в случая, когато оторизирани от държавата агенти боравят със специални разузнавателни средства и действат законосъобразно).

Всяко действие, което е извън гореспоменатите случаи или превишава законовите термини автоматично се счита за извършвано ***без право***.

Субективна страна

Престъплението по незаконно прихващане се извършва само с ***пряк умисъл***. От анализа на обекта на престъплението може да се направи изводът, че е възможно извършителят, предвиждайки резултата от действията си, да прихване (и евентуално да запише) пакети с данни в дадена компютърна система или между две такива системи без да цели това, като приема само възможността за постигане на този резултат.

Форми

Подготвителните действия, макар и възможни, не са инкриминирани и като такива не се наказват. Определени подготвителни действия се определят като престъпни сами по себе си, например според чл. 42 – нелегалният достъп до компютърна система или по чл. 46 – незаконни операции с компютърни устройства и програми.

Опитът се наказва (чл. 47 от закона).

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.5. Нарушаване целостта на компютърните данни

Чл. 44 от Закон 161/2003

(1) Действие, заключаващо се в промяна, заличаване или увреждане на компютърни данни или ограничаване на достъпа до тях без право, е престъпление и се наказва с лишаване от свобода от 2 до 7 години.

(2) Неупълномощен трансфер на данни от една компютърна система, е престъпление и се наказва с лишаване от свобода от 3 до 12 години.

(3) С предвиденото в алинея (2) наказание се наказва и неупълномощен трансфер на данни от дадено средство за съхранение на компютърни данни.

Защитен правен интерес

Представен е от съвкупност от социални отношения, които се пораждат около данните и информациите, съхранявани или предавани в електронна форма. Защитеният правен интерес е този на собственика или притежателя на права върху компютърните данни, за да се осигури неговото ефективно разполагане със съответните данни.

Извършители на престъплението

Активен извършител (деец) може да бъде всяко наказателноотговорно физическо лице. Като цяло, както стана ясно, деецът е лице с познания в областта на компютрите и електрониката, макар че има случаи (по-рядко, разбира се), в които този елемент не е налице.

Участието е възможно във всичките си форми: извършителство, подбудителство и съучастие.

Пострадал от престъплението е физическо или юридическо лице, притежател на правата над данните и информацията, считани за обект на престъплението.

Обективната страна на престъплението на престъплението по своята същност се реализира чрез множество алтернативни действия да промени, заличи или увреди компютърните данни, да ограничи достъпа до тях или да извърши пренос на данни без упълномощяване.

Действията, чрез които се реализира обективната страна на престъплението включват негативни ефекти спрямо данните, най-вече доколкото се отнася за способността им да функционират по предвидения от лицето, което разполага с тях, начин. Тоест, изключени са промените, заличаването и др., които нямат подобни последствия. Например, действия, които водят до усъвършенстване на програмата или на данните.

Промяната се състои в действията на извършителя с цел въвеждане на нови части или изтриване на определени части от компютърните данни, което като резултат води до получаването на нови компютърни данни, различни от първоначалните и не съответстващи на истинската стойност, която са имали първоначално.

Под **изтриване** се разбира действие с цел цялостно или частично елиминиране на бинарното представяне на компютърните данни, качени на носители за съхранение от типа хард диск, CD, дискета, флаш памет и др., което води до изчезване на съответните данни.

Изтриването на данни се приравнява по някакъв начин с разрушаването на материалните обекти. Може да става дума, обаче, и за разрушение на носителя на данни, на оптични дискове (тип CD-RW), флаш памет и др. Изтриването на бинарното представяне означава анулиране на стойностите „0” и „1”, респективно, пораждане на промени в съответното напрежение.

Изключително важен е фактът, че изтриването на компютърните данни не означава непременно необратимото им окончателно елиминиране. Най-често изтриването на данни е в резултат на команда от типа DELETE или FORMAT. В подобен момент данните, организирани в компютъра под формата на папки ще продължат да съществуват физически в носителя за съхранение, но системата ще третира съответните локации като “свободни” за бъдещо записване с наслагване.

По този начин, докато системата не заеме съответните локации с други данни, първоначалните данни (предполагаемо заличените) могат да бъдат възстановени. Въпреки че се счита, че след команда FORMAT магнитният диск е “форматиран”, а записаните на него данни автоматично се разрушават, технически, това се случва едва след изпълнение на шест подобни операции.

Увреждане, означава *промяна* в бинарното съдържание на компютърните данни чрез контролирани вмъквания или спорадични части “0” и “1” (байт), по начин, по който новата част не може да има в реалността кореспондираща логика.

В по-сериозни случаи унищожаването на данни може да бъде в резултат на конкретно засягане на компютърни инсталации чрез терористични актове, саботаж, специално изготвени или с обикновен характер, както и изтриването на данни с магнит или с вмъкване на инцидентни програми, логически бомби и т.н. От техническа гледна точка един от тези обикновени методи за унищожаване на данни е поставяне на магнит (доста силен) в непосредствена близост или направо в контакт с устройство за електронно или магнитно съхраняване на данни (плочите на хард диска, магнитното фолио на флопи диска, чиповете на флаш паметта и др).

Съществува **ограничаване на достъпа** тогава, когато авторът *прави нужното за изчезване на данните, но без да ги изтрива практически*, като следва съответните за това инструкции. Данните повече няма да бъдат на разположение на упълномощените лица и вследствие на това те не могат повече да си служат с тях.

Ограничаването на достъпа до компютърни данни е резултат на едно или повече действия на извършителя спрямо изчислителните системи или устройствата за съхранение на данни, така че след това упълномощения потребител да не може да ги открие в първоначалната им форма или чрез стандартните процедури за ползване на изчислителна техника. В случай на “физическо” ограничаване на достъпа до компютърните данни,

извършителят действа директно за блокиране на достъпа до източниците на една система чрез пренасочване на периферните устройства от типа на клавиатура или мишка. **В случай на "логическо" ограничаване**, например, извършителят може да промени таблицата за разпределяне на файловете FAT – File Allocation Table – компонент на оперативната система, която разпределя на всеки файл по една или повече порции от устройството за запаметяване, посредством отбелязване на съответното място за откриване след това.

Актуален пример за ограничаване на достъпа представляват атаките спрямо адреса на Интернет страници, като в резултат е невъзможно страницата да се отвори или изцяло се блокира съответната Интернет страница за достъп от страна на собствениците й или притежателите на права върху нея и най-вече от страна на посетителите.

Под **неупълномощен трансфер** се разбира *неупълномощено преместване* на бинарно представяне на информацията от актуалния носител на съхранените данни върху друг външен носител или дори вътре в същата компютърна система, но на друго място.

Мигрирането на данни от една компютърна система с определена хардуерна конфигурация или софтуер към друга система с различна конфигурация може да причини определени нарушения на данните, а информацията няма да може да бъде открита във формата, позната на потребителя. Все пак най-често подобни инциденти са случайни и се дължат по-скоро на професионализма на лицето, извършващо операцията, отколкото на евентуална престъпна намеса.

Преместването на данни може да има ефект върху целостта на компютърните данни. В такъв случай на една структурирана база данни, в която крайната информация е структурирана по определен логически ред, а на физическо ниво началните данни се откриват по-добре чрез установени алгоритми по местонахождение на устройството за съхранение на данни. Едно евентуално преместване на някои от тях може да причини невъзможност на програмата (или на главното приложение) да ги разпознава, което засяга целостта на крайните информации от гледна точка на очаквания от потребителите формат.

Практиката в тази област показва, че най-опасните инструменти, които променят компютърните данни са програмите от типа **Вирус, Червеи** или **Троянски кон**, които се репродуцират и/или действат в други програми, както и във файлове с данни, като програми за разрушаване.

Основно условие за това изброените горе операции да бъдат считани за незаконни действия е извършването им ***без право*.**

Казус:

На 01.09.2003 г. масмедиите оповестяват новината, че в Румъния се е появил нов компютърен вирус, като източник на тази новина са външни информационни канали.
Базирайки се на тази новина, фирма Softwin, специализирана в разработването на антивирусни програми, успява на идентифицира източника на този вирус и сезира Главна дирекция за борба с организираната престъпност и борба с трафика на наркотици към Главния инспекторат полицията.

Вследствие на предприетите мерки е идентифицирано лицето К. Д., на 25 години, студент в магистърска програма на Хидротехнически факултет към Университета в Яш, който е взел вируса от Интернет и след това го е модифицирал, вмъкнал е съобщение на румънски език, което е съдържало обидни думи по адрес на един преподавател от същия факултет и по отношение на учебното заведение и след това е насочил вируса към компютърната мрежа на Хидротехническия факултет.

Предприема се обиск на дома на извършителя, по време на който са иззети няколко компютъра, дискети, CD носители, както и най-различни документи. Служителите на гореспомената дирекция на полицията извършили преглед на конфискуваните компютърни системи от дома на К. Д. и от факултета, които допринесли за идентифициране на важни пароли за извършване на предполагаемото престъпление.

Субективна страна

Престъплението за промяна на компютърните данни се осъществява с ***пряк или косвен умисъл***.

В повечето случаи, **деецът цели да нанесе вреда**. Намерението да се получи незаконна изгода от едно такова действие не е необходимо условие и то принципно не е характерно за тази форма на престъпно поведение. Все пак е възможно да съществува специфична, но непряка мотивация, например желание да се навреди на конкурент.

Практиката е доказала, че най-често актът на нанасяне на компютърна вреда е мотивиран от желание за отмъщение на служител, чиито трудов договор е бил прекратен или предстои да бъде прекратен. Политически или идеологически мотиви също са характерни - например в случаите на терористични действия. В крайна сметка доста често това се прави и с цел привличане вниманието на обществеността или на дадена организация.

Форми

Подготвителните деяния, макар и възможни, не са инкриминарани и съответно не са наказвани като престъпления. Определени действия, обаче, сами по себе си представляват престъпления, напр. по смисъла на чл. 42 – незаконен достъп до компютърна система или на чл. 46 – нелегални действия с компютърни програми или устройства.

Опитът се наказва (чл. 47 от закона).

Престъплението се счита за приключено, когато извършителят е променил, заличил или увредил данните в една компютърна система, затруднил е достъпа до тези данни от страна на притежателите на права или е прехвърлил успешно бинарното представяне на избрани данни върху друго устройство за съхраняване на данни.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.5. Нарушаване функционирането на компютърните системи

Чл. 45 от Закон 161/2003

Действията предприети за сериозно увреждане функционирането на една компютърна система, извършени без права за това, чрез въвеждане, промяна, заличаване или увреждане на компютърни данни или чрез ограничаване на достъпа до компютърни данни, представлява престъпление и се наказва с лишаване от свобода от 3 до 15 години.

Защитеният правен интерес се състои в нормалното (доброто) функциониране на компютърните системи в обществото и тяхната надеждност с оглед на социалните нужди, за които са били въведени.

Извършители на престъплението

Активен извършител (деец) може да бъде всяко наказателноотговорно физическо лице в смисъла на досега направените разяснения .

Участието е възможно във всичките му форми: извършителство, подбудителство или съучастие.

Пострадал е физическо или юридическо лице, което притежава права над компютърната система, чието функциониране е нарушено.

Обективната страна се реализира чрез всяко действие, което сериозно нарушава функционирането на една компютърна система. Законовият текст прецизира и начините за реализиране на обективната страна, и по-конкретно: *въвеждане, предаване, промяна, заличаване* или *увреждане*, както и *ограничаване на достъпа* до компютърните данни.

Въвеждане на компютърни данни. Те могат да бъдат въведени по директен начин от клавиатурата или чрез трансфер от външно средство. От клавиатурата (или мишката) извършителят може да влезе в определени зони, запазени за изчислително оборудване

(например: зоната BIOS - Basic Input Output System, която контролира дейността на централната единица за обработване) или за собствената си оперативна система.

Грешните данни могат прогресивно да засегнат и функционирането на други компоненти, най-вече в условията на мрежа. Например, когато операторът на компютърната система за контрол на дейността на една хидроцентрала, въведе от клавиатурата серия параметри, интерпретирани погрешно от програмата за изпълнение.

Изпращането на компютърни данни може да се извършва от разстояние чрез използване на наличните опции, които са налице поради свързването на съответната компютърна система към компютърна мрежа (от типа LAN – местна или WAN – за широко ползване).

Най-често става дума за внедряване в дадената компютърна система на вируси, червеи или троянски коне. Пренасянето може да осъществява чрез:

- трансфер (копиране) в целената компютърна система на файлове или програми, заразени посредством външни носители;
- пренасяне/получаване на имейл съобщения с прикачени заразени файлове;
- сваляне от Интернет на файлове или програми, носители на код за увреждане.

Много често срещан случай е когато дадено лице, независимо от причината, изпраща чрез Интернет голям брой съобщения (без вирусно съдържание) до компютърната система на друга организация, като по този начин натоварва до максимум портовете за данни, блокирайки достъпа до тях отвън.

Пример за това е **Отказ от услуга (Denial of Service).** Тук, един Интернет източник, като например сървър или Интернет страница престават да функционират по съобразен начин, тъй като нарушителите лансират координирана атака, довеждаща до свръх натоварване на портовете на целта с множество фалшиви команди и става така, че системата не успява да ги администрира и напълно се обърква. Най-разпространеният тип атака DoS, например, препятства достъпа на Интернет потребителите до определена Интернет страница, което може да доведе до големи финансови загуби в контекста на една организация, чиято дейност пряко зависи от Интернет.

Друг начин за атака, състояща се в поемане на контрола върху една компютърна система или във въвеждане на увреждащи приложения, се осъществява с помощта на **Мобилен код**. Това е определена категория писмен код (на езиците Java, JavaScript и ActiveX) и е част от документ от типа HTML. Когато браузърът на потребителя зарежда Интернет страница, скритият мобилен код се сваля и се изпълнява от браузъра.

Основно условие, за да се определят гореспоменатите операции и да бъдат регламентирани като наказуеми действия, е те да бъдат извършени ***без права*** за това. В този смисъл законно ще действа едно физическо или юридическо лице, което на базата на специално сключен договор със собственика или притежателя на права над компютърната система, извършва действия по Ethical Hacking – Влизане със съгласие – чрез който се определя уязвимостта на системата и се предприемат адекватни мерки за сигурност, провокирайки нарушаване (дори **сериозно нарушаване**) във функционирането на съответната компютърна система.

Терминът ***сериозно нарушение*** не е ясно категоризиран чрез нормите за инкриминиране, но дава възможността на разследващите органи (по време на разследването) или на съдиите (по време на съдебния процес) да преценят стойността на нанесените щети, или нивото на създадената посредством нарушението обществена заплаха. Разграничение може да се прави, като се вземе предвид важността на дадената компютърна система за социалния живот (например: компютърната система на Националната служба за извънредни случаи 112 в съотношение с компютърната система – местна LAN мрежа – на едно училище).

Субективна страна

Престъплението по нарушаване на функционирането на една компютърна система може да бъде извършено ***с пряк или косвен умисъл***. Много често разликата между двете форми на вина се откриват в характера на въведените данни, които са прехвърлени, променени, изтрити, увредени или достъпът до тях е бил ограничен.

Например, може да определим като извършено с пряк умисъл деяние в случая, когато служител в определена организация в обедната почивка разпраща на всички колеги шега, която не съдържа обиди, под формата на имейл, към който е прикачил файл с много голям размер или дори заразен с вирус файл. От техническа гледна точка, резултатът от подобно действие със сигурност ще е временно блокиране на вътрешния имейл сървър, тоест – нарушаване на функционирането на сървъра на електронната поща на тази институция, като тази последица е предвидено и очаквано от служителя.

Форми

Подготвителните действия, макар и възможни, не се тълкуват като престъпление и като такива не са наказуеми. Определени подготвителни действия са инкриминирани сами по себе си, както в случая на чл. 43 – нелегално прихващане на излъчване на компютърни данни или на чл. 46 "Незаконни операции с компютърни устройства и програми".

Опитът се наказва според разпоредбите на чл. 47 от закона.

Престъплението се счита за завършено тогава, когато дадената компютърна система прояви дефект във функционирането или блокира. Ако това резултат не се реализира, тогава можем да говорим за подготвителни действия, осъществени от лицето или за извършване на друго престъпление (напр. незаконен достъп до компютърна система или промяна на компютърните информации).

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.6. Незаконни операции с компютърни програми или устройства

Чл. 46 от Закон 161/2003

(1) Представлява престъпление и се наказва със затвор от 1 до 6 години:

а) действие, което цели да се създаде, продаде, внесе, разпространи или да се направи достъпна, под всякаква форма, но без права за това, една компютърна програма или устройство, което е създадено или адаптирано с цел да се извърши едно от престъпленията, предвидени от чл. 42 – 45;

б) действие, което цели да се създаде, продаде, внесе, разпространи или предложи на разположение, под всякаква форма, но без права за това, една парола, код за достъп или други подобни компютърни данни, които предоставят пълен или частичен достъп до една компютърна система с цел да се извърши едно от престъпленията, предвидени от чл. 42 – 45;

(2) Със същото наказание се санкционира и притежанието, без право на такова, на едно устройство, компютърна система, парола, код за достъп или компютърна информация, от предвидените в алинея (1), с цел да се извърши едно от престъпленията, предвидени от чл. 42 – 45;

Защитеният правен интерес се състои от обществените отношения, свързани с доверието в данните, устройствата и компютърните програми, в смисъла на тяхното правилно и законно ползване, както и в правилното и законно извършване на търговските операции, свързани с тях.

Участници в престъплението

Активният извършител (деец) може да бъде всяко наказателноотговорно физическо лице.

Участието е възможно под всички форми: извършителство, подбудителство или съучастие.

Пострадал от престъплението е физическо или юридическо лице, което притежава права над компютърна система, податлива на достъп чрез извършване на инкриминирани действия, но в същото време може да бъде и собственикът или притежателят на авторските права върху променените или адаптирани хардуерни или софтуерни продукти с престъпна цел. За пострадал се счита и физическото или юридическо лице, притежател на правата или собственик (но не непременно потребител) на паролите, на кодовете за достъп или други подобни компютърни данни, които са били използвани по неправомерен начин за достъп до определена компютърна система.

Обективната страна се състои в действието по създаване, продажба, внасяне, разпространяване или правене достъпно на едно или повече устройства или компютърни програми, специално разработени или адаптирани за извършване на някое от споменатите вече по-горе престъпления.

Производството на едно компютърно устройство се състои в извършване на определени действия от технически характер, чрез които дадени електронни елементи се съчетават или взаимно се обвързват така, че полученият продукт да може да взаимодейства (директно или от разстояние) с компютърна система или да се превърне в съставна част от нея. Например, изработването на електронно устройство, с помощта на което могат да бъдат улавяни трансмисиите на пакети от данни в една компютърна мрежа.

Създаването на компютърна програма предполага изготвяне на логическа скица на програмата, в зависимост от преследваната цел и транслирането на инструкциите на програмен език (машинен код – Assembler, C++, Pascal, Visual Basic, Java и др.), за да могат да бъдат "разбрани" и след това изпълнени от съответната компютърна система. Добър пример за това може да бъде съставянето на програма, с помощта на програмен език от високо ниво C++, която след стартиране в компютъра позволява достъп на неупълномощено лице до ресурсите на компютърната система или до цялата мрежа посредством избягване на "идентификацията" чрез парола и потребителско име. Най-опасните програми, обаче, са тези които генерират компютърни вируси, троянски коне или "логически бомби".

Законодателят, все пак, иска да инкриминира и действията на лицето, което макар и да няма принос в създаването на подобно устройство или компютърна програма, го *внася/импортва* или го *разпространява*, или го *прави достъпно* на лице, което действа по непосредствен начин спрямо компютърната система.

В същото време, трябва да бъдат санкционирани и действията по производство, продажба, внасяне, разпространение или предоставяне на неупълномощено лице на паролите за достъп или всякакъв вид компютърни данни, които позволяват цялостен или частичен достъп до една компютърна система.

Субективна страна

Нелегалните операции с компютърни устройства или програми могат да бъдат извършени ***с пряк умисъл,*** класифицирани според целта. По този начин, описаните деяния в алинея 1 и 2 трябва да бъдат с цел извършване на някое от престъпленията, предвидени от чл. 42 – 45 (незаконен достъп до компютърна система, нелегално прихващане на предаване на компютърни данни, нарушаване целостта на компютърните данни, увреждане функционалността на компютърните системи).

Форми

Подготвителните действия, макар и възможни, не се тълкуват като престъпление и не са наказуеми.

Забелязваме, че инкриминираните деяния в чл. 46, б. а) – с) представляват подготвителни действия за престъпленията, предвидени в чл. 42 – 45, но румънският законодател е предпочел да ги инкриминира отделно, по отличителен начин.

Опитът се наказва според разпоредбите на чл. 47 от закона.
Престъплението се счита за приключено в момента на производство, продажба, внос, дистрибуция, предоставяне на разположение или за притежание, без право на това, на дадено устройство, компютърна програма, парола, код за достъп или друг тип информации, с цел извършване на престъпленията, описани по-горе.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.7. Компютърна фалшификация

Чл. 48 от Закона 161/2003

Действията по въвеждане, промяна или заличаване, без право на това, на компютърни данни или ограничаването на достъпа до тях, отново без право, и ако в резултат на тези действия се получават неотговарящи на истината данни, които се използват за постигане на „законни" цели, на правни последици (например, с цел да се създаде доказателство в хода на едно истинско съдебно производство), то те също представляват престъпление и се наказват с лишаване от свобода от 2 до 7 години.

Защитеният правен интерес се състои от обществените отношение, свързани с общественото доверие в сигурността и надеждността на компютърните системи, във валидността и истинността на компютърните данни, на целия модерен процес на обработка, съхранение или автоматичен пренос на данните от личен или обществен интерес.

Извършители на престъплението

Активният извършител (деец) може да бъде всяко наказателноотговорно лице. Измами от този род, по принцип, се осъществяват от посветени в компютърната наука лица, или от такива, които според естеството на работата си, имат достъп до компютърни данни и системи.
Участието е възможно под всички форми: извършителство, подбудителство или съучастие.

Пострадал

В конкретния случай на това престъпление, пострадал е физическо или юридическо лице, което е предопределило собствения си интерес и спрямо което се осъществяват правните последици (от морално или социално естество или заради унаследяване) в следствие на фалшифициране на компютърните данни.

Прилежащ (вторичен) пасивен субект е собственикът, притежателят на права или оторизираният потребител на компютърната система.

Обективната страна се реализира чрез алтернативно действие по въвеждане, промяна или изтриване на тези данни, или ограничаване на достъпа до тях. Тъй като тези нормативни подходи са били анализирани в рамките на престъпления за нарушаване целостта на компютърните данни, то те правят препратки към обясненията в съответния раздел.

Действията, чрез които се реализира обективната страна на престъплението, предполагат негативно въздействие спрямо данните по отношение на тяхната способност за функциониране, както и доказване на действия или ситуации по начин, който е предвиден от лицето, разполагащо с тях, като в крайна сметка се стига до ситуация, съответстваща на издаване на фалшиви документи или фалшифициране на оригинални документи.

С предложение за примерни наименования, фалшифицирането на компютърни данни може да се реализира под следните форми:
– измама, промяна или заличаване на данни в полетата със съществуващи бази данни на ниво на компютъризиран център за съхранение на лични данни, при банка или осигурително дружество и др. – чрез пряко действие от страна на извършителя спрямо клавиатурата или чрез копиране на данните върху външен носител;

– промяна на съхранени документи в електронен формат, чрез директна промяна или изтриване на думи и др.

В практиката, компютърната фалшификация е под някоя от следните форми:

- Подправяне на електронна поща;
- Подправяне на електронна препратка;
- Подправяне на Интернет адрес.

В местната практика най-често срещаните методи за извършване на компютърно фалшифициране са подправянето на електронните препратки и на Интернет адреси. Прилагани по "гениален" начин заедно с общественото инженерство, тези методи са известни в областта на компютърните престъпления като „Фишинг атаки". Целта на тези атаки не са организации или институции (финансови), а само Интернет потребителите, които поради незнание стават жертви на този род измама и предоставят достъп до лични данни, информация за банкови сметки или конфиденциални данни.

Казус:

През месец март 2007 властите предприемат мерки по отношение на факта, че на територията на област Констанца развива дейност международна групировка, която извършва измамни финансови операции чрез ползване на фалшиви инструменти за електронно плащане или фалшиви идентификационни данни, с помощта на които се генерират финансови трансфери, като получените суми след това се инкасират от системата Western Union. След това, през април 2007 година, една банкова институция сезира румънските власти за факта, че тя е била "цел" на атаки от типа „Фишинг".

Наблюдаването на въвлечената група лица, както и операциите по оперативен надзор са били свързани с тяхната специализация, съответно и напреднали познания в областта на компютърните технологии.

Вследствие на извършеното разследване е установено, че прилежащите данни към фалшивите финансови трансфери или тези, които са били нужни за повторно вписване в клонингите, получени чрез типични за компютърните измами материали (от типа „Фишинг"), като целта им е била финансови институции и техните клиенти. След изготвяне на клонинг на Интернет страницата на някоя банка (от чужбина), която се обслужва от различни сървъри, са били предавани чрез използване на приложения определен брой съобщения по имейл към различни потребители, клиенти на атакуваните финансови институции. Тези съобщения са съдържали неизменно една реклама или известие за анулиране, или ограничаване на достъпа на съответния клиент до банковата му сметка. За разрешаване на създадената ситуация клиентът е бил помолен да отвори конкретен линк и да попълни формуляр с всички посочени в него данни, съответно – име, номер на картата, дата на валидност, пин код и др. Веднага след попълване формулярът се препраща автоматично към специално създаден за целта имейл адрес. По този начин събрани, данните за идентификация на съответния инструмент за електроно плащане (карти) се ползват или за извършване на електронни операции (купуване на услуги за хостване, имена на домейни, телефонни услуги, за продукти или за финансов трансфер Western Union), или се ползват за фалшификация на банкови карти (чрез пре-написване на магнитната лента) с цел извършване на операции по теглене на пари в брой от банкомати.

В периода февруари – октомври 2007 год., виновните, които са осъзнали възможността да заобиколят изискванията за регистрация и след това ползване на системата за финансов електронен трансфер Western Union, осъществяват финансови трансфери чрез злоупотреба с данните за идентификация.

Извършените разследвания са определили, както начина на извършване на измамата за банков трансфер, така и предаването по SMS на контролния номер на банковия

трансфер и идентификация на изпращача (жертвата), така и името на получателя (един от виновниците).

За осъществяване на трансфера е била ползвана система за телефонно потвърждаване, било система за авто-потвърждаване, контекст в който инкасирането на така получените суми е трябвало да бъде осъществено в рамките на 20 минути. Едновременно с това, практикуваната престъпната схема е позволявала трансфер на суми от около 250 USD (като конфискуваните Western Union документи потвърждават осребряване на около 200-250 USD в EURO или RON).

Идентификационните данни на ползваните инструменти за плащане са били улавяни в голяма степен чрез „Фишинг", съответно – чрез извършване на престъпление по фалшифициране, което се състои в получаване на лични данни като: пароли, потребителско име, сметки, идентификационни данни за инструментите за електронно плащане; посредством създаване на фалшива реалност и предаване на съобщения с нереална информация, които са имали прилежащ интерфейс за електронно съобщаване, като част от банкова институция със собствени клиенти, предварително модифицирани за скриване на оригиналния източник.

Стойността на нанесените щети вследствие на извършеното престъпление, описано по-горе, достига приблизително 60.000 USD.

Разбиването на тази криминална групировка е било в резултат на близкото сътрудничество с Правния департамент на САЩ, както и с помощта на ФБР чрез своя представител в Букурещ, заедно със служителите на Главна дирекция за борба с организираната престъпност и на Бригада за борба с организираната престъпност в гр. Констанца, подкрепяни от офицерите от Румънската жандармерия – Батальон "Влад Цепеш".

Субективна страна

Престъплението за компютърно фалшифициране се извършва само с ***пряк умисъл***, определено според целта.

В условията на добавяне, промяна или изтриване на компютърни данни има наличие на престъпление, дори ако лицето е изкривило истинността на съдържанието на тези данни със "законна" цел (например, за да направи тест на реална правна ситуация). Също така, не е необходимо ефективно ползване на тези данни, а само получаването им с оглед осъществяване на поставената цел.

Преследваната цел е използване на неверните данни, получени с оглед осъществяване на правните последици. Данните са годни на извършване на престъпното деяние, ако успеят да създадат, да променят или да прекратят юридически отношения, създавайки права и задължения.

Форми

Действията по приготовление извършване на престъплението, макар и възможни, не са инкриминирани и не се наказват от закона.

Опитът се наказва (според чл. 50 от закона).

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.8. Компютърна измама

Чл. 49 от Закон 161/2003

Причиняването на имуществена щета на дадено лице, чрез въвеждане, промяна или изтриване на компютърни данни, посредством ограничаване на достъпа до такива данни или с възпрепятстване, по какъвто и да е начин, на функционирането на една компютърна

система, с цел лично, материално облагодетелстване или в полза на друго лице, съставлява престъпление и се наказва с лишаване от свобода от 3 до 12 години.

Защитеният правен интерес се състои в обществените отношения, които защитават имуществото на дадено лице тогава, когато присъствието на това лице в кибер пространството се изчислява чрез определен обем от съхранени данни в компютърната система или тези, които циркулират в дадена мрежа.

Субекти на престъплението

Активният субект (деец) може да бъде всяко наказателноотговорно физическо лице. Действията, свързани с този вид измама са, както и в предходния случай, често извършвани от посветени в областта на компютрите или от лица, които поради естеството на работата си, имат достъп до компютърни данни и системи.

Участието е възможно под всички форми: извършителство, подбудителство или съучастие.

Пострадал е лицето, чиито имуществен интерес е бил накърнен чрез действията на извършителя. И в този случай, прилежащ пасивен субект е собственикът, притежателят на права или законния потребител на една компютърна система.

Обективната страна на престъплението се реализира чрез алтернативно действие за въвеждане, модифициране или изтриване на данни, или ограничаване на достъпа до тях, както и на всякакъв род възпрепятстване на функционирането на една компютърна система. И тъй като, някои от тях вече бяха анализирани в рамките на престъплението за нарушаване целостта на компютърните данни, сега ще направим препратка към обясненията към това престъпление:

"Възпрепятстването на функционирането на дадена компютърна система" предполага извършване на някакво действие от такова естество, че да доведе до невъзможност за ползване, цялостно или частично, временно или постоянно, на съответната система. Например, извършителят действа в определен ден и час срещу компютърната система на борсата, успявайки да парализира електронните финансови сделки, което има сериозно отражение върху сделките и печалбите на компаниите, намиращи се в процес на покупко-продажба в съответния момент. В компютърна среда измамата може да има повече форми и често може да бъде объркана с традиционната измама, където средството за измама е компютъра.

Казус:

На 15 юли 2008 г. прокурорите от Дирекцията за разследване на престъпленията на организираната престъпност и тероризъм – Териториално бюро в гр. Вълча, заедно с полицаите от Главна дирекция за борба с организираната престъпност, извършиха домашен обиск на различни адреси в градовете Ръмнику Вълча, Драгашани, Букурещ, Александрия, Сибиу, Хунедоара.

В следствие на обиските при 26 виновници са били открити вещи, които имат връзка с обекта на разследваните случаи, като: лаптопи, персонални компютри и хард дискове, мобилни телефони, флаш памети, модеми, сим карти, рисийвъри, суичове, както и различни суми пари в леи, евро, британски паунди и долари.

Начинът на действие на членовете на престъпната група е бил чрез качване в Интернет на съобщения за продажба на стоки (които в действителност не са притежавали), в специализирани сайтове за електронна търговия (E-Bay.com, Equine.com, Craigslist.com).

Достъпът до тези сайтове по принцип е бил чрез използване на идентификационните данни на други лица, включително кредитните им карти, получени чрез пускане на спам съобщения информации, като по този начин са разкрили личните си данни (метод " Фишинг").

Така получените данни са били използвани за неупълномощена регистрация, посредством използване на самоличността на съответното лице, в сайтовете за електронна търговия.

След пускането в Интернет на съобщенията за продажба на стоки, те са карали жертвите да закупуват стоките и да извършват плащания или чрез услугите за бързо изпращане на пари (Western Union, Money Gram), или чрез депозиране в банкови сметки на получател с фиктивно име. Тези фалшиви личности са били ползвани от членовете на групата с цел получаване на изпратените от жертвите суми.

Получените от тази дейност суми били изпращани в страната чрез услугите за бързи парични преводи, като този път са ползвали фиктивна личност за изпращача и реална за получателя, които имат еднакво име, като се е целяло създаване на грешна представа с оглед на съществуваща семейна връзка.

Субективна страна

Компютърната измама се извършва само с ***пряк умисъл***, който се определя от целта. Действието се извършва с цел получаване на лична материална облага или ползи за друго лице.

За наличието на вина не е необходимо материалната щета да бъде ефективно причинена, а само да е съществувала възможност да бъде причинена и да е била предвиждана от извършителя.

Форми

Подготвителните действия, дори и възможни, не се считат за престъпления и не се наказват.

Опитът се наказва (според чл. 50 на закона). Най-често в този случай няма опит за извършване на това престъпление, а е налице компютърно фалшифициране.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.9. Разпространение на детска порнография чрез компютърни системи

Чл. 51 от Закон 161/2003

Разпространението, предаването, доставянето за себе си или друг на порнографски материали с малолетни чрез компютърни системи, или притежанието без права на порнографски материали с малолетни в една компютърна система, както и съхраняването, производството с цел разпространение, предлагане или предоставяне на разположение на такива компютърни данни, представлява престъпление и се наказва с лишаване от свобода от 3 до 12 години.

Опитът се наказва.

Защитеният правен интерес са обществените отношения, които се борят за закрила правата на малолетните.

Според чл. 35, т. 2,/б.i от Закон 161/2003, под *порнографски материали с малолетни* се разбира всеки материал, който представя малолетно лице с открито сексуално поведение или пълнолетно лице, което е представено като малолетно лице с открито сексуално поведение, или изображения, които макар и да не представят реално лице, симулират по правдоподобен начин малолетно лице с открито сексуално поведение. В чл. 35 се използва и термина „снимки", които дори и да не изобразяват реално лице, симулират по правдоподобен начин малолетно лице с открито сексуално поведение. Аудио записите не представляват „порнографски материали с малолетни" - само видео записите могат да бъдат считани за такива.

В дефиницията на „порнографски материали с малолетни” се прави връзка с откритото сексуално поведение. Това поведение може да означава сексуална поза, също както може да представлява и сексуален акт или всякакво друго поведение, което може да бъде считано за сексуално поведение. Поведението трябва да бъде експлицитно, а не имплицитно, тоест по пряк начин да произлиза от представените изображения, а не да бъде просто намек. Сексуалното поведение на малолетното лице, съдържащо се в съответния порнографски материал, трябва да бъде очевидно. Трябва да се подчертае, че дадена картина, филм, писмено произведение, снимка и т. н. има порнографски характер, ако „развратните” детайли са преднамерено използвани, за да подчеркаят неприличния характер и да отворят пътя на порнографията или проявите на сексуални аномалии.

Субект на престъплението

Активен субект (деец) може да бъде всяко наказателноотговорно физическо лице. В случай на производство с цел разпространение за субекти на престъплението са считани всички лица, които участват в различните етапи на процеса по изготвяне или производство на порнографските материали с малолетни, дори и тези лица, които са служели за модели (във фото сесии, заснемане на филм и т.н.).

Престъплението може да бъде извършено с участие под форма на извършителство, подбудителство или съучастие.

Жертва е малолетното лице, чието порнографско поведение е заснето, съхранено или разпространено чрез компютърните системи.

Обективната страна се състои от много различни начини на изпълнение, и по-точно:

- производство с цел разпространение;
- предлагане;
- предоставяне на разположение;
- разпространение;
- предаване;
- набавяне за себе си или за друго лице на порнографски материали с малолетни;
- притежаване, без право на такова, на порнографски материали с малолетни в една компютърна система или в устройство за съхранение на компютърни данни.

Производството с цел разпространение на порнографски материали с малолетни предполага изпълнение, подбор и комбиниране на тези материали. За наличие на законово нарушение в тази разновидност е необходимо тези материали да са били произведени с цел тяхното разпространение. Ако това не е така, а производството им е за лични цели, съответните действия не представляват материален елемент на нарушението. Все пак, това престъпление ще бъде регистрирано под формата на престъпление за притежание без право на такова, на порнографски материали с малолетни.

Предлагането на порнографски материали с малолетни означава предоставяне на тези материали на друго лице.

Под *предоставяне на разположение* разбираме осигуряване по всякакви начини на достъп, срещу заплащане или безплатно, на порнографски материали с малолетни, както и осигуряване на възможност на дадени лица да разполагат или ползват материалите с порнографски характер.

Разпространението на порнографски материали с малолетни е налице тогава, когато подобни материали са излъчвани или разпространявани по друг начин сред лица, които са ги заявили или до други лица. Дали разпространителят на порнографски материали с малолетни е точно лицето, което ги е произвело или някое друго лице, е без значение. Уточнено е, че в

понятието за разпространение влиза и излагането пред обществеността с/без цел продажба на съответните материали. В случай на разпространение считаме, че става дума за множество действия на предаване, които могат да бъдат едновременни или последователни.

Предаването/трансмисия на материалите, предвидени в инкриминиращата норма, представлява изпращане или/и предаване на обектите, в които са материализирани изображения с малолетни, имащи порнографски характер.

Набавянето за лично ползване или за друг представлява всяко действие, чрез което се придобиват порнографски материали с малолетни (закупуване, наемане, получаване, др.).

Притежаването, без право на такова, на порнографски материали с малолетни се състои в притежаването или съхраняването им, в нарушение на законовите разпоредби. Следователно, законосъобразното притежание на такива материали изключва наказателна отговорност.

За наличие на престъпление, свързано с детска порнография, е необходимо съответните деяния да се отнасят до порнографски материали с малолетни. Без изпълнение на това условие, което представлява отражение на съдържанието на престъплението и спецификата на обекта на престъплението, съответните действия не могат да съставляват обективната страна на споменатото престъпление.

От **субективна страна** престъплението може да бъде извършено както с пряк, така и с косвен умисъл.

Форми

Подготвителните действия, макар и възможни, не са инкриминирани и съответно не са наказуеми.

Опитът се наказва (според алинея 2 на този член).

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.10. Фалшифициране на електронни платежни инструменти

Чл. 24 от Закон 365/2002

Фалшифицирането на един електронен платежен инструмент се наказва с лишаване от свобода от 3 до 12 години и отнемане на някои права.

Със същото наказание се санкционира и използването, по какъвто и да е начин, на фалшифицираните електронни платежни инструменти или притежаването на такива с цел използването им.

Наказанието е с лишаване от свобода от 5 до 15 години и отнемане на някои права, ако предвидените в чл. (1) и (2) действия са извършени от лице, което според спецификата на своите служебни задължения:

- осъществява нужните технически операции за издаване на електронни платежни инструменти или за изпълнение на предвидените в чл. 1, т. 10 операции; или
- има достъп до механизмите за сигурност, приложими при издаване и използване на електронните платежни инструменти; или
- има достъп до данните за идентификация или до механизмите за сигурност при извършване на операциите, предвидени в чл. 1, т. 10.

Защитеният правен интерес обхваща всички обществените отношения, отнасящи се до общественото доверие (от лат. “fides publica”) в сигурността и надеждността на електронните платежни инструменти, като част от целия процес на обработване, съхранение и автоматично прехвърляне на данни и стойности.

Защититен правен интерес е и този на собственика на фалшифицирания електронен платежен инструмент (издаващ орган, финансова институция и т. н.), както и на притежателя или законния потребител на съответния електронен платежен инструмент, разпознат чрез

компютърните данни за идентифициране, съхранени или намиращи се в компютърната система на издаващата институция, както и на търговеца или приемащата банка.

Извършители на престъплението

Активен извършител

Активен извършител може да бъде всяко наказателно отговорно лице – случай ал. 1 и 2. Практиката е показала, че в голяма степен такива лица притежават познания в областта на компютърните технологии. Измежду тях значителен процент са експертите в изчислителните системи или компютърните мрежи, запознати с "пробива" в мерките за сигурност на компютрите или мрежите.

Според разпоредбите в ал. 3 е необходимо извършителят да бъде служител във финансовата институция, издала платежния инструмент или да бъде в някакви договорни отношения с нея, а при изпълнение на служебните си задължения да бъде ангажиран в технически или финансови операции с електронните платежни инструменти (издаване на карти, конфигуриране на данните за идентификация, прилагане на мерки за сигурност и др.).

Участието е възможно под всички форми: извършителство, подбудителство или съучастие.

Пострадал

Пострадал е физическото лице, притежател на права над електронния платежен инструмент или на идентификационните данни.

Също така, съществува и **вторичен пострадал**, или по-точно юридическото лице, собственик на електронния платежен инструмент (съответно – издаващата финансова институция), приемащият търговец или приемащата банка.

Обективна страна

Според условията упоменати в чл. 1, обективната страна се състои във фалшифицирането на електронен платежен инструмент. Според наказателноправната теория фалшифицирането става, по принцип, или чрез *промяна*, или чрез *подправяне* на даден обект.

В най-простата си форма **фалшифицирането на електронния платежен инструмент** представлява *въздействие на извършителя върху празни (неконфигурирани) карти (blank cards)* с помощта на специално предназначени за целта средства за конфигуриране.

Много сериозен проблем за юристите е получаването на нужните данни за конфигуриране (процеса на фалшифициране) на електронния платежен инструмент, когато извършителят е опитал различни технически методи, като: атака чрез обществено инженерство или атака чрез ползване на устройства, които имитират стандартните места, в които са използвани електронния платежен инструмент (*skimming*) и др.

Атаката с ***обществено инженерство*** е свързана с незнанието на потребителите в областта на компютрите и информационното общество. Най-често обществеото инженерство се извършва чрез посегателство върху информацията (подправяне на информация), вариант Фишинг. Превенцията срещу този род атаки е ограмотяване на потребителите.

След набавяне на нужните лични или финансови данни извършителят преминава към изработване на съответния електронен платежен инструмент.

Така наречения Скиминг ('SKIMMING') се проявява най-често сред недоволните служители или служители, които желаят да придобият по незаконен начин парични средства, както и служители, контактуващи с търговци. Въпреки това най-разпространените места са баровете или ресторантите, където клиентите избират да платят с банкови карти и заради удобството ги предоставят на обслужващия персонал за извършване на транзакцията.

В други случаи скимърът изработва специални устройства, които имитират интерфейса на банкоматите, или такива които се прилагат към тях с цел записване (получаване, копиране) на идентификационните данни на картите, въведени от потребителите. Тези устройства са придружени от мини-видео камери, които записват момента на въвеждане на пин кодовете на банковите карти.

От практиката в тази област показва, че фалшифицирането на един електронен платежен инструмент не може да бъде под формата на *изменение*, тъй като всяка промяна в обекта прави инструмента неизползваем и съответно няма условия на извършване на нарушение.

Под *подправяне* се разбира изработване, създаване или имитация на един електронен платежен инструмент. Не е релевантно, дали имитацията е съвършена или пък лоша, тъй като е достатъчно да може да циркулира и взаимодейства със съответните компютърни системи.

Подправянето (фалшифицирането) предполага използване на специално пригодени устройства, подобни на използваните във финансовите институции, които пренасят на магнитната лента на празната карта или съхраняват върху микропроцесор (чип) нужните данните, за да се създаде автентично впечатление, така че фалшификацията да бъде приета от мрежата на финансовите институции или на приемащите търговци.

За реализиране на обективната страна на предвиденото в ал. 1 престъпление, се изисква извършените фалшификации да могат да бъдат в обръщение, тоест да имитират или да се представят за електронни платежни инструменти на пазара в Румъния съгласно Регламента на Националната банка на Румъния, бр. 4 от 2002, спазвайки в същото време и условията за валидност.

Според предвиденото от ал. 2 извършителят действа за пускане в обръщение на един фалшив електронен платежен инструмент или ще притежава съответните фалшиви инструменти с цел на тяхното пускане в обръщение.

С действието *пускане в обръщение* се обозначава въвеждане (независимо за колко време) на фалшиви електронни платежни инструменти в икономическо-финансовата-парична система, изпълнявайки същата икономическа функция като истинските, реалните инструменти. Въвеждането в обръщение в икономическата среда визира кумулативното преминаване на фалшивият инструмент от владение на фалшификатора във владение на друго лице, продажбата или предоставяне на фалшифицираните инструменти на разположение на трети лица.

Притежаване на фалшиви електронни платежни инструменти означава тяхното приемане или запазване с оглед пускането им в обръщение.

В случая на притежание законът установява и второ условие, по-конкретно – притежанието да бъде извършено с цел пускане в обръщение. Липсата на това основно изискване отстранява престъпния характер на притежаването, а извършителят може да подведен под наказателна отговорност само ако са намесени и други елементи на благоприятстване (чл. 264 от НК) или на укриване (чл. 221 от НК) на деянието, според случая.

Ал. 3 на чл. 24 от Закон 365/2002 указа една интересна ситуация, свързана със способностите и уменията на извършителя. Ако е служител на финансова институция, чиято дейност включва издаване на електронни платежни инструменти или е в договорни отношения с подобна институция, в служебните му задължения влиза изпълнение на технически операции или процедури по издаване на карти, или управляването на финансови транзакции или на услуги на информационното общество. Всъщност извършителят ползва същите методи за фалшифициране на електронните платежни инструменти, описани по-горе, но от по-висша позиция, тъй като вече притежава данни (компютърни), отнасящи се до самоличността на лицето, чиито електронни платежни инструменти е фалшифицирал - банкова сметка, име за идентификация на инструмента и др.

Казус:

Прокурорите от Дирекция за разследване на престъпленията на организираната престъпност и тероризъм – Регионална дирекция в гр. Сучява – са предприели наказателнопроцесуални действия и са издали заповед за задържане за 24 часа на обвиняемите К. Н., Н. Д - А, Л. А - М, двамата от окръг Константа, разследвани, заедно с други лица, по наказателно дело за съставяне на организирана престъпна група с цел извършване на престъпления по измама с особено сериозни последствия.

Де факто, на обвиняемите К. Н. и Н. Д – А е повдигнато обвинение, че от началото месец май 2007 г. са сключили договори за банкови кредити с фалшиви документи, изработили са и притежават оборудване за фалшифициране на електронни платежни инструменти и са фалшифицирали инструменти за електронно плащане, при извършителство, но и под формата на подбудителство и съучастие, като щетите до този момент се оценяват на 2,5 милиарда леи. Все пак в хода на делото е извършена и първата оценка на щетите в резултат на извършване на действията на компютърното престъпление, достигайки сумата от 7.500 euro.

Третият обвиняем Л. А – М е обвинен в съучастие в престъпление по измама в особено голям размер и фалшифициране на информация, действия които се отличават с това, че са замесени много лица и са фалшифицирани документи за получаване на банкови кредити чрез измама, в което е намесил и фирма 'SC SMART CONCEPT' ООД - Константа, в която е управител и съдружник.

Наказателното дело започва през август 2007 г., следвайки разделянето от друг случай в компетенциите на разследване на прокурорите от Дирекция за разследване на престъпленията на организираната престъпност и тероризъм, като са осъществени две престъпления – трафик на хора и кибернетично престъпление, за които на извършителите е наложена мярка за неотклонение - предварителен арест.

Според прокурорското разпределение и издадената заповед за домашен обиск от съдебната инстанция, прокурорите заедно със служителите от Бригадата за борба с организираната престъпност и Анти-дрога от областите Сеучява и Константа са конфискували серия подготвителни документи за фалшифициране на използваните документи за измама на банките, както и устройства за клониране на карти, от общо 12 адреса, на които живеят обвиняемите.

Субективна страна

Престъплението фалшифициране на електронни платежни инструменти се извършва с **пряк или косвен умисъл** (за всеки от предвидените случаи в ал. 1, 2 или 3).

Форми

Подготвителните действия, макар и възможни, не са инкриминирани и като такива, не са наказуеми (виж Skimming-а).

Определени подготвителни действия могат да бъдат считани за престъпления сами по себе си, напр. според чл. 46 „Незаконни операции с устройства или компютърни програми" (в определени случаи) или чл. 49 „Компютърно фалшифициране" от Закон 161/2003.

Колкото до „кражбата на самоличност", това е по-скоро концепция, за която досега не е приета наказателноправна норма, макар че се среща доста често.

Опитът се наказва, според разпоредбите на ал. 4 от този член.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.11. Притежаване на оборудване за фалшифициране на електронни платежни инструменти

Чл. 25 от Закон 365/2002

Изготвянето или притежаването на оборудване, включително хардуер или софтуер, с цел фалшифициране на електронни платежни инструменти се наказва с лишаване от свобода от 6 месеца до 5 години.

Защитен правен интерес

Обществените отношения, касаещи общественото доверие в сигурността и надеждността на електронните платежни инструменти.

Извършители на престъплението

Активен субект

Свързваме го с всяко наказателноотговорно физическо лице, което е извършило подобно деяние. Субектът ще бъде подведен под отговорност за извършените от него деяния, свързани с осъществяваната от него дейност или в негов интерес, ако те са извършени при наличието на предвидената в закона форма на вина.

Участието е възможно във всичките му форми: извършителство, подбудителство или съучастие.

Пострадал

Това е банковата институция – кредитна или финансова, или оторизирана от лицето единица, която при изпълнение на законовите разпоредби издава електронни платежни инструменти или извършва операции с тях.

Обективната страна се състои било в едно действие на изработване или в притежание на определено оборудване (хардуер или софтуер) за посочената в закона цел.
В този контекст имаме налице подготвителна дейност за извършване на определеното в чл. 24 престъпление, обаче, като самостоятелно престъпление имайки предвид високата му степен на обществена опасност.

Действието по *изработване* предполага производство по всякакъв начин, производство на инструменти, извършване на адекватни операции за получаване на електронните, електромеханичните устройства и компютърни приложения, които са необходими за операциите по фалшифициране на електронните платежни инструменти.

Притежаването предполага съхранение, придобиване, укриване или транспортиране на нужното оборудване в рамките на дейността по фалшифициране.

Основно изискване за наличие на престъпление е оборудването или създадените компютърни приложения, изработени или придобити с цел фалшифициране на електронни платежни инструменти, да бъдат годни за това от техническа гледна точка.

Субективна страна

Престъплението по фалшифициране на електронни платежни инструменти инструменти се извършва с **пряк умисъл** според целта.

Ако изработеното или придобито оборудване или създадените компютърни приложения са използвани с цел фалшифициране на електронни платежни инструменти, с други думи – ако набелязаната от извършителя цел е постигната, тогава е налице съвкупност от престъпления и наказателно обвинение ще бъде повдигнато, както за изработването или притежанието на оборудване за фалшифициране, така и за самото фалшифициране.

Форми

Престъплението може да премине през всички присъщи на едно умишлено деяние, тоест от подготвителни действия, опит, извършване, завършване, но законовият текст инкриминира само завършеното деяние.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.12 Невярно деклариране във връзка с издаване или използване на електронни платежни инструменти

Чл. 26 от Закон 365/2002

Невярното деклариране на данни пред банка, пред кредитна или финансова институция или пред който и да е друг субект, който е упълномощен съгласно закона да издава електронни платежни инструменти или да приема операциите, предвидени в чл. 1, т. 10, с цел издаване или ползване на даден електронен платежен инструмент, се наказва с лишаване от свобода от 3 месеца до 2 години или с глоба.

Защитен правен интерес

Състои се в обществените отношения, свързани с доверието към направените декларации пред банката, пред кредитната или финансовата институция, упълномощени да издават и управляват електронни платежни инструменти, както и към декларации, които могат да породят правни или икономически последци.

Активен субект

Може да бъде всяко наказателноотговорно физическо лице, което е упълномощено или може да прави декларации, които създават правни последици.

Активен субект може да бъде и друго лице, тогава когато актът извършен от името или в негова полза от страна на неговите органи или представители.

Участието може да бъде във всякаква форма: извършителство, подбудителство или съучастие.

Пострадал

Това е физическо или юридическо лице, чиито юридически или финансови интереси са били накърнени с извършване на това действие.

Също така, съществува и **вторичен пострадал**, или по-точно, това е юридическото лице собственик на електронния платежен инструмент (съответно - издаващата финансова институция).

Обективната страна се реализира чрез подаване на декларация, която частично или изцяло не отговаря на истината.

Декларацията може да бъде направена по инициатива на дееца (който има намерение да получи електронния платежен инструмент) или по искане на финансовата институция (като стандартна процедура, необходима за издаване на електронния платежен инструмент), по принцип – писмено и пряко, на румънски език или евентуално на някой друг от официалните в езици на Европейския съюз.

Ако декларацията предполага дадена процедура или определени формални условия по отношение на начина, по който се приема такава декларация, неспазването на тези изисквания може да изключи приложението на наказателния закон.

Основно изискване за наличие на престъпление е декларацията да бъде направена пред банка, пред кредитна или пред финансова институция или пред друго лице, което е упълномощено от закона да издава електронни платежни инструменти.

Също така необходимо е декларацията с невярно съдържание да бъде годна, според закона и обстоятелствата, да породи правните или икономически последици, които деецът цели. Ако невярната декларация не може да служи за пораждане на последиците или е оттеглена преди да бъде обработена, тогава деянието няма да се счита за престъпление.

Пример за такова деяние е влизането във владение на банковата сметка на друго лице (‘ACCOUNT TAKEOVER’). Извършителят получава достатъчно лични данни за едно лице

(чрез предварително получаване на фактури, касови бележки, дубликати на квитанции след плащане с картата и т.н.) и след това се представя за това лице в отношенията (косвено с цел сигурност) с финансовата институция. Под някакъв претекст изисква от банката цялата електронна кореспонденция да му бъде доставена на имейл адрес под негов контрол и, евентуално, дори отбелязва промяна на домашния адрес.

След това обявява, че е загубил картата и иска издаване на нова карта, на новия адрес. За жалост по света има много банк, кредитни и финансови институции, които като част от услугите на информационното общество или заради грижа към клиента изпращат по куриер електронните платежни инструменти, което ги прави силно изложени на риск от достъп от страна на измамници.

Субективна страна

Престъплението по фалшифициране на електронни платежни инструменти се извършва с **пряк умисъл**, квалифициран според целта (без да бъде нужно тази цел да е ефективно реализирана).

Форми

Престъплението може да премине през фаза на подготвителни действия, на опит и на извършване.

Подготвителните действия и опитът не са инкриминирани и следователно не са наказуеми.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.13. Измамни финансови операции

Чл. 27 от Закон 365/2002

(1) Извършване на някоя от операциите в чл. 1, т. 10 чрез използване на електронен платежен инструмент, включително и на идентификационните данни, които позволяват неговото използване без съгласието на титуляра на съответния инструмент, се наказва с лишаване от свобода от 1 до 12 години.

(2) Със същото наказание се наказва и извършването на някоя от операциите, предвидени в чл. 1, т. 10 чрез неупълномощено използване на идентификационните данни или чрез използване на фиктивни идентификационни данни.

(3) Такова е и наказанието при неупълномощено предаване на друго лице на идентификационни данни с оцел извършване на някоя от операциите по чл. 1, т. 10.

(4) Наказанието е лишаване от свобода от 3 до 15 години и отнемане на определени права, ако предвидените в ал. 1 - 3 деяния са извършени от лице, което във връзка с изпълнение служебните си задължения:

a) осъществява нужните технически операции за издаване на един електронен платежен инструмент или за извършване на някоя от предвидените в чл. 1, т. 10 финансови операции.

b) има достъп до механизмите за сигурност, въведени при издаване на електронните платежни инструменти, или

c) има достъп до идентификационните данни или до механизмите за сигурност, въведени за извършване на някоя от предвидените в чл. 1, т. 10 операции.

Защитеният правен интерес

Състои се в обществените отношения, свързани с общественото доверие в сигурността и надеждността на компютърните системи, във валидността и истинността на компютърните данни, на целия процес на обработка, съхранение и автоматичен пренос на данните от личен или обществен интерес.

Защитен правен интерес е и интересът на собственика на електронния платежен инструмент (издаващ, финансова институция и др.), но и на законния притежател или потребител на съответния инструмент, идентифициран чрез компютърните данни, които са запазени или са в обръщение в компютърната система на издаващата институция.

Субект на престъплението

Активен субект

Може да бъде всяко наказателноотговорно физическо лице – в случая на ал. 1, 2 и 3. В условията на ал. 4 е необходимо извършителят да бъде служител в издаващата финансова институция или да е в договорни отношения с нея и във връзка с това негово качество да участва в извършването в технически или финансови операции с електронни платежни инструменти (издаване на карти, конфигуриране на идентификационни данни, въвеждане на мерките за сигурност и др.)

Участието е възможно във всичките му форми: извършителство, подбудителство или съучастие.

Пострадал

Това е физическото лице и законен притежател (титуляр) на електронните платежни инструменти или на данните за идентификация.

Съществува, обаче, и **вторичен пострадал** – юридическото лице – собственик на електронните платежни инструменти (съответно – издаващата финансова институция)

Обективна страна

По смисъла на ал. 1 се осъществява чрез действие за ползване на един електронен платежен инструмент и на прилежащите данни за идентификация (ПИН код, потребителски код, други референции) на някой от терминалите, предвидени от Регламента на Националната банка на Румъния 4/2002, без съгласието на законния титуляр. Връзката между електронния платежен инструмент и идентификационните данни е асоциативна, в зависимост от техническите детайли на местоположението (терминала), където се използва ефективно инструментът. Има ситуации, при които определени търговци използват POS терминали (например), които са настроени да не изискват идентификация на ползващото картата лице чрез въвеждане на ПИН код.

При условията на ал. 2, обективната страна се състои в трансфер на парични суми, теглене в брой или зареждане/изпразване на един инструмент за електронно плащане при условия, при които извършителят използва фиктивни идентификационни данни – по неупълномощен начин.

Ал. 3 предвижда неупълномощено изпращане на данни за идентификация към друго лице, с изричното изискване разпространението на тези данни да бъде с цел паричен трансфер, теглене в брой или захранване/изпразване на дадена стойностна единица, съхранена в електронен платежен инструмент.

Обективната страна по ал. 4 е подобен на вече изброените, като в този случай участието на извършителя е утежняващ елемент.

Пример за измамна финансова операция с електронни платежни инструменти е CARDING-а. Този термин е използван по принцип, за да се дефинира процеса на валидация на прилежащите към един електронен платежен инструмент идентификационни данни. По този начин извършителят представя данните на картата на някоя специализирана Интернет страница, която разполага с опция за извършване на плащания в реално време. Ако електронния платежен инструмент бъде разпознат в системата, извършителят ще бъде сигурен, че този инструмент е валиден и може да бъде ползван. Като цяло се избират услуги или продукти с малка стойност или се извършват електронни плащания на сайтове за електронна търговия с цел да се избегне сигнализиране на измамата към издаващата финансова институция.

Най-много измамни финансови операции се случват в Интернет. Електронната поща и Интернет са между основните пътища за измами към търговците, които продават или транспортират продукция, ползвайки възможностите на електронната търговия. Използваният термин в профилираната индустрия за покупки по каталог или за други подобни транзакции е CNP – Card Not Present, което означава, че не е нужна физическата проверка на електронния платежен инструмент. При тези условия търговецът се доверява изключително на доставените от притежателя на картата данни (или на лицето, което се представя за титуляр на картата), по телефона, електронна поща или онлайн формите или върху формулярите, публикувани в Интернет страниците, когато евентуалният купувач не се намира пред POS терминал. За продавача е трудно да провери на момента дали притежателят на картата законно оторизира транзакцията, а транспортните компании (shipping), например, гарантират само доставка на продуктите в добри условия на посочен адрес, като не изискват проверка самоличността на лицето, които ги получава.

Добре известно е, че електронните транзакции с малка стойност не се подлагат автоматично на проверка и има малка вероятност след това да бъдат разследвани от банковата институция или от съответния търговец, най-вече заради разликата в цената между евентуалната измама и стойността на самата операция по разследване.

Субективна страна

Престъплението измама с финансови операции се извършва с **пряк** или **косвен умисъл.**

Форми

Опитът се наказва според разпоредбите на ал. 5 от същия член.

Изпълнителното деяние е завършено по смисъла на ал. 1 с осъществяване на начално взаимодействие на съответния електронен платеже инструмент с компютърната система (в това число операции на гише, на стандартнен терминал катоPOS, ATM и др.) на банката, на кредитната или финансовата институция.

По предвидения начин в ал. 2 и 3 изпълнителното деяние е завършено, когато реалните идентификационни данни са били използвани или изпратени по неупълномощен начин, съответно – когато извършителят избира да ползва неотговарящи на действителността идентификационни данни.

По ал. 4 изпълнителното деяние е завършено в момента, в който данните, до които има достъп извършителя, поради дейност му в рамките на финансовата институция, са използвани за реализиране на паричен превод, теглене в брой или захранване/изпразване на електронния платежен инструмент.

Процесуални аспекти

Наказателното преследване започва по служебен път.

3.3.14 Приемане на извършени чрез измама финансови операции

Чл. 28 от Закона 365/2002

Приемането на някоя от описаните в чл. 1, т. 10 операции, със знанието, че тя се извършва с използване на фалшифициран електронен платежен инструмент или инструмент, който се ползва без съгласието на титуляра му, се наказва с лишаване от свобода от 1 до 12 години.

Със същото наказание се наказва и приемането на операции по чл. 1, т. 10, със знанието, че те се извършват с неупълномощеното използване на идентификационни данни или чрез използване на фиктивни идентификационни данни.

Защитен правен интерес

Състои се в обществените отношения, свързани с общественото доверие в сигурността и надеждността на компютърните системи, във валидността и истинността на компютърните данни, на целия процес на обработка, съхранение или автоматичен пренос на данните и парични фондове в рамките на банките, кредитните и финансовите институции, или от приемащите търговци.

Активен субект

Това е физическо лице, служител или лице в договорни отношения с банката, кредитината или финансовата институция, или с търговеца, и/или лицето, което въз основа на заеманата от него длъжност е отговорно за успешното осъществяване на финансовите операции, за които се ползват електронни платежни инструменти.

Участието е във всичките му форми: извършителство, подбудителство или съучастие.

Пострадал

Това е физическото лице, законен притежател на фалшифициран електронен платежен инструмент или на идентификационните данни, които са използвани без упълномощаване.

Има също така и вторичен пострадал, и това е юридическото лице – собственик на електронните платежни инструменти (съответно, издаващата финансова институция).

Обективната страна се реализира чрез приемане на една електронна финансова транзакция (паричен превод, теглене в брой и т.н.), със знанието, че тя е извършена с фалшив електронен платежен инструмент, без знанието на действителния титуляр или чрез използване на фиктивни идентификационни данни или пък на реални данни, но без изрично упълномощение .

Под *приемане* се разбира иницииране, извършването или одобрението на процедурата по извършване на транзакцията. Когато се отнася за търговци е налице ситуация, при която касиер *приема* използването на фалшифа карта чрез ползване на POS терминал, *приема* въвеждането на идентификационни данни (за които знае, че са използвани по неупълномощен начин или че са фиктивни), или *не прекъсва извършването на транзакцията.*

Когато се отнася за банки, кредитни или финансови институции, са налице упълномощени оператори, в чиито служебни задължения е управлението (одобрение на плащанията) на финансовите операции по електронен път.

Субективна страна

Престъплението се извършва само **с пряк умисъл.**

Форми

Подготвителните действия, макар и възможни, не се считат за престъпление и като не са наказуеми.

Опитът се наказва по ал. 3 на същия член.

Престъплението може да бъде извършено и в реална съвкупност с други престъпления като подпомагане на извършителя (предвидено и санкционирано от чл. 264 на НК), съответно – измамно управление (предвидено и санкционирано от чл. 214 на НК).

Процесуални аспекти

Наказателното преследване започва по служебен път.

Интересен елемент на тези престъпления е един нов аспект – организирания им и комплексен характер. Практиката показва, че много често типичните за електронната търговия престъпления се намират в истинско съревнование с компютърните престъпления и с тези на организираната престъпност.

3.3.15. Противоречиви аспекти. Предложения за "lege ferenda"

Практиката показва, че компютърните престъпления доказват, че в настоящия момент в Румъния е приет и се прилага комплекс от наказателни норми, които покриват най-често срещаните обществеоопасни деяния, свързани с компютърните системи.

Все пак, от анализа на разгледаните казуси можем да заключим, че на общо ниво, разпоредбите на Закон 161/2003 или 365/2002 са интерпретирани по спорен начин от страна на прокурори и съдии, които разбират по-малко техническите елементи на престъпленията – факт, който рефлектира негативно върху прецизността на наказателния процес и често тези ситуации могат да означават "спасителна врата" за извършителите на кибернетични престъпления.

3.3.15.1. Скиминг

По отношение на т.нар. Скиминг внимателният анализ показва, че това деяние може да бъде обхванато (някак пресилено) от разпоредбите на чл. 24 от Закон 365/2002 за електронната търговия като предшестваща форма на фалшифициране на електронен платежен инструмент, но не и към незаконен достъп до компютърна система (чл. 42 от Закон 161/2003), което може да се изведе и от анализа на следния казус:

Висшия касационен съд, Наказателно отделение, Решение номер 5288 от 15 септември 2006 год.

С наказателна присъда No 21/2006 на Съда в Хунедоара са осъдени обвиняемите К.К., Г.М., Т.И. и И.Ф. за извършване на престъпление срещу конфиденциалността и целостта на данните и компютърните системи, по чл. 42 ал. (1) и (3) от Закон 161/2003, за фалшифициране на електронни платежни инструменти по чл. 24 ал. (1) от Закон 365/2002, за фалшифициране на електронни платежни инструменти по чл. 24 ал. (2) от Закон 365/2002, за престъпления по извършване на измамни финансови операции по чл. 27 ал. (1) от Закон 365/2002 и за престъпление по квалифицирана кражба, предвидено в чл. 208 ал. (1), чл. 209 ал. (1) буква. a) и e) от НК, всички с прилагане на Чл. 41 ал. (2), ал. 33, буква a) и b) и чл. 34 ал. (1) буква b) от НК.

Съдът е отбелязал, че през месец май 2005 год, обвиняемите са се разбрали да използват четящи устройства за магнитните ленти на картите и една мини камера, предварително набавени, с цел да получат нужните данни за клониране на карти и извършване на теглене в брой.

За тази цел, обвиняемите няколко пъти са се местили на различни места, монтирали са устройствата и камерата на много банкомати, като така са получавали данните за ползваните карти на тези банкомати, след което са ги сваляли на компютър в дома на един от тях.

След получаване на всички данни и тяхното съхранение в компютър, виновниците са купували некриптирани карти и са залепяли върху тях етикет с кода или кодовете PIN, разчетени предварително с мини камерата. След което от компютъра на И.Ф. с приложено устройство за електронно записване са конфигурирали кода върху магнитната лента на картата чрез въвеждане на код, който съответства на копирания преди това PIN код, записан върху етикета.

На 28 юни, на 7 юли, на 8 юли, на 11 юли и на 21 юли 2005 год., виновните са теглили в брой с помощта на клонираните карти от банкомати на много банки.

С Решение номер 197/A от 22 юни 2006 год., Апелационния съд в гр. Алба Юлия, Наказателно отделение, е приел внесеното обжалване на виновните лица и като променя юридическото определяне на престъпленията според чл. 27 ал. (1) от Закон 365/2002 и чл. 208 ал. (1), чл. 209 ал. (1) бук. a) и e) от НК, с прилагане на чл. 41 ал. (2) на същия член, в едно единствено престъпление по смисъла на чл.. 27 ал. (1) от Закон 365/2002, с прилагане на чл. 41 ал. (2) от НК, и осъжда обвиняемите на основание на последните текстове, като намаля наложените им наказания.

Внесеното обжалване, наред с другите, от обвиняемия К.К., с което е поискал касиране на случая, предвиден в чл. 385[9] ал. (1) т. 12 С. наказателен процес., е неоснователно.

По отношение на молбата на К.К., с която се иска оправдателна присъда въз основа на чл. 11 т. 2 бук. а) отнесено към чл. 10 ал. (1) бук. d) НПК, за престъпленията предвидени в чл. 42 ал. (1) и (3) от Закон 161/2003 с прилагане на чл. 41 ал. (2) от НК и чл. 24 ал. (2) от Закон 365/2002, във варианта на пускане в обръщение на фалшиви електронни платежни инструменти, с прилагане на чл. 41 ал. (2) от НК, се констатира, че искането не е основателно.

Разпоредбите на чл. 24 ал. (1) от Закон 365/2002 предвиждат, че фалшифицирането на електронен платежен инструмент се санкционира с лишаване от свобода от 3 до 12 години и отнемане на някои права, а чл. 24, ал.(2) на същия закон се инкриминира пускането в обръщение по какъвто и да е начин на фалшиви електронни платежни инструменти или притежаването на такива с цел пускането им в обръщение.

От изследването на обективната страна на тези действия произтича, че съществуват две различни престъпления, като първото се отнася за фалшифициране на електронни платежни инструменти, а второто – за пускане в обръщение по какъвто и да е начин на фалшиви електронни платежни инструменти или притежаването на такива с цел пускането им в обръщение.

В конкретния гореспоменат случай, пускането в обръщение на електронните платежни инструменти е станало чрез теглене в брой, без да се налага прехвърлянето им на фалшифицираните на други лица. От друга страна, деянията на четиримата обвиняемите, които на базата на същите престъпни похвати, са фалшифицирали около 200 електронни платежни инструменти, и по този начин съответстват на обективната страна на престъплението фалшифициране на електронни платежни инструменти, предвидено в чл. 24 ал. (1) на Закон 365/2002, с прилагане на ал. 41 ал. (2) от НК.

Също така, действията на обвиняемите, който на базата на престъпни методи, са придобили електронни платежни инструменти с цел ползване, включват елементи от съставите на престъпления за фалшифициране на електронни платежни инструменти, предвидени от чл. 24 ал. (2) на Закон 365/2002, с прилагане на чл. 41 ал. (2) от НК.

Разпоредбата на чл. 42 ал. (1) на Закон 161/2003 инкриминира достъпа, без право на такъв, до компютърна система, който се наказва с лишаване от свобода от 3 месеца до 3 години или с глоба, а ал. (3) на същия член предвижда, че ако действието от ал. (1) е извършено чрез нарушаване на мерките за сигурност, наказанието за това е лишаване от свобода от 3 до 12 години.

Уточнява се фактът, че банкоматът е начин за събиране, обработване и предаване на компютърни данни, представени от номера на сметката на титуляра, които се съхраняват на ниво 2 на магнитната лента с черен цвят.

От друга страна чрез монтиране на четящо устройство за магнитните ленти на картите („skimmer") в слот-а на банкомата, през който се вкарва картата, се разчита магнитната лента, а получената информация се запазва, като така се нарушават мерките за сигурност за защита на номера на сметката и на извършените операции, както и борбата с ползването от друго лице на тези карти, с цел измама.

Може да се каже, че от практиката по това дело следва, че виновните са влезли в компютърна система, като по този начин са нарушили мерките за сигурност.

Следователно, действията на обвиняемите, които са монтирали на различни банкомати устройства за събиране на информацията от магнитните ленти и камера за наблюдение, като по този начин са влезли без право на това в системите на банките, чрез нарушаване на мерките за сигурност. Мрежата от банкомати представлява компютърна система в широк смисъл, и по този начин в престъплението се откриват съставни елементи за нарушаване на конфиденциалността на данните и целостта на компютърните системи според чл.42, ал. (1) и (2) на Закон 161/2003, с прилагане на чл. 41 ал. (2) от НК.

В конкретния случай извършените от обвиняемия К.К. действия съдържат елементи на престъплението по чл. 42 ал. (1) и (3) на Закон 161/2003, с прилагане на чл. 41 ал. (2)от НК и чл. 24 ал. (2) на Закон 365/2002 по отношение на електронната търговия, във варианта за пускане в обръщение на електронни платежни инструменти, с прилагане на чл. 41 ал. (2) от НК, няма не е имало основание за плащане в изискания смисъл.

Заради тези законови основания, обжалването на осъденото лице не е прието.

В този конкретен случай считаме, че Висшият касационен съд е отхвърлил по неоснователен начин жалбата на обвиняемите по отношение повдигането на обвинение за техните деяния на основание разпоредбата на чл. 42 ал (3) от Закон 161/2003, Раздел III – превенция и борба с компютърните престъпления, съгласно която достъпът, без право на такъв, до една система, с цел получаване на компютърни данни, чрез на въздействие върху мерките за сигурност, се санкционира лишаване от свобода от 3 до 12 години.

Можем да се съгласим, че с включването на банкоматите (ATM и др.) в категорията на компютърните системи, от техническа гледна точка те отговарят на изискванията, за да бъдат възприемани като такива. Въпреки това единствените елементи за сигурност на банкоматите са от логически тип, т.е. става дума за компютърни приложения, които проверяват валидността на една карта на базата на математически функции, преобръщат стойности като "истински" и "фалшив" за комбинацията от запазени данни върху магнитната лента на картата или получени чрез въвеждане на PIN кода от притежателя. Нарушаването на мерките за сигурност предполага директно взаимодействие на извършителя с това устройство или спрямо математическата функция, което е почти невъзможно от гледна точка на един *skimmer*.

В анализирания казус извършителят добавя към интерфейса, от пластмасов материал или метал, на банкомата едно специално устройство за обърквване на потребителите, като им създава представа, че се намират пред действителен банкомат и по този начин използва собствените им карти чрез изведената информация от тях. Извличането на данните от картите, включително тяхната обработка и комбиниране с уловените от мини камерата видео-изображения по време на въвеждане на PIN кодовете, което се осъществяват на по-късен етап.

Считаме, че тук става дума по-скоро за приложение на концепциите за обществено инженерство или за подготовка за фалшифициране на електронен платежен инструмент, а не за незаконен достъп до компютърна система чрез нарушаване на мерките за сигурност.

По отношение на същото действие на *skimming* някои специалисти са лансирали и идеята за наличие на престъпление "нелегално прихващане при предаване на компютърни данни" по чл. 43 от Закон 161/2003. Ние считаме, че това решение е погрешно, тъй като от техническа гледна точка в този случай не съществува предаване на компютърни данни в смисъла, предвиден от румънския закон. В главата, отнасяща се до "Компютърни престъпления", обяснихме какво се случва когато се улови/предаде поток от данни.

При *skimming*, практически, прихващането и "четенето" на данните от магнитната лента става преди картата да влезе в слот-а на банкомата и преди осъществяването на трансфер на компютърните данни между картата и ATM. Ако, например, устройството за *skimming* е разположено вътре в банкомата и така улавя трансфера на данни между магнитната лента и четеца на ATM, тогава бихме могли да считаме това за прихващане на една трансмисия и отнасяме случая към чл. 43 на Закон 161/2003, също, към незаконен достъп до компютърна система (банкомат) по чл. 42 на същия закон.

Следователно, считаме че в настоящия момент в Румъния, с актуалните юридически инструменти, обикновеният акт на Skimming не може да бъде лесно квалифициран като престъпление и по този начин не може да бъде санкциониран като такова (някои подготвителни действия в извършването на това престъпление може да съдържат елементи на друго престъпление). Все пак особено големият брой на деяния от този тип налага нуждата от съставяне на инкриминираща норма, като нейното систематично място може да

бъде само в съдържанието на чл. 24 от Закон 365/2002 (където се открива раздела за този вид нарушения от областта на компютърните престъпления). В този смисъл за внасяне на подобрения за Закон 365/2002 можем да предложим следния текст, който по наше мнение ще определи по категоричен начин престъпния характер на всяка форма на *skimming*:

Получаването, чрез измама, включително чрез ползване на специално създадени за тази цел технически устройства, или чрез използване на електронните средства за комуникация (телефон, факс или компютърни системи), на всякакъв род данни или информация, които са свързани с определен електронен платежен инструмент или банкова сметка, представлява престъпление и се наказва с лишаване от свобода от 6 месеца до 1 година.

3.3.15.2. „Кражба на самоличност"

Както много други страни и Румъния се сблъсква все по-често с един феномен от особена сериозност, който също изисква специално внимание от страна на законодателя: ***"кражбата на самоличност" чрез помощта на средствата за електронна комуникация.***

Като понятие *кражбата на самоличност* е едно безлично наименование, защото самоличността на едно лице на практика не е "откраднатa", а просто се дублира (утроява, и т. н.).

Въпреки това, получаването по незаконен начин на тази информация (често лични данни), която може директно да идентифицира едно физическо лице без неговото съгласие чрез въвеждане в заблуда или при неспазване на работните си задължения на от страна на служителите, споменати в Закон 677/2001 (за обработване на личните данни и свободното им движение), може да създаде сериозни нарушения, най-вече от финансов характер, но не само.

Например, можем да считаме за добре познато деянието, познато като „Фишинг". Понастоящем това деяние се наказва в съответствие с разпоредбите на чл. 48 на Закон 161/2003, който регламентира *компютърната измама*.

Казус:

Прокурорите от Дирекцията за разследване на престъпленията на организираната престъпност и тероризъм, приема на 16 май 2008 г., от страна на юридическите органи в САЩ, молба да се извърши разследване за установяване членовете на престъпна групировка в Румъния, както и установяване на IP адрес, извършване на домашен обиск (които бе извършен днес – 19 май 2008 год.) на седем места - в градовете Букурещ, Крайова, Каракал и Бузау.

На практика Прокуратурата на Калифорния – DC и ФБР започва разследване по отношение на дейността на една група за организирана престъпна дейност, занимаваща се с кражба на самоличности, измами и компютърни престъпления.

По този начин американските власти подвеждат под отговорност на 15 май 2008 год. лицата: С.А.П., Ш.С.И., М.К., И.Н., П.Б.Б. и други за извършване на престъпления и организиране на група с престъпна дейност, фалшифициране на електронни платежни инструменти, притежание на оборудване с цел фалшифициране на електронни платежни инструменти и осъществяване на неоторизиран достъп.

Тази престъпна група извършва престъпни дейности за измама, чрез ползване на фалшиви електронни платежни инструменти за генериране на парични преводи.

Членовете на престъпната група са получили хиляди банкови сметки и свързани с Интернет кредитни/дебитни карти, използвайки метода за извършване на измами, наречен „pshishing-ul". Те са изпращали по Интернет на евентуалните жертви на измамата и притежатели на сметки съобщения от определена Интернет страница, наподобяваща легитимната Интернет страница на банковата или финансова институция. Притежателите на карти са били поканени да въведат данните за достъп до сметката и други лични данни ***във*** *или* ***чрез*** *тази страница.*

Съучастниците на извършителите, които са създали и управлявали Интернет страниците за „pshishing" и са изпращали съобщения по имейл, спам или други съобщения,

свързани с измамата, са локализирани в Румъния и в други държави и са си сътрудничили с участниците в САЩ, включително с лидерите - главни заподозрени за престъплението, в конкретния случай, лицата S. W. L. и H. T. T. Последните са използвали данните, доставени от обвинените в Румъния лица, за създаване на устройства за достъп (карти) и за да получат достъп и да теглят пари в брой от сметките на жертвите, действайки като "инкасатори"и координатори на самоличностите и на измамните устройства за достъп, за да могат да теглят пари в брой от банкомати и за пазаруване на стоки и услуги чрез терминалите за купуване. Като общо правило получените продукти са били разделяни на равни процентни стойности между съучастниците в Румъния, които са доставяли данните от устройствата за достъп.

Размерът на щетите са изчислени на стойност над 1 милион щатски долара.

Все пак един внимателен анализ на престъплението ни показва ясно, че само един от етапите на явлението Фишинг може наистина да бъде включен в рамките на компютърна измама, по-точно – създаването на фалшивата Интернет страница, с цел да се заблудят потребителите, че влизат в истинската страница на съответната институция.

В случаите на Фишинг, обаче, важен компонент е съобщаването на данни по имейл, тъй като в този момент потенциалните жертви са подмамени (чрез добре изготвени съобщения по електронната поща) да използват фалшивата страница или да съобщят своите лични и финансови данни. Понастоящем от законова гледна точка това действие (за подмамване на потребителите) се попада в обхвата на обективната страна на престъплението компютърно фалшифициране, но ние твърдим, че съществуването (създаването) на самостоятелна инкриминираща норма би могла да бъде много полезна и ще предложи на разследващите органи една много по-обхватна юридическа база за борба срещу компютърните престъпления.

В този смисъл искаме да направим следното законово предложение (по-обхватно):

Получаването на всеки вид информация, чрез която може пряко да се идентифицира едно лице, без негово съгласие или пък чрез заблуда, и ако е извършено чрез използване на съобщителна техника, или чрез използване на компютърни системи, или телекомуникации, представлява престъпление и се наказва с лишаване от свобода от X до Y години.

Или

Получаването на всеки вид информация, чрез която електронния платежен инструмент на дадено лице, може да се идентифицира директно, без съгласието на това лице или пък чрез въвеждане в заблуда, и ако действието е извършено с помощта на съобщителна техника, чрез използване на компютърни системи, или телекомуникации, представлява престъпление и се наказва с лишаване от свобода от X до Y години.

Ако действието в ал. 1 е било извършено чрез използване на електронни или електромеханични устройства, специално разработени за прихващане и запазване на данните в аудио, видео или електронен (skimming) формат, наказанието с лишаване от свобода от X до Y години.

От гледна точка на законодателната техника, считаме за препоръчително включването в съдържанието на Закон 161/2003 на подобен текст или комбинация от двата текста, посочени по-горе.

3.3.16. Заключения

При разследването на престъпления в една толкова бързо развиваща се област, както настоящия пример с компютърните престъпления, е ясно, че не само натоварените с прилагането на закона трябва да бъдат в течение с последните новости, но и всеки участник в обществените отношения, заинтересуван от този проблем. Законът, дори и да следва технологична неутралност, трябва да може да покрива основните незаконни действия, които се осъществяват във виртуалното пространство. В този смисъл авторите на това изследване отрито подкрепят идеята за необходимост от по-често дискутиране на темите, свързани с

тези проблеми, в което да участват не само директните участници в борбата срещу компютърните престъпления, а и лица от частния сектор, академичните среди и като цяло всеки, който е част от гражданското общество и би могъл да внесе друга перспектива на национално, регионално или международно ниво.

4. Международни инициативи за противодействие на компютърната престъпност

Поради специфичния си обект на посегателство или средство за извършване на деянието - информационните технологии, компютърните престъпления много често имат трансграничен характер. Бързото развитие и разпространение на тези технологии позволява на извършителите на престъпления, намиращи се в една държава, да извършват посегателства срещу обекти, намиращи се в една или повече други държави. Трансграничният характер на компютърната престъпност затруднява нейното разкриване и наказване само посредством националните законодателства на отделните държави и налага съсредоточаването на все повече усилия към създаването на международни инструменти за превенция и противодействие на това явление.

4.1. Инициативи на Организацията за икономическо сътрудничество и развитие (ОИСР)

Първите стъпки в областта на международното сътрудничество за противодействие на компютърните престъпления са инициирани в рамките на Организацията за икономическо сътрудничество и развитие (ОИСР). Още в началото на 80-те години на миналия век ОИСР започва да се занимава задълбочено с проблемите на неприкосновеността на информацията, като в резултат на това са приети няколко препоръки и декларации относно защитата на данните при тяхната автоматична обработка и трансграничен обмен. През 1983 г. в рамките на организацията е създадена експертна комисия за проучване на компютърните престъпления и необходимостта, която те пораждат, от промени в наказателното законодателство на държавите-членки. През 1986 г. комисията публикува доклада „Престъпления, свързани с компютри: анализ на правната политика", който анализира различните подходи по отношение на компютърната престъпност, използвани в националните законодателства на отделните държави-членки, и предлага списък с деяния, които е препоръчителни да бъдат криминализирани във всички държави-членки.[109] В края на XX и началото на XXI век усилията на ОИСР се съсредоточават върху сигурността на информационните системи, незаконното и вредно съдържание в Интернет, крпитирането, сигурността на данните в глобалните мрежи и защитата на потребителите в електронната търговия.

4.2. Инициативи на Организацията на обединените нации (ООН)

Първите инициативи на ООН за противодействие на компютърната престъпност също са свързани с проблемите на неприкосновеността на данните и тяхната защита при автоматична обработка и обмен, както и с правното значение и доказателствената стойност (включително в наказателните производства) на компютърните записи и борбата с расистското и ксенофобско съдържание в Интернет.

През 1990 г., в рамките на VIII Конгрес на ООН по превенция на престъпността и третиране на извършителите, е приета специална резолюция относно свързаните с компютри престъпления, в която държавите-членки се призовават да усъвършенстват националното си наказателно законодателство (както материално, така и процесуално), като предвидят мерки за ефективното разкриване, разследване и наказване на компютърната престъпност. В изпълнение на тази резолюция през 1994 г. ООН публикува „Наръчник за превенция и контрол а на свързаните с компютри престъпления", в който се разглеждат няколко групи въпроси – същност на компютърните престъпления, материалноправна защита на неприкосновеността на данните и тяхната поверителност, процесуалноправни въпроси,

[109] Виж Computer-Related Crime, Analysis of Legal Policy, OECD, Paris, 1986.

свързани с разследването и наказването на компютърните престъпления, превенция на престъпността в компютърна среда и международно сътрудничество.[110]

4.3. Инициативи на Съвета на Европа (СЕ)

Най-съществен принос в развитието на международното сътрудничество в областта на компютърните престъпления има Съветът на Европа. Както при повечето други международни организации, ангажирани в превенцията и противодействието на компютърната престъпност, първите инициативи на СЕ също са в сферата на защитата на неприкосновеността на данните. Така през 1981 г. е приета Конвенция № 108 на Съвета на Европа от 28.01.1981 г. за защита на лицата при автоматизираната обработка на лични данни.[111] Наред с другите разпоредби конвенцията задължава всяка страна да установи съответстващи санкции и компенсации при нарушаване на разпоредбите на вътрешното право, с които се въвеждат в действие принципите за защита на данните, залегнали в конвенцията. В края на миналия и началото на нашия са приети и препоръки, отнасящи се до защитата на неприкосновеността на данните в отделни сфери на обществения живот (медицински данни, данни използвани за научни или статистически цели и т.н.). СЕ приема и поредица препоръки, свързани с незаконното и вредно съдържание в електронните медии и Интернет, като насилие, насаждане на омраза и т.н.

През 1989 г. СЕ приема Препоръка № R(89)9, която съдържа списък на минимума посегателства, които следва да бъдат инкриминирани от държавите-членки с цел постигането на обща наказателна политика в областта на компютърните престъпления, както и списък с други посегателства, за чието инкриминиране не е постигнат консенсус.[112] През 1995 г. е приета втора препоръка, отнасяща се до наказателно-процесуалните аспекти на създаването и използването на информационните технологии, в която се препоръчва на държавите-членки да предвидят правила във вътрешното си законодателство, уреждащи претърсването на компютърни системи и изземването на компютърни данни.[113]

През 1997 г. към СЕ е създадена Експертна комисия по престъпленията в кибернетичното пространство, която има за основна задача да изследва и дефинира новите престъпления, юрисдикцията на държавите и наказателната отговорност във връзка с комуникацията чрез Интернет. Въз основа на резултатите от работата на експертната група е подготвен проект за Конвенция за престъпленията в кибернетичното пространство, която е приета на 109 заседание на Комитета на министрите на 8 ноември 2001 г. и е открита за подписване на срещата в Будапеща, Унгария, на 23 ноември 2001 г.[114]

Конвенцията за престъпления в кибернетичното пространство на Съвета на Европа дава определения на основните понятия във връзка с компютърните престъпления и предвижда конкретни мерки, които държавите-членки трябва да предприемат на национално равнище в областта на материалното и процесуалното наказателно право. Дефинирани са

---

[110] Виж United Nations Manual on the prevention and control of computer-related crime, International review of criminal policy, № 43 и 44, 1994.

[111] Конвенция № 108 на Съвета на Европа от 28.01.1981 г. за защита на лицата при автоматизираната обработка на лични данни, ратифицирана със закон, приет от Тридесет и деветото Народно събрание на 29 май 2002 г., обнародван, ДВ, бр. 56 от 7 юни 2002 г., издадена от Министерството на вътрешните работи, обнародвана, ДВ, бр. 26 от 21 март 2003 г., в сила от 1 януари 2003 г.

[112] Виж Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies).

[113] Виж Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies).

[114] Виж Конвенция за престъпления в кибернетичното пространство, приета на 109-ото заседание на Комитета на министрите на Съвета на Европа и открита за подписване в Будапеща на 23 ноември 2001 г., ратифицирана със закон, приет от Тридесет и деветото Народно събрание на 1 април 2005 г., обнародван, ДВ, бр. 29 от 5 април 2005 г., издадена от Министерството на правосъдието, обнародвана, ДВ, бр. 76 от 15 Септември 2006 г., в сила за Република България от 1 август 2005 г.

четири основни понятия – компютърна система, компютърни данни, доставчик на услуги и данни за трафика.

Конвенцията определя четири основни категории престъпления: правонарушения срещу тайната, неприкосновеността и възможността за ползване на компютърни данни и системи (незаконен достъп, незаконно прихващане, посегателства срещу неприкосновеността на компютърните данни и компютърните системи, злоупотреба с устройства), компютърни престъпления (компютърна фалшификация и компютърна измама), престъпления, свързани със съдържанието (детска порнография) и престъпления, свързани с посегателства срещу авторското право и сродните му права (масово разпространение на пиратски копия на защитени творби и др.). Предвидени са и разпоредби, уреждащи инкриминирането на съучастието и опита за извършване на компютърно престъпление, както и въвеждането на отговорност, включително наказателна, за юридически лица, когато престъплението е извършено в полза на юридическо лице от свързано с него физическо лице.

В областта на наказателния процес конвенцията съдържа правила относно бързото запазване на данните, съхранявани в компютърните системи, и на данните, свързани с трафика, реда за предоставяне на такива данни, претърсването и изземването на съхраняваните компютърни данни, събирането в реално време на данни за трафика и на данни, свързани със съдържанието.

В сферата на международното сътрудничество конвенцията въвежда няколко нови форми на взаимодействие в допълнение към традиционните механизми, предвидени в Европейската конвенция за екстрадиция и Европейската конвенция за взаимопомощ по наказателни дела. Предвидено е и създаването на постоянно действаща мрежа за контакти (т.нар. мрежа 24/7), която да осигурява съдействие при разследването на компютърни престъпления.

През Допълнителен протокол към Конвенцията за престъпления в кибернетичното пространство относно криминализирането на актовете на расизъм и ксенофобия, извършени посредством компютърни системи.[115] Допълнителният протокол дава определение на понятието „расистски или ксенофобски материал" и посочва четири групи престъпления – разпространение на расистски и ксенофобски материал чрез компютърни системи, заплашване с расистски и ксенофобски мотиви, обида с расистски и ксенофобски мотиви, отричане, омаловажаване, одобрение или оправдание на актове на гиноцид или престъпления срещу човечеството. Протоколът съдържа и разпоредби относно инкриминирането на помагачеството и подбудителството към такива престъпления.

4.4. Инициативи на Европейския съюз (ЕС)

В края на 80-те и началото на 90-те години компютърните престъпления стават обект на внимание и от страна на ЕС. През 1987 г. по искане на Европейската комисия е подготвен докладът „Правни аспекти на компютърните престъпления и сигурността"[116], а през 1998 г. Европейската комисия представя на Съвета резултатите от изследване на тема „Правни аспекти на компютърните престъпления в информационното общество", по-известно като изследването COMCRIME.[117] Първите законодателни актове на равнище ЕС, имащи отношение към компютърните престъпления, са предимно в областта на защитата на личните данни, интелектуалната собственост и противодействието на незаконното и вредно съдържание в Интернет. Повечето от тези документи не предвиждат конкретни мерки в

[115] Виж Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003.

[116] Виж Sieber, Kaspersen, Vandenberghe, Stuurman, *The Legal Aspects of Computer Crime and Security - A Comparative Analysis with Suggestions for Future International Action*, document prepared for the Commission of the European Communities, 1987.

[117] Виж *Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME-Study)*, prepared for the European Commission by Prof. Dr. Ulrich Sieber, University of Würzburg, 1998.

областта на наказателното право, а само обръщат внимание на необходимостта от санкциониране на нарушенията в тези сфери.

През октомври 1999 г. на срещата в Тампере, Финландия, Европейският съвет излиза със заключение, че престъпленията в областта на високите технологии следва да бъдат включени в усилията за уеднаквяване на дефинициите и санкциите. Европейският парламент също призовава за приемане на уеднаквени определения на компютърните престъпления и за ефективна хармонизация на законодателството, особено в областта на материалното наказателно право. В хода на работата по проекта за Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа Съветът на Европейския съюз приема Обща позиция относно преговорите по конвенцията и включва някои елементи от нея като част от стратегията на Съюза за противодействие на престъпленията в областта на високите технологии.[118]

На 26 януари 2001 г. Европейската комисия приема предложение до Съвета и до Европейския парламент, озаглавено „Създаване на сигурно информационно общество чрез подобряване на сигурността на информационните инфраструктури и противодействие на компютърните престъпления".[119] В предложението са обобщени видовете компютърни престъпления, инкриминирани в държавите-членки на ЕС – престъпления против неприкосновеността на личните данни, престъпления, свързани с разпространението на незаконно съдържание, икономически компютърни престъпления и престъпления срещу интелектуалната собственост. На 6 юни 2001 г. Европейската комисия приема и второ предложение под заглавие „Мрежова и информационна сигурност: предложение за общ европейски подход".[120] През същия месец е приета и Препоръка на Съвета от 25 юни 2001 г. относно точките за контакт, предоставящи 24-часови услуги за обмен на информация в борбата срещу престъпленията в сферата на високите технологии.[121]

Една година по-късно, на 19 април 2002 г., е публикувано и предложение на Европейската комисия за Рамково решение на Съвета относно атаките срещу информационните системи.[122] Решението е прието на 24 февруари 2005 г. и има за цел да подобри сътрудничеството между съдебните и другите компетентни власти, в това число полицията и други специализирани правоприлагащи служби на държавите-членки, чрез сближаване на правилата в наказателното право в сферата на атаките срещу информационните системи.[123] Това е и най-значимият законодателен акт в областта на компютърните престъпления на равнище ЕС. Рамковото решение дава определения на понятията „информационна система", „компютърни данни" и „неправомерен" достъп и задължава държавите-членки на ЕС да инкриминират във вътрешното си законодателство определени престъпления, като неправомерния достъп до информационни системи и неправомерната намеса в системата или данните. Освен това предложението задължава държавите-членки да инкриминират също и подбудителството, помагачеството и

[118] Виж Обща позиция от 27 май 1999 година, приета от Съвета на основание член 34 от Договора за Европейския съюз по проведените в Съвета на Европа преговори, относно проекта за Конвенция за престъпленията в кибернетичното пространство (1999/364/ПВР), Официален вестник n° L 142 , 05/06/1999 стр. 0001 – 0002.

[119] Виж Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (COM(2000)890).

[120] Виж Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *Network and Information Security: Proposal for A European Policy Approach* (COM(2001)298).

[121] Виж Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, Official Journal C 187, 03/07/2001 P. 0005 – 0006.

[122] Виж Commission proposal for a Council framework decision on attacks against information systems, presented by the Commission on April 19, 2002 (COM(2002)173).

[123] Виж Рамково решение 2005/222/ПВР на Съвета от 24 февруари 2005 година относно атаките срещу информационните системи, Официален вестник n° L 069 , 16/03/2005 стр. 0067 – 0071.

съучастието, както и опита към извършване а такива престъпления. Предвидени са още правила относно наказанията, отговорността на юридически лица и юрисдикцията.

4.5. Други международни инициативи

Различни инициативи по различни проблеми, свързани с компютърните престъпления, са предприети и от редица други международни институции и организации.

През 1997 г. подгрупата по високи технологии на главните експерти на Групата на Осемте (Г-8) – организация на седемте най-развити индустриални държави в света (САЩ, Великобритания, Франция, Германия, Канада, Япония и Италия) и Русия – приема десет принципа и план за действие за борба с компютърните престъпления, а през март 1998 г. е създадена и мрежа от експерти (работеща постоянно 24 часа в денонощието, 7 дни в седмицата), за подпомагане на разследването на престъпленията в областта на високите технологии. Основните цели на тази мрежа са да осигури, че извършителите на компютърни престъпления не се ползват със закрила никъде по света и че правоприлагащите органи разполагат с необходимите технически и правни средства за откриването на извършителите на такива престъпления и тяхното своевременно привличане към отговорност. Прието е принципите да се прилагат както чрез сключването на международни договори, така и чрез приемането на национални закони и политики. Много други държави извън Г-8 също се присъединяват към новосъздадената мрежа.

В рамките на работата си в сферата на интелектуалната собственост през 2004 г. Световната търговска организация (СТО) приема Споразумение относно свързаните с търговията аспекти на интелектуалната собственост, с което задължава държавите – страни по споразумението да предприемат мерки за инкриминиране на определени посегателства срещу интелектуалната собственост.[124]

Инициативи за противодействие на компютърната престъпност се предприемат и в рамките на различните форми на международно полицейско сътрудничество. Така например европейската работна група по компютърните престъпления към Интерпол, формирана през 1990 г., е автор на „Наръчник за разследване на престъпленията срещу информационните технологии".

Принос към развитието на международната правна уредба за противодействие на компютърната престъпност има и Международната асоциация по наказателно право – неправителствена организация в рамките на ООН и Съвета на Европа.[125]

[124] Виж Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), WTO, 1994.

[125] Виж повече за работата на Международната асоциация по наказателно право в областта на компютърните престъпления http://www.penal.org.

5. Авторско право в Интернет и онлайн нарушения на авторските права

Измежду правните проблеми, които се появяват във връзка с Интернет, едва ли не първо място заема авторското право. Доколкото Интернет ще се използва все повече като инструмент за продажба и доставка на информация и резултати от творчески дейности без хартия и граници, въпросите по защита на правата на интелектуалната собственост на материали, достъпни в Интернет, ще придобиват все по-голямо значение.

Авторското право е една от най-важните защити на интелектуалната собственост в Интернет най-вече поради следните две причини.

На първо място, по-голямата част от материалите, които се предават по Интернет (текст, изображение, звукови сигнали) са произведения в юридическия смисъл и по този начин представляват предмет на авторското право.

На второ място, доколкото самата природа на електронните комуникации изисква многократно копиране на данни в процеса на тяхното предаване по каналите на мрежата и запознаването с тях, естествено възниква въпросът за спазването на авторските права при такова копиране.

Всяко поведение на ползвателите на Интернет влияе върху правото на авторите и техните правоприемници. Казано по друг начин, не е възможно да се направи нещо в Интернет, което потенциално да не засяга нечии авторски права. Разглеждането на Web-страниците, съхраняването на част от тяхното съдържание в паметта на компютъра, препращане на съобщения от електронната поща – всички тези действия включват възпроизвеждане на обекти, защитени от авторското право.

Преди да се разгледат проблемите със защитата на авторските права в Интернет, е необходимо да се определят материалите, достъпни в Интернет, които се защитават от авторските права и какви са изискванията за обектите на авторското право.

5.1. Защита на авторското право на материалите в Интернет

Във всички страни (където то съществува) авторското право защитава произведения на литературата, науката и изкуството. Правилото е, че националните закони и международните конвенции по авторско право съдържат приблизително, но не и изчерпателно изброяване на обектите, подлежащи на правна защита. Обикновено се изброяват литературни, музикални и аудиовизуални произведения, фотографии, картини рисунки, илюстрации, карти, планове, скици и др.[126]

В същото време обекти като съобщаване на новините за деня или текущи събития, които имат характер на обикновена медийна информация, произведения на фолклора, а също така и държавни документи, символи и знаци, обикновено не са защитени[127].

Всички гореспоменати литературни и художествени произведения могат да се намерят в Интернет в големи количества и всички те могат да претендират за защита на авторското право. Но само доколкото принадлежат към една или друга категория произведения, указана в закона, което не е достатъчно.

5.1.1. Критерии за защита на авторските права

За да се получат защита съгласно закона за авторските права, гореспоменатите произведения трябва да отговарят на определени критерии. На първо място, трябва да бъдат „оригинални" в юридическия смисъл и на второ място, трябва да са изразени в „обективна форма".

---

[126] *Виж,* Закон за авторското право от 1976, 17 U. S. C. §102 (a); Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.). Чл. 3(1); Бернска конвенция за закрила на произведенията на литературата и изкуството; Парижки акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (1).

[127] *Виж,* §105, Чл. 4.

5.1.1.1. Оригиналност

Първият критерий се приема от различните държави приблизително еднакво. Съдилищата в страните от англосаксонското право тълкуват критерия „оригиналност" широко: произведението просто трябва да бъде резултат от независимия труд и таланта на автора, т. е. да не бъде копирано от друго произведение, чиито авторски права принадлежат на друго лице, и които по мнението на съдия от Върховния съд на САЩ О'Коннор, „имат поне някакво минимално ниво на творчество".[128]

Съдилищата в континенталните страни на Западна Европа, освен този критерии, взимат под внимание и дали личността на автора е изразена в произведението, носи ли то печат от неговата индивидуалност. Въпреки това, в наши дни тези изисквания стават все по-гъвкави, поради появата на нов тип произведения, чиито процес на създаване включва автоматизирани елементи.[129]

В България критерият „оригиналност" няма легално определение. Споменава се само творческият характер като признак на дейността, в резултат на която се е появило произведението. Давайки легално определение на термина „автор", законът указва, че това е „физическо лице, в резултат на чиято творческа дейност е създадено произведение".[130] От тук може да се направи извод, че законът признава за обекти на защита резултатите от творческия труд.

„Оригиналността" в авторското право не означава „художествени достойнства" и не предполага високо естетическо ниво на произведенията и безупречен художествен вкус, с който е било създадено. Както е указал апелативният съдия Познер от САЩ, „художествената оригиналност не означава същото като юридическата концепция за оригиналност в Закона за авторските парва".[131]

„Оригиналността" също така не е синоним на „новостта". „Произведението може да бъде оригинално, даже ако много прилича на други произведения, при условие, че това е в резултат на случайност, а не на копиране".[132] По такъв начин, две идентични произведения, създадени от различни автори независими един от друг, ще бъдат защитени с авторските права, даже ако едно от тези произведения, създадено по-късно, не се явява ново.

Това, че защитеното произведение трябва да е плод на творчество, не означава, че нивото на това творчество трябва да е високо. Всъщност „нивото на творчество", което се изисква е изключително ниско; даже незначителен творчески елемент е достатъчен. По-голямата част от произведенията преодоляват тази бариера сравнително леко, доколкото имат някаква творческа искра".[133]

Гореспоменатото в пълна степен се отнася и за произведения, намиращи се в Интернет. Даже най-обикновените от тях, като съобщения по електронната поща, много лесно биха удовлетворили законодателните изисквания за „оригиналност".

Въпреки че стандартът действително е много нисък, съществуват редица обекти, които не му отговарят. Законодателството на САЩ в областта на авторско право даже съдържа списък, в който подробно са изброени подобни обекти - чисти бланки, произведения, които изцяло съдържат обществена информация, като календари, таблици за мерки и тегло или разписания на спортни събития.[134]

---

[128] Фейст Пъбликейшънс Инс. срещу Рурал Телефоун Сървисис Ко. (Feist Publications, Inc. v. Rural Telephone Service Co), 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[129] T. K. Drier. La qualité d'auteur et les nouvelles technologies du point de vue des traditions de droit civil/ Symposium de l'OMPI, Paris, 1994.

[130] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г..) – Чл. 5

[131] Грасен срещу Брадфорд Ексчейндж (Gracen v. Bradford Exchange), 698 F. 2d 300 (7th Cir.1983).

[132]Фейст Пъбликейшънс Инс. срещу Рурал Телефоун Сървисис Ко. (Feist Publications, Inc. v. Rural Telephone Service Co.), 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[133] Ibid.

[134] *Виж* 37 C. F. R., § 202.1 (a), (c) и (d).

Голямо количество подобни обекти, които не са защитени, са достъпни в Интернет и повечето от тях са обикновени данни. Авторското право на повечето юрисдикции не разпространява своята защита върху обикновените данни, „дори да са били изразени, описани, пояснени, илюстрирани в произведението".[135]

Ако авторското право закриляше факти, представляващи обикновени данни, това би ограничило свободния информационен оборот и обмена на мнения. „Авторското право предоставя на авторите правото на оригинално изображение, но поощрява и други свободно да надстрояват над идеите и информацията, изразени в произведенията. Това е способ, с чиято помощ авторското право способства за прогреса на науката и изкуството".[136]

Базирайки се на тези съображения, авторското право не защитава домейн имена и електронни пощи, а също и ключове на кодове, използващи се в криптографията и електронните подписи, които се явяват просто факти.

5.1.1.2. Фиксация

Подходите към втория критерий не са еднакви в страните, принадлежащи към различни правни системи. В САЩ, например, под закрилата на авторско право попадат произведения, „фиксирани върху материален носител към настоящия момент или такива, които ще бъдат изобразени по-късно, така че да могат да бъдат възприети, възпроизведени или по някакъв друг начин съобщени непосредствено или с помощта на машини или приспособления".[137] При това, произведението се счита за „фиксирано", ако материалният му носител се явява „достатъчно постоянен и стабилен за това, да бъде възпроизведено или по друг начин съобщено в течение на период с по-голяма продължителност от промеждутъчната"[138]. Авторското право не се интересува толкова от „времевата продължителност на съществуване на копията, колкото от това, какво може да бъде извършено с тях докато съществуват".[139]

В резултат на този подход, в съответствие с американското законодателство устни, драматични и хореографски произведения, незаснети като филм или върху какъвто и да е носител на информация в „реалния" свят, произведения, които се предават в режим „реално време" без техни едновременни записи (например, излъчване на спортни събития) във „виртуалния" свят на Интернет, не се считат „фиксирани" и съответно не подлежат на закрила от страна на авторското право.[140] Същевременно чрез Интернет са достъпни оригинални произведения, които са фиксирани в цифров вид на магнитен носител, лазерен диск или в паметта на компютъра (дори в оперативната памет макар и „само за милисекунда"). По същия път вървят и другите държави на англосаксонското право. Това напълно съответства на изискванията на Бернската конвенция относно закрилата на литературни и художествени произведения (наричана за краткост Бернска конвенция), която запазва за законодателството на държавите-членки „правото да укажат, че литературни и художествени произведения или някакви техни определени категории не подлежат на закрила, ако не са закрепени в определена материална форма".[141]

---

[135] Закон на Украйна за авторското право и сродните му права в редакцията от 14 юли 2001 г.., Голос України, 16. 08. 2001 г., бр. 146, Ст. 8, ч. 3.

[136] Фейст Пъблике йшънс Инс. срещу Рурал Телефоун Сървисис Ко. (Feist Publications, Inc. v. Rural Telephone Service Co.), 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[137] Закон за авторското право от 1976 г., 17 U. S. C. §102(a).

[138] §101(Определение за „фиксиран").

[139] Триад Системс Корпорейшън срещу Саутастърн Експрес Ко. (Triad Systems Corporation v. Southeastern Express Co.), 31 U.S.P.Q. 2d (BNA) 1239, 1243 (N.D. Cal. 1994)

[140] *Виж* U.S. Departement of Commerce, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property 32 (1995).

[141] Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (2).

В страните от континентална Европа законите за авторско право изискват произведението, на което се предоставя закрила да има въплъщение в определена форма, но тя не е задължително да бъде „материална". Така, българският закон разпространява своята закрила върху произведения, изразени в „обективна форма", т. е. такава, която позволява възприемане на произведения от органи на възприятието. Съответно, наравно с устни, драматични и хореографични произведения и произведения, намиращи се в Интернет, отговарят на установените в закона изисквания за изображения в обективна форма и биват закриляни от авторското право в България, независимо от техния запис върху материален носител на информация.

5.1.1.3. Формалности

В страните от Бернския съюз, в който участват държавите-членки по Бернската конвенция, в това число и България, закрилата на публикуваните в Интернет произведения, които отговарят на критерия за оригиналност и фиксиране, настъпва автоматично в момента на тяхното създаване, както при всички други произведения. Това означава, че за възникване и осъществяване на авторско право върху такива произведения „не е нужна регистрация на произведенията или някакво друго специфично оформление, а също и спазване на други формалности".[142]

Законодателството на повечето от страните, обаче, поощрява авторите да спазват формалности, като поставяне върху всеки екземпляр от произведението знака за закрила на авторско право © или сродните му права (р),[143] държавна регистрация и депозиране.

5.2. Видове произведения в Интернет и особености на тяхната закрила от авторското право

Ще бъдат конкретно разгледани произведенията в Интернет и в какво се състои особеността на закрилата от страна на авторското право на всяко от тях.

5.2.1. Литературни произведения

Литературните произведения във всичките си видове се явяват типични обекти на закрила на авторското право в повечето държави. В тази категория произведения попадат книги, брошури, статии и други писмени произведения.[144]

Давайки определение на термина „литературно произведение", американският Закон за авторското право указва, че това е произведение, „изобразено чрез слова, цифри или други словесни или цифрови символи или знаци, без да обръща внимание на природата на материалния им носител - книги, периодични издания, ръкописи, звукозаписи, филми, касети, дискове".[145]

Българският закон, обаче не съдържа легално определение за литературно произведение, което да конкретизира кои произведения могат да бъдат категоризирани, като „произведения на научната и техническата литература, на публицистиката и компютърни програми".[146]

---

[142] Закон на Украйна„за авторското право и сродните му права в редакцията на Закона за внасяне на изменения в закона за авторското право и сродните му права от 14 юли 2001 г., „Голос України" – 16.08.2001 г., бр. 146, Ст. 11, ч. 2.

[143] *Виж*, напр.: Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Допълнителни разпоредби. §1.

[144] *Виж* Закон за авторското право от 1976 г., 17 U. S. C. §102 (a) (1); Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.); Чл. 3(1) п. 1; Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г., Ст. 2 (1).

[145] Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение на „литературни произведения").

[146] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.), Чл. 3(1), п. 1.

Днес голяма част от материалите, достъпни в Интернет, са именно литературни произведения. Съобщения на електронни пощи, рекламна и справочна литература, каталози, речници, текстове, поместени на сайтове WWW, FTP и gopher, послания, разпространявани чрез списък от имейли и дискусионни групи - това са все литературни произведения по смисъла на авторското право.

Трябва да се обърне особено внимание на **компютърните програми**, които са своеобразен обект на интелектуална собственост, на който Интернет дължи съществуването си и който авторското право приравнява именно към литературни произведения.[147]. Те управляват както самите компютри, така и информационния поток помежду им, обединявайки ги в информационни мрежи. Именно компютърните програми правят възможно търсенето и запознаването с материали, разменяни в Интернет и „превеждат" други произведения, предавани в Интернет, от компютърен език на понятен за човека, и обратното. В същото време, те самите биват предавани по Интернет в големи количества като самостоятелни произведения, както и като части от съставни произведения. Именно простотата на мигновено разпространение на компютърни програми в глобален мащаб е основната заплаха за авторите на програми и техните правоприемници, в сравнение с която заплахата на техните права от компактдискове е нищожна.

Американският Закон за авторското право дава следното определение на термина „компютърна програма", а именно „набор твърдения или инструкции, използвани непосредствено или косвено в компютъра с цел постигане на определени цели".[148]

Българският закон не съдържа легална дефиниция за компютърна програма или софтуер, като теорията приема, че компютърната програма е „поредица от инструкции, способни да накарат машината (компютъра) да обработи информацията, да посочи и изпълни определена функция и/или да постигне определен резултат".[149]

Закрилата на компютърните програми като обекти на интелектуална собственост показва известна специфика спрямо общата уредба. За свободното използване на компютърни програми е предвидено специално изключение – съгласно чл. 71, т. 1 ЗАПСП, лицето, което законно е придобило правото да използва компютърна програма, може без съгласието на автора и без заплащане на отделно възнаграждение да изготвя резервно копие от програмата, ако това е необходимо за съответния вид използване, за който е придобита програмата. В същото време при компютърните програми не се допуска тяхното възпроизвеждане върху какъвто и да е носител, от физическо лице за негова лична употреба, дори при условие, че не се извършва с търговска цел (чл. 25, ал. 2). В противен случай бихме били изправени пред нарушение на авторското право, изразяващо се в несанкционирано от автора възпроизвеждане на произведението за цели, надхвърлящи по обем предвидените в закона.

Чл. 70 от ЗАПСП посочва границите, в които законният ползвател на компютърната програма може да я използува. Той може да зарежда програмата, да я изобразява върху екран, да я изпълнява, предава на разстояние, да я съхранява в паметта на компютър, да я превежда, преработва и да внася други изменения в нея, ако тези действия са необходими за постигане на целта, заради която е придобито правото да се използва програмата, включително и за отстраняване на грешки. Това са на практика имуществените права върху компютърна програма, които освен ако страните на са уговорили друго, ползвателят на програмата придобива по силата на лицензионния договор с автора.

---

[147] *Виж*: Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Чл. 3(1) т. 1; Споразумение относно търговските аспекти на правата на интелектуална собственост (Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994), Маракешко споразумение за установяване на Международната търговска организация (Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments – Results of the Uruguay Round vol. 31//33 I. L. M. 81 – 1994 – Art. 10 (1))

[148] Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение на „компютърна програма").

[149] Маркова, М., Компютърните програми и базите данни в системата на интелектуалната собственост и борбата с пиратството им, сп. „ИНСО", 2002, кн. 9, с. 21

Следва да се посочат две особености на компютърните програми като обект на закрила от авторското право. Първо – програмата е съставена от алгоритъм, и второ – тя се явява в определен смисъл негов еквивалент. Това означава, че някои от основните черти на алгоритъма са свойствени и за програмата. Едновременно с това, програмата може да бъде разглеждана като способ за реализиране на алгоритъма, и като такава тя се характеризира с определени отличителни черти, според които за целите на изследването на програмата като обект на правна закрила, е възможно да се подчертае следното: за разлика от алгоритъма, представляващ последователност от логическо-математически операции за преобразуване на информация, програмата съдържа последователност от команди, които описват процес на реализация на алгоритъма и обезопасяват ръководството на този процес. Обективна форма на изражение на програмата се явява записът на формализиран език на еднотипни компютри.

Именно това изражение се явява обект на закрила от авторското право. Идеи, които стоят в основата на компютърна програма, изразени в нея и описани от нея, не се закрилят от авторското право. Тяхна защита се явява прерогатив на друг отрасъл на правото на интелектуална собственост – патентното право.

Съгласно чл. 6 от българския Закон за патентите (ЗП) патенти се издават за изобретения от всички области на техниката, които са нови, имат изобретателска стъпка и са промишлено приложими. Изрично е посочено, че компютърните програми не се считат за изобретения. Уточнява се, че изключването на посочените обекти се прилага, доколкото се иска правна закрила за самите тях като такива. Тази разпоредба е заимствана от чл. 52, ал. 2 от Европейската патентна конвенция (ЕПК), по която България е страна и следва да се тълкува по начина, по който я тълкува Европейското патентно ведомство.

Казаното означава, че една компютърна програма взета сама по себе си не подлежи на патентоване, освен ако отговаря на всички изисквания на чл. 6 от ЗП и притежава качеството „технически принос", в който случай програмата се определя като „компютърно внедрено изобретение". Компютърно внедрените изобретения включват такива устройства като мобилните телефони, интелигентните домакински съоръжения, устройства за контрол на двигателите и изобретения, касаещи компютърни програми.

Откъде идва двойнствения режим на защита на компютърните програми – като обекти на авторско право и като патентоспособни изобретения?

Разпоредбата, че компютърните програми „като такива" не са годни за патентоване обекти визира, че сами по себе си те са защитени от авторското право. Авторското право защитава като литературно произведение формата, конкретните редове код, написани от програмиста и предоставя възможността да се забрани копирането или комерсиализирането на този код от трети лица. В същото време, авторското право не защитава идеите, заложени в софтуера, това, което софтуерът прави в машината или как машината под контрола на софтуера взаимодейства с околната среда. Ако такъв процес би включвал решаване на технически проблем по изобретателски начин (т. е. начин, който е нов и не е очевиден), тогава може да е налице патентоспособно изобретение. Това е, което се има предвид под компютърно-внедримо изобретение. Предоставянето на такъв патент е напълно в съответствие с принципите на европейското патентно право. Понастоящем близо 15% от всички патентни заявки, подадени в Европейското патентно ведомство, са свързани с компютърно-внедрими изобретения. Това означава, че от над 110 000 заявки, получени в Европейското патентно ведомство през 2001 година, повече от 16 000 са били свързани с иновации в компютърните технологии. С течение на годините практиката на Европейското патентно ведомство се либерализира по отношение на критериите за патентоспособност и като резултат понастоящем патенти се предоставят за компютърно-внедрими изобретения при условие, че те имат „технически принос".

Концепцията за закрила на компютърни програми чрез патентното право има не само много привърженици, но и много противници. При патентоването на компютърни програми са налице редица твърде съществени практически затруднения:

1. Процедурата по патентоване е много продължителна, като за преминаването през нея се изискват от 2 до 5 години, а срокът на живот на самото програмно осигуряване може да е по-кратък. Известно е, че компютърните програми остаряват твърде бързо.

2. Няма регистър на програмното осигуряване, следователно липсва възможността за откриването на онези аналози, респективно прототипи, които да послужат като база за сравнение с новото решение при провеждането на една патентна експертиза.

3. Поради голямата трудност при разкриването на случаите за нарушаване на правата за обекти от този тип, пълната публикация на описанието на обекта, каквато е възприета в патентните документи, от една страна, е нецелесъобразна, а от друга страна, може да се окаже прекалено обемиста за един патентен документ, което подхожда повече на една научна публикация, отколкото на патентно описание.

Следователно дори в съвременния си вид авторското право е в състояние достатъчно добре да се справи с една нова за него задача – закрилата на компютърните програми. Затова погледите на учените и практиците не случайно са обърнати към неговите институти при търсенето на подходящи методи за такава закрила.

В условията на програмния бум и при възможността за светкавично разпространение на „пиратски" копия на програми чрез Интернет, не признаващ държавни граници, без съмнение е по-привлекателен този механизъм за закрила, който не изисква големи формалности и много време за експертиза. В този смисъл най-ефективен е методът за закрила на компютърни програми въз основа на авторското право, при което няма процедура за проверка и на практика не се изисква изпълнението на някакви формалности. Не е за пренебрегване и фактът, че установяването на правна закрила на авторските права на национално ниво автоматично включва и международна закрила на програмата, осигурена от международните конвенции в областта на авторското право тази закрила се разпростира върху почти всички страни на света.

5.2.2. Фотографии и други статични изображения

По степен на информационна натовареност сред предаваните чрез Интернет произведения на първо място се нареждат литературните произведения, след които са фотографските и другите статични изображения на компютърния екран (карти, схеми, диаграми и други подобни).

При това въпросните изображения могат да бъдат създавани на монитора чрез специални програми, предназначени за улесняване на потребителите при използването на самия компютър (операционни системи) и за Интернет обслужване (програми, предназначени за сърфиране в мрежата – браузъри и други приложни програми) или да бъдат качени в Интернет и да имат независим от компютрите на потребителите характер.

В първия случай изображението върху екрана представлява част от компютърна програма, нейния интерфейс, който се закриля заедно с цялата програма, а във втория случай изображението е цифрова фотография и се закриля като обикновена фотография[150], или е резултат от прехвърляне в цифрова форма (сканиране) на обикновена фотография или друго двуизмерно (картина, рисунка) или триизмерно (скулптура, сграда) произведение, и при евентуалното му съответствие с критерия за оригиналност е закриляно като произведение, което е производно от същите. (За производните произведения ще стане дума по-долу.)

5.2.3. Музикални произведения и звукозаписи

[150] *Виж,* Закон за авторското право от 1976 г., 17 U. S. C. §102 (a) (2); – Ст. 8 ч. 1 п. 10; Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Чл. 3(1) т. 7; Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (1).

Музикалните произведения, както свързаните с текст, така и тези без текст, традиционно са закриляни от авторското право.[151] Трябва да се прави разлика между понятията „музикално произведение" и „звукозапис". Последният също е резултат от творчески труд, но представлява вторичен резултат, резултат от фиксирането в материална форма на изпълнението на първото. Правата върху музикалното произведение принадлежат на неговия автор, правата върху изпълнението – на изпълнителя, а върху звукозаписа – на неговия продуцент. Двете последни групи субективни права в страните с континентално право се наричат сродни права и по своя правен характер са аналогични на авторските.

Българският закон, като следва разпоредбите на Конвенцията за закрила на продуцентите на звукозаписи срещу неразрешено възпроизвеждане на техните звукозаписи от 1971 г., по смисъла на която звукозапис е „всеки предназначен за изключително слухово възприемане запис на звуци"[152], определя „звукозаписа" като „резултат от звукозаписването"[153], а „звукозаписването" – като „фиксиране върху траен материален носител на поредица звуци по начин, позволяващ тяхното възприемане, възпроизвеждане, презаписване, излъчване по безжичен път или предаване чрез кабел или друго техническо средство".[154]

В американския Закон за авторското право се уточнява, че това могат да бъдат „серии от музикални, гласови или други звуци, но като се изключат звуците, които съпровождат кинофилмите или други аудиовизуални произведения".[155]

Следователно, звукозаписът може да представлява звукозапис не само на музикални, но и на други – устни, драматични, музикално-драматични, хореографски произведения, а също така, на практика, на всички звуци, които подлежат на евентуално записване.

Все повече музикални произведения и звукозаписи се появяват в Интернет и ако излъчванията на музикални произведения на живо все още се ограничават с частни случаи, то разпространяването на тези произведения чрез Интернет във вид на звукозаписи, запаметени под такива цифрови формати като WMA и MP3, вече е станало обичайно явление. Популярността на разпространението на звукозаписи чрез Интернет се обяснява с това, че при тази форма на разпространение липсва необходимостта от набавянето на техните традиционни екземпляри – на носителите, съдържащи звукозаписи (плочи, касети, компактдискове и други подобни), които значително усложняват процеса на доставка на звукозаписите до слушателите и оскъпяват тяхното използване.

5.2.4. Аудиовизуални произведения

С появата на киното в обхвата на авторското право се включиха кинофилмите, към които в процеса на развитие на техниката бяха добавени и други аудиовизуални произведения. Българският закон определя тази категория именно така – „филми и други аудиовизуални произведения".[156]

Под „аудиовизуално произведение" обикновено се разбира произведение, което се състои от серия взаимосвързани, съдържащи или не съдържащи звуков съпровод, изображения, предназначени за възпроизвеждане изключително и само чрез определени технически средства.[157] Към аудиовизуалните произведения се причисляват

---

[151] Отново там, §101 (определение на „картина, графика и скулптурни произведения"), §102 (a) (1) – Чл. 33(1) т. 7, Ст. 2 (1).

[152] Конвенция за закрила на продуцентите на звукозаписи от неразрешено възпроизвеждане на техните звукозаписи от 29 октомври 1971 г. – Чл. 1 (a).)

[153] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Допълнителни разпоредби. §2 т. 8.

[154] Отново там, §2 т. 7.

[155] Закон за авторското право от 1976г. , 17 U. S. C. §101 (определение на „звукозаписи").

[156] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Чл. 3(1) т. 4.

[157] *Виж.,* Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение за „аудиовизуални произведения"); Закон на Украйна за авторското право и сродните му права в редакцията на закона за внасяне

кинематографичните произведения, а също така произведенията, „изразени по начин, аналогичен на кинематографичния”.[158]

Като пример за спадащи към тази категория произведения в украинския закон се споменават „кинофилмите, телевизионните филми, видеофилмите, диапозитивите, слайдовете и други подобни, които могат да бъдат игрални, анимационни (мултипликационни), неигрални или други”.[159]

Докато в американския Закон за авторското право се посочва, че по характера си аудиовизуалните произведения трябва да са предназначени за представяне с помощта на „машини или такива приспособления като прожекционен апарат ... или електронно оборудване, независимо от характера на материалните обекти, било то филмови ленти или касети, в които са обществени”.[160] Като изхожда от тази разпоредба, авторското право на САЩ причислява към аудиовизуалните произведения кино и видеофилмите, телевизионните предавания[161], а също така видеоигрите[162].

Аудиовизуалните произведения, особено онези, които са запаметени под цифрова форма, уверено си пробиват път към Интернет. Такива техни варианти като видеофилмите, видеоконференциите, рекламните клипове, музикалните видеоклипове и анимационните филми[163] вече се срещат масово в Интернет. Несъмнено тепърва предстои появата в Интернет на все по-голям брой и на все по-висококачествени аудиовизуални произведения заедно с нарастването на пропускателната способност на каналите за връзка и с усъвършенстването на TCP/IP протоколите.[164]

5.2.5. Производни произведения

Произведенията, представляващи резултат от творческата преработка на произведенията от всички гореспоменати категории, се закрилят от авторското право като производни произведения наравно с произведенията, върху чиято основа са били създадени, без накърняване на правата на авторите на изходните произведения.[165]

В българския закон се споменават следните производни произведения:

1. преводи и преработки на съществуващи произведения и фолклорни творби;
2. аранжименти на музикални произведения и на фолклорни творби.[166]

В американския закон производните произведения са изброени по-подробно, а именно това са „произведенията, базиращи се на едно или повече от едно предходно съществуващи”: „преводи, музикални аранжименти, сценична обработка, литературна обработка, филмова версия, звукозапис, репродукция, кратко изложение, съкратен вариант

на изменения в закона за авторското право и сродните му права от 14 юли 2001 г., „Голос України”, 16.08.2001 г., бр. 146, Чл. 1.

[158] Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Чл. 2(1)

[159] Закон на Украйна за авторското право и сродните му права в редакцията на закона за внасяне на изменения в закона за авторското право и сродните му права от 14 юли 2001 г., „Голос України”, 16.08.2001 г., бр. 146, Ст. 1.

[160] Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение за „аудиовизуални произведения”).

[161] *Виж* Ви Джи Ен Континентал Броадкастинг Ко. срещу Унайтед Видео Инс. (WGN Continental Broadcasting Co. v. United Video, Inc.), 693 F. 2d 622, 626 (7 Cir. 1982).

[162] *Виж* Мидуей Мфг. Ко. срещу Артик Интелидженс Инс. (Midway Mfg. Co. v. Artic Int'l, Inc.), 704 F. 2d 1009, 1011 (7 Cir.), *cert. denied,* 464 U. S. 823 (1983).

[163] Виж, напр.: www.mult.ru.

[164] *Виж*: www.korrespondent.net/main/68092/.

[165] *Виж,* Закон за авторското право от 1976 г., 17 U. S. C. §103; Закон на Украйна за авторското право и сродните му права в редакцията на закона за внасяне на изменения в закона за авторското право и сродните му права от 14 юли 2001г., „Голос України”, 16.08.2001 г., бр. 146, Ст. 1, стр. 8, ч. 1, п. 14; Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (3).

[166] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Чл. 3(2) т. 1, 2.

или каквато и да било друга форма, в която може да бъде преработено, превърнато или адаптирано дадено произведение".[167]

Разбира се, в Интернет се срещат много преводи, репродукции на картини, нови версии на компютърни програми и производни произведения на същите. Но много от поместените в Интернет произведения са производни по силата на това, че оригиналните произведения просто не могат да бъдат поместени в мрежата.

Работата е там, мнозинството от произведенията предвид самия им характер и изразна форма не подлежат на директно поместване в Интернет, защото мрежата признава само една форма на фиксиране – цифровата. Казаното се отнася до устните, драматичните, хореографските произведения, пантомимите, произведенията на изобразителното изкуство (картини, рисунки, гравюри, скулптури и други подобни) и архитектурата, научните произведения (илюстрации, карти, планове, скици и други подобни) и произведенията на приложното изкуство.

Заедно с това литературните (включително компютърните програми), музикалните, аудиовизуалните и фотографските произведения, след като вече са запаметени под цифрова форма или с лекота, с чисто технически средства се поддават на прехвърляне в такава форма, се поместват като такива в Интернет.

Същите произведения, които са фиксирани в традиционни дву- или три- измерни форми, стават достъпни за Интернет потребителите само благодарение на изображенията, получени в резултат на тяхното фотографиране, заснемане на кино- или видео-лента или сканиране. Тъкмо тези изображения представляват производни произведения.

Нещо повече, ако получените фото-, кино- или видео-материали не са запаметени под цифрова форма, то тогава резултатите от прехвърлянето на тези материали в цифрова форма също могат да бъдат производни произведения при условие, че отговарят на критерия за оригиналност. Оригиналността на производните произведения, получени в резултат от прехвърляне на други произведения в цифрова форма, се състои например в творческа обработка на изображението, корекция на дефектите на оригинала или промяна на цветовете (оцветяване), каквито се извършват при реставрацията на стари фотографии и филми.

5.2.6. Сборници и други съставни произведения

Сборниците от произведения, спадащи към всички изброени по-горе категории, включително и производни произведения, при условие, че съответстват на критерия за оригиналност, подлежат на закрила от авторското право „като такива, без накърняване на правата на авторите на всяко от произведенията, представляващи съставна част от такива сборници".[168] Оригиналността на сборниците се състои в това, че те са резултат от творчески труд по подбор, координиране или подреждане на материалите, влизащи в техния състав.[169]

Според българския закон към тази категория произведения спадат „периодичните издания, енциклопедиите, сборниците, антологиите, библиографиите, базите данни и други подобни, които включват две или повече произведения или материали."[170]

Американският закон именува сборника „компилация", като под такава се подразбира „произведение, образувано от събиране и съчетаване на предходно съществуващи материали

---

[167] Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение на „производни произведения").

[168] Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (5).

[169] *Виж,* Закон за авторското право от 1976 г., 17 U. S. C. §101 (определени на „компилация"); Закон на Украйна за авторското право и сродните му права в редакцията на закона за внасяне на изменения в закона за авторското право и сродните му права от 14 юли 2001 г., „Голос України", 16.08.2001 г., бр. 146, Ст. 8, ч. 1, п. 15; Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г. – Ст. 2 (5).

[170] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.) – Чл. 3(2) т. 3.

или данни" и включва в това понятие термина „колективно произведение".[171] А под последното се подразбира „произведение от рода на периодично издание, антология или енциклопедия, в което определено количество компоненти, представляващи сами по себе си отделни и независими произведения, са обединени в едно цяло".[172]

Както се вижда от цитираните разпоредби на законите по авторско право, сборниците са закриляни от авторското право независимо от това дали включените в тях материали са обект на правна закрила. Такива материали, наред със закриляните произведения, могат да бъдат и обектите, които не се закрилят, включително и обикновените данни.

Както беше посочено по-горе, обикновените данни като имена и адреси, номера на резервни части, валутни курсове и котировки на ценни книжа и други подобни представляват факти и като такива не подлежат на закрила от авторското право. Това се отнася до всички факти – научни, исторически, биографични и до новините на деня. Както всички останали обекти, които не са закриляни, те също спадат към обектите за общо ползване и могат свободно да се използват от всеки.[173]

Но сборниците от обекти, спадащи към тези за общо ползване, могат да бъдат закриляни от авторското право. Такива сборници в Интернет най-често са **базите данни.** Тези произведения значително облекчават процесите за пазене, предаване и търсене на информация, запаметена в електронен вид.

По смисъла на българския закон база данни е „съвкупността от самостоятелни произведения, данни или други материали, подредени систематично или методично и индивидуално достъпни по електронен или друг път; компютърните програми, използвани за създаването или функционирането на бази данни, записите на отделно аудиовизуално, литературно или музикално произведение, както и събирането на звукозаписи с музикални изпълнения върху компактдиск не са база данни по смисъла на този закон".[174] Като се базираме на това определение, напълно в реда на нещата е да предположим, че към базата данни законът причислява освен електронните и тези системи, които се управляват посредством механични приспособления и в които търсенето се осъществява с помощта на такива приспособления.

Затова по-конкретно е определението, което се съдържа в законодателството в областта на авторското право на Руската федерация и според което базата данни представлява „обективна форма на представяне и организация на съвкупност от данни (например: статии, сметки), систематизирани по такъв начин, че тези данни да могат да бъдат намерени и обработени с помощта на ЕИМ".[175] По такъв начин в съответствие с руското авторско право под база данни се подразбира изключително и само електронна база данни.

Американският закон не съдържа дефиниция за база данни, но несъмнено включва както традиционните, така и електронните сборници от „материали или данни" в термина „компилация", което се вижда от цитираното по-горе определение.

Разбира се, обхватът на закрила на авторското право за бази данни, състоящи се от произведения, които не са закриляни, или от обикновени данни е по-малък от обема на охраната, предоставян на базата данни, включваща закриляни материали. В случая с базата данни, състояща се от елементи, които законодателно се отнасят към тези за общо ползване,

---

[171] Закон за авторското право от 1976 г., 17 U. S. C. §101 (определение за „компилация").
[172] Отново там, §101(Определение на „колективни произведения").
[173] Виж., напр. Закон на Украйна за авторското право и сродните му права в редакцията на закона за внасяне на изменения в закона за авторското право и сродните му права от 14 юли 2001 г., „Голос України", 16.08.2001 г., бр. 146, Ст. 30, ч. 2; Фейст Пъбликейшънс Инс. срещу Рурал Телефоун Сървисис Ко. (Feist Publications, Inc. v. Rural Telephone Service Co.), 499 U. S. 340, 111 S. Ct. 1282, 1287, 1288, 1289, 1290, 1293 (1991).
[174] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.), Допълнителни разпоредби, §2, т. 13.
[175] Закон на Руската федерация за правната закрила на програмите за електронноизчислителни машини и бази данни от 23 септември 1992 г. № 3523-1, официален печатен орган на РФ „Ведомости Съезда народных депутатов РФ и Верховного Совета РФ", 1992 г., бр. 42, Чл. 2325, Чл. 1.

авторското право закриля само подбора, координацията и подреждането на материалите, влизащи в състава на такива бази данни. Авторското право обаче не забранява свободното използване на същите тези материали.

Нещо повече, много от базите данни не подлежат на закрила от авторското право като не отговарящи на критерия за оригиналност, въпреки евентуалните значителни усилия и инвестиции, които се изискват при тяхното съставяне. Пример за такива бази данни могат да бъдат телефонните справочници, чийто азбучен принцип за изграждане далеч не е оригинален.[176]

Същевременно в съвременното право за интелектуална собственост набира сила тенденцията за предоставяне на закрила *sui generis (чрез особено право)* на базите данни, които не са закриляни от авторското право.

Така, през 1996 година Европейският съюз прие Директива[177], според която на правна закрила подлежат онези бази данни, чиито съставители са направили значителни инвестиции в получаването, верификацията и презентацията на техните съставни части. Процесът на имплементация на нееднозначно възприетата Директива в националното законодателство на държавите – членки на Европейския съюз се проточи: от 15 държави-членки към началото на 2000 година нейната имплементация бе осъществена само в девет държави[178].

Законопроект с аналогично съдържание сега е в процес на разглеждане от Конгреса на САЩ.[179] Предложеният закон забранява възпроизвеждането и търговското използване изцяло или на значителна (като количество или качество) част от „избрана информация", която е била съставена, подредена и се поддържа от друго лице чрез инвестиране на значителни парични и други ресурси по такъв начин, че това да причинява вреда на наличния или потенциален пазар за пласмент на въпросното друго лице. Предлаганият срок на закрила е 15 години. Предвидените методи за закрила на правата на съставителите на сборници включват компенсиране на щетите и налагане на съдебна забрана. За умишлените нарушения се въвеждат наказателно-правни санкции.

При базите данни българският закон закриля два вида права на интелектуална собственост. Веднъж това е авторското право, което принадлежи на лицето, което е извършило подбора или подреждането на включените произведения и/или материали, освен ако в договор е предвидено друго (чл. 11. ЗАПСП). Промените в ЗАПСП от ДВ, бр. 77 от 2002 г. предвиждат създаването на *sui generis* право на производителя на бази данни. Производителят на бази данни е дефиниран като „физическото или юридическото лице, което е поело инициативата и риска за инвестиране в събирането, сверяването или използването на съдържанието на база данни, ако това инвестиране е съществено в количествено или качествено отношение." (чл. 93б, ал. 2 ЗАПСП). Особеното право на производителя на базите данни продължава 15 години.

Правото на производителя на бази данни не е авторско или сродно на авторското. То се състои в правото на такъв производител да не допуска извличането на част от съдържанието на базата данни върху друг носител или повторното й използване под друга форма, включително разпространение на копия или предоставяне по цифров път, без негово разрешение. Това право възниква за производителя на базата данни, независимо от това, дали базата сама по себе си е новаторска и притежава елемент на оригиналност – т. е. дали има характер на произведение, резултат на творческа интелектуална дейност и дали е годен обект на авторско право. За да бъдат обект на авторско право, базите данни трябва да бъдат

---

[176] *Виж* Фейст Пъбликейшънс Инс. срещу Рурал Телефоун Сървисис Ко. (Feist Publications, Inc. v. Rural Telephone Service Co.), 499 U. S. 340, 111 S. Ct. 1282 (1991). – P. 1291-1293.

[177] Директива 96/9/ЕО на Европейския парламент и на Съвета от 11 март 1996 г. относно правната закрила на базите данни, OJ L 077 от 27.03.1996 г., p. 20.

[178] *Виж,* Въвеждане и приложение на Директива 96/9/ЕО относно правната закрила на базите данни 379, достъпна на http://ec.europa.eu/internal_market/copyright/docs/databases/etd2001b53001e72_en.pdf.

[179] Закон за пиратството срещу сборници информация (Collections of Infromation Antipiracy Act (Reported in the House)), H.R.354. RH; http://www.codata.org/codata/data_access/linn.html.

резултат от собствен подбор, систематизация и подреждане; като именно подборът и подреждането се закрилят от авторското право. Събраните по определен начин произведения, данни или други материали трябва да бъдат закриляни или от авторското право или от правото *sui generis*, или и от двете. Тяхното съдържание обаче не се ползува от същата закрила – то е нещо много по-различно от базата данни като сбирка.

Въвеждането на този нов вид право е продиктувано от развитието на дигитално записващата техника, която дава възможност за електронно копиране и пренареждане съдържанието на база данни, без това да представлява нарушение на каквото и да е авторско право. Това право действа без оглед на това дали базата данни или части от нея се ползват от закрилата на авторско право или на сродни на него права (чл. 93д ЗАПСП). Спецификата на посочените права на производителя на бази данни се изразява във факта, че то се основава не на творчество, което е обичайно за закрила на правата върху интелектуална собственост, а на направената инвестиция[180].

Към съставните произведения спадат също така **уебсайтовете** и **мултимедийните произведения**. Тези два вида произведения са широко застъпени в „мрежата на мрежите", а уебсайтовете изобщо са явление присъщо само на Интернет и повечето от мрежовите ресурси се съдържат именно в тях.

По физическата и правната си същност уебсайтовете са близки до базите данни. В качените на уебсайта текстове обикновено се съдържат препратки към други информационни ресурси, поместени в същия или в друг сайт. Уебсайтовете са механизми за достъп до систематизирана информация и в качеството си на оригинали подлежат на закрила също като базите данни.

Мултимедийни произведения са тези произведения, които представляват резултат от съчетаването на две или повече категории произведения под една форма.[181] Най-благоприятната от всички налични понастоящем форми за такова съчетание, разбира се, е цифровата.

Ако възможността за закрила на мултимедийните произведения по авторското право не буди съмнения, то определянето на обхвата на тази закрила е изключително утежнено. Проблемът е там, че мултимедийните произведения се раждат в следствие на процеса на конвергенцията на различни обекти на закрила от авторското право, възможна благодарение на съвременните информационни технологии.

По традиция в авторското право се обособяват няколко групи закриляни обекти, всяка от които се състои от няколко вида произведения, като при това на едната група може да се предоставя закрила с различен обхват от предоставяния на другата група. Смисълът на подобно деление е, че то позволява да се отчитат всички особености и качествените различия между всички категории охранявани произведения.

Появата на цифровите технологии направи възможна трансформацията на всички закриляни от авторското право обекти в цифрова форма и тяхното обединяване в рамките на едно произведение. Какво, например, представлява интерактивната учебна програма по история на литературата и изкуството с аудио- и видео- съпровод, компютърна програма, литературна творба, аудиовизуално произведение? За съжаление, съвременното авторско право не дава еднозначни отговори на тези въпроси.

5.3. Използване на произведения в Интернет

В информационната епоха, при наличието на възможност за достъп до информацията, намираща се в електронните мрежи, на практика от всяка точка на земното кълбо и едновременно от неограничен кръг лица, с особена острота се поставя въпросът за засилена закрила на лицата – носители на правата на интелектуална собственост. В най-голяма степен

[180] Каменова, Цв., Авторско право. Международно и национално, С., 1999, с. 416.
[181] *Виж* Thomas J. Smedinghoff, The Software Publishers Association Legal Guide to Multimedia 4 (1994).

въздействия търпят авторските и сродните права (права върху произведения на литературата, науката и изкуството; права на продуценти и изпълнители, права на производители на бази данни и създатели на компютърни програми и др.).

Основна функция на авторското право като правен институт е да осигури защита на носителите на авторски права (автори или лица, на които е отстъпено изключителното право на ползване) срещу неразрешено използване на техните творби от страна на трети лица. Тази закрила се осъществява чрез обявяване за незаконно, т. е. за нарушение, на всяко възпроизвеждане, публично представяне, предаване и разпространение на произведението, включително и по Интернет, без съгласието на носителя на авторското право върху него.[182]

Съгласно чл. 18 от ЗАПСП авторът има изключителното право да използва създаденото от него произведение и да разрешава използването му от други лица. В ал. 2 на чл. 18 са изброени действията, които се считат за използване и представляват имуществените права на автора. Сред тях най-съществено значение за електронната търговия и доставчиците на онлайн услуги имат т. 1, 2 и 10:

- Ø възпроизвеждане на произведението;
- Ø разпространение на произведението сред неограничен брой лица; и
- Ø предлагането на неограничен брой лица на достъп до произведението, който да може да бъде осъществен от място и по време, индивидуално избрани от всеки от тях.

Определенията за възпроизвеждане и разпространение се съдържат в §2, т. 3 и т. 4 от ДР на ЗАПСП. Съгласно новите редакции на тези дефиниции възпроизвеждане на произведение е „прякото или непрякото размножаване в един или повече екземпляри на произведението или на част от него, по какъвто и да е начин и под каквато и да е форма, постоянна или временна, включително запаметяването му под цифрова форма в електронен носител". Разпространение на произведение е „продажбата, замяната, дарението, даването под наем, както и съхраняването в търговски количества, а също и предложението за продажба или даване под наем на оригинали и екземпляри от произведението".

Произведението може да бъде използвано със съгласието на автора, освен когато законът предвижда друго, като авторът има право на възнаграждение за всеки вид използване на произведението и за всяко поредно използване на същия вид (чл. 19 и чл. 35 ЗАПСП). Следователно използването на произведения като компютърни програми, мултимедийни продукти, музика, филми, бази данни и пр., включително тяхното възпроизвеждане върху магнитен или оптичен диск, зареждането през Интернет на друг диск (сървър) или съхраняването им в паметта на компютъра както и последващото им разпространение или предлагане на достъп до тях на неограничен брой лица следва да се прави само след получаване на съгласието на носителя на авторското право. Това съгласие се дава посредством сключен с автора договор за използване на произведение (лицензионен договор), при което авторът отстъпва на лицето – ползвател изключителното или неизключителното право да използва създаденото от него произведение при определени условия. С промените от бр. 77 на ДВ от 2002 г. е направено допълнение на дефиницията за ползватели на произведения в §2, т. 6 на ЗАПСП, като изрично е допълнено, че такива са „физическите и юридическите лица, като доставчици на съдържание в Интернет и други, които довеждат произведението до знанието на читателите, зрителите и слушателите пряко или чрез други лица – разпространители". С този текст за първи път е въведено в българското законодателство като легален термин понятието „доставчици на съдържание в Интернет" (такива са онлайн медиите, Интернет порталите, ресурсни и информационни сайтове и пр.). Създаването на позитивно-правна уредба, уреждаща статута на тези субекти е от изключително значение, доколкото в дигиталната епоха в традиционната верига, доставяща интелектуалните продукти до крайните потребители – автор --> издател

[182] Апостолова, Р., Защита на разпространението на филми и развлекателен софтуер по Интернет, сп. „Собственост и право", 2002 г., кн. 6, с. 64

(продуцент) --> разпространител, ролята на разпространител (а често и на издател) все по-често играят именно доставчиците на съдържание в Интернет. Без ясно дефиниране на техните права и задължения чрез законови и договорни инструменти съществува реална опасност от лишаване на носителите на авторски права от възможността да управляват своите имуществени права, включително правото да получават възнаграждение за всяко използване на произведенията им.

С промените, направени в ЗАПСП през 2000 година, бе въведено ново имуществено право за авторите да разрешават или забраняват използването на тяхното произведение чрез предаването по безжичен път или чрез кабел или друго техническо средство на достъп на неограничен кръг лица до произведението или част от него по начин, позволяващ да бъде осъществен от място и време, индивидуално избрани от всеки от тях (чл. 18, ал. 2, т. 10). Така се акцентира върху правото на авторите да разрешават или забраняват публикуването на своето произведение в Интернет. Самото наличие на музикални произведения, филми, компютърни програми или игри – обект на авторско право на публично достъпен Интернет адрес, поддържан от доставчик на съдържание в Интернет, без съгласието на носителя на това право, представлява нарушение на действащото законодателство и за него следва да се носи съответната гражданска, административна или наказателна отговорност. Тази отговорност е за лицето, възпроизвело произведението. В случай, че това е доставчикът на онлайн услуги или той е бил уведомен за нарушението и въпреки това не е предприел мерки по преустановяването му - отговорността е за него. Отговорност следва да се носи и при неоторизирано разпространение на произведението, когато на сайт на доставчик на онлайн услуги може да се поръчат по изготвен от него каталог произведения, за което липсва съгласието на носителите на авторски права върху тях.

Без съгласието на авторите свободното използване на произведения е допустимо само в случаите, посочени в закона, при условие, че не се пречи на нормалното използване на произведението и не се увреждат законните интереси на носителя на авторското право. С последните изменения на чл. 24 от ЗАПСП е добавена нова хипотеза, според която без съгласието на носителя на авторското право и без заплащане на възнаграждение е допустимо временното възпроизвеждане на произведения, ако то има преходен или инцидентен характер, няма самостоятелно значение, съставлява неделима и съществена част от техническия процес и се прави с единствената цел да позволи предаване в мрежа чрез посредник. Това изключение включва действия по време на предаване по Интернет като преглеждане на страници (*browsing*) и кеширане (*casheing*), при условия, че посредникът не изменя информацията. Така в електронната търговия се дава възможност на доставчиците на достъп до Интернет да посредничат при предаването на електронни документи – обекти на авторско право, без да е необходимо съгласието на носителя на правото за всяко възпроизвеждане на произведението.

Съгласно чл. 25 ЗАПСП без съгласието на носителя на авторското право, но при заплащане на компенсационно възнаграждение е допустимо възпроизвеждането на произведения, независимо върху какъв носител, от физическо лице за негова лична употреба, при условие, че не се извършва с търговска цел. Компенсационното възнаграждение се заплаща не директно от физическите лица – възпроизвеждащи произведенията за лично ползване, а от лицата, които произвеждат или внасят празни звуконосители или видеоносители и апарати, предназначени за записване или възпроизвеждане по репрографски начин. Това възнаграждение се заплаща по определения в чл. 26 ЗАПСП ред на организации, представляващи отделните категории носители на права по този закон.

Новоприетият чл. 25а на ЗАПСП (в сила от 01.01.2003 г.) предвижда, че при използването на произведения по чл. 24 и чл. 25 без съгласието на носителя на авторското право, това използване не може да се извършва по начин, който е съпроводен с премахване, повреда, унищожаване или разстройване на технически средства за защита, без съгласието на носителя на авторското право. С посочената разпоредба се прави опит за имплементиране в националното законодателство на нормата на чл. 6 от Директива 2001/29/ЕС, задължаваща

страните-членки на ЕС да създадат условия за ефективна защита срещу извършване на действия, насочени към заобикаляне по какъвто и да е начин на използвани технологични средства за защита от неправомерно използване на обектите на авторско право.

Следва да се отбележи, че и двете посочени изключения не се отнасят до компютърните програми, за които се прилагат специалните правила на чл. 70 и 71 от ЗАПСП, разгледани подробно по-горе.

5.4. Особености на поместените в Интернет произведения като предмет на авторското право и проблеми на правната им закрила

Особеностите на поместените в Интернет произведения като предмет на авторското право са обусловени от специфичната форма на тяхното фиксиране. Цифровата форма на фиксиране на тези произведения прави възможни техните уникални, по-рано невъзможни, физически свойства и обуславя значителните проблеми на тяхната правна закрила.

5.4.1. Технически и правни аспекти

По-долу са посочени техническите фактори, на които са подчинени поместените в Интернет произведения, и предизвиканите от тези фактори правни проблеми.

1) Липса на загуба на качеството при възпроизвеждане. За разлика от екземплярите на произведенията, изготвени с прилагане на аналогови методи за копиране (като фотокопирни апарати, видео- и аудио- магнетофони, факс апарати и т. н.), цифровите екземпляри представляват идеални копия без каквато и да било загуба на качеството. Първото цифрово копие абсолютно не се различава от хилядното копие, направено от един и същи оригинал. Тъй като всяко копие е идеално, не съществуват качествени ограничения, които да попречат на пиратите да направят колкото си искат копия и получателите на въпросните копия няма да изпитат нужда да се обърнат към легален източник, за да направят копие, което да не отстъпва по качеството си на оригинала.

2) Незначителност на разходите за възпроизвеждане и разпространение. За разлика от практиката на разпространение на обикновените екземпляри на книги, списания, музикални касети или компактдискове, видеокасети или програмно осигуряване, стойността на копието на поместено в Интернет произведение е незначителна, като същото важи и за разходите, свързани с доставката на това копие на крайния потребител по мрежата. Като се вземе предвид, че стойността на поддръжката на уебсайта не зависи от обема на получената от този сайт информация (такива са реалностите на съвременния пазар на телекомуникациите), за пиратите нарушенията на авторското право не са съпроводени с кой знае колко значителни разходи.

3) Способност да се действа анонимно. Като използват съществуващите днес технологии, „пиратите" са способни да действат в Интернет анонимно, без да оставят следи от дейността си. Анонимността е една от опасностите в Интернет, защото поне на теория позволява на пиратите безнаказано да причиняват вреда, като с това отричат общия принцип на юриспруденцията, според който лицата, причинили вреда, имат задължението да я компенсират. Като резултат може да се предвиди по-големият брой на нарушенията в ситуация, в която същите ще остават безнаказани, отколкото в случаите, когато на техните извършители ще се наложи да понесат отговорността си за стореното.

Анонимната дейност, обаче, не е специфичен проблем на авторското право, а засяга всички престъпления и деликти, които се извършват в Интернет. По такъв начин би било по-целесъобразно да се обърнем към проблема за вредата, която причинява анонимността като такава, а не да се занимаваме с разработката на мероприятия, които закрилят само притежателите на авторските права. Нещо повече, съществува нещо като естествено ограничаване на сферите и мащабите на анонимните действия, особено когато тези действия имат търговски характер. На определен етап дейността може да стане достатъчно значима, за

да остави най-малкото косвени доказателства (както в „реалния", така и във „виртуалния" свят), позволяващи да бъде идентифициран нарушителят.[183]

3) Необразовани потребители. Мнозина, ако не мнозинството от потребителите не разбират съществуващата система за закрила на авторските права[184]. Проблемът на необразованите потребители засяга както „реалното", така и „виртуалното" пространство, обаче Интернет позволява на такива потребители доста лесно да разпространяват произведения, които се закрилят от авторското право. В много от случаите подобно разпространение може, дори неумишлено, да причини вреди, като например, в случая на препращането на трети лица на произведения, които са закриляни от авторското право и са получени от потребителя по законен начин от притежателя на авторските права. По такъв начин ние можем да получим серия от относително незначителни нарушения, които сумарно могат да доведат до значителни загуби за притежателите на авторските права.

5.4.2. Социологични и културни аспекти

Освен върху техническите и правните аспекти, които имат значително влияние върху положението на нещата при закрилата на поместените в Интернет произведения, си струва да се спрем и върху някои основни проблеми, свързани с отношението на потребителите към интелектуалната собственост като цяло и в частност към авторското право. По-долу се разглеждат определени социологични и културни аспекти на Интернет общността и тяхното евентуално влияние върху желанието на потребителите да плащат за използването на поместените в Интернет произведения, респективно върху желанието да се използват обектите, закриляни от авторското право, в съответствие с неговите норми.

Отношението на потребителите към авторското право варира от тезата, че „интелектуалната собственост изобщо не трябва да е обект на закрила", до императива за „задължителната и максимално качествена закрила на авторските права". Могат да бъдат обособени пет основни сегмента на гореспоменатия спектър от мнения[185]:

1) „Информацията трябва да е свободна". Привържениците на тази теза смятат, че всяка интелектуална собственост трябва да принадлежи на цялото общество и може свободно да се използва от всички негови членове. И въпреки че не е лесно да се открият заклети привърженици на тази идея, много по-лесно е да се намерят такива, които смятат, че всичко намерено от тях в Интернет може да се използва безплатно.

2) „Право на препратка". Привържениците на тази идея вярват, че произведенията могат свободно да се използват при условие, че се посочват техните източници. Сигурно пак няма де е лесно да се открият безусловни привърженици на тази идея, но още по-трудно е да се намерят хора, дори сред авторите, които поне от време на време не са прибягвали до прилагането ѝ на практика.

Колкото и да е неприятно, изискването за задължителността на препратката се съдържа в законодателството далеч не на всички страни и често не се отнася за всички категории произведения[186] (в това отношение българският закон представлява едно добро изключение[187]), макар че етичните норми, формирани сред Интернет потребителите, като правило поощряват препратките.

3) „Ограничено използване на произведенията". Привържениците на тази идея смятат, че творците, създаващи обекти на интелектуална собственост, трябва да имат определени права, които да закрилят техните произведения, но същевременно отричат абсолютния характер на въпросните права. Привържениците на идеята за ограничено използване на произведенията се стараят да намерят баланса между необходимостта от закрила на правата

---

[183] *Виж* Lance Rose. The Emperor's Clothes Still Fit Just Fine, Wired., февруари 1995 г., p. 103, 104; Philip E. Ross. Cops Versus Robbers in Cyberspace, Forbes., 9.09.1996 г., p. 134, 137

[184] *Виж* Jessica Litman, *The Exclusive Right to Read*, 3 Cardozo Arts & Ent. L. J. 29, 50-51 (1994).

[185] *Виж* Lance Rose. Is Copyright Dead on the Net, Wired., ноември 1993 г., p. 112

[186] Mark A. Lemley. Rights of Attribution and Integrity in On-line Communications, J. On-line L., 1995, Art. 2.

[187] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.), Чл. 24, ал. 3.

на творците и допустимостта на нарушаването на авторските права, продиктувано от техния стил на живот или от нуждите на бизнеса.

Тази гледна точка с по-голяма или по-малка точност отразява позицията на съвременното авторско право на много юрисдикции, където едновременно със сигурната закрила на притежателите на авторските права, при определени обстоятелства се разрешава и свободното използване на произведенията.

4) „Неимуществени права". Под неимуществени права на автора, естествено, се подразбира неговото право „да изисква признаването на авторството му върху произведението и да противодейства на всяко извъртане, изкривяване или друго изменение на въпросното произведение или на всяко друго посегателство върху произведението, способно да накърни честта или репутацията на автора".[188]

Изобщо, неимуществените права са рожба на идеята, че авторските произведения представляват продължение на самия автор, така че авторът може да контролира начина, по който обществото възприема автора чрез неговите произведения. В отношенията между автора и всеки потенциален потребител (включително с цесионерите и лицензиантите) доктрината на неимуществените права предоставя безспорни предимства на първия, а в много от юрисдикциите, например, в България[189], авторът не може да прехвърли (преотстъпи) своите неимуществени права.

5) „Силни права на авторите". Привържениците на тази идея смятат, че авторът трябва да притежава съществени пълномощия за контрол върху използването на неговото произведение. Те биха отишли дори по-далеч от неимуществените права, предоставяйки на автора и правото за контрол върху всички случаи на използване на неговото произведение.

Поради съображения, свързани с формирането на държавна политика в областта на закрилата на авторските права, би било целесъобразно да се замислим за начина, по който съвременното авторско право би могло да повлияе върху поведението на хората, придържащи се към гореспоменатите гледни точки. Важно е да се отбележи, че поддръжниците на идеята, че „трябва да има свобода на информацията", са способни с голяма лекота да престъпят нормите на авторското право, независимо от строгите санкции за нарушаването им, като при това укрепването на нормите на авторското право с цел оказване на влияние върху поддръжниците на свободното използване на информацията няма да има особен смисъл.[190] Като се вземе предвид, че благодарение на Интернет културата е нараснал броят на противниците на силните права върху интелектуалната собственост, едно насочено към усилване правата на авторите ново законодателство в сферата на авторското право едва ли ще постигне желаните резултати.

Погледнато от исторически аспект, нещата се развиха така, че в ролята на главни популяризатори на Интернет се изявиха учените и технолозите, мнозина от които могат да бъдат причислени към привържениците на идеята, че „трябва да има свобода на информацията" (или към привържениците на „правото на препратка").[191] С течение на времето се привнесе друго отношение към интелектуалната собственост.

Да вземем, например, поколението на хората, които още не са навършили 30 години. Почти цял живот те са имали лесен достъп, често в собствените си домове, до голямо количество устройства, които са могли да използват за нарушаване на авторските права: аудио- и видео-магнетофони (и относително евтини празни касети), висококачествени и евтини копирни машини, факсове и може би най-мощния начин за копиране – персонален компютър. В резултат на това поколението под 30 години израсна, имайки възможността лесно и евтино да експроприира интелектуална собственост. Що се отнася до студентите, малцина от тях са закупили по-голямата част (или дори поне нещо) от програмното

[188] Бернска конвенция за закрила на произведенията на литературата и изкуството. Парижкият акт от 24 юли 1971 г., с изменения, внесени на 2 октомври 1979 г.
[189] Закон за авторското право и сродните му права (изм. ДВ бр. 59 от 20 юли 2007 г.), Чл. 16.
[190] *Виж* Lance Rose. The Emperor's Clothes Still Fit Just Fine, Wired., февруари 1995, p. 104.
[191] Kathy Rebello. Making Money on the Net, Bus. Week., 27.09.1996 г.

осигуряване за своя компютър, вместо просто да вземат „на заем" необходимите програми от познати или от съседи в общежитието. А колко от тях вместо това са съставяли сборници от любимите си песни? Колко от тях са презаписвали музика на своя касета от нечии плочи? Дали съществуват или дали е възможно да бъдат изобретени механизми, които ефикасно да убедят такива хора, че техните действия са забранени от съществуващата система?

Първоначалните потребители на Интернет се обединиха с поколението на тези, които още нямат 30 години и заедно формираха интересна Интернет психология. Интернет обществото с все по-голям нихилизъм се отнася към опитите да се докаже, че да речем, изпращането на съобщения на електронната поща в списъците за разпращане[192] или създаването на сайт на феновете на някой филм[193] може да представлява нарушение на авторското право.

Нещо повече, тъй като голям брой от притежателите на авторски права безвъзмездно се разделят с ценна интелектуална собственост, у потребителите се създава навик повсеместно да очакват само безплатни материали. При тези обстоятелства потребителите не бързат да плащат за интелектуалната собственост, понеже са наясно, че някъде трябва да съществува и безплатна алтернатива. Необходимостта да бъдат изпълнени дори незначителни формалности, като например да се попълни регистрационен формуляр, отблъсква много потребители. Навикът за безплатно използване все повече усложнява стремежа на притежателите на авторски права да получават такси от потребителите.

Макар че идеята за правното огрaмотяване на Интернет общността изглежда абсолютно реална, опитите да се промени самата мрежа с цел привеждане на нейното ползване в съответствие със съществуващите норми на авторското право ще изискват значими усилия. Нещо повече, всички стремежи за създаването на система за борба с „дребните нарушения" са обречени, тъй като те са неефективни от гледна точка на съотношението между обществените разходи и ползата за обществото.[194] На практика, този подход с времето може да докаже своята непродуктивност дори за притежателите на авторски права.[195]

Значително по-приложимо изглежда комплексното прилагане на методите на авторското право и на икономическите фактори, а именно – реализацията в Интернет на моделите за кръстосано субсидиране, подобни на съществуващите в радиото и телевизията, където не се взема такса от аудиторията на дадени програми, а се правят отчисления от организациите, които ги излъчват, за използването на защитени от авторското право материали, които се осъществяват от средствата, постъпващи от рекламодателите.

5.5. Изводи към този раздел

През последното десетилетие Интернет действително се превърна в основа на „информационната супермагистрала" на бъдещето. Развивайки се днес със смайващи въображението темпове, тази „мрежа на мрежите" се превърна от начин на общуване в образователните и изследователските кръгове в арена на напрегната конкурентна борба.

Днес Интернет се превърна в основен начин за разпространение най-разнообразна информация в глобални мащаби. Тази информация често се предава чрез Интернет във вид на произведения, подлежащи на закрила от авторското право на всяка от страните на Бернския съюз, включително и в България и Румъния, наравно с произведенията, фиксирани в по-традиционни форми, при условието за съответствие на установените от

---

[192] *Виж* Mitch Betts. On-line Pay Per View, ComputerWorld, 5.06.1995 г., p. 58

[193] *Виж* Constance Sommer. Film Rights Falling Through the Net, San Jose Mercury News, 10.12.1996 г., p. 10E.

[194] *Виж* Margie Wylie. Can Copyright Survive the Digital Age? Should It?, Digital Media: A Seybold Report, 3.07.1995 г.; Steve G. Steinberg. Seek and Ye Shall Find (Maybe), Wired., Май 1996 г.

[195] *Виж* Jessica Litman, The Exclusive Right to Read, 3 Cardozo Arts & Ent. L. J. 29, 46 (1994).

законодателството на страната критерии за закрила, независимо от изпълнението на каквито и да било формалности.

Може да се направи обаче изводът, че притежателите на авторски права се сблъскват със значителни рискове, обусловени от съществуването на информационните технологии. Интернационалният характер на Интернет и цифровата форма на фиксиране на поместените в мрежата произведения значително усложняват процеса на реализация на правата от авторите и от техните правоприемници.

Независимо от това ние разполагаме с очевидни свидетелства, че продължават да се създават обекти на интелектуалната собственост, включително само за тяхното разпространение чрез Интернет. Действително, огромно, почти неподдаващо се на изчисляване количество обекти на интелектуалната собственост продължава да се появява и да се разпространява в Интернет, въпреки наличието на гореспоменатите проблеми.[196] По такъв начин, въпреки твърденията на тези, според които заплахите, каквито представляват информационните технологии за закриляните от авторското право произведения, няма да спомагат за тяхното по-нататъшно създаване и разпространение, подобни твърдения са лишени от достатъчно реални основания.

В същото време може да се предположи, че съчетаването на Интернет културата с общите последствия от техническата еволюция променя отношението към авторското право в обществото. Културата днес обединява в себе си разбирането на необходимостта от закрила на авторските права с проявата на търпимост към дребните, но многобройни нарушения на същите. С други думи казано, ние желаем да зачитаме чуждите права върху интелектуалната собственост, но същевременно не искаме да променим нашия обичаен начин на живот, като той е свързан с многобройни, макар и дребни, почти битови, но все пак противозаконни действия. Опитите това отношение, предизвикано от социални и културни фактори, да бъде променено изключително чрез методите на авторското право (и още по-лошо – опитите за налагане на далеч по-строги наказателни санкции), няма да имат търсения ефект.

[196] *Виж* Steve G. Steinberg. Seek and Ye Shall Find (Maybe), Wired., май 1996 г., p. 108.

6. Компютърни измами

6.1. Въведение

Известен е широк спектър от компютърни измами, много от които представляват вече съществуващи измами, но са пренесени в електронна среда, напр. „схеми Понци" (пирамидални продажби или инвестиции). Интернет, обаче, значително намалява разходите за осъществяване на много от тези измами, тъй като използването на електронна поща, Интернет страници, бюлетин бордове, средства за незабавна комуникация и чат стаи заместват пощата и факса. Това означава, че извършителите могат да си позволят да си поставят за цел по-широк кръг от хора и така да работят с доста по нисък процент успешни отговори: напр. на извършител, който изпраща 1000 писма по пощата му е необходим 1% успеваемост, за да покрие разходите си, докато на извършител, който изпраща 1 000 000 писма по електронната поща му е необходим едва 0.00001% успеваемост, за да си възвърне вложеното.

Измами, за които е необходимо масово разпространяване на фалшива информация, напр. дъмпингови схеми с акции (*'pump and dump' stock schemes*) също се улесняват от ползването на чат стаи, форуми, Интернет бордове и електронна поща. Такива измами обикновено изискват бързи отговори от страна на потърпевшите, за да могат извършителите да имат време да осъществят измамата преди тя да е изобличена или преди цената на акциите рязко да спадне. Интернет предлага евтини, бързи и често анонимни инструменти, с които извършителите да разпространяват невярна информация. Сериозното разрастване на Интернет страниците за търгове, напр. eBay също е подходяща среда за различни измами.

С развитието на компютърните технологии, извършителите разработват специални нови видове измами, свързани с тези технологии, напр. фишинг, фарминг и клик измами (*phishing, pharming and click-through frauds*). Електронната среда на измамите непрекъснато се променя и могат да се появят нови измами, като и по-сложни разновидности на вече съществуващи такива. Както правораздавателните органи и правни системи разработват нови методи за справяне с компютърните измами и обществото става все по-предпазливо относно електронни сделки и отношения, така и измамите стават все по-убедителни и все по-автоматизирани. Някои от гореспоменатите измами попадат под националните закони, както за компютърна злоупотреба, така и за измама. Компютърните измами традиционно се уреждат допълнително и от законите за защита на потребителите. Таблица 1, по-долу, очертава актуалните ключови компютърни измами.

Борбата с компютърните измами път често се усложнява от широкото разпространяване на Интернет по света, което позволява на извършителите по-лесно да насочват усилията си към потърпевши в други юрисдикции и намалява вероятността за успешно противодействие от страна на националните правораздавателни органи и власти за защита на потребителите. Правораздавателните органи в други юрисдикции често са изправени пред практически или законови пречки (или понякога просто не желаят) да предоставят ефективна помощна чужди граждани. Правораздавателните органи са затруднени от:

- Технологични проблеми като способността на извършителите да действат с псевдоними или анонимно или да провеждат действията си чрез верига от електронни системи и/или услуги;
- Правни проблеми като затруднения при категоризирането на определени видове измами съгласно съществуващото национално законодателство, при осигуряването на необходимите доказателства за повдигане на обвинение или за осъждане, при проверяването, че събраните доказателства отговарят на изискванията за допускане за разглеждане в съда;

- Проблеми, свързани с недостиг на информация като липса на познания сред следователите, прокурорите и съдебната власт за използваните технологии или за механизма на компютърната измама. При по-сложни измами е трудно да се обясни по достъпен начин какво е естеството на престъпното деяние на неспециалисти като съдебни заседатели.

Последните международни инициативи за борба с компютърните измами са насочени към хармонизиране на правните разпоредби, за да се подпомогне ефективното трансгранично правораздаване, както и към инициативи за трансгранично сътрудничество (напр. обмяната на данни между националните органи за защита на потребителите). Тези инициативи са подкрепени от национални схеми за осведомяване на потребителите и системи за докладване на измами от потребителите.

Таблица 1: Примери за компютърни измами

Измама	**Вид измама**	**Ниво на технически познания**	**Същност на измамата**	**Цел на измамата**
Кражба на самоличност	Не/електронна	ниско	Използват се откраднати данни като информация за кредитни/дебитни карти за пазаруване в Интернет. Откраднатата информация се придобива по не/електронен път (вж. фишинг по-долу). Широкото ползване на кредитните карти с чип и ПИН в Обединеното кралство доведе до намаляване на измамите с кредитни карти по неелектронен път за сметка на измамите с кредитни карти по електронен път, където самата карта не участва.	Кражба на самоличност чрез кредитни/дебитни карти обикновено се извършва с цел придобиване на вещи с висока стойност, които извършителят лесно може да препродаде. Откраднатите карти често се използват за закупуване на стоки от магазини или продавачи в Интернет, като по този начин избягват мерките за сигурност при сделки лице в лице. .
Търговски измами	Не/електронна	ниско	Има голям брой търговски измами, които използват електронни услуги като електронна поща, средства за незабавна комуникация и Интернет страници. Много голяма част от тях започват като измами по факс или по пощата. Често са варианти на следните измами:	
			Извършителят изпраща съобщение по електронна поща до фирма, лице или продавач на търг с цел закупуване на стоки чрез кредитна карта.	Кредитната карта е фалшива или откраднатата и при доставката на стоките, продавачът няма да получи плащане или плащането ще бъде върнато от кредитната институция.
			Извършителят предлага стоки за продажба, често на много ниски цени (най-често на Интернет страници за търгове).	Купувачът праща плащане или депозит, но не получава заявените стоки или получава нискокачествени, дефектни или фалшиви стоки.
			Извършителят търси да закупи стоки от фирма, лице или продавач на търг и предлага да заплати с финансов инструмент, напр. с чек, който е за сума, по-голяма от цената на стоките. Извършителят изисква от продавача да извади разходите си (и често и комисионна) и да върна оставащата сума с чек или по банков път на извършителя или на трета страна-съучастник.	Финансовият инструмент е фалшификация, продавачът ще загуби, както стойността на продаваните стоки, така и парите, върнати на извършителя или на трета страна-съучастник.

			Извършителят изисква помощ при прехвърляне на пари от чуждестранно дружество или от чужда държава. Парите могат да бъдат във връзка с предложение за работа, търговска сделка или благотворителна дейност. Извършителят може да поиска от потърпевшия банков трансфер за плащане на мита/административни такси/подкупи или преводни нареждания, като процент от стойността им трябва да се върне на потърпевшия.	Пари не са замесени, но извършителят просто ще открадне сумата, изпратена за плащане на мита/административни такси/подкупи или преводни нареждания. По подобен начин, финансови инструменти, изпратени до потърпевши ще бъдат откраднати или фалшиви, т.е. без стойност, а преведените пари- откраднати.
			Извършителят убеждава лица или малки фирми да им достави стоките повторно. Такава дейност може да бъде отделна задача, търговски отношения или друга съвместна инициатива. Когато потърпевшият приеме, той получава предварително надписани етикети с данните на доставчика, които да се използват за доставяните стоки. Също така може да получи финансов инструмент, напр. чек, който да покрие разходите за повторното доставяне. След това той получава от извършителя стоките, поръчани в Интернет. Потърпевшият поставя новите етикети, които доставчикът приема да достави на реалния адрес на извършителя.	Извършителят използва откраднати кредитни карти да пазарува едновременно от различни Интернет страници. Обикновено се използва адресът за кореспонденция на картата, но за адрес на доставка се пише този на потърпевшия. В повечето случаи извършителят е събрал достатъчно информация за потърпевшия, за да стане клиент на доставчика, в резултат на което потърпевшият трябва да заплати за повторното доставяне. Когато се изпраща финансов инструмент на потърпевшия, с който да заплати за повторното доставяне, той е фалшифициран или откраднат.
Схеми за изкуствено занижаване на цените на акциите	Не/електронна	ниско	Фалшива и/или подвеждаща информация се разпространява в чат стаи, форуми, Интернет бордове и по електронна поща с цел рязко понижаване на цената на акциите на дадено дружество.	Извършителите изчакват докато цената спадне на определено ниво и тогава купуват акциите; след това изчакват да се повиши, докато става ясно, че слуховете са неверни и продават акциите на печалба.
Дъмпингови схеми с акции	Не/електронна	ниско	Фалшива и/или невярна информация се разпространява в чат стаи, форуми, Интернет бордове и по електронна поща с цел рязко	Когато купи акции на ниска цена преди измамата и цената достигне определено ниво (*Pump*), извършителят продава закупеното преди цената на

(*Pump-and-dump schemes*)			повишаване на цената на слабо търгувани акции или акции на фиктивни дружества.	акциите да се понижи отново (*Dump*) и по този начин покачва цената и инвеститорите остават с акции на много ниска стойност.
		средно	При по-сложна разновидност на тази схема извършителите проникват в профилите за търгуване на акции на няколко потърпевши (чрез хакване или фишинг) с електронни брокери като E*Trade като продава съществуващите акции и използва средствата за закупуване на на слабо търгувани акции, като по този начин им повишава цената.	Когато купи акции на ниска цена преди измамата и цената достигне определено ниво (*Pump*), извършителят продава закупеното преди цената на акциите да се понижи отново (*Dump*) и по този начин покачва цената и инвеститорите остават с обезценени акции.
Клик измами (*Click-through fraud or click fraud*)	Електронна	Ниско до средно	Много Интернет реклами са част от система на плащане на клик (*pay-per-click*), където рекламодателят плаща на собственика на системата на базата на това колко пъти ползвателите кликват на рекламите. Собственикът на системата след това дели приходите със собствениците на Интернет страниците, където са качени рекламите. Например: системата на Гугъл Adsense. При клик измамите, кликването на рекламите в такива Интернет страници цели да се придобие друго предимство, освен това, посочено в рекламата.	Клик измамите имат две основни цели: Конкуренция- конкурентни фирми кликват на рекламата в Интернет на съперника си с намерението да увеличат разхода му, а не да получат повече информация за продукта или услугата. Приходи – собственик на Интернет страница, който хоства рекламите и използва софтуер или плаща на лица да кликват на реклами на неговата страница с цел да се увеличи прихода си от търсачката, а не да получи повече информация за продукта или услугата.
Измами на търгове	Електронна	Средно	Извършителят прониква в профила на законния продавач (обикновено чрез фишинг), който обикновено е с висока репутация и след това основава Интернет магазин.	Купувачите нареждат плащането, но не получават рекламираните стоки или получават некачествени, дефектни или фалшиви стоки. Личните и финансовите данни на потърпевшия могат да се използват за по-нататъшна кражба на самоличност.
Ескроу измами (*Escrow*)	Електронна	Средно до високо	Купувачите и продавачите стават все по-предпазливи, особено при Интернет търгове и затова извършителите могат да предложат ползването на трета страна посредник (escrow service) за осъществяване на размяна	Купувачите нареждат плащане на третата страна, но не получават заявените стоки. Продавачите, които пращат стоките на извършителите не получават плащане. Освен това, ако продавачите са предоставили данни за кредитна карта на фалшивата

			на парите за стоките. Понякога се компрометира истинска Интернет страница на трета страна посредник и се създава фалшива подобна страница от извършителите (вж. фарминг) или просто трета страна посредник не е автентична.	трета страна, те могат да са изложени на кражба на самоличност.
Фишинг	Електронна	Средно до високо	Изпращането на спам съобщения, привидно от финансова институция като банка, които изискват информация за сметки или друга лична или финансова информация. Съобщенията могат да съдържат линк към фалшивата Интернет страница, който използва кода и дизайна на автентичната страница. Така всяка въведена информация достига до извършителя.	Първоначалната цел на фишинг измамите обикновено е незаконен достъп до банкови сметки, картови сметки и сметки в Paypal. Някои фишинг атаки целят придобиването на незаконен достъп до услуги, като ISP и VoIP профили; компрометираните профили могат да се превземат и използват за спамиране, отклоняване на атаки срещу услуги и др.
Фарминг	Електронна	Високо	Пренасочване на трафик от една страница към друга, която се ръководи от извършителя, като се променя хост файла на компютъра на потърпевшия посредством компрометиране на рутъра на местната мрежа или възползване от уязвимостта на софтуера на DNS сървърите (DNS сървърите са устройствата, които отговарят за преобразуването на Интернет наименованията в реални адреси). Извършителят може да получи достъп до компютъра или рутъра на потърпевшия, когато той кликва на линкове или отваря приложения към съобщения.	Фармингът е пряко свързано с фишинг, дотолкова доколкото спам имейлите са първичното средство на атакуване. Както при фишинга, основните цели на фарминг измамите обикновено са незаконен достъп до банкови сметки, картови сметки и сметки в Paypal или незаконен достъп до услуги.

Източници на информацията в тази таблица включват: Американски център за оплаквания от престъпления в Интернет<http://www.ic3.gov/>; Инициатива „Стърлинг" на общинска полиция в Обединеното кралство <http://www.met.police.uk/fraudalert/>.

6.2. Международни инициативи

Както и с други видове компютърни престъпления, наднационални институции, като например ОИСР, Съветът на Европа и Европейският съюз, изтъкват факта, че без наличието на трансгранично сътрудничество борбата с компютърните измами би била напълно невъзможна. В резултат на това са организирани множество международни инициативи, насочени към борба с компютърни измами и/или осигуряващи защита на потребители в електронното пространство/през граница. Целта на тези инициативи е да гарантира, че страните участници:

- приели адекватни правни мерки в областта на наказателното право на национално ниво за справяне с електронните измами, включително и са приспособили съществуващото законодателство, така че да станат технологично неутрално или приложимо, както към съществуващите форми на некомпютърни измами, така и към измами, ползващи новите технологии;
- се опитали да хармонизират, доколкото е възможно, тези правни мерки в областта на наказателното право на национално ниво и свързаните с тях разпоредби с цел подпомагане на сътрудничеството на правораздавателните органи и системите за ускорено екстрадиране;
- са уредили механизмите за трансгранично сътрудничество между правораздавателните органи и другите регулаторни органи, включително национални агенции за превенция на измами и за защита на потребителите.

Организирани са също множество инициативи, които, без да са специално създадени за борба с компютърните измами, оказват своето влияние, например договори, свързани със сигурността на компютърни системи и мрежи.

6.2.1. Организация на обединените нации

През 1990 г. на 8^{мия} Конгрес на Обединените нации за превенция на нарушения и третиране на нарушителите е одобрена резолюция, която изисква от страните членки да увеличат усилията си в борбата срещу компютърни престъпления с помощта на следните мерки, ако е необходимо:

- модернизация на наказателните закони и процедури на национално ниво;
- подобряване на компютърната сигурност и превантивни мерки;
- приемане на подходящи мерки за обучение; и
- изработване на правила за етика при използването на компютри.

Препоръчва се също така Комисията на обединените нации за превенция и контрол на престъпленията да спомага за развитието и разпространението на цялостна рамка от указания и норми, която да помогне на държавите-членки в справянето с компютърни престъпления. През 1994 г. Обединените нации публикуват Наръчник на Обединените нации за превенция и контрол на компютърни престъпления. Този наръчник разглежда въпроси, свързани с компютърните престъпления, материални наказателни закони за защита на личността, процесуално право и нуждите и пътищата на международното сътрудничество.

На 4 Декември 2000 г. на Общото събрание е приета Резолюция за борба с наказуемата злоупотреба с информационни технологии(A/res/55/63), съгласно която:

„(а) Държавите следва да осигурят такива закони и практики, които не позволяват наличието на убежища за хора, наказуеми за злоупотреба с информационни технологии;

(б) Сътрудничеството между правораздавателните органи в разследването и преследването на международни случаи на наказуема злоупотреба с

информационни технологии трябва да бъде координирано между всички страни, свързани с конкретния случай;

(в) Страните трябва да обменят информация относно проблемите, които срещат в борбата си срещу наказуемата злоупотреба с информационни технологии;

(г) Служителите на правораздавателните органи трябва да са обучени и оборудвани за борба с наказуемата злоупотреба с информационни технологии

(д) Правните системи трябва да защитават поверителността, целостта и наличието на данни и компютърни системи от неправомерни нарушения и да осигурят наказание за наказуемите злоупотреби;

(е) Правните системи трябва да разрешават запазването на и бързия достъп до електронни данни, свързани с конкретни криминални разследвания;

(ж) Режими за съдействие трябва да осигуряват навременно разследване на наказуеми злоупотреби с информационни технологии и навременно събиране и обмен на доказателства при такива случаи;

(з) Обществеността трябва да бъде информирана за нуждата от превенция и борба срещу наказуемата злоупотреба с информационни технологии;"

6.2.2. Г-8

През 1997 г. Г-8 създава Подкомисия за високотехнологични престъпления, която се фокусира върху:

- създаване на международна 24-часова мрежа от лица за контакт специализирани във високите технологии, които да улесняват комуникацията на правораздавателните органи при разследванията.
- развитие на компютърни правни принципи за обстоятелства, при които дигитални доказателства са изтеглени в една държава, а автентичността им трябва да бъде установена от съдилища в друга държава.
- инструкции за проследяване на терористични и престъпни комуникации през граница.

През декември 1997 г. Г-8 приема десетте Принципа за борба с високотехнологични престъпления и План за действие за борба с високотехнологични престъпления от десет точки (виж по-долу). Основните принципи включват:

- разработване на широкообхватни материални и процесуални закони за борба с компютърните престъпления на международно ниво;
- координация на разследването и преследването на високотехнологични престъпления на международно ниво;
- защита на поверителността, целостта и наличието на данни и системи от неправомерни нарушения и осигуряване на наказания за сериозните злоупотреби;
- координация на работата на Г-8 в областта на високотехнологичните престъпления с работата на други подобни международни структури с цел избягване на дублиране в действията.

6.2.3. Съвет на Европа

През 2001 г. Съветът на Европа приема Конвенцията за престъпленията в кибернетичното пространството (ETS 185). Целта на Конвенцията е да хармонизира елементите на наказателното материално право за нарушения на национално ниво и свързаните с това разпоредби в областта на престъпленията в кибернетичното пространство

(Глава II, Раздел 1, Заглавия 1-5); да осигури правомощия, свързани с наказателното процесуално право на местно ниво, необходими за разследването и преследването на такива нарушения (Глава II, Раздел 2, Части 1-5); и да установи бърз и ефективен режим на международно сътрудничество (Глава III, Раздел 1, Заглавия 1-4 и Раздел 2, Заглавия 1-3). Конвенцията е съставена от Съвета на Европа в Страсбург с активното участие на държавите наблюдатели на Съвета на Европа – Канада, Япония и САЩ. Ратифицирана е от 22 държави-членки на Съвета на Европа, а също така е отворена и за държави, които не са членки, сред които САЩ вече са я ратифицирали. Раздел 1 от Глава II (въпроси на материалното право) покрива както наказателни разпоредби, така и други свързани с него разпоредби в областта на компютърните или свързаните с компютри престъпления и включва раздели върху компютърни фалшификации и компютърни измами:

Член 7 – Компютърни фалшификации

Всяка Страна следва да предприеме такива законодателни и други мерки, каквито са необходими за установяване на наказуеми нарушения по смисъла на националното право, когато същите са извършени преднамерено и неправомерно въвеждане, промяна, изтриване или укриване на компютърни данни, което води до неавтентичност на данните, с намерение да бъдат използвани за правни цели така сякаш са автентични, независимо от това дали данните са директно четливи и разбираеми. Страната може да изиска умисъл за измама или друга подобна нечестна умисъл да бъде отнесена пред аташета на наказателна отговорност.

Член 8 – Компютърни измами

Всяка Страна следва да предприеме такива законодателни и други мерки, каквито може да са необходими за считане за наказуеми на нарушения по смисъла на националното право, когато същите са извършени преднамерено и неправомерно, като се предизвиква загуба на имущество на друго лице чрез:

а) всякакъв вид въвеждане, промяна, изтриване или укриване на компютърни данни,

б) всякакъв тип намеса във функционирането на компютърната система, с измамна или нечестна умисъл за неправомерно получаване на икономическа изгода за себе си или за друго лице.

Както Член 7, така и Член 8 съдържат широки дефиниции и някои видове нарушения, потенциално попадащи в тези дефиниции, в юрисдикции като Обединеното кралство, са уредени по-скоро в законодателството за компютърни злоупотреби, отколкото в дефинициите на компютърни измами. Ясно е обаче, че техники за измами свързани с идентификацията, включително техники за шпиониране, софтуери за прихващане („снифъри") на TCP/IP пакети, фишинг съобщения ("phishing messages"), „които имат вид на легитимни покани за подаване на лична информация, например фалшив PayPal, e-Bay или запитвания за банкиране с препратки към фалшиви Интернет страници или използващи „надписи, препращащи към различни страници", които използват пробиви в сигурността на легитимни страници, за да събират незаконно данни" (*de Hert, González Fuster & Koops 2006*) биха попаднали под разпоредбите на Конвенцията.

С оглед на процесуални правни въпроси Конвенцията изисква държавите да установят минимален набор от процесуални инструменти на национално ниво, така че правораздавателните органи в държавата да имат достатъчно правомощия да извършват определен вид разследващи дейности, които са характерни за наказуеми компютърни нарушения. Такива процесуални правомощия включват: навременно запазване на съхраняваните данни, навременно запазване и частично разкриване на трафик на данни, производствени заповеди, търсене и конфискуване на компютърни данни, събиране на трафик на данни в реално време и прихващане на данни за съдържанието.

Конвенцията също така предвижда набор от общи принципи в сферите на международно сътрудничество, екстрадиране, взаимопомощ и доброволно подаване на информация като:

- между държавите ще се осигурява международно сътрудничество „до възможно най-широка степен";
- задължението за съвместна дейност обхваща не само престъпленията установени в споразумението, но и събирането на електронни доказателства, винаги когато това е свързано с наказуеми нарушения
- разпоредби за международно сътрудничество не отменят вече съществуващи разпоредби на международни споразумения по тези въпроси.

Освен това са създадени правила за екстрадиране на заподозрени при конкретни условия (отново отстъпващи на вече съществуващи споразумения или алтернативни договаряния относно екстрадицията), както и за установяване на други форми на сътрудничество в сферата на криминалното разследване и преследване, например мрежа от лица за контакт, които са достъпни денонощно за осигуряването на незабавна помощ за целите на разследванията или процедури по наказуеми нарушения, свързани с компютърни системи и данни или за събирането на доказателства в електронна форма за наказуеми нарушения.

6.2.4. ОИСР (Организация за икономическо сътрудничество и развитие)

ОИСР играе важна роля за стимулирането на международната дейност срещу трансгранични измами като има за цел осигуряване на доверието на потребителя и ръста на глобалната дигитална икономика. През 1999 г. Инструкциите за защита на потребителя в контекста на електронната търговия предлага страните-членки на ОИСР да се борят с трансграничните измами чрез повишаване на „обмяната на информация, координацията, комуникацията и съвместните действия" сред „съдебните, регулаторни и правораздавателни органи."

През юни 2003 г. са приети Инструкциите за защита на потребителите от измами и подвеждащи практики през граница на ОИСР. Те установяват общата рамка за борба с презграничните измами - електронни или не - чрез по-близко, по-бързо и по-ефективно сътрудничество между агенциите за защита на потребителите (АЗП). Основните елементи на Инструкциите са:

Рамки за борба с трансграничните измами и подвеждащи търговски практики на национално ниво

- Държавите-членки трябва да имат ефективна правна уредба, АЗП, институции, практики и съвместни инициативи, които да ограничат измамите/подвеждащи търговски практики срещу потребителите.
- Държавите-членки трябва да осигурят техните АЗП да имат правомощия да получават доказателства, достатъчни за разследвания и да предприемат навременни действия срещу измами/ подвеждащи търговски практики.
- Държавите-членки трябва да разполагат с подходящите съдебни и административни механизми, които да позволяват на АЗП да запазват доказателства, особено такива от нетраен характер, докато същите могат да бъдат изследвани, включително и в случаите, когато АЗП са помощни агенции в други страни, подлежащи на съответните предпазни мерки.

- Държавите-членки трябва да развият механизми за сътрудничество и подаване на информация между и сред техните АЗП и другите правораздавателни агенции за целите на борбата с измамите/ подвеждащите търговски практики.
- Държавите-членки трябва да идентифицират и отстраняват препятствия за ефективно сътрудничество за налагането на закони, предназначени за защита на потребителите от измами/ подвеждащи търговски практики на национално ниво.
- Държавите-членки трябва да информират потребителите относно измами/ подвеждащи търговски практики, предприемайки подходящи съвместни инициативи.
- Държавите-членки трябва да преценят как в определени случаи техните АЗП могат да използват доказателства, решения и влезли в сила заповеди от АЗП в друга страна, за да повишат способността си за предотвратяване на подобни дейности в собствената си страна.

Принципи за международно сътрудничество

- Държавите-членки трябва да повишат своята способност да си сътрудничат в борбата с трансграничните измами/подвеждащи търговски практики като в същото време приемат, че съвместната дейност по конкретни разследвания и случаи остава по преценка на АЗП, от които е поискано съдействие.
- АЗП трябва да координират своите разследвания и правораздавателна дейност, за да избегнат намеса в разследвания и правораздавателна дейност на АЗП, която се провежда в други държави-членки.
- АЗП трябва да се опитват да разрешават несъгласия, които могат да възникнат във връзка със съвместната дейност.
- Държавите-членки и техните АЗП трябва да използват съществуващите международни мрежи и да влизат в подходящи двустранни и многостранни споразумения или други инициативи.
- Държавите-членки трябва да дават възможност на своите агенции за политика по защита на потребителите (АПЗП) при обсъждания с АЗП да поемат водещата роля за развитието на рамка за борба с измами/ подвеждащи търговски практики.
- Държавите-членки трябва да назначат АЗП и АПЗП, които да действат като лица за контакт с цел улесняване на сътрудничеството съгласно Инструкциите.

Уведомяване, подаване на информация, съдействие при разследвания и конфиденциалност

- Държавите-членки и техните АЗП трябва незабавно, систематично и ефективно да уведомяват АЗП в други страни членки относно разследвания, които по някакъв начин са свързани с тези страни.
- Държавите-членки трябва да повишат способността на АЗП да подават информация във времеви рамки, които улесняват разследвания свързани с измами и подвеждащи търговски практики срещу потребители, а именно:
    - обществено достъпна и друга неповерителна информация;
    - жалби от страна на потребителите;
    - информация, позволяваща бързо откриване/идентифициране на лица, занимаващи се с измами/подвеждащи търговски дейности (напр. адреси, регистрации на Интернет домейни);
    - експертни мнения и базата информация, върху която се основават тези мнения; и
    - документи, информация свързана с трета страна и др., получени чрез съдебни процеси и други наложени процеси.

- Държавите-членки трябва да работят съвместно за развитието на бързи и ефективни методи за събиране и подаване на информация, с които да противодействат на скоростта, с която лицата, занимаващи се с измами и подвеждащи търговски практики, могат да нанесат вреди на голям брой потребители, напр. по Интернет.
- Държавите-членки трябва да действат относно разпространението на доказателства през различните юрисдикции чрез упълномощаване на техните АЗП, директно или чрез подходящите съдебни/административни механизми, да получават информация и осигуряват съдействие на чуждестранни АЗП при разследвания и действия, подлежащи на съответната защита.
- Държавите-членки, техните АЗП и други компетентни органи трябва да работят съвместно и с регистри на имена на домейни и др. за намаляването на случаите с фалшиви имена, маршрутизираща информация и невярна информация относно притежатели на имена на домейни.
- Държавите-членки трябва да осигуряват необходимата конфиденциалност на информацията, която се обменя съгласно Инструкциите, особено когато се подава поверителна бизнес или лична информация.

Правомощия на агенциите за защита на потребителите

- Всички АЗП, чиито територии са засегнати от измами и подвеждащи търговски практики срещу потребителите, трябва да имат съответните правомощия за разследване и предприемане на действия на своя територия.
- Държавите-членки трябва да дават възможност на своите АЗП да предприемат действия срещу търговски предприятия, занимаващи се с измами и подвеждащи търговски практики срещу чуждестранни потребители.
- Държавите-членки трябва да дават възможност на своите АЗП да предприемат действия срещу чуждестранни търговски предприятия, занимаващи се с измами и подвеждащи търговски практики срещу собствените им потребители.
- Предходните 3 точки могат да подлежат на други двустранни договаряния между страните или на други договаряния в рамките на организация за регионална икономическа интеграция.

Обезщетяване на потребителите

- Държавите-членки трябва да изследват съвместно ролята на обезщетяването на потребителите при разглеждане на проблема с измамите и подвеждащи търговски практики, отдавайки специално внимание на развитието на ефективни системи за обезщетяване през граница.

Сътрудничество в частния сектор

- Държавите-членки трябва да си сътрудничат с търговски предприятия, групи индустриалци и групи потребители за подпомагане на целите на Инструкциите и да настояват за тяхното съдействие и подкрепа особено за инструктиране на потребителите и да насърчават отнасянето на съответните оплаквания до АЗП.

Инструкциите са приети на международно ниво като ефективно средство за третиране на измами и подвеждащи търговски практики срещу потребители, напр. Споразумението за зона за свободна търговия (Споразумение за зона за свободна търговия между Австралия и Съединените щати), подписано между Австралия и Съединените щати и влязло в сила през януари 2005 г., изрично приема Инструкциите като ценен съществуващ механизъм за налагане на сътрудничество за защита на потребителите. Няколко агенции за защита на потребителите в държавите-членки на ОИСР прилагат неофициални споразумения за одобряване на такова подаване на информация, напр. подписването на Протоколи за

подаване на информация между Канадското бюро по конкуренцията, Федералната комисия по търговия на Съединените щати, Австралийската комисия за конкуренцията и потребителите (АККП) и Службата за честна търговия („СЧТ") на Обединеното кралство между 2003 г. и 2004 г. Повече подробности относно действията на държавите-членки на ОИСР на национално ниво могат да бъдат намерени в Доклада по изпълнение на инструкциите на ОИСР за 2003 г. за защита на потребителите от измами и подвеждащи търговски практики зад граница (2006 г.).

6.2.5. Европейски съюз

Общо взето законодателството на ЕС не предвижда цялостен подход към електронните измами, както и закони за престъпленията в кибернетичното пространството. Още през 2001 г., обаче, Съветът на министрите одобрява информационната мрежа, достъпна 24 часа за борба срещу престъпления свързани с високите технологии и препоръчва на държавите-членки да се присъединят – Препоръка на Съвета относно мрежата от лица за контакт, достъпна 24 часа за борба срещу престъпленията свързани с високите технологии (2001 г.). Това предложение е разглеждано по-наскоро в Член 11 от Рамковото решение на Съвета във връзка с атаки срещу информационни системи (2005/222/JHA), според което „държавите-членки трябва ... да използват съществуващата мрежа от оперативни лица за контакт отнесени в Препоръката на Съвета от 25 юни 2001 г. към лица за контакт, достъпни 24 часа за обмяна на информация за борбата срещу престъпленията, свързани с високите технологии."

Европейската комисия също така приема конкретно Инструкциите на ОИСР като важна стъпка в подхождането към проблема с транс-граничните измами на международно ниво. Това признаване също е отразено и в приемането на Регламента на ЕС за сътрудничество между органите на национално ниво, отговорни за налагането на закони за защита на потребителите (2006/2004/ЕС), който има за цел създаването на цялостна мрежа за защита на потребителите в ЕС и който съдържа много принципи, подобни на тези в Инструкциите. Тъй като това е Регламент, той е директно приложим и задължителен в държавите-членки на ЕС без необходимост да се прилага в националното законодателство.

Регламентът установява мрежа от органи, чиято отговорност е да следят прилагането на законодателството на потребителите. Целта му е да осигури спазването на законодателството и гладкото функциониране на вътрешния пазар. Регламентът се прилага за нарушения на законодателството за защита на потребителите само в рамките на Общността.

Всяка държава-членка назначава Компетентните органи и Отделна служба за съгласуване, които да отговарят за прилагането на Регламента. Тези Компетентни органи имат разследващи правомощия и правомощия за действия за прилагане на Регламента и ги изпълняват в съответствие с националното право. Компетентните органи трябва да действат незабавно за прекратяването на всякакви установени нарушения, използвайки подходящо законово средство. В повечето случаи това е възбрана, а това позволява предприемане на бързи действия. Възбраната позволява прекратяване или забрана на незаконни дейности и отвеждане на търговци-измамници на съд в други държави-членки.

Съгласно член 8(3), Комисията за защита на потребителите и Компетентните органи могат ефективно да назначат за подизпълнители в случаи през граница други изпълнителни органи, които имат интерес от прекратяването на нарушения на закона за потребителите в тяхната юрисдикция (Органи по Член 8(3)).

Регламентът установява рамка за взаимопомощ, която включва обмяна на информация, искания за налагане на мерки и координация в следенето на пазара и изпълнителни действия. Когато Компетентен орган узнае за нарушение в рамките на Общността, той трябва да уведоми Компетентните органи на други държави членки и Комисията. Също така при поискване от страна на друг Компетентен орган той осигурява

всякаква информация свързана с нарушението, необходима за установяване на това дали имало нарушение. Освен това той трябва да вземе всички необходими изпълнителни мерки за прекратяването или забраната на нарушението в рамките на Общността.

Компетентните органи трябва да информират Комисията относно нарушенията в рамките на Общността, взетите мерки и техния ефект, както и координацията на действията им. Подадена информация може да бъде използвана единствено с цел осигуряване спазването на законите, защитаващи интересите на потребителите. Комисията съхранява и обработва информацията, която получава, в електронна база данни. Молби за съдействие трябва да съдържат достатъчно информация, която да позволи на Компетентния орган да изпълни молбата. В определени обстоятелства Компетентният орган може да откаже да уважи молба за изпълнителни мерки или за информация или да реши да не изпълни задълженията си. В такъв случай той информира заявителя, Компетентен орган и Комисията за основанията за отказ за изпълнение на молбата за съдействие.

Държавите членки взаимно се информират и уведомяват Комисията относно техни действия от интерес за Общността, например:

- Изпълнителна координация: обучение на служителите на техните АЗП, събиране и класифициране на потребителски жалби;
- Административна координация: осигуряване на информация и съвети за потребителите, подкрепа на дейностите на представители на потребителите.

Трябва също да се отбележи, че държавите членки на ЕС са ратифицирали Конвенцията на ЕВРОПОЛ, която предвижда рамка на полицейско сътрудничество срещу организираната престъпност, включително и престъпленията в кибернетичното пространство.

Прилагане на законите срещу измами и на други регулаторни стратегии спрямо електронната среда

Както става ясно по-долу, когато става въпрос за прилагане на националните закони срещу измами и на други регулаторни стратегии спрямо електронната среда, международният опит предлага няколко ключови елемента, които да осигурят възможната степен на успех. Необходимо е правителствата на държавите да:

- изследват своите съществуващи закони срещу измама и други свързани с това закони като осигурят сформирането от същите на вътрешно-последователна система и това, че те могат да бъдат прилагани към електронната среда/използването на нови технологии, т.е. не са съставени по начин, който да изключва, ограничава или възпрепятства използването им от правораздавателните органи и АЗП;
- осигурят възможността за законодателите, регулаторите, правораздавателните органи, АЗП и представители на съдебни и юридически професии достатъчно да разбират технологиите и техниките, които се налага да наблюдават, напр., когато представители на юридическа професия се сблъскат със случаи на фишинг и фарминг, те трябва да могат да разбират как се използва тази технология, да идентифицират кога и как законът е бил нарушен и да наложат съответните законови санкции;
- да осигурят в случаи на измама възможността за получаване и подаване на доказателства от национални правораздавателни органи и АЗП както на национално, така и, ако е необходимо, на международно ниво – теоретически чрез международни мрежи от компетентни органи, които могат да работят с информация по бърз, систематичен и ефективен начин;
- да включат частния сектор, включително търговски предприятия, групи индустриалци и групи потребители както по отношение на обучение и консултации (т.е. да се

възползват от опита на частния сектор), така и в стремежа за ангажиране на организации на частния сектор в регулаторни процеси, например включването на секторни групи в саморегулиращи се практики, които възпрепятстват измамническо поведение, напр. доставчици на Интернет услуги, регистри на имена на домейни и др.

6.3. Подходът на Обединеното кралство

До известна степен тези въпроси вече са разглеждани в Обединеното кралство. Освен приемането на адекватни мерки, които да отговарят на неговите международни задължения/изисквания, включително и присъединяването към 24-часовата информационна мрежа на Г-8, Службата за лоялна търговия на Обединеното кралство е подписала Протоколи за подаване на информация между нея и редица органи за защита на конкуренцията и потребителите на други страни. По отношение на Регламента на ЕС за сътрудничество между органите на национално ниво, отговорни за налагането на закони за защита на потребителите (КЗК) Обединеното кралство е назначило Службата за лоялна търговия като своя Отделна служба за съгласуване, както и редица органи, включително СЛТ, Орган на гражданската авиация (ОГА), Министерството на търговията и индустрията (Гибралтар), Орган за финансовото обслужване (ОФО) и Регулиращия орган по медикаменти и здравеопазване (РОМЗ) като Компетентни органи. В допълнение редица органи по Член 8(3) са упълномощени, включително и Независимата комисия за контрол на стандартите на телефонните услуги (ICSTIS - телефонен регулатор). СЛТ е свързана и с Международната мрежа за защита на потребителите (ICPEN).

През 2006 г. е приет нов Закон срещу измамите, който има за цел опростяване на съществуващия закон, по-голямата част от който се е съдържала в Законите срещу кражба от 1968/1978 г., които са счетени за неподходящи за настоящата правна среда, тъй като същността на измамата значително се е изменила през последните години до голяма степен в резултат на новите технологии. Законът срещу измамите не е единствената наказателна разпоредба, която може да се използва срещу наказуеми/измамнически действия (напр. законите за защита на потребителите), но той предлага нов подход в борбата срещу измамите.

Законът въвежда общото понятие за ‘измама’ на мястото на осем конкретни нарушения на закона, например ‘придобиване на имущество чрез измама’ и нарушаване на общото право чрез ‘конспирация с цел измама’. Новото нарушение е наказуемо с до 10 години затвор и/или глоба.

Според новия Закон съществуват три начина за извършване на измама:

- Фалшиво представяне – то замества нарушението на придобиване на имущество чрез лъжа, хитрост или измама, но също така включва нарушения, като например вписване на неверни данни, квалификации или фиктивно деклариране в автобиография. Оказва се, че така може да се улови фишинг, доколкото лице, което изпраща фишинг съобщения, фалшиво представя електронните съобщения като изпратени от легитимна финансова институция.
- Неразкриване на информация – като например неразкриването на неизтърпяна наказателна присъда или други факти, когато има законово или друго задължение затова
- Злоупотреба с положение – например, когато служител копира данните на клиент на своя работодател с цел създаване на конкурентно дружество.

Две основни изисквания трябва да бъдат изпълнени преди страна да може да бъде обвинена по някоя от трите точки по-горе

- Поведението на ответника трябва да е нечестно.
- Ответникът трябва да има намерение да извлече изгода или да предизвика загуба за друго лице.

Няма никаква необходимост, обаче, от доказване на фактическа полза или загуба или на измама, причинена от поведението на ответника.

Освен въвеждането на нарушението за измама, Законът също така създава две нови понятия за нарушения, насочени срещу измами свързани с технологиите – „нечестно ползване на услуги" и „притежаване на принадлежности за употреба при измами". Първото може да се използва за преследване на измами свързани с електронни кредитни карти, а второто за инкриминиране на техники за фишинг, позволяващи изпращането на големи количества електронни съобщения, които са представени за известна марка с надеждата чрез измама да се накарат жертвите да влязат във фалшива електронна страница, която например ги прилъгва да разкрият данни на банкови сметки.

По отношение на участието на частния сектор в намаляването на компютърните измами са предприети редица инициативи на частния сектор, много от които имат за цел да обучат потребителите как да се предпазват от компютърни измами или да позволят на потребителите да докладват за потенциални измами.

Banksafe Online
http://www.banksafeonline.org.uk/
Educational and Reporting

Cardwatch
http://www.cardwatch.org.uk/
Educational

6.4. Принципи на Г-8 и план за действие за борба с високотехнологични престъпления (10 принципа и план за действие от 10 точки)

6.4.1. Принципи

С настоящето приемаме следните ПРИНЦИПИ, които трябва да се защитават от всички страни:

1. Не трябва да има убежище, за онези които злоупотребяват с информационните технологии.
2. Разследването и повдигането на обвинение, свързано с високотехнологични престъпления трябва да се координират измежду засегнатите страни независимо от това в коя страна са извършени.
3. Служителите на правораздавателните органи трябва да трябва да са обучени и оборудвани за справяне с високотехнологични престъпления.
4. Правните системи трябва да защитават конфиденциалността, целостта и наличието на данни и системи от незаконното им нарушаване и да гарантира, че сериозните злоупотреби се наказват.
5. Правните системи трябва да позволяват съхраняване и бърз достъп до електронни данни, които често са жизненоважни за успешното разследване на престъпления.
6. Режимите за взаимопомощ трябва да гарантират навременно събиране и обмяна на доказателства при случаи на международни високотехнологични престъпления.
7. Не се изисква разрешение за трансграничен електронен достъп на правораздавателните органи до обществено достъпна информация.
8. Трябва да се развиват и прилагат съдебни стандарти за възстановяване и верифициране на електронни данни за ползване при разследване на престъпления и повдигане на обвинение.
9. Доколкото позволява практиката, информационните и телекомуникационните системи трябва да са създадени, така че да спомагат за предотвратяване и откриване на злоупотреби с мрежата и освен това трябва да улесняват проследяването на престъпници и събиране на доказателства.
10. Работата в тази област трябва да се координира с дейността на други международни форуми, за да се избегне дублиране на усилия.

6.4.2. План за действие

В подкрепа на следните принципи, насърчаваме нашите служители да:

1. Да използват развитата ни мрежа от компетентен персонал, за да гарантират навременна и ефективна реакция при международни високотехнологични престъпления и да назначат лице за контакт, което да е на разположение 24 часа.
2. Да предприемат адекватни действия, за да гарантират че достатъчен персонал на правораздавателните органи с висока квалификация и подходящо оборудване е разпределен, за да се бори с високотехнологичните престъпления и да съдейства на правораздавателните органи на други страни.
3. Да преразглеждат правните ни системи, за да се уверят че правилно инкриминират злоупотреби с телекомуникационни и компютърни системи и подпомагат разследването на високотехнологични престъпления.
4. Да отдават внимание на въпроси, свързани с високотехнологични престъпления, където е необходимо, когато водят преговори за споразумения за взаимопомощ и сътрудничество.
5. Да продължат да изследват и да разработват практически решения относно запазването на доказателства преди изпълняването на искането за взаимопомощ, трансгранични издирвания и компютърни претърсвания на данни, когато местоположението не е известно.

6. Да разработват бързи процедури за получаване на данни за трафик от всички носители на информация по веригата на комуникация и да изследват методи за по-бързо разпространяване на данните на международно ниво.
7. Да работят съвместно със сектора, за да гарантират че новите технологии улесняват усилията ни за борба с високотехнологичните престъпления и за запазване и събиране на важни доказателства.
8. Да гарантират, че можем, при спешност и необходимост, да приемем и да отговорим на исканията за взаимопомощ относно високотехнологични престъпления по бързи, но надеждни средства за комуникация, включително гласова или електронна поща или факс с искане за писмено потвърждение, където е необходимо.
9. Да насърчават органи за разработване на международно признати стандарти в областта на телекомуникациите и информационните технологии да продължат да задават на публичния и частния сектор високи стандарти за надеждни и сигурни телекомуникации и технологии за обработване на данни.
10. Да разработват и прилагат съвместими съдебни стандарти за възстановяване и верифициране на електронни данни за целите на криминални разследвания и повдигане на обвинение.

7. РАЗПРОСТРАНЕНИЕ НА ПОРНОГРАФИЯ ПО ЕЛЕКТРОНЕН ПЪТ

7.1. Въведение

Основният проблем при боравенето с порнографията, разпространявана по електронен път, е, че въпросът какво трябва да покрива терминът „порнография" е изключително субективен. Самият термин „порнография" често се избягва при съставянето на правни текстове заради неговата субективност – това, което се счита за „порнография" от един, за друг може да бъде „велико произведение на изкуството", „защитено обществено-политическо или сексуално изразяване" или просто няколко ваканционни снимки.

> „Това, което се възприема за порнографско, варира от човек до човек, от култура до култура, през различните периоди. Терминът „порнография" в дискусии и дебати може да се използва с по-общо значение и да се отнася до материал, който е с открито сексуално значение, или с по-специфично значение и да се отнася до материал, който е с открито сексуално значение, създаден основно, за да предизвиква сексуална възбуда у гледащите го, до материал, който е с открито сексуално значение, който поставя в подчинено положение жените или е вреден за жените и децата, или пък с някакво друго определение, взето предвид" (*Casavant & Robertson, 2007*).

Например, във Великобритания, въпреки, че е доста популярно думата „порнография" да се използва в медиите, терминът до голяма степен се избягва в съответното национално законодателство, което доскоро се е занимавало с това дали въпросният материал е „нецензурен" или „неприличен". Все пак, докато това означава, че съдилищата не са били сезирани за спор относно това какво е и какво не е „порнографско", при това положение нито „нецензурен", нито „неприличен" се поддават лесно на дефиниране, и тази трудност при дефинирането се отразява и на британското законодателство, и на съществуващата съдебна практика. С приемането на британския Закон за наказателното правосъдие и нелегалната имиграция от 2008 г. (вж. по-долу), британското наказателно право сега дефинира „екстремно порнографско изображение" като изображение, което:

- е от такова естество, че логично трябва да се приеме, че е било създадено единствено или основно с цел сексуална възбуда; и НЕ е част от поредица от изображения, които поставени в контекст не са порнографски;
- И изобразява по открит и реалистичен начин, което и да е от следните неща:
    - деяние, което заплашва човешки живот;
    - деяние, което води до или е вероятно да доведе до сериозно нараняване на ануса, гърдите или гениталиите;
    - деяние, което включва полово сношение с човешки труп; или
    - лице, извършващо полово сношение или орален секс с животно (независимо дали животното е мъртво или живо);
    - И при което всеки разумен човек, гледащ изображението би си помислил, че всяко такова лице или животно е реално;
- И е изключително противно, възмутително или от друг нецензурен характер.

Вероятно това може да бъде възприето като демонстрация на факта колко е трудно да бъде създадена разбираема и в същото време сравнително точно обяснена дефиниция на всяка подкатегория на порнографията.

В повечето държави, ако не и във всички, съществува ясното разбиране, че създаването на порнографски материал, включващ деца, подлежи на инкриминиране. Въпреки това, дори в този случай, съществуват значителни спорове между държавите

относно това какво трябва да покрива „детската порнография”. Някои държави считат за детска порнография материали, включващи лица под 18 години, други са поставили границата на материали, включващи лица под 16 години. Някои държави инкриминират създаването, предлагането, разпространяването, доставянето и притежанието на детска порнография; други ограничават инкриминирането до създаването, предлагането и разпространението. Някои държави изискват доказателства, че действително малолетно лице е било въвлечено в създаването на порнография, други инкриминират също и материали, които изглеждат така сякаш са въвлекли малолетно лице (напр. когато лице над 18 години се преструва, че е под 18 години, или когато невинни изображения на малолетни лица са слети с порнографски изображения) и/или изображения, които изобразяват малолетни лица, въвлечени в сексуални действия (напр. скици или комикси).

Тези значителни културни различия са направили много трудно развиването на една последователна международна реакция спрямо регламентирането на електронните „порнографски” материали. Наличието на „порнографски” материали в Интернет, различни от детска порнография, е широко разпространено и приложимостта на националните законодателства спрямо доставчиците, контролиращи уебсайтове, списъци с електронни адреси и други механизми за разпространяване, базирани извън границите на съответната държава, често пъти е ограничена. Някои държави са потърсили начин да разрешат проблема, като поставят правни ограничения на доставчиците на Интернет услуги (ISPs) в рамките на тяхната юрисдикция. Подобни изисквания може да включват: блокиране на определени уебсайтове или поредица от IP адреси; инсталиране на филтриращ софтуер, който пречи на потребителите да свалят определени типове материали и предаване на властите на информация относно потребители, осъществяващи достъп до такива материали. При държавите с един единствен доставчик на Интернет услуги (често собственост на държавата) има тенденция тези подходи да са по-лесно осъществими отколкото в държави с конкуриращи се в частния сектор доставчици на Интернет услуги, където може да бъде оспорвано, че налагането на подобни правни задължения върху доставчиците на Интернет услуги има значителен ефект срещу конкуренцията. За държавите с конституционни разпоредби относно свободата на словото също може да се окаже, че налагането на филтриране или други блокиращи технологии, касаещи доставчиците на Интернет услуги, ще бъде в противоречие с тези разпоредби, когато държавите спират разпространението на законни материали или отказват достъп до материали, които възрастните имат право да гледат, за да предпазят децата.

7.2. Международни инициативи

7.2.1. Организацията на обединените нации (ООН) и Международната организация на труда (МОТ)

След Международната конференция за борбата с детската порнография в Интернет, проведена във Виена през 1999 г., която призова за глобално инкриминиране на производството, разпространението, изнасянето, предаването, внасянето, умишленото притежание и рекламирането на детска порнография и подчерта важността на по-близкото сътрудничество и партньорство между правителствата и Интернет индустрията, Общото събрание на ООН прие Факултативен протокол относно търговията с деца, детската порнография и детската проституция (Протокол относно търговията с деца).

Протоколът относно търговията с деца беше първият международен документ, който дефинира термина „детска порнография”. Той изисква от държавите да третират деяния, свързани с такова поведение, като престъпления и предвижда механизми за сътрудничество на изпълнителната власт, за да се преследват нарушителите. Също така протоколът установява и широко приложими за юрисдикциите основания във връзка с нарушенията и

деянията да екстрадират нарушителите, с цел гарантиране, че нарушителите ще бъдат преследвани независимо от това къде са задържани.

Протокол относно търговията с деца

Член 2

[...]

(в) детска порнография означава всяко представяне, с каквито и да било средства, на дете в действителни или симулативни явни сексуални дейности или друго излагане на интимни части на дете с предимно сексуални цели.

Член 3

1. Всяка държава страна гарантира, че като минимум следните действия и дейности са напълно застъпени (са обект) в наказателното й право независимо от това, дали нарушенията са извършени на нейна територия или извън нейните граници от отделен индивид или от организирана група:

[...]

(в) производство, разпространение, внасяне, изнасяне, предлагане, продажба или притежаване за горните цели на детска порнография по смисъла на чл. 2.

Протоколът също допълва *Конвенция №182 на Международната организация на труда (МОТ) относно забраната и незабавни действия за ликвидирането на най-тежките форми на детския труд*, приета на Международната конференция на труда през 1999 г., която изисква от държавите страни да предприемат незабавни и ефективни действия, за да гарантират ликвидирането на използването, доставянето или предлагането на дете, наред с другите неща, и за производство на порнография или порнографски изяви.

Конвенция № 182 на МОТ относно забраната и незабавни действия за ликвидирането на най-тежките форми на детския труд

Член 2

За целите на тази конвенция терминът "дете" ще се прилага за всички лица под 18-годишна възраст.

Член 3

За целите на тази конвенция изразът "най-тежките форми на детския труд" обхваща:

[...]

(б) използването, доставянето или предлагането на деца за проституция, за производство на порнография или порнографски изяви;

[...]

(г) работа, която по своето естество или при обстоятелствата, при които се упражнява, е възможно да увреди здравето, безопасността и морала на децата.

В много държави възрастта, на която съгласието за сексуални действия има правно значение, е между тринайсет и шестнайсет години и ако едно дете на тази възраст се е съгласило да извърши полов акт, не е било извършено престъпление, включващо детска проституция или детска порнография. Протоколът изисква от държавите страни да инкриминират действия, свързани с детска проституция и детска порнография без оглед на националното законодателство или възрастта, на която съгласието има правно значение.

Той не дефинира конкретно термина „дете”, но държавите, подписали Конвенцията за правата на детето, са задължени по член 1, който дефинира „дете” като „всяко човешко същество на възраст под осемнадесет години, освен в случаите, когато според националното законодателство, приложимо за детето, пълнолетие се достига по-рано.”

Макар че тези инициативи не бяха насочени единствено към проблема с детската порнография в Интернет, ясно е, че очевидното увеличаване на наличието на такива електронни материали бе ключовия мотив за тяхното приемане.

7.2.2. Съвет на Европа

Съветът на Европа прие *Конвенцията за престъпленията в кибернетичното пространство* (ETS 185) през 2001 г. Конвенцията има за цел да хармонизира престъпните елементи от националното материално наказателно право и съответните постановления в областта на киберпрестъпленията (Глава II, Раздел 1, член 1-5); да осигури вътрешни наказателни процедурно-правни правомощия за разследване и съдебно преследване на такива нарушения (Глава II, Раздел 2, член 1-5); и да установи бърз и ефективен режим на международно сътрудничество (Глава III, Раздел 1, член 1-4 & Раздел 2, член 1-3). Тя беше изготвена от Съвета на Европа в Страсбург с активното участие на наблюдателите в Съвета на Европа от Канада, Япония и САЩ. Тя е ратифицирана от 22 държави-членки на Съвета на Европа и също така е отворена за нечленуващи държави, една от които – САЩ, я е ратифицирала. Раздел 1 на Глава II (материално правни въпроси) обхваща и инкриминиращите норми, и други свързани норми в областта на кибернетичните престъпления и компютърните престъпления и включва постановление, занимаващо се с въпроса за детската порнография, който е единственият, свързан със съдържанието. Всички правонарушения, изброени в Конвенцията, трябва да са извършени умишлено и „без право". Нормите бяха замислени така, че да отразяват Факултативния протокол към Конвенцията на ООН относно правата на детето в частта му, засягаща детската порнография.

Член 9 – Престъпления, свързани с детска порнография

1. Всяка държава приема законодателните и други мерки, необходими за инкриминирането съгласно вътрешното й право, на следните деяния, когато са извършени умишлено и без законно основание:

(а) производството на детска порнография за целите на нейното разпространяване чрез компютърна система;

(б) предлагане или предоставяне на възможност за достъп до детска порнография чрез компютърна система;

(в) разпространяване или предаване на детска порнография чрез компютърна система;

(г) снабдяване с детска порнография чрез компютърна система за себе си или за другиго;

(д) притежаване на детска порнография в компютърна система или на електронен носител

2. За целите на предходната алинея 1 в „детска порнография" следва да се включват всички порнографски материали, които представят визуално:

(а) непълнолетно лице, което демонстрира открито сексуално поведение;

(б) лице, което изглежда като непълнолетно и демонстрира открито сексуално поведение;

(в) реалистични картини, представящи непълнолетно лице, демонстриращо открито сексуално поведение.

3. За целите на предходната алинея 2 терминът „непълнолетно" включва всяко лице под 18-годишна възраст. Държавите обаче могат да въведат изискването за по-ниска възрастова граница, която трябва да е най-малко 16 години.

4. Всяка държава може да си запази правото да не прилага, изцяло или частично, алинея 1(г) и 1(д) и 2(б) и 2(в).

Обяснителният меморандум към Конвенцията дефинира „открито сексуално поведение" като поведение включващо: а) полово сношение, включително генитално, орално-генитално, анално-генитално или орално-анално, между малолетни лица или между

възрастно и малолетно лице, от същия или от противоположен пол; б) содомия; в) мастурбиране; г) садистична или мазохистична сексуална злоупотреба; или д) похотливо излагане на гениталиите или срамните части на малолетно лице. Той също предвижда „националните стандарти" да определят това, което съставлява порнографията. Държавите може да се установят резерви, относно доставянето и притежаването на детска порнография и на изображения на възрастни, изглеждащи като деца, или на трансформирани или компютърно-генерирани образи, където не се насилва дете (псевдо-фотографии). Конвенцията не определя нивата на наказание, оставяйки това на държавите, но член 13 изисква наказания, които да са „ефективни, пропорционални и възпиращи".

Съветът на Европа е предприел една следваща стъпка за борбата с електронната детска порнография след *Конвенцията за престъпленията в кибернетичното пространство*, с приемането на *Конвенцията за закрила на децата срещу сексуална експлоатация и сексуално насилие* (CETS 201), която беше отворена за подписване през октомври 2007 г. Двадесет и девет държави-членки на Съвета на Европа са я подписали, въпреки че по време на писането на този доклад все още нямаше ратификации. Конвенцията ще влезе в сила, когато има 5 ратификации, като поне 3 трябва да са от държави-членки на Съвета на Европа. Конвенцията е с широк обхват и изисква от държавите, страни по нея, наред с другите неща да направят следното:

- да вземат предпазни мерки, включително проучване, набиране и обучаване на хора, които работят в контакт с деца, информират децата за рисковете и ги учат да се защитават, както и да следят за спазването на мерките и за нарушители или потенциални нарушители;
- да създадат програми за подкрепа на жертвите, за окуражаване на гражданите да докладват подозренията си за сексуална експлоатация и сексуално насилие и да открият теленофонни и Интернет „горещи линии" за деца;
- да гарантират, че определени типове поведение се класифицират като престъпления, като например участие в сексуални действия с дете под законната за възраст, детска проституция и порнография;
- да инкриминират използването на информационни и комуникационни технологии, в частност Интернет, за сексуално увреждане или сексуално насилие към деца, например чрез сближаване ("*grooming*"), (напр. сприятеляване с и установяване на емоционална връзка с дете, с цел понижаване на задръжките на детето за сексуална злоупотреба).

Член 20 – Правонарушения, свързани с детска порнография

1. Всяка страна следва да предприеме необходимите законодателни или други мерки, за да гарантира, че следното умишлено поведение, в случаите, когато е извършено без право, е инкриминирано:

(а) производство на детска порнография;

(б) предлагане или предоставяне на достъп до детска порнография;

(в) дистрибуция или предаване на детска порнография;

(г) набавяне на детска порнография за себе си или за друго лице;

(д) притежаване на детска порнография;

(е) съзнателно придобиване на достъп до детска порнография, чрез информационни и комуникационни технологии.

2. За целта на този член, терминът „детска порнография" следва да означава всеки материал, който визуално изобразява дете, въвлечено в действително или симулирано открито сексуално поведение или каквото и да е изобразяване на половите органи на детето основно за сексуални цели.

3. Всяка страна може да си запази правото да не прилага, изцяло или частично, параграф 1 (а) и (д) относно производството и притежаването на порнографски материал:

– състоящ се изцяло от симулирани или реалистични изображения на несъществуващо дете;

– включващ деца, които са достигнали възрастта, определена за прилагането на член 18, алинея 2, където тези изображения са произведени и притежавани от тях с тяхно съгласие и единствено за тяхно лично ползване.

4. Всяка страна може да запази правото си да не прилага, изцяло или частично, параграф 1 (е).

[…]

Член 23 – Склоняване на деца към сексуални действия (*solicitation of children for sexual purposes*)

Всяка страна следва да предприеме необходимите законодателни или други мерки, за да инкриминира умишленото предлагане на среща, посредством информационни и комуникационни технологии, от страна на възрастен към дете, което не е достигнало възрастта, определена за прилагане на член 18, параграф 2, с цел извършване на което и да било от деянията, установени съгласно член 18, параграф 1 (а) или член 20, параграф 1 (а), срещу него или нея, където това предложение е било последвано от физически действия, водещи до такава среща.

Докато до голяма степен изглежда, че членове 20-23 от Конвенцията дублират други международни инициативи, като тези на ООН, МОТ и ЕС (вж. по-долу), в Обяснителния меморандум се предлага Конвенцията да се състави така, че да отговори на осъзнатата липса на изчерпателно национално наказателно законодателство в държавите, страни по нея, особено що се отнася до трафика на деца, „секс-туризма" и детската порнография, на липсата на ясно дефинирана минимална възраст за съгласие за сексуални взаимоотношения и на липсата на защита на децата срещу насилие в Интернет.

Също така, има ясно очакване (член 9), че частният сектор, включително секторът на информационните и комуникационните технологии (напр. доставчиците на Интернет услуги) трябва да участва в изработването и изпълнението на политиките за превенция на сексуалната експлоатация и сексуалното насилие над деца и да изпълни вътрешни норми чрез саморегулиране и съвместно регулиране, например, като поеме отговорността за контрола върху материалите, които управлява и обслужва и като осигури най-добрата система за наблюдение на дейностите в Интернет и логинг процедурите.

7.2.3. Европейски съюз

ЕС публикува Зелена книга за защитата на малолетните и човешкото достойнство (COM (96) 483 final) през 1996 г. Това откри дебат относно защитата на малолетните и на човешкото достойнство при аудиовизуалните и информационните услуги, включително Интернет услугите. Един продължителен процес на консултиране доведе до приемането на *Препоръка за развиването на конкурентноспособността на европейските аудиовизуални и информационни услуги чрез насърчаване на националните рамки, насочени към постигане на сравнимо и ефективно ниво на защита на малолетните и на човешкото достойнство* от Съвета. Наред с другите постановления, от доставчиците на Интернет услуги бе поискано да разработят правила за добро поведение, за да може по-добре да се прилага и разяснява настоящото законодателство.

Препоръката предложи насоки за развитие на национална саморегулиране по отношение на защитата на малолетните и на човешкото достойнство. Саморегулирането трябваше да бъде базирано на три ключови елемента:

§ включването на всички заинтересовани страни (правителство, производствен сектор, доставчици на услуги и на достъп, потребителски асоциации) в създаването на правила на поведение;

§ изпълнението на правилата на поведение от производствения сектор;

§ оценяване на взетите мерки.

Препоръката беше тясно свързана с Решение № 276/1999/ЕС, с което се приема дългогодишен план за действие на Общността относно насърчаването на безопасното използване на Интернет чрез борба с незаконното и вредно съдържание в световните мрежи, който на свой ред препраща назад към Съобщение на Европейската комисия относно незаконното и вредно съдържание в Интернет (COM (96) 487 final).

ЕС до голяма степен е избегнал по-мащабен дебат относно порнографията в електронното пространство, най-вече защото „стандартите на Общността", свързани с допустимостта на порнографските материали, варират значително в различните държави-членки. Областите, в които ЕС е играл активна роля, са били да се търси начин за борба със сексуалната експлоатация на деца и с детската порнография и да се насърчава по-широкото участие в схеми за осигуряване на „сигурност" в Интернет чрез методи, като:

- горещи линии, които да позволяват на гражданите да докладват случаи на незаконно съдържание;
- развойна дейност относно работата и ефективността на филтриращ софтуер и услуги;
- технологични мерки, позволяващи на потребителите да ограничават количеството на нежелано и вредно съдържание (напр. класиране на уебсайтове по качество, транс-медийно класиране на съдържание, техники за класиране и филтриране);
- мерки за саморегулация, включително консултиране и подходящо представляване на засегнатите страни; правила на поведение (напр. работа с уведомителни процедури, транс-гранични правила на поведение); национални органи, улесняващи сътрудничеството на общностно ниво; и национална оценка на рамките за саморегулация;
- разпространение на информацията за сигурността в Интернет сред голям брой потребители, особено чрез използване на множество организации и канали за електронно разпространение.

Тези инициативи са се съдържали в поредица от Решения на Съвета, включително в Решението, с което се приема дългогодишен план за действие на Общността относно насърчаването на безопасното използване на Интернет чрез борба с незаконното и вредно съдържание в световните мрежи (276/1999/ЕС), и Решението, с което се установява многогодишна програма на Общността относно насърчаване на безопасното използване на Интернет и новите електронни технологии (854/2005/ЕС).

Докато са съществували различни мерки, които да позволят на Европейския съюз да се бори със сексуалната експлоатация на деца (напр. съвместният план за действие от 1999 г. и удължаването на мандата на Европол през 1999 г.) или с разпространението на съобщения с незаконно и вредно съдържание по Интернет, след 2000 г. се почувства, че е необходимо да се въведе специфичен инструмент за борба с детската порнография в Интернет, с оглед на установения мащаб на проблема. *Решението на Съвета за борба с детската порнография в Интернет* (2000/375/ПВР) изиска от държавите-членки да предприемат мерки за:

- окуражаване на Интернет потребителите да информират изпълнителните власти, ако заподозрат, че в Интернет се разпространява материал, съдържащ детска порнография;
- гарантиране, че правонарушенията се разследват и наказват например чрез сформиране на специализирани групи в рамките на правораздавателните органи;

- гарантиране, че правораздавателните органи реагират бързо, когато получат информация за предполагаеми случаи на производство, обработка, разпространение и притежание на детска порнография;
- гарантиране, че Европол, в рамките на мандата си, е бил информиран за предполагаеми случаи на детска порнография;
- редовно проверяване дали, като се има предвид техническото развитие, техните наказателно-правни процедури трябва да се изменят с оглед на борбата с детската порнография в Интернет;
- разследване на всички мерки, които могат да помогнат за елиминирането на детската порнография в Интернет, и обмен на информация за добри практики;
- разучаване на възможностите за задължаване на Интернет доставчиците да уведомяват компетентните органи за материали, съдържащи детска порнография, които се разпространяват чрез тях, да изтеглят тези материали от обращение, да запазят материалите, за да ги предоставят на властите, и да създадат свои собствени системи за контрол;
- стимулиране на производството на филтри и други технически средства за превенция на разпространението и за улесняване на разкриването на такива материали.

За се да улесни сътрудничеството между държавите-членки, бе изготвен списък с 24-часови национални звена за контакт и специализирани звена, Европол бе официално включен в събирането на информация за предполагаемите случаи на детска порнография и се свикваха редовни срещи между националните специализирани служби.

Тези мерки бяха засилени през 2004 г. от *Рамковото решение за борба със сексуалната експлоатация деца и детската порнография* **(**2004/68/ЈНА**).** То изисква от държавите-членки да гарантират, че следното международно поведение (включително подбудителство, помагачество, съучасти и опит) е наказуемо:

- принуждаване на дете да проституира или облагодетелстване от такава или от друга експлоатация на дете за подобни цели;
- участие в сексуални действия с дете, в които е използвана принуда, насилие или заплахи, в които пари или други форми на възнаграждение или разплата са давани като заплащане на детето в замяна на сексуални действия, или в които е извършена злоупотреба с признато положение на доверие, власт или влияние над детето;
- независимо дали е извършено чрез компютърна система или не:
    - производство на детска порнография;
    - дистрибуция, разпространение или предаване на детска порнография;
    - доставяне или осигуряване достъп до детска порнография;
    - придобиване и притежаване на детска порнография.

Държавите-членки трябва да предвидят наказания, които включват лишаване от свобода от най-малко една до три години. За определени деяния, извършени при утежняващи вината обстоятелства, наказанията трябва да бъдат лишаване от свобода от най-малко пет до десет години.

Рамковото решение предоставя списък с утежняващи вината обстоятелства, който не изключва установяването и на други обстоятелства по националното законодателство:

- жертвата е дете под възрастта за съгласие за секс по националното законодателство;
- нарушителят умишлено или поради безразсъдство е застрашил живота на детето;
- правонарушенията включват тежко насилие или тежка вреда на детето;

- правонарушението е било извършено в рамките на престъпна организация, според дефиницията на Съвместно действие 98/733/ПВР, определяща за престъпление участието в престъпна организация в държавите-членки на Европейския съюз.

Държавите-членки могат да предприемат мерки, с които да гарантират, че лицата, осъдени за едно от гореизброените правонарушения, са лишени от правото да упражняват професионални дейности, свързани с надзор на деца.

Решението също изисква от държавите-членки да гарантират, че юридическите лица могат да бъдат държани отговорни по наказателното и гражданското право за извършването на гореспоменатите правонарушения, както и за подбудителство, помагачество, съучастие и опит. Тази отговорност е допълваща към отговорността, носена от физическите лица. Едно юридическо лице се счита за отговорно, ако заради него е извършено престъпление от друго лице, което действа самостоятелно или като част от орган на юридическото лице, или което има правомощия за вземане на решения. Санкциите за юридически лица трябва да включват наказателноправни и ненаказателноправни глоби и други санкции, като например временно или постоянно лишаване от възможността да се осъществяват търговски дейности, ликвидация по съдебен ред или лишаване от право на ползване на обществени блага и помощи.

За да се избегне едно престъпление да остане безнаказано заради конфликт на юрисдикциите, с Решението се установяват критерии за определяне на юрисдикция. Една държава има юрисдикцията, ако:

- правонарушението е извършено на нейната територия (териториален принцип);
- правонарушителят е гражданин на тази държава-членка (принцип на активната правосубектност);
- правонарушението е извършено заради юридическо лице, учредено на територията на тази държава-членка.

Държава, която отказва да екстрадира своите граждани, трябва да предприеме необходимите мерки, за да ги преследва за правонарушения, извършени извън нейната територия.

Един скорошен доклад на Европейската комисия, *Доклад на Комисията въз основа на член 12 от Рамково решение 2004/68/ПВР на Съвета от 22 декември 2003 г. относно борбата със сексуалната експлоатация на деца и детската порнография* (COM(2007) 716 final), отбелязва, че:

> „…предвидените в Рамковото решение на Съвета изисквания са спазени от почти всички държави-членки или в резултат на съществуващи преди това национални закони, или чрез приемането на ново, специално законодателство. … Що се отнася до детската порнография, изискването за инкриминиране на производството на порнографски материали с деца е спазено в общи линии, въпреки че не е възможно да се направи точна оценка на обхвата на случаите, в които не се търси наказателна отговорност за детска порнография с деца, чиято възраст е между тази на юридически валидно съгласие и 18 години. … сега държавите-членки в общи линии разполагат със специфични наказателноправни разпоредби, които инкриминират сексуалната експлоатация на деца и детската порнография и предвиждат ефективни, съразмерни и възпиращи наказания … възникват и нови проблеми, като например измамно подмамване на деца с незаконни цели чрез Интернет (манипулиране или т.нар. „зарибяване“) … В светлината на тези дискусии и резултатите от тях Комисията може да обмисли необходимостта от актуализиране и по-голяма категоричност на настоящото Рамково решение по отношение на … по-специално престъпленията, извършени чрез електронни комуникационни мрежи и информационни системи”.

Понастоящем Комисията изучава нов набор от мерки за ограничаване на детската порнография. Сред тях е създаването на звена за контакт за всички въвлечени участници, като например финансови институции и доставчици на Интернет, за може бързо да се блокират незаконните уебсайтове и плащанията, направени през тях. През есента на 2007 г. финансовият сектор учреди контролна група, която да осъществи подготвителните мерки. През 2008 г. те ще подадат проект за финансиране от Комисията, за да се създаде това *one-stop-shop* звено.

Асоциацията на горещите линии в Интернет INHOPE, координирана от Ирландия, беше основана през 1999 г. INHOPE е една от малкото международни реакции към незаконното съдържание и незаконните дейности в Интернет и тя е частично финансирана от Програмата за действие на ЕК „Безопасен Интернет" и Microsoft. INHOPE улеснява и координира работата на 18 национални горещи линии за борба срещу незаконното съдържание в Интернет. Горещите линии наблюдават Интернет и те са мястото, на което широката общественост може да докладва за незаконно съдържание в Интернет, като например детска порнография. След това горещата линия разглежда поверително всеки сигнал, като отнася незаконните материали до съответните правораздавателни агенции или до доставчиците на Интернет услуги за по-нататъшни действия. Докато една единствена гореща линия може да има успех на национално ниво за справяне с проблема, влиянието ѝ е ограничено, когато съдържанието се управлява и обслужва в чужда държава или когато извършителят се намира в чужбина. Мрежата INHOPE е важно средство за координиране на обмена на информация и експертиза между горещите линии по цял свят.

7.2.4. Прилагане на закони за борба с порнографията и други регулационни стратегии в електронна среда

Както беше демонстрирано до този момент, проблемът с контрола на разпространението на порнографията по електронен път е сложен. За държавите може да е трудно да построят ясни дефиниции на типовете порнографски контексти, които желаят да бъде инкриминирани, и за тях може да е проблемно (така както Съединените щати се бориха да направят това в продължение на повече от едно десетилетие след Закона за благоприличие в комуникациите от 1996 г. (Krause 2008)) да балансират защитата на малолетните и на други уязвими групи с конкуриращите се конституционни принципи, като например свобода на словото и свобода на изразяване в електронна среда.

Много държави не са склонни да се борят с проблема с „порнографията с възрастни", като се опитат да инкриминират нейното разпространение по електронен път. Дори в САЩ, където в миналото беше предприета сравнително твърда политика на действие, изглежда, че има недостатъчен интерес от страна на законодателните органи или на местните власти или относно създаването на допълнителни закони, или относно активното прилагане на съществуващите закони. Вместо това, съществува тенденция действията да се фокусират върху спиране на достъпа до нея, особено от страна на малолетни и други уязвими групи. Редица технологични схеми за блокиране на съдържание се използват в различни държави за цели, включващи отказване на достъп до порнография, включително в Китай (схема със защитна стена (*firewall*), която променя връзките – „Великата китайска защитна стена"), в Саудитска Арабия (уеб-базирана проксисистема с универсален списък на забранени уебсайтове от доставчик на филтриращ софтуер, засилвана от еднотипни локатори на ресурси (URLs), докладвани от гражданите, подавани чрез уеб-формат), и в Норвегия. (*Clayton 2005*)

Детската порнография е различна материя. Въпреки че остават значителни разлики в дефинициите (напр. относно това дали да се инкриминират изображения, за които не се използват действителни деца, като например псевдо фотографиите, или използването на актьори, които само приличат на деца) и вариращи обосновки на политиките (напр. превенция на директната вреда върху децата при създаването на детска порнография, или

превенция на косвената вреда върху децата при електронен достъп до обезпокоителни материали, или когато детската порнография се използва, за да „съблазни или окуражи деца да участват в сексуални действия") между държавите, еднакво ясно е, че съществува важен национален, регионален и международен консеснус, че детската порнография трябва да е незаконна и че наличността ѝ в Интернет ще изисква както действия от страна на държавния и частния сектор, така и значително транс-гранично сътрудничество за справяне с проблема.

За някои държави е било трудно да рационализират третирането на лице под 18 години като „дете" за целите на защитата на децата от сексуална експлоатация и детска порнография в случаите, в които тяхната юридически значима възраст за съгласие за сексуални действия може да е значително по-ниска (в ЕС юридически значимата възраст за съгласие варира в законодателствата на държавите-членки от 13 г. в Испания до 17 г. в Ирландия). Въпреки това от *Конвенцията на МОТ за най-тежките форми на детски труд,* през *Конвенцията на ООН за правата на детето,* през *Решението на ЕС за борба с детската порнография в Интернет* от 2000 г., до *Конвенцията на Съвета на Европа за защита на децата от сексуална експлоатация и сексуално насилие*, изглежда, че се появява международен консенсус относно това, че всяко дете под 18 г. трябва да бъде категорично защитавано от експлоатация в детска порнография, че трябва да съществуват само ограничени изключения между признатата от закона възраст за съгласие за сексуални действия и че вероятно е необходимо хармонизирането на признатата възраст за съгласие за сексуални действия.

7.3. Подходът на Великобритания

Великобритания е предприела сравнително активен подход към проблема с електронната „порнография", въпреки че до скоро не използваше думата в законодателството си.

7.3.1. Правна уредба на нецензурно съдържание (Obscenity legislation)

Британският *Закон за нецензурните публикации* от 1959 г. (ЗНП) гласи, че „една статия следва да бъде считана за нецензурна, ако нейният ефект, взет като цяло, ... е такъв, че *води до покваряване и развращаване* на лицата, които има вероятност ... да прочетат, видят или чуят материалите, съдържащи се или изобразени в нея". Ключовите проблеми, които съдебните заседатели трябва да вземат предвид, когато оценяват определен материал, са:

- *Възможността за съответния материал да бъде счетено за вероятно, че покварява и развращава.* Би ли могъл страничен наблюдател да стигне до извода, че тези, които гледат материала, може да се покварят и развратят от него?
- *Вероятната публика на материала*, като това ще формира част от оценката на неговата склонност да покварява и развращава. Когато се решава дали материалът е нецензурен, важен определящ фактор е съображението каква ще е вероятната му публика. Това е така, защото някои потенциални аудитории се считат за по-податливи към покваряване и развращаване от други. На децата се гледа като на публика, която е особено уязвима в това отношение. По този начин, материал, публикуван във форум или в медиите, който е достъпен за деца, винаги ще подлежи на по-строго регулиране, отколкото материал, който не е.

Ако една статия е нецензурна, то е правонарушение тя да се публикува или да се дава за публикация с цел печалба. *Законът за нецензурните публикации* от 1959 г., изменен от *Закона за наказателно правосъдие и обществен ред* от 1994 г., определя издателя като лице във връзка с нецензурния материал, което:

§ разпределя, разпространява, продава, отдава под наем, предоставя или дава на заем или което предлага за продажба или за отдаване под наем, или;

§ в случай на статия, съдържаща или съставляваща материал, който да бъде гледан, или запис, го показва, пуска или прожектира, или, в случаите, когато данните се съхраняват електронно, препраща информацията.

По този начин, трансферът на нецензурен материал или ръчно, чрез използване на компютърни дискове или други носители, или по електронен път от един компютър до друг, чрез мрежа или Интернет (напр. изпратен по електронната поща или качен на уебсайтове), ще попада в обхват на закона.

Британският *Закон за нецензурните публикации* от 1964 г. регламентира като престъпление притежаването, държането или контрола на нецензурна статия с оглед публикуването й с цел печалба. Като резултат на това, нецензурният материал, качен на уебсървър, ще бъде обхванат дори когато лицето само предостави достъп до информацията, за да бъде прехвърлена или свалена по електронен път от други, така че те да могат да имат достъп до материалите и да ги копират. В делата *R v Arnolds, R v Fellows* (1997 г.) съдът поддържал тезата, че доколкото законодателството изисква някакви действия от страна на „издателя", такива са били осъществени от факта, че един от жалбоподателите бил предприел „всички необходими стъпки не просто да съхрани информацията на компютъра си, но и да я направи достъпна до други компютри по целия свят чрез Интернет. Той си кореспондирал по електронната поща с тези, които искали достъп до нея, и наложил определени условия преди да им позволи това". Въпреки това, след решението по делата *R v Perrin* (2002 г.) обвиняемият публикувал представителен уебсайт, достъпен безплатно до всички, имащи достъп до Интернет, който включвал снимки на хора, покрити с фекалии, корпофилия или корпофагия и мъже, участващи във фелацио. Така прокуратурата ще трябва да доказва, че има вероятност повече от пренебрежимо малкият брой хора, склонни да бъдат покварени и развратени, да видят материала.

Някои издатели на нецензурни материали във Великобритания са търсили начин да избегнат британския закон за нецензурните публикации, като качват материалите си на уебсървъри в други страни. В делото *R v Waddon* (2000 г.) обвиняемият подготвил нецензурния материал в Англия и го качил от Англия на уебсайт в САЩ, от който след това бил свален от полицейски служител в Лондон. Уадън твърдял, че материалът не бил публикуван във Великобритания по смисъла на ЗНП (1959 г.) и по този начин бил извън юрисдикцията на съда. Съдът обаче поддържал тезата, че Уадън бил въвлечен и в препращането на материала към уебсайта, и в препращането му обратно към тази държава тогава, когато полицейският служител се сдобил с достъп до уебсайта – и е имало, по смисъла на ЗНП (1959 г.), публикация в уебсайт в чужбина, когато изображенията са били качени там, а след това още една публикация, когато тези изображения са били сваляни, на което и да е друго място.

Накратко, базиран във Великобритания издател на електронни порнографски материали, включващи възрастни, може да бъде преследван за нецензурни публикации, ако съдебните заседатели намират, че е вероятно материалите да развращават и покваряват определена аудитория. Един уебсайт с открит достъп е ефективно отворен за света, включително за деца, и така вероятността да развращава и покварява онези, за които е вероятно да имат достъп до него, ще бъде голяма. Публикуването на материалите извън Великобритания няма да спре съдебното преследване за нецензурни публикации, ако материалите са достъпни във Великобритания. Не е нужно преследваните материали да са базирани на изображения. Повдигнати са обвинения срещу автора на блог материал, описващ подробно въображаемо отвличане, измъчване и убийство на членовете на поп групата 'Girls Aloud' (*R v Walker,* 2008 г.).

7.3.2. Правна уредба на неприлично съдържание (Indecency legislation)

По отношение на детската порнография съответните части на изменения *Закон за защита на децата* 1978 (ЗЗД) се занимават с фотографски изображения на деца под 18 години (или лица, които изглеждат под 18 години). Законът регламентира като

правонарушение правенето, производството, разрешаването да се правят, разпространението, показването и притежаването с намерение да се разпространяват или показват, или публикуването на неприлични фотографии или псевдо-фотографии на деца. Законът дефинира „разпространението" много общо. За да са действително притежавани, не е необходимо материалите да са били предавани от едно лице на друго, материалите просто трябва да са били изложени или предложени за придобиване. ЗЗД също инкриминира реклами, които предполагат, че рекламодателят разпространява или показва неприлични фотографии на деца, или има намерението да го направи.

Законът за наказателно правосъдие и обществен ред от 1994 г. (ЗНПОР) изменя ЗЗД като добавя, че понятието „фотография" да включва:

> „данни, съхранявани на компютърен диск или чрез други електронни средства, които могат да се конвертират във фотография".

Тази дефиниция на фотография покрива дигитални изображения на физически фотографии (по този начин файловете в .gif и .jpeg формат, свалени от FTP сайтове към уебсайтове или съставени от Usenet съобщения, ще бъдат третирани като фотографии).

В допълнение, ЗНПОР прибавя и дефиниция за „псевдо-фотография":

> „Псевдо-фотография" означава изображение, направено или чрез компютърна графика, или по какъвто и да е друг начин, което изглежда като фотография".

Така, псевдо-фотография означава всяко изображение, което може да бъде сведено до изображение, изглеждащо като фотография, и ако изглежда, че изображението показва дете, тогава следва да се третира като такова на дете. Това означава, че няма нужда за създаването на изображението да е било използвано дете. Всъщност Законът регламентира неприлично изображение, което може и да не се базира на жив субект. Измененията във връзка с псевдо-фотографията се занимават със случаи, в които например се използва трансформиращ софтуер, за да се създават изображения, които изглеждат сякаш са на деца, от изображения на възрастни.

Законът за наказателно правосъдие и нелегална имиграция от 2008 г. (ЗНПНИ) допълнително изменя дефиницията на „фотография".

„Към фотография също се отнася следното:

а) копиране или друго изобразяване, създадено чрез електронни средства или по друг начин (от каквото и да е естество):

(i) което само по себе си не е фотография или псевдо-фотография, но

(ii) което произхожда от цялата или от част от фотография или псевдо-фотография (или комбинация от едното или от двете); и

б) данни, съхранявани на компютърен диск или чрез други електронни средства, които могат да се конвертират в изображение по смисъла на ал. а."

Терминът „неприличие" не е дефиниран нито в ЗЗД, нито в друг закон, в който се появява. В основата си, изглежда, че преценката е в това дали въпросното нещо нарушава настоящите стандарти за благоприличие, или ако използваме американската фразеология, нарушава съвременните обществени стандарти. При положение, че обществените стандарти на поведение на възрастните имат тенденцията да са по-завишени, когато са въвлечени деца, изображение, включващо гол възрастен, което може да е абсолютно допустимо, може да бъде третирано като неприлично, ако изображение или псевдо-изображение на дете се направи по подобен начин.

Разпоредбите, дискутирани по-горе, имат ясна връзка с дейностите в Интернет. Качването на неприлични снимки на уебсървър почти неизбежно би означавало, че те ще бъдат разпространени; когато подобни снимки се съхраняват на компютър, съвсем достоверно може да се каже, че те са притежание на някого; електронна препратка към уебсайт може да се счита за реклама; а съобщение по електронната поща, предлагащо подобни снимки в цифров или хартиен формат, определено би било считано за такава.

Лице, обвинено по ЗЗД за разпространение, показване или притежаване с цел показване или разпространение, има две възможни оправдания:

- § не са видели изображението и не са знаели или подозирали, че то е неприлично;
- § имало е законно основание за притежаването или разпространяването на изображението, напр. за академично изследване или в процеса на събиране на доказателства.

Също така, за правонарушение се счита притежанието на неприлично изображение на дете или на лице, което прилича на дете. Наличните оправдания са:

- § те са имали законно основание да притежават фотографията или псевдо-фотографията;
- § те не са видели фотографията или псевдо-фотографията и не са знаели, нито са имали основание да подозират, че е била неприлична;
- § фотографията или псевдо-фотографията им е била изпратена, без те предварително да са били попитани и те не са я задържали за дълго време.

По отношение на компютърното създаване или притежание на неприлични фотографии на деца, в делото *R v. Bowden* (2000 г.) британските съдилища защитаваха тезата, че умишленото сваляне и/или принтиране на компютърни данни на неприлични изображения на деца от Интернет съставлява „създаване" на неприлична фотография и по този начин е престъплено деяние по чл. s1(1)(a) от *Закона за защита на детето* от 1978 г. По отношение на неумишленото съхраняване на компютърни данни на неприлични изображения на деца на кеш паметта на компютъра, в делото *Atkins v DPP* (2000 г.) съдът поддържаше тезата, че не съставлява автоматично „създаване", нито пък тяхното наличие в кеш паметта на компютъра не означава задължително, че е било извършено правонарушение по чл. s160 от *Закона за наказателно правосъдие* от 1988 г., тъй като при такива обстоятелства трябва да се докаже, че обвиняемият е знаел, че притежава фотографиите или че някога ги е притежавал.

В делото *R v Smith and Jayson* (2002 г.) Смит бил получил неприлична фотография като приложение към съобщение по електронна поща, а Джейсън разглеждал неприлична псевдо-фотография в Интернет. И в двата случая техният браузърен софтуер автоматично е запазил изображенията на временната Интернет кеш памет на компютрите им. Що се отнася до Смит, съдът поддържал тезата, че никакво престъпно деяние на „създаване" или „притежаване" на неприлична псевдо-фотография не е било извършено само от отварянето на приложение в съобщение по електронната поща, при което получателят не е знаел, че то е съдържало или е имало вероятност да съдържа неприлично изображение. Въпреки това, когато отварянето на приложението от Смит било разглеждано в контекста на доказателствата, свързани с неговите действия, съдът не му вярвал, че не е знаел за естеството на приложението. Джейсън твърдял, че неговият акт на разглеждане на неприлична псевдо-фотография не съставлява необходимия умисъл да „създаде" фотография или псевдо-фотография. Съдът, обаче, поддържал тезата, че актът на съзнателно сваляне на неприлично изображение от Интернет на компютърен екран е акт на създаване на фотография или псевдо-фотография, тъй като изискваният умисъл е „преднамерен и съзнателен акт със знанието, че изображението е или може да бъде неприлична фотография или псевдо-фотография на дете."

В заключение, един действащ на територията на Великобритания създател, собственик или издател на порнографски Интернет материали, включващи деца, може да бъде преследван за неприличие, ако съдебните заседатели установят, че въпросните материали съдържат изображения на деца под 18 години (или на лица, които изглеждат под 18 години), които нарушават съвременните стандарти за благоприличие, и тези материали са или фотографии, или изглеждат като фотографии. Сваляне то и/или съхраняването на неприлично изображение съставлява извършването на правонарушение, свързано с изображение. Само притежаването също е правонарушение (с изключение на някои специфични обстоятелства).

7.3.3. Правна уредба на екстремна порнография

Според британския *Закон за наказателно правосъдие и нелегална имиграция* от 2008 г. (ЗНПНИ) е престъпление лице да притежава „екстремно порнографско изображение". Както бе отбелязано по-горе, „екстремно порнографско изображение" е изображение, което:

- § е от такова естество, че логично трябва да се приеме, че е било създадено единствено или основно с цел сексуална възбуда; и НЕ е част от поредица от изображения, които поставени в контекст не са порнографски;
- § И изобразява по открит и реалистичен начин което и да е от следните неща:
  - o деяние, което заплашва човешки живот;
  - o деяние, което води до или е вероятно да доведе до сериозно нараняване на ануса, гърдите или гениталиите (препратките към всяка част от тялото се отнасят и до всяка част, която е хирургично изградена, напр. чрез операция за смяна на пола);
  - o деяние, което включва полово сношение с човешки труп; или
  - o лице, извършващо полово сношение или орален секс с животно (независимо дали животното е мъртво или живо);
  - o И при което всеки разумен човек, гледащ изображението би си помислил, че всяко такова лице или животно е реално;
- § И е изключително противно, възмутително или от друг нецензурен характер.

Лице, обвинено по ЗНПНИ за притежание на екстремно порнографско изображение, има три възможни оправдания:

- § имал е законно основание да притежава въпросното изображение;
- § не е видял въпросното изображение и не е знаел, нито е имал някакво основание да подозира, че това е екстремно порнографско изображение;
- § изображението му е било изпратено, без лицето предварително да е било попитано и то не го е задържало за дълго време.

Съществува допълнително оправдание за лице, обвинено по ЗНПНИ за притежание на екстремно порнографско изображение, в което правонарушението е свързано с изображение, показващо деяние, което заплашва човешки живот; деяние, което води до или е вероятно да доведе до сериозно нараняване на ануса, гърдите или гениталиите; или деяние, което включва полово сношение с човешки труп, и обвиняемият може да докаже

- § че той пряко е участвал в деянието или във всяко едно от показаните деяния, И че деянието или деянията не са включвали причиняване на каквато и да е вреда, която не е по взаимно съгласие, на което и да е лице, И когато изображението показва деяние, което включва полово сношение с човешки труп, че това, което е показано като човешки труп, всъщност не е било труп.

Към днешна дата изглежда, че не е имало никакви съдебни преследвания по този закон.

7.3.4. Правна уредба на „зарибяването"

„Зарибяването" най-общо се определя като процес, при който едно лице се сприятелява с дете, за да спечели доверието му и да създаде ситуация, при която детето ще позволи на извършителят да има сексуални контакти с него и няма да каже на никого. Това е сериозен проблем в Интернет пространството. Изследвания в САЩ показват, че между 5 – 20 % от децата са били подстрекавани по Интернет. В Обединеното кралство, съгласно Закона за сексуалните престъпления от 2003 г. за престъпление се счита срещата с дете с намерение за сексуален контакт с него, където лицето (над 18 години):

- § е осъществило среща или е общувало с дете (под 16 години) два пъти преди това И:

- § или се среща с детето ИЛИ пътува с цел да се срещне с дете (в която и да е част на света) И
- § по това време има намерение да извърши сексуално престъпление.

Законодателството инкриминира срещите след сексуалното „зарибяване", а не самото сексуално „зарибяване". Така дава възможност на полицията да провежда активно охраняване по Интернет – полицаи се представят за податливи деца в чат стаи и изчакат извършителите да се свържат с тях. Извършителите, които се уговарят да се срещнат с полицаите под прикритие могат да бъдат арестувани на базата на наличието на доказателства, които доказват сексуално намерение. В процеса на „зарибяване" често се използва порнография.

7.4. Други мерки

Фондацията за наблюдение на Интернет (ФНИ) е британски независим самоуправляващ се орган, финансиран от Европейския съюз и широкия Интернет сектор, включващ доставчици на Интернет и съдържание, мобилните оператори и производители, филтриращи дружества, търговски асоциации и финансовия сектор (напр. Асоциация за услуги по клирингови разплащания). Тя предоставя канал на британското общество и ИТ специалисти да съобщават за потенциално незаконно съдържание чрез гореща линия в Интернет. Потенциално незаконното съдържание в Интернет включва съдържание със сексуално насилие над деца, управлявано и хоствано навсякъде по света и съдържание с престъпно подстрекаване към расова омраза, управлявано и хоствано в Обединеното кралство. ФНИ също така:

- § помага доставчиците на Интернет и хостинг дружествата да противодействат на злоупотребяването с техните мрежи чрез национална услуга за „уведомяване и сваляне", която им сигнализира за потенциално незаконно съдържание в техните системи;
- § предоставя уникални данни на правораздавателните органи в Обединеното кралство и чужбина, за да подпомагат разследванията на разпространители на потенциално незаконно Интернет съдържание;
- § Подпомага инициативата на сектора за защита на потребителите от непреднамерено излагане на потенциално незаконно съдържание, управлявано и хоствано в чужбина, като блокират достъпа до него чрез предоставяне на актуализиран списък със URLs на сексуално насилие над деца.

Съгласно ФНИ, в резултат на дейностите й, по-малко от 1% от съдържанието със сексуално насилие над деца (ФНИ използва този термин вместо „детска порнография"), известно на ФНИ, очевидно се управлява и хоства в Обединеното кралство от 2003 г., което представлява спад в сравнение с 18 % през 1997 г. Актуализираният списък със URLs на сексуално насилие над деца на ФНИ се ползва от Cleanfeed, система за блокиране на съдържание на Британската телекомуникационна компания (БТК) и WebMInder, който се използва от голям брой доставчици на Интернет. ФНИ е член на INHOPE.

Нов Британски съвет за безопасност на децата в Интернет (БСБДВ) бе учреден през септември 2008 г., за да обедини над 100 организации от публичния и частния сектор, които работят с правителството и разработват препоръки от Доклада на Байрън „По-голяма безопасност за децата в дигиталния свят". Ролята на Съвета е да подобри регламентирането и културата на ползване на Интернет, да разреши проблеми, свързани с тормоза по Интернет, по-безопасни услуги на търсене и видео игри с насилие. Той ще е пряко подчинен на министър-председателя.

Съветът ще участва в развитието на Британска стратегия за безопасност на децата в Интернет, която ще се приеме през 2009 г. и ще:

- § развие комплексна кампания за осведомяване на обществото за безопасност на децата по Интернет сред правителството и сектора, включително и информация на принципа „на едно гише" относно безопасност на децата в Интернет.
- § предложи конкретни мерки в подкрепа на уязвими деца и млади хора като сваляне на незаконни Интернет страници, които съдържат вредно поведение;
- § насърчи отговорно рекламиране, насочено към децата в Интернет;
- § развие доброволни кодекси на поведение за Интернет страници с потребителско съдържание, като изисква от такива страниците да премахнат неподходящото съдържание в рамките на определен период.

7.5. Добри практики

Както става ясно от дискусията по-горе, има няколко често допълващи се подхода за разглеждане на въпроса за контролащ и, където е необходимо, инкриминирането на различни форми на Интернет порнография. Добрите практики в тази област за повечето държави вероятно ще се състоят в гарантиране на адекватна правна уредба, която да изпълнява поетите международни ангажименти, като взема предвид национални фактори, които могат да се отразят на ефективното и ефикасно развитие на политиките и уредбата в тази област. По този начин, държавите, в краткосрочен и дългосрочен план трябва да дерогират от или да си запазят правото да не прилагат, както е разрешено различни аспекти на национални споразумения, докато не се хармонизират съществуващите национални правила и практики (напр. възрастта за съгласие).

Когато се разработват национални правни подходи към контролирането и, когато е необходимо, инкриминирането на различни форми на електронна порнография, е важно да се обмислят внимателно типовете среда, в които се намират материалите понастоящем и в които може да бъдат достъпни в бъдеще, по отношение на влиянието, което регулирането може да има върху пазара – затегнатото регулиране може да предизвика бариера за навлизането на нови дейности и технологии; или върху други правни принципи, като свобода на словото и свобода на изразяване – социалните норми се променят във времето и може да бъде трудно да се гарантира, че строгите регулаторни режими ще могат да се променят с времето. Във Великобритания подходът към нецензурните/неприличните материали се е доказал като гъвкав с промяната на социалните норми във връзка с порнографията с възрастни – това, което е могло да се счита за нецензурно през 50-те години на 20 век, сега може да бъде възприемано като преобладаваща култура или начин за артистично изразяване; въпреки всичко, тази гъвкавост е дошла отчасти за сметка на сигурността – може да има известна резервираност на словото/изразяването просто, защото няма ясно правило относно това какво е нецензурно/неприлично. Това са въпроси, които националните законодателни органи и съдилищата трябва да вземат предвид.

По всяка вероятност опитът да се използват само националните правни подходи няма да се окаже успешен. Както и в други области на кибернетичните престъпления, като например измамите и прането на пари, ако се очаква правоприлагащите органи и контролът да са ефективни, трябва да съществува възможност за обмен на информация и, когато е уместно, на доказателства между компетентните органи и регионалните власти на международно ниво, бързо, систематично и ефективно.

Мобилизирането на обществения и частния сектор в подрепа на целите на регулирането, включително и на частните фирми, индустриалните групи и потребителските групи, по отношение на обучаване и консултиране (напр. възползване от техническите познания на частния сектор) и по отношение на търсенето на начин да се въвлекат организации от частния сектор в регулаторните процеси, като например въвличането на секторни групи в саморегулаторни практики, често пъти може да постигне значително повече от подхода „командвай и контролирай", спуснат отгоре надолу. В много случаи е от полза за организациите от частния сектор, като доставчици на Интернет услуги и други

доставчици на услуги на информационното общество, да могат да контролират своите собствени среди, тъй като неконтролираната порнография може да е пречка за окачествяването на техните услуги като подходящи например за семейството или безопасни за деца. Така целта на правителствата може да бъде да им осигури необходимата законодателна и/или финансова подкрепа, за да се направи това.

8. ПРАНЕ НА ПАРИ ПО ЕЛЕКТРОНЕН ПЪТ

8.1. Въведение

Терминът "Пране на пари" не е легален в международното право, въпреки че изпълнителното деяние на това престъпление включва използване на незаконни средства, които да изглеждат законни. Престъплението се дефинира по следния начин:

> *Преобразуване или прехвърляне на имущество със знанието, че то е придобито чрез престъпление, с цел укриване или прикриване на неговия незаконен произход или подпомагане на лице, участвало в извършването на основното престъпление, за да се избегнат правните последици от неговите действия; или укриването или прикриването на истинския характер, произход, местонахождение, разпореждане, прехвърляне, собственост или права върху това имущество със съзнанието, че то е придобито чрез престъпление.* (Член 6, Конвенция на ООН срещу транснационалната организирана престъпност, приета през ноември 2000г., в сила от септември 2003г).

„Основният състав", свързан с прането на пари, включва престъпна дейност, в основата на която е създаването на облаги, които след като се „изперат", и води до престъпление, свързано с пране на пари. Подобни престъпления могат да включват сделки с наркотици, рекет, обир или кражба, корупция, подкуп и измама. Общата тенденция на международно ниво в последно време е увеличаване на броя на подведените под отговорност лица за основни престъпления, свързани с пране на пари.

Престъпленията, свързани с пране на пари, се считат за особено сериозни, защото те:

- стимулират престъпно поведение, правейки го доходоносно;
- предоставят на вътрешната и транснационалната организирана престъпност парични потоци, с които да извършват по-нататъшни престъпления; и
- заплашват вътрешната и международната финансова система и нейните институции.

Наред с това, след събитията от 11 септември, съществува засилен интерес към тероризма и свързаното с него финансиране, тъй като достъпът и използването от терористите на суми, които от гледна точка на прането на пари може да са много малки, може да има диспропорционален ефект върху широката публика.

Прането на пари, както много други форми на престъпления, извършвани по електронен път, има значителна офлайн история – всъщност, за него се е твърдяло (вероятно неправилно), че самото понятие произхожда от факта, че мафията е притежавала пералните на самообслужване или „обществените перални" в Съединените щати. Какъвто и да е произходът на понятието, обикновено се счита, че прането на пари има три основни етапа:

- Разполагане/укриване. Незаконно придобитите пари, които трябва да бъдат изпрани, се въвеждат в икономиката, често посредством търговски концерни, които съзнателно или несъзнателно може да са част от схемата за изпиране, и които предоставят връзката между извършителя на изпирането на парите и финансовия сектор. Една обикновена схема за пране на пари може просто да добавя плащания в брой към съществуващ поток от приходи, т.е. да слага парични средства от незаконен хазарт в оборота на един гараж за самообслужване, от където се правят плащания до извършителя на изпирането, под някакъв привидно законен претекст. Големи и/или множество малки суми от незаконни средства, обаче, изпрани по такъв начин, могат да привлекат вниманието.
- Наслояване/преместване. За да се избегне привличането на вниманието при по-усъвършенстваните схеми за пране на пари, извършителят на прането влиза в сложни

мрежи от сделки, които могат да използват трансфери, продажби и покупки на активи, за да разбият първоначалната сума и да прикрият първоначалната точка на въвеждането на парите в икономиката.

- Инвестиране/Интегриране. След като парите са били успешно изпрани, т.е. придобити са от определен законен източник на приходи, те могат да бъдат използвани от извършителя на прането за инвестиране в активи или начин на живот.

Пример:

Г-н А., извършител на пране на пари, придобива пари чрез основно престъпление – трафик на наркотици. Той създава многобройни анонимни сметки в един Виртуален свят (ВС), който поддържа своята собствена вътрешна валута, ВС долар, с фиксиран курс към щатския долар. Той кредитира сметките с ВС долари, като използва кредитна карта или електронни плащания. Балансите по сметките във ВС долари се съхраняват електронно от собствениците на Виртуалния свят, а виртуалните средства могат да се използват във виртуалния свят за закупуване на „земя" или за търговия с виртуални стоки и услуги – Разполагане.

Г-н А. и други потребители, действащи от негово име, използват сметките, за да се въвлекат в търговски дейности помежду си и с други невинни потребители във Виртуалния свят, и тази дейност се координира чрез кодирани съобщения, изпратени от г-н А., използващ система за чат, създадена във Виртуалния свят. Г-н А. желае да поеме до 15% от загубата на стойността на „мръсните" пари, влезли в системата, за да произведе „чисти" пари – Наслояване.

Балансите или печалбите, направени от членовете на Виртуалния свят във ВС долари, могат да бъдат прехвърлени обратно в реалния свят, като щатски долари чрез PayPal или друго средство за електронно плащане или чрез сключване на сделки с други играчи чрез външни електронни аукциони, и след това – до различни банкови сметки, притежавани от г-н А. – Интегриране.

Националните правни стратегии следва да бъдат насочени към всичките тези три етапа, обикновено чрез създаването на правни задължения за банки или други институции, предоставящи финансови услуги (напр. агенции за парични трансфери, институции за електронни пари); за частния сектор (напр. адвокатски кантори, агенции за недвижими имоти); и дори на частни лица за докладване на подозрителни финансови дейности.

От самото начало на криминализирането му, прането на пари има важно международно значение, най-вече защото (както при измамите, извършвани по електронен път) международното пране на пари усложнява правната материя и включва множество национални правозащитни органи (LEAs). Навлизането на Интернет технологиите и особено на услугите на електронната търговия/електронното банкиране допълнително създава трудности поради фактори, като например:

> "…липса на регистрация лице в лице, възможна анонимност на потребителите, скорост на сключване на сделките, ограничена човешка намеса, голям брой сделки, международно присъствие, ограничени правораздавателни компетенции, трудности на традиционните финансови институции да наблюдават и откриват съмнителни финансови транзакции… когато се използва доставчик на услуги за плащане по Интернет…" (FATF 2008)

Тези трудности може да се задълбочат на местата, където националните правни системи са съсредоточили отчетните си задължения върху офлайн финансови услуги и дейности или все още трябва да възложат тези задължения на нови типове организации, занимаващи се с онлайн/електронни „трансфери на стойност", т.е. виртуален обмен на „скъпоценни метали".

Заслужава да се отбележи, че важни международни финансови трансфери дълго време са минавали през неформални системи за паричен трансфер (IMTS, известни също като

алтернативни или паралелни системи за превод на пари), например *hawala* или *hundi* (Южна Азия); *fei ch'ien, chiti, chop shop* или *flying money* (Китай). Тези традиционни системи обикновено действат в рамките на сплотени общности, като често пъти използват линии на комуникация, изградени из целия свят в течение на десетилетия. IMTS привличат клиенти поради тяхната простота, ефективност, надеждност и ниски разходи в сравнение с други налични възможности. Често те са нерегламентирани или действат незаконно в страните, където такива дейности са регламентирани, и са значително улеснени от електронните комуникации (Jost & Sandhu 2000). Докато *hawala* и *fei ch'ien* са установени отдавна, изглежда, че подобни IMTS са се развили неотдавна като механизъм на работещите в чужбина лица от Африка и Източна Европа за изнасяне на средства в техните родни страни от страни като Великобритания, като по този начин избягват таксите за банкови транзакции, комисионната за обмен на чужда валута, митническия контрол и данъците. Докато много от тези трансфери може да са прости, израз на желание за евтин и прост метод за превод на средства до близките им в чужбина, то е ясно, че IMTS може да предложи високоефективен и труден за регулиране механизъм за международно изпиране на пари.

Доставчикът на електронни пари/валута е една съвременна версия на тези ITMS. Пример за такъв доставчик е услугата WebMoney <http://www.wmtransfer.com/>, със седалище в Русия, който позволява на притежателите на сметки в няколко страни да прехвърлят средства по цял свят, без да използват формалния банков сектор. Докато услугите с електронни пари са доказали своята популярност, предоставяйки бърза, рентабилна и потенциално анонимна услуга за своите клиенти, увеличаващите се доказателства, че техните услуги са били използвани за международно изпиране на пари означават, че те са под все по-голям натиск да хармонизират услугите си с международните практики срещу прането на пари. (NDIC 2008)

Таблица 1: – Примери за пране на пари по електронен път

Вид	Естество на прането на пари	Цел	Пример
Прикриване на произхода на средствата	Извършителят използва трети лица да закупува луксозни стоки срещу пари в брой от физически съществуващи магазини. След това подставените лица предлагат стоките за продажба на много ниска цена в уебсайтове за електронна търговия. Плащанията за електронните продажби се извършват към банкови сметки, свързани с извършителя.	Извършителят търси възможност да прехвърли във финансовата система средствата (често пъти придобити от незаконни дейности, като проституция, комар, пласиране на наркотици) от на пръв поглед законни дейности.	Г-н А. има 5000 долара, придобити от пласиране на наркотици. Той плаща на г-н Б., г-н В. и г-н Г. да посетят бутикови магазини и да закупят бижута и дизайнерски стоки срещу заплащане в брой. След това стоките се предлагат за продажба в електронен аукцион, като се използват различни самоличности, чрез доставчик на услуги за разплащане по електронен път, също използващ различни самоличности. Плащането по електронните продажби се извършва към чуждестранните банкови сметки на г-н А.
Прикриване на доказателства от продажби на откраднати или фалшиви стоки	Извършителят продава откраднати или фалшиви стоки в електронни аукциони под различни самоличности. Парите от тези продажби се използват за закупуване на „чисти” стоки или електронни услуги, които на свой ред могат да бъдат продадени по нормален начин.	Извършителят търси възможност да отдалечи и самоличността си и произхода на парите от свързването им с откраднатите или фалшиви стоки.	Г-н А. продава фалшив софтуер в електронен аукцион, като използва различни самоличности, като му се плаща посредством доставчик на услуги за разплащане по електронен път, също използващ различни самоличности. След това г-н А. използва средствата, съхранявани при доставчика на услуги за електронни разплащания, за закупуването на законни стоки/услуги чрез аукционна къща, които могат да бъдат препродадени в електронни или физически съществуващи магазини.
Прикриване на доказателства за търговия с нелегални стоки или услуги	Извършителят търси възможност да използва доставчик на услуги за електронни разплащания, който да събира постъпленията от незаконна дейност, извършвана в една държава, и да ги прехвърля в друга.	Извършителят търси начин да прикрие самоличността на получателя на средствата и да усложни всяко разследване, провеждано от разследващите органи, чрез добавяне на транс-граничен елемент. Допълнителни трудности могат да възникнат в	Г-н А., гражданин на държавата Х, продава материали или услуги, които са незаконни в държавата Х (например наркотици, оръжие, проституция) на местни и чуждестранни клиенти посредством уебсайт. Плащанията за направените поръчки се събират посредством доставчик на услуги за

		случаите, в които дейността, генерираща средствата, е незаконна в първата държава, но е законна във втората.	електронни разплащания и се прехвърлят в банковата сметка на г-н А. в държавата У.
Прикриване на доказателства за измамнически транзакции	Извършителят поставя реклами за несъществуващи стоки на търговски уебсайтове. Купувачите са инструктирани да изпращат средствата посредством платежно нареждане на фиктивно лице в друга държава Плащането се прихваща от трето лице, което го препраща, използвайки подправена самоличност, или до извършителя, или до следващия по веригата от трети лица, работещи за извършителя.	Извършителят търси начин да прикрие самоличността на получателя на средствата и да усложни всяко разследване, провеждано от националните органи, чрез добавяне на транс-граничен елемент. Допълнителни трудности могат да възникнат в случаите, в които дейността, генерираща средствата, е незаконна в първата държава, но е законна във втората.	Г-н А., гражданин на държава Х, предлага за продажба скъпи бижута посредством търговски уебсайт. На купувачите от други страни се казва да изпращат платежните нареждания на г-ца Б. в държава У. Парите, изпратени на г-ца Б., всъщност се прибират от г-н В. Той (получавайки 10% от всяко платежно нареждане) е инструктиран посредством кратко съобщение (или от г-н А. или от друг „мениджър на паричния поток”, работещ за г-н А.) да изпрати парите на г-н Г. (който всъщност може да е самият г-н А. или друго трето лице, работещо за г-н А.).
Прикриване на целта на плащането	Извършителят предлага несъществуващи стоки за продажба в търговски уебсайт и приема „поръчки” само от конкретно трето лице.	Извършителят търси начин да прехвърли парите на трето/и лице/а без да буди подозрение относно целите на трансфера.	Г-н А. желае да осъществи плащане от 5000 долара за престъпната дейност на г-н Б. Той от своя страна поставя рекламно съобщение за продажба на кола, оценена на 5000 долара, на търговски уебсайт. Г-н А. дава да се разбере, че ще купи колата и изпраща 5000 долара по чуждестранната банкова сметка г-н Б. Никаква кола не е доставена. Г-н А. няма да маркира тази транзакция като измамническа, а електронната следа за „продажбата” чрез уебсайта осигурява на г-н Б. основание за паричния превод.
	Извършителят предлага реални стоки за продажба, но на изкуствено завишена или подчертано занижена цена.	Това има подобен ефект като прехвърлянето на пари от извършителя на трето лице/а, но допълнително преимущество се	Г-н А. предлага за продажба посредством електронен аукцион статуетка от китайски порцелан, закупена на цена от 500 долара. Международният интерес към

	Изкуствено завишените цени лесно могат да бъдат използвани в електронните аукциони, където справедливата пазарна стойност на стоките трудно може да бъде измерена и взаимодействието между потенциалните купувачи (включително „фалшиво наддаване”) може да доведе до необичайно изменение на цените.	явява оставената следа за действителна доставка. В този случай правозащитните органи трябва да докажат, че платената цена е значително непропорционална спрямо пазарната стойност на стоките.	подобни произведения на изкуството е голям и колекционерите често пъти заплащат за такива стоки много повече от пазарната цена. Г-н Б. предлага 2500 долара за статуетката. Г-н А. или заради колекционерския интерес, или чрез фалшиви наддавания, направени от допълнителни сметки, които той е открил, повишава цената на статуетката до цена, която е предварително уговорена с г-н Б. - на 2000 долара.
Укриване на данъци и на ДДС	Компания поръчва стоки, за които заявява, че ще бъдат изнесени, но след това ги продава на вътрешния пазар, избягвайки заплащане на ДДС, акцизи и други местни данъци. Продажбите по Интернет (посредством кредитна карта или електронно плащане) се използват с цел създаване на впечатление, че компанията осъществява легален износ за международни клиенти.	Компанията цели да представи своите бизнес дейности като законни операции, като по този начин мами националните данъчни служби и усложнява всякакви разследвания от страна на националните служби чрез добавяне на трансграничен елемент.	Компания Б. в държавата Х закупува безмитни стоки с цел продажба на международния пазар. Компанията претендира, че изнася стоките на законни международни клиенти посредством уебсайт, през който получава плащания от кредитни карти. В същото време обаче платежните нареждания на „клиентите” и плащанията се извършват от служители на компания Б. посредством чуждестранни кредитни карти и банкови сметки. Те се захранват със средства чрез директни преводи от държавата Х, или други страни, чрез фалшиви имена и прикриващи компании. Реално стоки не се изнасят.
Нелицензирани/ незаконни парични трансфери Модерен еквивалент на паралелните банкови системи,	Извършителят закупува „електронната стойност” под формата на „електронна валута” или „виртуални ценни метали”. След като веднъж е придобил „електронната валута” или „електронните ценни метали”, всичките или част от притежанията могат да бъдат прехвърлени по	Извършителят търси начин да прехвърли сума с фиксирана „стойност” посредством електронна парична услуга или виртуален обмен на ценни метали, основно без това да бъде наблюдавано или без да е разрешено от националните органи за борба с прането на пари.	Г-н А. от държавата Х отваря сметка на името на Platinum E-change Ltd., виртуален търговец на „ ценни метали”, поддържащ потребителски сметки, съдържащи виртуални авоари от ценни метали. Г-н А. използва Platinum E-change Ltd за трансфер на средства за услуга по обмен на „виртуални ценни метали”, като компанията играе ролята на посредник за

като *hawala*	електронен път на трето лице срещу стоки или услуги. В много юрисдикции сделките с „виртуални ценни метали", които са всъщност опциони за покупка на големи количества ценни метали на специфична цена (деривати), остават извън обсега на националните ограничения/регулиране на паричните трансфери. Освен това търговецът на „виртуални ценни метали" и/или самите борси, често използвани за улесняване на трансферите, в много случаи са извън юрисдикцията, в която се намира извършителят.		виртуалните ценни метали, които търговците купуват или продават за техните клиенти, които имат сметки при тях. Г-н А. прехвърля своите 1.5 милиона долара във „виртуални ценни метали", поддържани от Platinum E-change Ltd, посредством услугата за виртуален обмен на „ценни метали", към г-н Б. в държавата У, който продава опционите и използва средствата, за да закупи имущество за г-н А. в държавата У. Независимо от размера трансферът не се докладва на съответните власти за превенция на прането на пари нито в държавата Х, нито в държавата У, тъй като нито Platinum E-change Ltd., нито услугата за виртуален обмен на „ценни метали" попадат в съответната национална регулаторна рамка или под ограниченията, свързани с паричните трансфери, а двете компании са базирани в държавата Z, която е с ограничено банково регулиране.

Таблицата представлява извлечение от следните доклади на Специалната група за финансови действия (FATF/GAFI) – междуправителствен орган, чиито цели са развиването и популяризирането на национални и международни политики за борба с прането на пари и финансирането на терористични действия.

- FATF (2006) *Report on New Payment Methods*, 13 October 2006. http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf
- FATF (2008) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems*, 18 June 2008. http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

8.2. Международни инициативи

Въпреки че прането на пари има дълга история, съгласуваните международни усилия за борбата с него са се развили относително скоро, с международни договори, като *Конвенцията на ООН за борбата срещу незаконния трафик на упойващи и психотропни вещества* (1988) (Виенската конвенция) и *Конвенцията на ООН срещу транснационалната организирана престъпност* (2000) (Конвенцията от Палермо). Двата акта се стремят да подпомогнат държавите, страни по договора, да включат в законодателството си клаузи за борбата срещу прането на пари (БПП), като част от усилията си да осуетяват престъпления като трафик на наркотици и на хора. Други международни организации, включително Банката за международни плащания (БМП), Съвета на Европа, Интерпол, Организацията за икономическо сътрудничество и развитие (ОИСР) и групата от международни банки Wolfsberg също са участвали в създаването на мерки, включително насоки за добри практики, експертни съвети, национални оценки на КПП и насърчаване на международното сътрудничество.

Понастоящем ключовият елемент на международния подход към прането на пари е Специалната група за финансови действия – СГФД (Financial Action Task Force – FATF), която е била основана през 1989 г. от страните от G7. Основните задачи на СГФД са да изследва техниките и тенденциите при прането на пари и да изготви препоръки за мерки във връзка с БПП. В момента СГФД се състои от тридесет и четири члена: 32 държави и две регионални организации (Европейската комисия и Съвета за сътрудничество на страните в Персийския залив), представляващи повечето основни финансови центрове по света. СГФД също така работи чрез 8 регионални органа, подобни на СГФД, които на регионално ниво събират други държави, които са поели ангажимента да изпълнят 40+9-те Препоръки и са се съгласили да бъдат обект на взаимни оценки относно своите системи за БПП/БФТ. Пет от тези регионални органа, подобни на СГФД, са асоциирани членове на СГФД:

- Групата за борба срещу прането на пари от Азиатския и Тихоокеанския регион (the Asia/Pacific Group on Money Laundering – APG);
- Специалната група за финансови действия от Карибския регион (the Caribbean Financial Action Task Force – CFATF);
- Комитета на Съвета на Европа по оценка на мерките срещу изпиране на пари (the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures – MONEYVAL);
- Специалната група за финансови действия от Южноамериканския регион (the Grupo de Acción Financiera de Sudamérica – GAFISUD); и
- Специалната група за финансови действия от Средноизточния и Северноафриканския регион (the Middle East and North Africa Financial Action Task Force – MENAFATF).

Трите останали регионални органа, подобни на СГФД, работят по въпроса за придобиване на асоциирано членство:

- Евро-азиатската група за борба с прането на пари и с финансирането на терористични действия (Eurasian Group on combating money laundering and financing of terrorism – EAG);
- Групата за борба срещу прането на пари от Източноафриканския и Южноафриканския регион (Eastern and South African Anti Money Laundering Group – ESAAMLG); и

- Международната група за борба срещу изпирането на пари в Африка (Groupe Inter-gouvernemental d'Action Contre le Blanchiment en Afrique – GIABA).

През 1990 г. СГФД издаде своите „Четиридесет препоръки" (виж по-долу), които бяха изготвени с цел осигуряване на система от мерки за противодействие срещу прането на пари. Препоръките покриват:

- Националните съдебни и изпълнителни системи, с цел гарантиране уместността на подходящите мерки за криминализиране на прането на пари;
- Националните финансови системи и тяхното регулиране, с цел изискването финансовите институции и други организации (например, банки и счетоводни фирми) да предприемат подходящи мерки (например, проверка за статута на клиентите и отчетни изисквания);
- Международното сътрудничество с цел създаване на ефективни вътрешни регулаторни органи и обвързване с международно сътрудничество.

В основата си тези препоръки формират базата за всички вътрешни и регионални режими по отношение на борбата срещу прането на пари (БПП). Те регламентират принципите за действие и позволяват на страните да използват мярка за гъвкавост при прилагането на тези принципи според техните специфични обстоятелства и конституционни рамки. Между 2001 г. и 2004 г. СГФД издаде също девет Специални препоръки, които като се комбинират с Четиридесетте препоръки при прането на пари, оформят основната рамка за откриване, предотвратяване и спиране на финансирането на тероризма и терористичните действия. (виж по-долу)

Освен своите "40 + 9" препоръки, СГФД издаде списък с т.нар. „Несътрудничещи страни и територии" ("Non-Cooperative Countries or Territories" – NCCTs), обикновено наричан „Черният списък" на СГФД. Първоначално, през 2000 г., списъкът включва 15 държави, които са били считани от СГФД за несътрудничещи в международните усилия срещу прането на пари. Подобна липса на сътрудничество обикновено се оформя като неуспех при предоставянето на служители на чужди изпълнителни власти на информация, като банкова сметка и документи за комисионерство, както и информация за фиктивни компании и други финансови средства, често използвани при прането на пари. Черният списък е съставен от екипа на СГФД на базата на въпросник с 25 точки. Ако се открие, че една държава не отговаря на критериите по повече от една точка, тя автоматично се квалифицира като „несътрудничеща" или „частично несътрудничеща" в зависимост от броя на неизпълненията.

Черният списък е имал значителен ефект при постигането на сътрудничество от Несътрудничещите страни и територии (NCCTs), защото въпреки че вкарването в Черния списък на СГФД не води до формални санкции, транзакциите, идващи от или прехвърляни към държава от Черния списък на СГФД, е по-вероятно да бъдат счетени за съмнителна дейност, която в повечето държави-членки на СГФД автоматично ще доведе до по-стриктно регулаторно разглеждане (и значително повече документация). Резултатът от това е, че много финансови институции няма да провеждат стопанска дейност с партньори, базирани в Несътрудничеща страна или територия. Още 8 държави са били добавени в Черния списък през 2001 г., но оттогава засилените опити за съгласуваност са означавали липса на повече добавяни в списъка страни и спад в използването на Черния списък. Към момента на изготвяне на тази глава нямаше държави, които скоро да са включени в Черния списък, освен че трябва да се отбележи отстраняването на Мианмар от списъка през 2006 г.

Взаимният процес на оценяване е ключова част от работата и на СГФД, и на регионалните органи, подобни на СГФД. Чрез този процес СГФД наблюдава изпълнението на *40+9-те Препоръки* от юрисдикциите на членуващите държави и оценява цялостната ефективност на системите им за БПП/CFT. Всяка юрисдикция на държава-членка се проучва на свой ред от СГФД или в някои случаи от МВФ заедно с финалния доклад, приет от СГФД. Целта на тези оценки е да се прецени дали необходимите закони, разпоредби и други мерки, изисквани по новите стандарти, са в сила, дали е било налице цялостно и правилно прилагане на всички необходими мерки и дали установената система е ефективна. Докладите на СГФД за взаимни оценки са достъпни до всички членове и наблюдатели, обсъждат се на открити пленарни заседания в СГФД и след като се одобрят, се публикуват на уебстраницата на СГФД. *Ръководството за БПП/БФТ за държави и оценители 2007* предоставя инструкции и насоки за всички държави и органи, които правят такива оценки.

8.2.1. Съвет на Европа

Съветът на Европа е приел *Конвенцията на Съвета на Европа относно изпиране, претърсване, изземване и конфискация на придобитото от престъпление (Конвенцията от Страсбург)* (ETS 141) през 1990 г. Конвенцията цели да улесни международното сътрудничество и взаимопомощта при разследването на престъпления и проследяването, изземването и конфискуването на облагите от престъпление, като предоставя известна ефективност и сътрудничество между държавите-членки на Съвета на Европа, дори при липса на пълна законодателна хармонизация. Тя е била ратифицирана от всичките 48 членки на Съвета на Европа, а също така е отворена за държави, нечленуващи в Съвета на Европа, една от които – Австралия, е ратифицирала Конвенцията.

Конвенцията беше актуализирана и разширена през 2005 г. с приемането на *Конвенцията на Съвета на Европа за пране на пари, претърсване, изземване и конфискация на придобитото от престъпление и за финансиране на тероризма* (CETS 198). Това покрива превенцията и контрола и на прането на пари, и на финансирането на тероризма и включва механизъм за осигуряване на правилното прилагане на нейните разпоредби от страните.

През 1997 г. е основан Комитетът на Съвета на Европа по оценка на мерките срещу изпиране на пари (MONEYVAL), който разглежда мерките за борба с прането на пари и за борба с финансирането на тероризма в държавите-членки на Съвета на Европа (и в държавите, кандидатстващи за присъединяване към условията), които не са членове на Специалната група за финансови действия (СГФД). Държавите-членки на Съвета на Европа, които членуват в MONEYVAL, но впоследствие са станали членки на СГФД, могат да запазят пълноправното си членство в MONEYVAL (например, Руската федерация). Той оценява дали мерките, предприети от членките са в съответствие с всички приложими международни стандарти в правните, финансовите и изпълнителните сектори чрез процес на взаимни оценки на базата на преглед от останалите членки. Неговите доклади предлагат подробни препоръки за начините за подобряване на ефективността на вътрешните режими за борба с прането на пари и финансирането на терористи и възможностите на държавите да предоставят международно сътрудничество в тези области.

Настоящи членки по Конвенцията са Албания, Грузия, Румъния, Андора, Унгария, Руската федерация (също член на СГФД), Армения, Латвия, Сан Марино, Азербайджан, Лихтенщайн, Сърбия, Босна и Херцеговина, Литва, Словакия, България, Молдова, Словения, Хърватска, Малта, Македония, Кипър, Монако, Украйна, Чехия, Черна гора, Естония и Полша. През януари

2006г., на Израел е бил даден статут на активен наблюдател към MONEYVAL, което му дава възможност да участва в оценителния процес. Настоящият председател е г-н Васил Киров от България. Последната оценка на България, в Третия кръг на оценяване, е била проведена през април 2007 г., а Докладът е бил предаден през април 2008г. Последната оценка на Румъния, в Третия кръг на оценяване, е била проведена през май 2007г., а Докладът е бил предаден през юли 2008 г. (виж по-долу)

8.2.2. Европейски съюз

ЕС е приел три директиви относно прането на пари, последната от които е била издадена през октомври 2005г. ЕС клони към приемането на 40-те препоръки на СГФД, като най-новата директива на ЕС гласи, че „действията на Общността трябва да продължават да бъдат специално съобразени с Препоръките на Специалната група за финансови действия" и че насоките на ЕС трябва да са в съответствие с тези стандарти.

Първоначалната *Директива на Съвета относно превенцията на използването на финансовата система за целите на прането на пари* (91/308/ЕЕС) на ЕС е предоставила на държавите-членки основата за превенция на престъпното вкарване на парични средства във финансовата система. Директивата дефинира понятията за кредитна институция, финансова институция и пране на пари и задължава държавите-членки да гарантират, че прането на пари е забранено и че кредитните и финансовите институции (включително '*bureaux de change*') ще изискват идентификация от своите клиенти посредством доказателствен документ, освен в случаите, когато клиентът не е също кредитна или финансова институция. Изискването за идентификация е важало, когато една транзакция или няколко свързани транзакции надвишават ECU 15 000 или когато кредитните или финансовите институции заподозрят пране на пари (дори в случаите, когато транзакцията е под този праг).

От кредитните и финансовите институции също се е изисквало:

- да пазят копие от справките за изискваните доказателствени документи, в продължение на поне пет години след като са приключили взаимоотношенията им с клиента, както и доказателствени документи и справка за транзакциите в продължение на поне пет години след извършването на транзакциите;
- да не разкриват, че на властите е подавана информация или че се е провеждало разследване. На кредитните и финансовите институции е бил даден имунитет от отговорност за случаите, в които разкриването им на информация пред властите е било за законосъобразна цел;
- да информират властите, отговорни за борбата с прането на при, ако открият факти, които могат да съставляват доказателство за пране на пари;
- да установят процедури за вътрешен контрол и комуникация, с цел да предотвратят и избегнат операции, свързани с пране на пари, и да вземат подходящи мерки за информираност на техните служители относно разпоредбите, съдържащи се в директивата.

Втората *Директива на Европейския парламент и на Съвета за изменение и допълнение на Директива 91/308/ЕЕС на Съвета относно превенцията на използването на финансовата система за целите на прането на пари* **(**2001/97/ЕС) на ЕС е увеличила броя на престъпленията, към които се прилагат разпоредбите, и е разширила обхвата на професиите, които трябва да ги

съблюдават, включвайки адвокати, одитори, счетоводители, нотариуси, управители на казина и агенти по недвижими имоти. Тя също е разрешила учредяването на екипи за финансово разследване във всяка държава-членка, за която се готвят доклади за подозрителни транзакции (ДПТ).

Третата *Директива на Съвета относно превенцията на използването на финансовата система за целите на прането на пари и за финансиране на тероризма* (2005/60/ЕС) е отменила ефективно първата и втората директива.

Съгласно Директивата прането на пари, осъществявано на международно ниво, включва:

- преобразуване или прехвърляне на имущество, придобито от престъпна дейност и от участие в такава дейност, с цел укриване или прикриване на неговия незаконен произход;
- подпомагане на лице, въвлечено в извършването на така дейност, да избегне правните последици от своите действия;
- укриването или прикриването на истинския характер, произход, местонахождение, разпореждане, прехвърляне, права или собственост върху това имущество;
- придобиването, притежаването или използването на имущество, със знанието, че по време на получаването, това имущество е било придобито от криминална дейност.

Изисква се знание, че имуществото е придобито от криминална дейност. Намерението, знанието или целта могат да бъдат заключени от обективни фактически обстоятелства. Директивата, също така, криминализира участие в сдружавания с цел извършване, опити да се извърши и подпомогне, подстрекателство за, съветване за и улесняване на извършването на което и да било от гореспоменатите деяния. Прането на пари трябва да се счита за такова дори в случаите, когато криминалните дейности, причинили изпирането на имуществото, са били извършени на територията на друга държава-членка на ЕС или на територията на държава, която не е членка на ЕС.

Под „финансиране на тероризма" в Директивата се разбира предоставянето или събирането на средства по всякакви начини, с намерението те да бъдат използвани или със знанието, че те ще бъдат използвани, изцяло или частично, за провеждането на терористични атаки, включително вземане на заложници, изготвяне на фалшиви административни документи, ръководене на терористична група и др.

Директивата (чл.2) важи за:

- кредитни институции;
- финансови институции;
- юридически или физически лица, упражняващи своите професионални дейности, включително одитори, външни счетоводители данъчни консултанти; нотариуси и други независими юристи, действащи за или подпомагащи планирането и изпълнението на транзакции за клиенти, например:
    - купуване и продаване на недвижимо имущество или бизнес обекти;
    - управление на пари, ценни книжа или други активи на клиентите;
    - откриване или управление на банкови, спестовни или гаранционни сметки;
    - организиране на предоставянето на вноски, необходими за създаването, функционирането и управлението на компании;

- създаването, функционирането и управлението на тръстове, компании и подобни структури;

- тръстове или компании, предоставящи услуги, които още не са покрити от първите две точки;
- брокери на недвижими имоти;
- физически или юридически лица, търгуващи със стоки, където плащанията се правят в брой, в размер на EUR 15 000 или повече, независимо дали транзакцията се извършва чрез една операция или чрез няколко операции, които изглеждат свързани;
- казина.

От лицата, изброени в чл.2., се изисква да приложат мерки за проверка на правния статут на клиента в следните случаи:

- когато установяват бизнес взаимоотношения;
- когато се извършват извънредни транзакции, възлизащи на EUR 15 000 или повече;
- когато има съмнения за пране на пари или финансиране на тероризъм, независимо от това дали лицето е освободено от задължения или дали е надвишен прага;
- когато има съмнения относно достоверността или адекватността на придобитите по-рано идентификационни данни на клиента.

Тези мерки за проверка на правния статут включват:

- идентифициране на клиента и проверка на неговата самоличност;
- получаване на информация за целта и желаното естество на бизнес отношенията; и
- когато е необходимо, идентифициране и проверка на самоличността на получателя и т.н.

Степента на изискваната проверка се определя от включения обект на чувствителна към риска основа в зависимост от типа клиент, бизнес отношенията и т.н. и може да се призоват и трети страни да изпълнят тези изисквания. При определени обстоятелства Директивата позволява по-малка или по-опростена проверка.

В случаите, когато има голям риск от пране на пари или финансиране на тероризъм, от субектите по чл. 2 се изисква да направят по-подробна проверка. Тя включва допълнителни мерки за проверка или удостоверяване на приложените документи, например:

- ако клиентът не е присъствал физически за целите на идентификацията;
- по отношение на трансгранични отношения с ответни институции от страни, които не са членки на ЕС;
- да позволи оценяване от страна на контролиращи органи на борбата с прането на пари и финансирането на тероризма към институции на трети страни и др.

Освен гореспоменатите условия, съществува споразумение кредитните и другите финансови институции да не поддържат анонимни сметки или анонимни банкови книжки.

От всяка държава-членка се изисква да създаде и да предостави адекватни ресурси за национално Звено за финансово разузнаване (ЗФР), което трябва да има необходимите

правомощия за достъп до финансовата, административната и съдебната информация, от която има нужда. Националното Звено за финансово разузнаване (ЗФР) отговаря за получаването, изискването, анализирането и разпространяването до компетентните органи и разгласяването на информация, която засяга потенциално пране на пари или потенциалното финансиране на тероризъм. Субектите по чл. 2 са длъжни да информират националното си ЗФР възможно най-скоро след като разберат, заподозрат или имат разумни основания да подозират, че се извършва, било е извършено или е направен опит за извършване на пране на пари или финансиране на тероризъм. По искане на ЗФР те трябва да представят цялата необходима информация, изискана от законодателството. В случаите, когато има подозрения за пране на пари или за финансиране на тероризъм, от субектите по чл. 2 се изисква да се въздържат от извършването на транзакции, докато не уведомят ЗФР за това. Държавите-членки имат свобода на действие дали да изискват от независимите юристи, нотариусите, одиторите, външните счетоводители и данъчните консултанти да информират националните ЗФР, ако получат информация, за която мислят, че свидетелства за извършване на или опит за пране на пари или финансиране на тероризъм, докато предоставят правна консултация или докато трае съдебния процес.

Фактът, че информацията е била предадена до ЗФР, може да не бъде разкриван на клиента или да други трети лица освен за целите на съдебното изпълнение. Субектите по чл. 2 трябва да съхраняват документите и придружаващите ги други доказателства поне пет години след края на бизнес отношенията или след провеждане на транзакцията. От тях също така се очаква да въведат подходящи мерки и процедури за проверка на клиента, за докладване на информацията, съхраняване на документите и т.н. и да гарантират, че съответните служители познават ефективните разпоредби.

От държавите-членки се изисква да съгласуваност законодателството си с разпоредбите на Директивата. В случаите, в които няма съответствие с приетите национални разпоредби, трябва да е възможно въпросните субекти по чл. 2 да бъдат държани отговорни за тези правонарушения. Наказанията трябва да са ефективни, пропорционални и разубеждаващи. От държавите-членки беше изискано да приведат в сила необходимото национално законодателство, за да са в съответствие с Директивата от 15 декември 2007 г.

8.3. Приложение на БПП/БФТ в електронна среда

Очевидно е, че повишеното внимание към мерките по проверка на клиента (ДДК или ОСК – Опознай Своя Клиент) е един от основните компоненти на една ефективна система за борба срещу прането на пари (БПП) и за борба срещу финансирането на тероризма (БФТ). Подобна проверка не означава единствено, че организацията първоначално идентифицира самоличността на клиента, а когато оценката на риска счита за необходимо, да се извършва проверка на тази самоличност, но означава също, че трябва да се изследват подробно всички транзакции, извършени в хода на бизнес отношенията, за да се гарантира, че направените транзакции съответстват на известния профил на клиента, и да се разреши наблюдение на профила на транзакциите на клиента и предприемане на действия при някакви отклонения от нормалното му състояние. Някои от първите компании, занимаващи се с електронни пари и електронна търговия са били или неспособни, или не са желаели да възприемат мерки за такава проверка; а някои нови компании, занимаващи се с електронна търговия, като например виртуалните светове, все още не са заели напълно с последствията от въвличането на своите клиенти в транзакции във

виртуалната среда, като например продажбата на виртуална собственост, които имат потенциала да доведат до истински финансови транзакции.

Като се вземе в предвид сравнително новото естество на електронните пари и електронна търговия, международното координиране на реакциите към рисковете за пране на пари по електронен път е сравнително недостатъчно. Това е довело до редица национални подходи, включително изпълнение на действията при пране на пари срещу операторите на *hawala* (Великобритания) и срещу дилъри на виртуални ценни метали за „извършване на нелицензирана дейност по парични транзакции" (САЩ). Понастоящем съществуват малко, ако изобщо има някакви, национални мерки за БПП/БФТ, занимаващи се специфично с електронната търговия. Спорно е, че всъщност такива специфични мерки са излишни при потенциалния обхват на съществуващите мерки за БПП/БФТ, особено в рамките на ЕС, където е в сила Третата Директива за БПП/БФТ. Едно от съществените притеснения е било, че компаниите, занимаващи се с електронни пари и електронна търговия, биха желали да разположат всичките си дейности или части от тях в международни и офшорни юрисдикции със слабо регулиране на БПП/БФТ, като по този начин им дава възможност да избегнат регулаторния контрол и да затруднят съдебното разследване. На практика, както може да се види от ефекта на Черния списък на СГФД, прекият и косвеният натиск срещу потенциално слаби юрисдикции и срещу самите компании, занимаващи се с електронни пари и електронна търговия, често води до намаляване на това безпокойство, при много такива компании (напр. гореспоменатите WebMoney), които активно търсят начин да демонстрират усилията си да бъдат в съответствие с международните стандарти за БПП/БФТ.

Докато сред компаниите, занимаващи се с електронни пари и електронна търговия, е имало определена съпротива относно приемането на мерки за БПП/БФТ, особено при положение, че те могат да ограничат обхвата на анонимните транзакции, които потенциално са полезен пазарен стимул за компаниите, занимаващи се с електронни пари, трябва да се отбележи, че съпротивата към засилената проверка на клиентите не е феномен, ограничен до електронните компании. Третата директива на ЕС относно БПП/БФТ е била много критикувана за налагане на по-тежък регулаторен товар върху малките финансови и нефинансови обекти отколкото рискът от значително пране на пари в действителност оправдава. Следователно не е необходимо подобна съпротива да означава, че електронните пари и електронните дейности са вътрешно противопоставени на мерките за БПП/БФТ, а по-скоро, че съществуват опасения, че един всеобщ международен подход към регулирането на БПП/БФТ, който не взема предвид разходите/печалбите от транзакциите с електронни пари, дори от дребните анонимни транзакции, може да бъде неподходящ за определени юрисдикции и пазарни ниши. Пример за това може бъде WebMoney, услуга за електронни пари, която е била развита за пазара в и около Русия, където достъпът до традиционните банкови услуги може понякога да бъде ограничен и кредитните и дебитните карти невинаги са приложима възможност за плащане. Тъй като WebMoney се е превърнал в по-широк международен феномен, изглежда, че някои аспекти от услугата са по-рисковани по отношение на прането на пари, заради което услугата е привлякла вниманието на органите по БПП, особено в САЩ. Реакцията на WebMoney е била да елиминира най-рисковите аспекти на своята услуга, но да запази някои рискови елементи при комбинирана оценка на риска и анализ на разходите и печалбите.

8.4. Добри практики

В идеалния случай, търговците на дребно (електронни и физически) и лицата, осъществяващи парични преводи, трябва да имат относително еднакви задължения относно БПП/БФТ. Целта на тези мерки при електронните услуги не може да е пълното изкореняване на прането на пари, тъй като това не е реалистична цел както за електронните, така и за физическите среди, а по-скоро електронните услуги да станат по-малко гостоприемна за действие област за извършителите на пране на пари.

Специфичните слаби области, които са отбелязани в националните оценки на физическите (offline) мерки за БПП/БФТ, включват:

- Недостатъчно внимание на транзакции със страни с повишен риск;
- Незадоволителна разкриваемост и анализ на необикновено големи или подозрителни в друго отношение транзакции;
- Незадоволителни системи за отчитане на подозрителни транзакции;
- Незадоволителни насоки за разкриване на подозрителни транзакции;
- Незадоволителни програми за БПП/БФТ във финансовите институции и търговските дружества, и недостатъчно пълномощия за съдействие с изпълнителните органи;
- Неуспех при възлагането на задължения на финансовите институции и търговските дружества за предприемане на разумни мерки за извличане на информация относно самоличността на клиентите;
- Липса на процедури за взаимно подпомагане (напр. воденето на архив и придобиването на доказателства при разследване и съдебно преследване на престъпления, свързани с прането на пари) по криминалните въпроси;
- Незадоволителни вътрешни политики, процедури, контрол, одит и обучителни програми;
- Невъзможност за незабавното докладване до националните Звена за финансови разследвания, ако дадени институции подозират, че средствата произлизат от престъпна дейност;
- Слаб международен обмен на информация относно подозрителни транзакции, както и относно замесените хора и дружества.

Има вероятност подобни слабости да бъдат открити в Интернет, където електронните търговци на дребно и лицата, извършващи парични преводи, имат сравнително по-малко опит с престъпленията, свързани с пране на пари, отколкото банките и другите финансови институции,

и често са имали недостатъчен стимул за дейности, като повишаване на информираността в сектора, добри практики в индустрията или национално регулиране, за да подобрят своите мерки за БПП/БФТ.

В своя доклад от 2008г., озаглавен *„Слабостите в търговските уебсайтове и платежните системи в Интернет по отношение на прането на пари и финансирането на тероризма”,* СГФД отбелязва четири ключови области, за които се смята, че могат да допринесат за справянето с рисковете от пране на пари при търговските уебсайтове и платежните системи в Интернет:

- По-добра осведоменост за рисковете от пране на пари: Всички замесени страни, включително субектите от частния сектор, традиционните финансови институции и правителствените органи, трябва да разбират общите и специфичните секторни/технологични рискове във връзка с прането на пари, възникнали при електронни търговски услуги и парични преводи. Без това разбиране:

  - електронните услуги и парични преводи могат да бъдат обект на ключови рискове и модели за пране на пари, които са били идентифицирани и каталогизирани във „физически (offline) сценарии”;

  - традиционните финансови институции могат да се провалят в ролята си при разкриването и наблюдението на подозрителни финансови транзакции във връзка с електронните услуги и паричните преводи;

  - всякакви регулаторни стратегии, предлагани от правителството, могат да доведат до риск от проваляне на дефинирането и изпълнението на целите на БПП/БФТ, подходящи за онлайн средата, и също така могат да навредят на развитието на този сектор.

  Развиването от страна на регулатори и търговски асоциации на индикатори за подозрителни финансови транзакции (червени флагове) и справочни материали за техниките, използвани при прането на пари или финансирането на тероризма (типологии), може да помогне за повишаване на информираността за рисковете, както и провеждането на обучителни програми и целенасочени дискусии за частния сектор.

- Сходни национални регулаторни стратегии и цели: Като се вземе предвид международния характер и разпространеност на Интернет, от голямо значение е правителствата да наложат подобни разпоредби, изискващи идентификация на клиентите, проверка на техния статус, поддържане на архив и отчитане на транзакциите, от доставчиците на Интернет разплащателни услуги по цял свят, за да се избегне изместване към страни със слабо или липсващо регулиране.

- Стимулиране на добрите практики в индустрията: Възможността за идентифициране и насърчаване на добрите практики в индустрията може да бъде:

- използвана за повишаване на международния стандарт чрез осигуряване на ясна цел за ниско рискови практики, като по този начин се позволява на банките, финансовите институции и други доставчици на електронни услуги да идентифицират и да не осъществяват тези електронни търговски услуги и парични преводи, които са в разрез с тези практики;
- важна част от обучителните програми и целенасочените дискусии за частния сектор.

- Продължаване и развитие на международното сътрудничество: Поради международния характер на Интернет и на дейностите на търговските уебсайтове, международното сътрудничество ще бъде ключов фактор в борбата срещу прането на пари. Държавите трябва да работят съвместно за идентифицирането на подходящи БПП/БФТ стратегии/разпоредби за търговските уебсайтове и платежните системи в Интернет и за изработването на ефективни мерки, ако съгласуването им се провали. Международното сътрудничество е необходимо и за гарантиране, че лицата, които работят под различни юрисдикции, не се оказват по подразбиране извън всякакъв регулаторен контрол. В случаите, в които има подозрения за пране на пари, държавите трябва да могат да осигурят бърз и ефикасен обмен на информация и да са създали подходящи процеси за взаимно подпомагане.

Тази област все още се развива и новите продукти на електронната търговия/електронните пари ще доведат до нови рискове. Следователно непрекъснато ще съществува нуждата от нови смекчаващи стратегии.

Таблица 2: Рискове за БПП/БФТ при електронните транзакции

Деяние във връзка с изпиране на пари	Проблем при електронните транзакции	Описание	Възможни решения
Разполагане	Анонимност на услугите	Някои електронни търговски/разплащателни услуги позволяват регистрирането и/или транзакциите да се извършват анонимно, например чрез електронна поща.	§ Да се изисква лицата, предоставящи електронните търговски услуги и парични преводи, да не поддържат анонимни сметки. § Да се изисква финансовите институции, занимаващи се с електронните търговски услуги и платежни преводи, които позволяват анонимни сметки, да третират тези транзакции като рискови или високо рискови. § Да се поставят ограничения на сумите, които могат да бъдат трансферирани към или от анонимни сметки, или за цялата сума, и/или за всяка отделна транзакции. Да се използват ограничения на дейността.
	Липса на визуален контакт между клиент и доставчик	Традиционните механизми за проверка, използвани от лицата, предоставящи офлайн търговски услуги и парични преводи, не са налични при електронни търговски услуги и парични преводи	§ Електронна проверка на самоличността (например електронни карти за самоличност), с цел подпомагане на доставчиците на електронни търговски услуги и парични преводи да намалят риска от пране на пари. § Да се изисква от доставчиците на електронни търговски услуги и парични преводи да наблюдават финансовите транзакции, да следят за и да предприемат мерки при отклонения в обичайна транзакционна дейност на

			клиентите. § Да се изисква от финансовите институции, занимаващи се с електронни търговски услуги и парични преводи, да третират подобни транзакции като високо рискови. § Да се напомня на финансовите институции, занимаващи се с електронни търговски услуги и парични преводи, да наблюдават за необичайни или непропорционални транзакции по отношение на техните собствени клиенти. § В случаите, когато електронни търговски услуги и парични преводи се осъществяват чрез финансова институция, да се използва процеса на директното таксуване, за да се потвърди самоличността на клиентите (напр. PayPal)
	Много регистрации/самоличности	Използването на много (и евентуално анонимни) регистрации при покупка или продажба на стоки може да създаде проблеми при прегледа, наблюдението и възстановяването на транзакции и парични потоци.	§ Да се изисква от доставчиците на електронни търговски услуги и парични преводи да не поддържат анонимни сметки. § Да се използва електронна проверка на самоличността, за да се намали възможността от създаване на много сметки. § Да се изисква от доставчиците на електронни търговски услуги и парични преводи да имат процеси за справяне с кражби на самоличност.
	Отдалечен достъп	Интернет услугите могат да бъдат използвани от всяка точка на света, напр. от Интернет клубове. Хората могат да се	§ Да се изисква от доставчиците на електронни търговски услуги и парични преводи да не поддържат анонимни

		свързват посредством уеб терминали, несвързани или нерегистрирани към техните профили.	сметки. § Да се използва електронна проверка на самоличността, за да се намали възможността от създаване на много сметки. § Да се изисква от доставчиците на електронни търговски услуги и парични преводи да имат процеси за справяне с кражби на самоличност.
	Анонимни методи за разплащане	Ако за кредитиране на електронни сметки се използват предплатени карти, чекове/карти за подаръци или суми в брой, произходът на средствата може да се проследи по-трудно.	§ Да се изисква доставчиците на електронни търговски услуги и парични преводи да не позволяват анонимни методи за разплащане. § Да се поставят ограничения на сумите, които могат да бъдат трансферирани към или от анонимни сметки, или за цялата сума, и/или за всяка отделна транзакции.
Наслояване	Скорост на транзакциите	Електронните транзакции между продавачи и купувачи се извършват много бързо – доставчиците на електронни търговски услуги и парични преводи може да имат много малко време за реакция при подозрително поведение.	§ Може изкуствено да се въведат закъснения, за да се позволи ръчна проверка на необичайни транзакции или на сметки със завишена употреба. § Да се извършва проверка в реално време на клиенти, техните дейности и транзакции. § Да се извършва пълен одит на търговските транзакции и плащания. § Да се използват ограничения на дейностите, напр. само определен брой транзакции на сметка на ден.
	Чуждестранни/многожество юрисдикции	Международният характер на транзакциите може да означава, че юрисдикцията, която регламентира електронни търговски услуги и парични преводи, може да не е компетентна да разследва и да завежда дела	§ Да се изисква финансовите институции, занимаващи се с електронни търговски услуги и парични преводи, които позволяват анонимни сметки, да третират тези транзакции

		срещу прането на пари. Допълнително могат да възникнат ситуации, когато нито един държавен орган няма ясната отговорност да регулира и наблюдава дейностите.	като рискови или високо рискови. § Да се окаже натиск върху държавите, които не са хармонизили законодателствата си, посредством СГФД и нейните регионални групи и да се работи за хармонизирането на БПП/БФТ правилата по *40+9-те Препоръки*, за да се намалят проблемите, попадащи под обхвата на чуждестранни юрисдикции.
	Обем и размер на плащанията	Големият брой транзакции и различните суми по всяка транзакция правят още по-трудно за доставчиците на електронни търговски услуги и парични преводи да дефинират критерии за наблюдение и проверка на транзакции.	§ Да се извършва автоматично наблюдение чрез рискови модели, създадени за засичане на незаконни дейности, необичайни транзакции и мащабни дейности, на базата на съществуваща информация, например получена от клиенти (самоличност, адрес, електронна поща, използван IP адрес), от вътрешни източници (предишни транзакции, страна, където се намира имуществото, местоживеене на клиента), от външни източници (страни, рискови за определени форми на пране на пари/финансиране на тероризъм).
	Ограничена човешка намеса	Личното взаимодействие, често асоциирано с офлайн транзакциите, което е ключова част от водещата мярка за разкриването на пране на пари „опознай своя клиент”, не е достъпно и трябва да се замени с механизми за разкриване от второ ниво.	§ Да се извършва автоматично наблюдение чрез рискови модели, създадени за засичане на незаконни действия, необичайни транзакции и мащабни дейности, на базата на съществуваща информация
	Неадекватни или липсващи технически решения за одитиране, поддържане на	Осигуряването на сложни механизми за разкриване на престъпления от второ ниво често пъти не е приоритет при	§ Да се забрани на финансовите институции, които не покриват минималните изисквания за

	архив или докладване на подозрителни транзакции	осъществяване на електронни търговски услуги и парични преводи особено при по-дребните услуги. Дори там, където се използват автоматични системи, те може да се използват ограничено при разкриването на сложни схеми за пране на пари.	автоматично наблюдение във връзка с БПП/БФТ, да се занимават с електронни търговски услуги и парични преводи. § Да се изисква от всяка финансова институция, занимаваща се с електронни търговски услуги и парични преводи, да оценява риска във връзка с БПП/БФТ от тази дейност. § Да се поставят ограничения на сумите, които могат да бъдат трансферирани към или от сметка към електронни търговски услуги и парични преводи с ограничен капацитет за наблюдение.
Интегриране	Възможност за закупуване на скъпи стоки	Възможно е да се закупят стоки на висока цена, ценни метали, недвижимо имущество или ценни книжа от търговски уебсайтове чрез Интернет система за разплащане.	§ Да се изисква всички транзакции на висока стойност, направени чрез Интернет система за разплащане, да бъдат маркирани като високо рискови. § Да се изисква всички транзакции на висока стойност, направени чрез Интернет система за разплащане, да се маркират като високо рискови, ако клиентът купува за първи път. § Да се изисква всички транзакции на висока стойност, направени чрез Интернет система за разплащане, да се маркират като високо рискови, ако съответната транзакция е необичайна, или заедно с други доказателства се вмества в модел за пране на пари/финансиране на тероризъм.
	Анонимни методи за разплащане	Ако предплатени карти, чекове/карти за подаръци могат да бъдат закупени, или суми в брой могат да бъдат получавани от електронни сметки (напр. изтегляне от	§ Да се изисква доставчиците на електронни търговски услуги и парични преводи да не позволяват анонимни методи за разплащане.

		банкомати), дестинацията на средствата може да се проследи много по-трудно.	§ Да се поставят ограничения на сумите, които могат да бъдат трансферирани от една сметка анонимно, или за цялата сума, и/или за всяка отделна транзакции.

8.5. Кратко ръководство за *40-те Препоръки* на СГФД

8.5.1. Правни системи (съгласно Конвенциите на ООН)

1. Правните системи трябва да определят широк обсег на правонарушения, свързани с пране на пари, като криминализират прането на пари, свързано със всички сериозни правонарушения, и като обхванат поне посочения обсег от правонарушения.

2. Правните системи трябва да установяват стандарти за доказване на правонарушения, свързани с прането на пари, и за разясняване на факта, че наказателната, гражданската и административната отговорност ще важи за лицата.

3. Всяка страна трябва да има орган, който да конфискува незаконните средства и да прилага временни мерки, като замразяване на средства или изземване, с цел борба с правонарушенията, свързани с прането на пари.

8.5.2. Превантивни мерки (да се предприемат от финансови институции и нефинансови субекти)

4. Законите за защита на личните данни не трябва да са пречка за прилагането на препоръките.

5. Финансовите институции и нефинансовите субекти трябва да имат задължението да провеждат проверка на клиентите, включително и идентифициране и проверка на тяхната самоличност.

6. Финансовите институции и нефинансовите субекти трябва да имат установени специални мерки за политически уязвими лица.

7. Финансовите институции и нефинансовите субекти трябва да имат установени специални мерки, които да играят ролята на съответно банкиране.

8. Финансовите институции и нефинансовите субекти трябва да имат установени мерки при заплахи от пране на пари от страна, идващи от създаването на новите технологии и от дейности, извършвани без личен контакт.

9. Финансовите институции и нефинансовите субекти трябва да разчитат на трети страни за идентификация на клиенти и за въведените дейности.

10. Финансовите институции и нефинансовите субекти трябва да се придържат към изискването за петгодишно съхраняване на данните.

11. Финансовите институции и нефинансовите субекти трябва да обръщат специално внимание на сложни и необичайно големи транзакции и на всички необичайни видове транзакции.

12. Идентификацията на клиентите трябва да се прилага при специално посочените нефинансови субекти и професии.

13. Финансовите институции и нефинансовите субекти трябва да имат задължението да докладват подозрителни транзакции на звената за финансово разследване.

14. Да се установи правната закрила на лицата, добросъвестно докладващи за подозренията си, както и забрани срещу издаване на информация.

15. Финансовите институции и нефинансовите субекти трябва да имат установени мерки за вътрешен контрол, хармонизиране и одит.

16. Изискванията за докладване и мониторинг на подозрителни дейности трябва да се прилагат при специално посочените нефинансови субекти и професии.

17. Всяка страна трябва да притежава ефективни, съразмерни и разубеждаващи санкции срещу правонарушения, свързани с прането на пари.

18. Всяка страна трябва да не позволява създаването на фиктивни банки.

19. Финансовите институции и нефинансовите субекти трябва да вземат предвид наблюдението на трансграничното пренасяне на пари в брой и да развият система за докладване на валутни транзакции над определена сума.

20. Финансовите институции и нефинансовите субекти трябва да вземат предвид прилагането на изискванията на СГФД към компании извън специално определените нефинансови субекти и професии.

21. Специално внимание трябва да бъде обърнато на високо рисковите държави.

22. Изискванията във връзка с БПП трябва да се прилагат за чуждестранните клонове и филиали.

23. Финансовите институции трябва да бъдат обект на адекватно регулиране, контрол и наблюдение.

24. Специално определените нефинансови субекти и професии да бъдат обект на адекватно регулиране, контрол и наблюдение.

25. Компетентните органи трябва да осигурят насоки за докладване, както и обратна връзка с цел ефективност.

8.5.3. Институционални и други мерки

26. Всяка страна трябва да има установено звено за финансови разследвания.

27. Всяка страна трябва да има определен изпълнителен орган за борба с прането на пари и финансирането на тероризма.

28. Изпълнителният орган трябва да притежава адекватни правомощия за разследване.

29. Регулаторните органи трябва да притежават адекватни правомощия да наблюдават и да осигуряват съгласуваност с изискванията на БПП/БФТ.

30. Компетентните органи трябва да притежават адекватни ресурси, интегритет и да са обучени за нуждите на БПП/БФТ.

31. Трябва да бъдат развити ефективни механизми за сътрудничество на местно ниво.

32. Институциите трябва да поддържат статистики за докладване, разследване, завеждане под отговорност и взаимно правно сътрудничество.

33. Институциите трябва да установят мерки за възпиране на незаконна употреба от страна на дружествата и навременна информация относно пълната собственост и контрол.

34. Институциите трябва да установят мерки за предотвратяване на незаконната употреба на правни споразумения (напр. тръстове), и да осигурят навременна информация относно завещатели, попечители и бенефициенти.

8.5.4. Международно сътрудничество

35. Всяка страна трябва да приеме Конвенцията от Виена (*Конвенцията на ООН за борбата срещу незаконния трафик на упойващи вещества и психотропни средства*, 1988), Конвенцията от Палермо (*Конвенцията на ООН срещу транснационалната организирана престъпност*, 2000), Конвенцията за борба срещу финансирането на тероризма и други международни конвенции.

36. Всяка страна трябва бързо да осигури взаимна правна помощ.

37. Всяка страна трябва да предоставя правна помощ въпреки липсата на взаимно криминализиране.

38. Всяка страна трябва да има правомощия за незабавно идентифициране, замразяване, изземване и конфискуване на имущество, придобито чрез средства от пране на пари и финансиране на тероризма.

39. Всяка страна трябва да признае прането на пари за обуславящо екстрадиция престъпление.

40. Всяка страна трябва да осигури широк спектър от възможности за международно сътрудничество.

8.6. Специални препоръки за борба с финансирането на тероризма

1. Да се ратифицират и изпълняват съответните конвенции и резолюции на ООН.

2. Да се криминализира финансирането на тероризма.

3. Да се изпълняват мерките по замразяване и конфискуване на активи, собственост на терористични организации или придобити вследствие на терористични действия.

4. Задължение за предоставяне на информация относно подозрителни транзакции, което важи при подозрения за финансиране на тероризма.

5. Да се осигури сътрудничество при воденето на съдебни процеси по делаза финансирането на тероризма.

6. Да се въведат мерки за спиране на неподходящо използване на услуги за трансфер на пари и ценни стоки.

7. Страните да бъдат призовани да изискват адекватна информация за автора на трансферите на средства и на свързаните с това съобщения.

8. Страните да бъдат призовани да преразгледат адекватността на законите във връзка с организациите с нестопанска цел, за да се предотвратят злоупотребите с терористични цели.

9. Да се създадат мерки за разкриване на физически трансграничен пренос на валута и ценни книжа.

От:
Оценка на финансовия сектор: Ръководство
http://www.financelearning.org/fsapbook/ch08.pdf

Таблица 3: Членове на СГФД

Аржентина	Франция	Япония	Русия
Австралия	Германия	Люксембург	Сингапур
Австрия	Гърция	Мексико	Южна Африка
Белгия	Съвет за сътрудничество на страните от Персийския залив	Холандия	Испания
Бразилия	Хонг Конг, Китай	Нова Зеландия	Швеция
Канада	Исландия	Норвегия	Швейцария
Дания	Ирландия	Китай	Турция
Европейската комисия	Франция	Япония	Великобритания
Финландия	Италия	Португалия	САЩ

Република Корея и Индия стават наблюдатели съответно на 27 юли 2006г. и 27 ноември 2006г., като понастоящем и двете работят в посока присъединяването им като членове на СГФД.

9. ВИСОКОТЕХНОЛОГИЧНИЯТ КИБЕРТЕРОРИЗЪМ: АТАКИ И СРЕДСТВА ЗА ПРОТИВОДЕЙСТВИЕ

9.1. Въведение

Последните новини, свързани с (предполагаемия) инцидент с надеждността в системата на Федералната авиационна администрация, който причини забавяне и отмяна на полети за период, по-голям от 24 часа, ни насочиха към важността на сигурност на критичната инфраструктура. Денинг 2000 дефинира термина „кибертероризъм" като „доближаване на тероризма и киберпространството". Обикновено под този термин се разбират незаконни атаки и заплахи за атаки срещу компютри, мрежи и информацията, съхранявана в тях, когато се прави с цел заплашване или принуждаване на правителство или негови членове за съдействие при постигане на политически или обществени цели. Освен това, за да се определи като кибертероризъм, една атака трябва да има като резултат насилие срещу лица или имущество, или поне да причинява достатъчно вреда, като поражда страх. Атаки, водещи до смърт или телесна повреда, експлозии, самолетни катастрофи, отравяне на водата или тежки икономически загуби могат да бъдат примери за това. Сериозни атаки срещу критичната инфраструктура могат да бъдат деяния на кибертероризъм в зависимост от тяхното въздействие. Атаки, които нарушават несъществени услуги или които са предимно скъпо струваща неприятност, не биха могли да се определят като кибертероризъм.

9.2. Нарастваща заплаха

Сюзън У. (Бренер, 2006) предлага своите собствени семантични и оперативни определения за кибертероризъм. Семантично Бренер е дефинирал „кибертероризъм" като „използването на компютърни технологии за осъществяването на терористични цели. Това е преследването на терористични планове чрез други средства, т.е. компютри вместо оръжия и самоделни експлозивни устройства (Improvised Explosive Devices)". Бренер прави разграничение между „кибертероризъм" с неговите идеологически цели, „киберпрестъпленията" с техните индивидуални цели (напр. пари, секс, отмъщение и т.н.) и „кибервойна" с нейните държавни цели (напр. политически, икономически и тактически). Разбира се, както Бренер отбелязва, тези разграничения бързо се размиват. Например, има деяния на спонсориран от държавата тероризъм и спонсорирани от държавата престъпления. Освен това, разграничението между „лични" цели и държавна дейност се размива, защото се базира на териториален суверенитет. Престъпленията обикновено се разглеждат като вътрешна заплаха, а войната е външна заплаха, като тероризмът се разглежда като едно от двете или и двете. Но компютрите подриват това разграничение, като правят територията несъществена при много от целите. Бренер цитира кибератаките от октомври 2006г. от страна на Народна република Китай, насочени към Министерството на търговията на САЩ. Естеството на атаката е все още неизвестно. Много експерти говорят за кибернетични престъпления, кибернетичен тероризъм, кибернетична война, като предлагат първични и вторични оперативни определения. Първичното оперативно определение, разиграно с понятието „Оръжия за масово унищожение" (ОМУ), разкрива връзката между понятието „кибертероризъм" с три различни типа ОМУ:

- Оръжия за масово унищожение *(weapons of mass destruction);*
- Оръжия за масово заблуждение *(weapons of mass distraction);*
- Оръжия за масово разрушение *(weapons of mass disruption).*

По отношение на „оръжията за масово унищожение" един продавач на решения за сигурност (*security vendor*) е бил справедливо обвинен заради употребата на такива хиперболични определения като „Електронен Пърл Харбър" и „Електронен 9/11", като се отбелязва, че е малко вероятно компютри да могат да предизвикат такова демобилизиращо

избиване като това, преживяно на 11 септември, и че такива определения поощряват едно погрешно разбиране как компютрите могат да бъдат използвани за осъществяване на терористични цели. Докато част от ефекта на 11 септември очевидно е бил електронен, също така следва да се отбележи, че широкоразпространеното вярване, че „кибертероризъм" е преувеличено понятие, целящо да разпространява „С.Н.С." (т.е. „страх, несигурност и съмнение"), е базирано на такова преувеличаване.

Понятието „оръжия за масово заблуждение" от друга страна се отнася до използването на грешна информация, за да се демобилизират гражданите. Като пример за това Пауър (2006) споделя един анекдот за фалшивия доклад за една надвиснала катастрофа (т.е. че е имало ядрено оръжие в куфар при масова транзитна система, обслужваща заливите на Сан Франциско). Според източника на Пауър, който е анонимен служител на правителството, била издадена заповед за евакуация на милиони хора.

Пауър отбелязва, че „кибертероризъм" може да бъде използван като „оръжие за масово заблуждение", за да се преувеличи или подчертае реалната атака, напр. чрез преувеличаване на въздействието на атаката или чрез погрешно идентифициране на целите.

Целите на „кибертероризма" като „оръжие за масово разрушение" биха били да демобилизира цивилното население и да създаде хаос, като атакува инфраструктурните компоненти, като например електрическата мрежа, финансовите системи, системата за контрол на въздушния трафик и/или транзитните системи.

Като пример от реалния живот би могло да е от полза да спомена въздействието на атаката Botnet върху една болница в Сиатъл. Атаката спря компютрите на отделението за вътрешни болести, вратите на операционната зала и пейджърите на докторите.

Вторичното оперативно определение на „кибертероризъм" го определя като „инструмент", напр. използването на Интернет за организационни и пропагандиращи дейности или дейности, свързани с набиране на средства, генериране на печалба или пране на пари. Но с това вторично оперативно определение възникват проблеми – много от дейностите (пропаганда, други комуникации, трансфер на средства, проучване) могат да бъдат законни.

9.3. Важността на осведомеността и образоваността в борбата с кибертероризма: преминаване отвъд шума и измамата

Както беше отбелязано преди, разпространителите на С.Н.С. са причинили много вреди на нашата кауза, така че ние наблягаме на това, че осведомеността и образоваността в областта на сигурността в кибернетичното пространство трябва да бъдат планирани така, че да ангажират, просвещават и да дават възможности на работната сила или на гражданите вместо да сеят страх сред тях или да налагат контрол върху тях.

Също така е наложително да се използват четири жизненоважни елемента при изготвянето на осведомителното и образователното съдържание: използване на интригуващи теми, позоваване на достоверни източници, представяне на правдоподобни сценарии и, най-важното – връзка с настоящите събития и с личния живот на хората.

Подчертавайки темите за достоверността и правдоподобността, ние задаваме въпроса „Къде се намира кибертероризмът в скалата на рисковете и заплахите?" Защото перспективата и пропорционалността са ключови при осведомяването и образоваността в областта на кибертероризма. Перспективата и пропорционалността изразяват достоверност.

Според виждането на автора на тази глава съществува „противоречиво сходство", криза на сигурността на 21 век, в която кибертероризмът не е нищо повече от подразделение на тероризма и на кибернетичните престъпления и следователно се подрежда по средата и съответно към края в дългия списък на сериозни рискове и заплахи:

- Глобално затопляне
- Разпространение на ядрено оръжие
- Пандемия и други здравни кризи
- Природни бедствия

- Тероризъм (с „кибертероризъм" като подразделение)
- Провалили се държави
- Проблеми на устойчивостта (напр. енергия, вода, пренаселеност)
- Организирана престъпност (напр. трафик на хора, търговия с наркотици, фалшифициране)
- Кибернетични престъпления (с „кибертероризъм" като подразделение)

За да продължим да наблягаме на темите за достоверността и правдоподобността, обърнете внимание на полезните паралели между „птичи грип" и „кибертероризъм". Въпреки че птичият грип е бил регистриран в почти 50 страни от 2003 г., с него са заразени по-малко от 300 души, а са починали по-малко от 200.

И все пак, милиарди долари се харчат за подготовка за сериозна пандемия на птичи грип. Защо? Защото два от трите фактора, създаващи пандемия, са вече налице и ако третият фактор (предаване от човек на човек) се задейства, милиони хора може да умрат и регионалните и световната икономики може да загубят стотици милиарди долари.

Но дори и птичият грип да не стане пандемия, планирането, обученията и подготовката ще спомогнат при справянето с каквито и да е здравни кризи, които неизбежно ни сполетяват. Рискът от кибертероризъм трябва да се разглежда и към него да се подхожда по подобен начин. Не можем да си позволим да допускаме, че няма да се случи, защото досега не се е случвало (или вероятно просто защото не е обявено, че вече се е случило).

По отношение на въпросите „Кой?" и „Защо?" при кибертероризма анализът на нашето разузнаване предлага едно по-различно виждане за списъка с обичайните (и необичайните) заподозрени:

- Последователи на Джихад, имащи за цел да нанасят съкрушителни икономически и психологически удари;
- Нации-държави[197], т.е. хегемони и авторитарни държави (*rogues*), имащи за цел да объркват и да омаломощават противниците;
- Поклонници на култове и индивидуалисти, имащи за цел да ускорят идването на апокалипсиса и да сринат обществения ред;
- Престъпни елементи, имащи за цел да изнудват и да прилагат репресивни мерки;
- Корпоративни врагове, имащи за цел да пречат на конкурентите си;
- Политически врагове, имащи за цел да подриват демократичните институции.

Въпреки че като цяло общоприетото мнение свързва кибертероризма с последователите на Джихад или нациите-държави, според автора на тази глава, много по-вероятно е светът да претърпи деяния на кибертероризъм, извършени от поклонници на култове и индивидуалисти, които се стремят да наложат странните си виждания за света.

9.4. Създаване на паралел между кибертероризма и „осезаемия" тероризъм: „екскурс" върху главните събития от последните 30 години

Култът Аум Шинрикио (към Върховната истина), който беше отговорен за атаката със зарин в Токийското метро през 1995 г., и Теодор Качински (известен също като „Юнабомбъра"[198]), който беше отговорен за шестнайсет бомбени атаки чрез писма за периода от 1978 г. до 1995 г., илюстрират тези заплахи.

В своето брилянтно изследване „Култът в края на света" Дейвид Е. Каплин анализира обхвата и тревожните последици от инцидента с Аум Шинрикио:

"През 1984 г. гуруто Шоко Асахара имал школа по йога с една зала, една шепа последователи и една мечта: да доминира света. Едно десетилетие по-късно култът Аум към

[197] *„Nation-states"* или *„супер-сили". Б.пр.*
[198] Т.нар. *"Unibomber"*

Върховната истина може да се похвали с 40 000 последователи в шест страни и световна мрежа, която му осигурява високотехнологични лазери, лабораторно оборудване и оръжия. Историята на Аум се пренася от гъсто населените градове на Япония към планински усамотени места, където някога са се били самураи, а след това в чужбина – към Манхатън и Силиконовата долина, Бон и австралийската пустош, и най-накрая към Русия. Именно там, сред опасните останки от Съветската империя, култът намери готови доставчици на военни съоръжения, подготовка и, много вероятно, атомна бомба."

Но вероятно най-невероятният обрат на сюжета е, че историята не завърши със залавянето на Шоко Асахара и на други лидери на култа.

През 2000 г. *BBC* съобщи: "Агенцията по отбраната в Япония отложи стартирането на нова компютърна система, след като откри, че тя използва софтуер, разработен от членове на култа Аум Шинрикио. Агенцията по отбраната е била само една от 90 правителствени организации и частни компании, които неволно са поръчали софтуер, произведен от култа." (*BBC, 01/03/2000*)

Дори през септември 2006 г. култът все още беше източник на тревога: "Японски служители на органите за сигурността нахлуха днес в 25 офиса на Култа към Страшния съд, стоящ зад атаките с невропаралитичен газ в токийското метро през 1995 г., след като неговият основател загуби и последното обжалване на смъртната си присъда. 'Откакто беше финализирана смъртната му присъда, се страхуваме, че последователите му може да планират нещо неправомерно,' каза говорителят на Разузнавателната агенция за обществена сигурност". (*The Australian, 16/09/2006*)

Точно както историята на Аум Шинрикио дава шокиращ пример за това какво може да направи един култ, целящ предизвикване на хаос, като използва кибертероризма като инструмент, забележителната история на Тед Качински, Юнабомбъра, илюстрира какво може да извърши сам един напълно умствено разстроен индивид. Работейки без съучастници и живеейки в усамотение в една колиба в планината Монтана, без телефон, автомобил, електричество и течаща вода, Качински се изплъзваше от националното издирване на ФБР в продължение на много години. През цялото време той никога не се издаде, дори като изработваше безупречни бомби в писма и ги доставяше, незабелязан, за да извърши многобройни убийства и опити за убийство. До момента, в който не изпрати своя „Манифест на Юнабомбъра" до вестниците за публикация, и на Давид Качински не му хрумна, че идеите и стилът на писане удивително приличат на тези на брат му Тед.

Най-честият въпрос, който си задаваха стотици анализатори, беше: „Защо го е направил?"

"Индустриалната революция и нейните последствия са бедствие за човешката раса… Следователно ние пропагандираме революция срещу индустриалната система. Тази революция може да използва или да не използва насилие; може да бъде внезапна или да бъде един сравнително плавен процес, обхващащ няколко десетилетия..." (*UNABOMBER Manifesto*)

Представете си какво може да направи един киберЮнабомбър, като използва кибертероризма, за да се цели в критична инфраструктура. Представете си колко дълго би могъл да се измъква от разпознаване и залавяне.

Авторът на тази глава предлага също толкова достоверно да погледнем и на това как деянията на кибертероризъм произхождат от елементи на организираната престъпност – или като преследване на печалба, или в усилието да се заплашат правителства и общества.

Разглеждането на този откъс от скорошни новини може също да е от полза:

"Киберизмамите все повече се извършват от престъпни организации, които искат да печелят от сложни уловки, а не от хакери, запалени по идеята да си създадат име онлайн, според щатския висш държавен служител Кристофър Пейнтър, заместник-началник в Отдела за компютърни престъпления и интелектуална собственост към Министерството на правосъдието.

ФБР оценява, че всички видове компютърни престъпления в САЩ струват на индустрията около $400 милиарда, докато във Великобритания Министерството на търговията и индустрията обяви, че компютърните престъпления са се увеличили с 50% през последните две години.

Нарастваща тревожност предизвиква фактът, че киберизмамниците могат да се целят в службите за спешни случаи с цел изнудване или че терористите може да се изкушат да атакуват критични комунални мрежи, като водоснабдителна или електрическа мрежа. Пейнтър казва, че наскоро е имало случай в САЩ, в който двама млади хакери по невнимание изключили всички светлини на местното летище." (*Reuters 15/09/2006*)

Други аспекти на изложението са отразени в анализа и препоръките от две скорошни статии в рубриката „Война и мир в кибернетичното пространство" на *Elservier Sience*, „Десет години в пустошта. Ретроспекция. Част 2: Киберсигурност = Национална сигурност" и „Казус: Един смел нов подход към информираността и образоваността и как той достигна позорна съдба".

9.5. Настоящи и бъдещи технически тенденции

Едно от основните правила за информационна сигурност, прилагано към защитата на критичната инфраструктура и изпълнение на мерките срещу компютърните престъпления, е недостатъците на сигурността да бъдат отговорно разкривани. Това ще помогне на собствениците на системи да отстранят възможните проблеми. Една от най-важните конференции на света по практическа сигурност (BlackHat.com) е демонстрацията на това колко важно е разкриването на сигурността и колко много може да се експлоатира от „конвенционалните" хакери и кибертероризма.

На последната конференция Blackhat в Лас Вегас двама изследователи на сигурността демонстрираха нова техника за тайно прекъсване на Интернет трафика в степен, която по-рано беше смятана за недостъпна за всеки извън разузнавателните служби като Националната агенция по сигурността.

Тактиката използва т.нар. Интернет протокол - BGP (*Border Gateway Protocol*), за да позволи на атакуващия да наблюдава тайно некриптиран Интернет трафик навсякъде по света и дори да го модифицира, преди да достигне дестинацията си.

Демонстрацията е най-новата атака, която подчертава фундаменталните слабости на сигурността при някои от най-съществените Интернет протоколи. Тези протоколи бяха широко разработвани през 70-те години на 20 век, като се допускаше, че всеки възел от зараждащата се тогава мрежа ще е надежден. През юли беше припомнено на света колко налудничаво е това допускане, когато изследователят Дан Каминski разкри сериозна уязвимост на DNS системата. Експертите твърдят, че новата демонстрация цели потенциално по-голяма слабост. Това е една от най-опасните и големи недостатъци на Интернет сигурността, които някога е имало. Държавите трябва да съзнават тези проблеми и да ги решават, преди да е станало твърде късно.

9.6. Ролята на кибернетичните разследвания в борбата с кибернетичните престъпления и кибертероризма

Ще дискутираме компютърната експертиза в следващата глава на този доклад. Въпреки това е важно да се помни, че кибернетичните разследванията са фундаментална част от дискутираната материя. В същото време кибертерористите познават възможностите на кибернетичните разследвания и се опитват да ги заобиколят.

Днешните електронни следователи се сблъскват с няколко основни проблема, включващи:

- Анти-експертиза;
- Липса на организация и обмяна на информация;

- Различни следователски и правни стандарти;
- Липса на необходимите умения.

"Анти-експертизата" включва различни методи, които влияят отрицателно на съществуването, количеството и/или качеството на доказателствата от местопрестъплението или които правят изследването и анализа на такива доказателства или по-трудно, или невъзможно за провеждане.

Примерите от реалния живот включват документирани атаки срещу инструменти за медиен анализ (напр. FTK, EnCase, iLook, WinHex, TCT, Sleuthkit и др.) и инструменти за анализ на трафика.

„Трансмогрифията" е пример за инструмент, който осуетява медийния анализ; той разбива файловите сигнатури на EnCase, като ви позволява да маскирате и да разкривате файловете си като какъвто и да е тип файл.

Onion рутерът е пример за инструмент, който ви позволява да избегнете анализ на трафика.

Целта на *onion* рутирането е да стане напълно невъзможно за трети страни да извършват анализ на трафика.

Целта се постига, като при мрежите се прилагат криптографски техники. По този начин пакетите, преминаващи по веригата от *onion* рутери се появяват като анонимни.

На практика има една група *onion* рутери, разпространени в обществената мрежа, всеки от които има задачата да криптира връзките на контактите и да работят последователно като прокси.

Терористите и престъпниците използват *onion* рутирането по няколко начина:

- За обмен на файлове: *onion* рутирането дава възможност на потребителите да прикриват своето местоположение, като в същото време предлагат разнообразни услуги, като например web публикуване или сървър за изпращане на съобщения по чата, а също и сигурна равноправна мрежа (*peer-to-peer network*). (Този метод се използва за обмен на детска порнография.)
- За управление на терористични операции: използвайки „точки за рандеву" в *onion* рутерите, други потребители на *onion* рутерите могат да се включват към скрити услуги, без да разпознават мрежите си.
- „Слепи" групи: по този начин група хакери, например, може да нахлуе в една система и да я остави отворена за друга група, терористична клетка, която не ги познава.

На 11 септември 2006 г. германската полиция претърси седем доставчика на Интернет услуги и лица. Въпреки че беше потвърдено, че шест компютъра (възли на *onion* рутери) са били конфискувани, поддръжниците на Германските граждански свободи твърдят, че десетки (ако не и стотици) други компютри също са били конфискувани. Системите, иззети при тази хайка, не са били конфискувани заради работата им като анонимни проксисървъри, използващи мрежов протокол за *onion* рутиране. Предпоставката за конфискуването била, че сървърите се появили в сървър лог на уебсайт за детска порнография. (*Wikinews*)

Но както споменахме, има някои други предизвикателства, с които се сблъскват днешните електронни следователи.

Липсата на организация и информационен обмен може да бъде преодоляна чрез международни споразумения, следователски групи и професионални сдружения.

Разликите в разследването и законовите процедури могат да бъдат преодолени чрез искания за коментар (RFCs), работни срещи за проучване на компютърната експертиза (DFRWs) и въвеждане на стандарти.

Липсата на необходимите умения може да бъде преодоляна чрез обучения и виртуални общности.

Skype и други "Сигурни VOIP" представят някои предизвикателства, които експертите по законно прихващане на информация все още се борят да преодолеят. По

същия начин стаганографията, виртуалните машини и скритите канали представят предизвикателства, за които технологичните доставчици все още не са произвели ефикасни детектори.

9.7. Важността на про-активните решения

Какво трябва да направят правителствата на източноевропейските държави по отношение на компютърна експертиза? Да сформират свои екипи за реагиране при инциденти и да създадат национални лаборатории по компютърна експертиза, като бъдат обучавани и консултирани от експерти от други страни, членуващи в НАТО и ЕС. Да започнат да работят върху методики, а след това върху инструменти и техники. Сформирането на национален екип за реагиране при инциденти трябва да е задължително и трябва да разполага с лаборатория за експертиза. Холандия предлага отличен пример за това.

Какво трябва да правят телекомуникационните и другите инфраструктурни компании в новите държави? Техният приоритет номер едно трябва да бъде незабавното инициране на изграждането на логинг инфраструктура. Тя трябва да бъде свързана, но не и ограничена до логинг в мрежи, логинг при свързване, приложения при бази данни и логинг при споделяне на информация (срещу вътрешни злоупотреби). Също така, те трябва да работят върху изграждането на система за реагиране на инциденти, съставена от процеси, процедури и технологии. Също така е много важно функциите по сигурността да бъдат отделени от вътрешния одит.

Какво трябва да правят съдиите и магистратите? Авторът на тази глава вярва, че трябва да се поемат два различни (но съвместни) пътя. Първият е правна хармонизация, а вторият трябва да бъде ясна програма по обмен във връзка със сигурността и техническото разследване.

Правната хармонизация ясно се базира на ефективно признаване и прилагане на Конвенцията от Будапеща (бел. пр. *Конвенция за престъпления в кибернетичното пространство*, 2001 г.).

Конвенцията е първото международно споразумение относно престъпления, извършвани чрез Интернет и други компютърни мрежи, занимаваща се в частност с авторското право, компютърните измами, детската порнография и нарушенията на сигурността на мрежата. Тя съдържа също поредица от правомощия и процедури, като например тези при претърсването на компютърни мрежи и прихващане на информация.

Основната цел, изложена в Преамбюла, е създаването на обща криминална политика, целяща защита на обществото от кибернетичните престъпления, особено чрез приемане на подходящо законодателство и поощряване на международното сътрудничество.

Конвенцията цели предимно (1) хармонизиране на вътрешното наказателно материално право и свързаните с него разпоредби в областта на кибернетичните престъпления; (2) осигуряване на правомощия в областта на вътрешното наказателно процесуално право, необходими за разследването и воденето на дела за такива престъпления, както и за престъпления, извършени чрез компютърна система или доказателства, свързани с тях, които са в електронна форма; (3) установяване на бърз и ефикасен режим на международно сътрудничество.

Конвенцията дефинира следните престъпления: незаконен достъп, незаконно прихващане на информация, достъп и промяна на информацията, проникване в информационни системи, злоупотреба с устройства, компютърно фалшифициране, компютърни измами, престъпления, свързани с детска порнография, и престъпления, свързани с авторското право и сходните му права. Тя също регламентира такива процесуални правни въпроси като ускорено запазване на съхранявана информация, ускорено запазване и частичното разкриване на данни за трафика, реда за производство, търсене и осъществяване на достъп до компютърни данни, събиране на данни за трафика в реално време и

осъществяване на достъп до данни, свързани със съдържанието. Освен това, Конвенцията съдържа разпоредба за специален тип трансграничен достъп до съхраняваните компютърни данни, който не изисква разрешение (със съгласие или там където е публично достъпен), и осигурява изграждането на денонощна мрежа, осигуряваща бърза техническа помощ на подписалите я страни.

Конвенцията е резултат от четиригодишен труд на европейски и международни експерти. Тя бе изменена с Допълнителен протокол, чрез който всички публикации, съдържащи расистка или ксенофобска пропаганда, се обявяват за престъпления. Понастоящем, кибертероризмът също се изучава в рамките на Конвенцията.

Очевидно е, че от източноевропейските страни се изисква да прилагат документите, които са подписали, и ако все още не са подписали Конвенцията, трябва да го направят възможно най-скоро. От магистратите се изисква да изпълняват принципите, въведени от Конвенцията, като използват специализирани полицейски органи (ако има такива) и/или поддържащите такива инициативи.

Като бивш полицейски служител, който активно е работел върху борбата с кибернетичните престъпления и кибертероризма, авторът на тази глава също смята, че основен метод, използван за превенцията на кибертероризма, е споделянето на информацията от разследването. Най-напредналите полицейски и съдебни служби периодично изпращат информацията, събрана при активните разследвания или до която е достигнато чрез проучване, на следователите.

Кибернетичните програми са уникални по своето естество. Въпреки това, вземането на про-активни мерки за разследване с помощта на инструменти като *Honey Pots/Nets* и *Undercover Operations* увеличава възможностите ни да предотвратим кибертерористична атака. Щатското правителство, например, е стартирало следните инициативи за борба с кибертероризма: оперативни кибергрупи (*Cyber Task Forces*), публично-частни съюзи, Международна помощ за кибернетични разследвания, Мобилни екипи за кибер-помощ, Екипи за кибердействия, обучение на разследващите органи във връзка с кибернетичните престъпления, Център за кибернетични разследвания и Помощ при кибертактическо-аналитични казуси. Тези програми представляват стратегическа рамка и инструмент за програмно управление на всички служби, разследващи компютърни престъпления, в дадена страна.

Специализирана програма за кибернетични обучения е координирана с Лабораторните отдели за инженерни изследвания, обучителните звена, националните криминални центрове за служители, частния сектор, университетите и други, за да се предоставят обучения на правителствените служби, занимаващи се с този вид престъпления, оперативните групи (*Task Forces*), служители на международни правоохранителни органи и др.

В случай на кибертерористична атака полицията (и съответното съдебно звено) ще проведе интензивно разследване, за да определи източника, включително и мотива и целта на атаката. В електронната ера, събирането на такива данни може да се окаже изключително трудно. Компютърната индустрия също извършва дейности, свързани с базова сигурност, като например развиване на криптографски хардуер, който ще служи за филтриране на опитите за въвеждане на злонамерен код или за спиране на неоторизирана дейност. Продължителните проучвания в тези области ще послужат на държавите в тяхната борба с кибертероризма.

Последно, но не и по значение, са симулациите на инциденти и кибертероризъм. Изследователи към Тексаския университет в Сан Антонио, например, извършиха пробно тестване на способността на града да предотврати проникването на кибертерористи в компютърните системи на града.

Центърът за инфраструктурна сигурност към Тексаския университет в Сан Антонио е работил с местни и национални органи и частния сектор върху проект, наречен „Черен екран”.

„Черен екран” включва Националната гвардия в Тексас, общинските власти на Сан Антонио и Бексар Каунти, водоснабдителната система на Сан Антонио и градските комунални услуги. Компаниите от частния сектор включвали банки, енергийни и комуникационни компании. Една от потенциалните заплахи, които са били обект на изследване в проекта, е електронна атака на канализационната система. Например, кибертерористите биха могли да проникнат в компютърната система и да отклонят потока на отпадните води към питейните води.

Такива примери също могат да бъдат приложени в други части на света.

9.8. Заключение

Технологичната ера, в която живеем, е принудила държавите да се ангажират с нови национални предизвикателства пред сигурността. Няколко потенциални „съперника” имат равностойни възможности в областта на кибернетичното пространство и постоянно извършват наблюдения, събират техническа информация и начертават критичните направления, които могат да бъдат използвани при бъдещи конфликти. Заплахата на кибертероризма е нещо, което не може да бъде изтрито или заличено. Въпреки това, има няколко стъпки, които могат да се предприемат, на международно ниво, за да се смекчи самата заплаха. Най-важната стъпка е да се раздели киберпревенцията от кибервъзстановяването, като основни участници и в двете направления са специалистите по сигурността, полицейските служители и магистратите.

10. Компютърна експертиза

10.1. Въведение

Съществуват няколко насоки за борба с кибернетичните престъпления. Едната от тях е свързана с правната и съдебната система, а втората засяга техническите аспекти по време на разследване. В тази глава ще разгледаме и двата аспекта, като ще направим преглед и на най-новите технологии.

Правната страна на темата е международно отразена през 2001 г. в Конвенцията за престъпленията в кибернетичното пространство на Съвета на Европа, позната още като Конвенцията от Будапеща. Одобрена и подписана от почти всички страни-членки на ЕС от Югоизточна Европа, Конвенцията изисква предприемането на редица процесуални и технически стъпки, описани в настоящата глава.

Раздел 4 – Претърсване и изземване на съхраняваните компютърни данни

Член 19 – Претърсване и изземване на съхраняваните компютърни данни

1. Всяка страна приема законодателните и други мерки, необходими за да оправомощи своите компетентните органи да извършват претърсване или да получат достъп по сходен начин до:

а) компютърна система или до част от нея, както и до компютърните данни, съхранявани в нея; и

б) носител на компютърна информация, позволяващ да се съхраняват компютърните данни на нейна територия.

2. Всяка страна приема законодателни и други мерки, необходими, за да се гарантира, че когато нейните органи извършват претърсване или получават достъп по сходен начин до конкретна компютърна система или до част от нея, в съответствие с алинея 1(а), и имат основания да смятат, че издирваните данни се съхраняват в друга компютърна система или в част от нея, намираща се на нейна територия, и че тези данни са достъпни на законно основание от първоначалната система или тази първоначална система осигурява достъп до тях, горепосочените органи следва да бъдат в състояние да разпространят бързо претърсването или сходния достъп към другата система.

3. Всяка страна приема законодателните и други мерки, необходими за да овласти компетентните си органи да изземват или да осигуряват по сходен начин компютърни данни, достъпът до които е бил осигурен по реда на алинеи 1 и 2. Тези мерки включват следните правомощия:

а) да изземват или да осигуряват достъп по сходен начин до компютърна система или част от нея или носител на компютърна информация;

б) да правят и да запазват копие от тези компютърни данни;

в) да опазват неприкосновеността на съответните съхранявани компютърни данни; и

г) да изключат достъпа или да изтрият тези компютърни данни от компютърната система, в която се прави справка.

4. Всяка страна приема законодателни и други мерки, необходими, за да овласти компетентните си органи да нареждат на всяко лице, запознато с начина на функциониране на компютърната система или на мерките, прилагани за защита на компютърните данни, които тя съдържа, да предоставя необходимата информация, която е необходима в разумна степен, за да даде възможност за прилагане на мерките, посочени в алинеи 1 и 2.

5. По отношение на правата и процедурите, посочени в настоящия член, се прилагат членове 14 и 15.

Раздел 5 – Събиране в реално време на компютърни данни

Член 20 – Събиране в реално време на данни относно трафика

1. Всяка страна приема законодателни и други мерки, необходими , за да овласти компетентните си органи:

а) да събират или да записват данни чрез прилагането на технически средства, съществуващи на нейна територия;

б) да задължават доставчиците на услуги в рамките на съществуващите технически възможности да:

(i) събират или да записват чрез прилагане на технически средства, съществуващи на нейна територия, или

(ii) да сътрудничат и да подпомагат компетентните органи в събирането и записванетона данни за трафика в реално време, свързани с определени съобщения на нейна територия, предавани чрез компютърна система.

2. Когато една страна, поради установените принципи на своя правопорядък, не може да приеме мерките, записани в алинея 1(а), тя може в замяна на това да приеме законодателни и други мерки, които са необходими за осигуряването на събирането в реално време или на записването на данни за трафика, свързани с конкретни съобщения, предавани на нейна територия, чрез прилагането на технически средства, съществуващи на нейна територия.

3. Всяка страна приема необходимите законодателни и други мерки, за да задължи доставчик на услуги да запази в тайна съществуването и всяка информация за упражняването на всяко от правомощията по настоящия член.

4. По отношение на правата и процедурите, посочени в настоящия член, се прилагат членове 14 и 15.

Член 21 – Прихващане на данни, свързани със съдържанието

1. Всяка страна приема законодателни и други мерки, които могат да се окажат необходими във връзка с тежки престъпления, определени като такива във вътрешното право, за да овласти своите компетентни органи да:

а) събират и запаметяват данни чрез прилагането на технически средства на територията на тази страна; и

б) да задължават доставчиците на услуги, в рамките на наличните технически възможности, да:

(i) да събират или да записват данни чрез прилагане на технически средства, съществуващи на територията на тази страна,

или

(ii) да сътрудничат и да подпомагат компетентните органи за събирането и записването, в реално време на данни за трафика, свързани с конкретни съобщения на нейна територия, предавани чрез компютърна система.

2. Когато една страна, поради установените принципи на своя вътрешен правопорядък, не може да приеме мерките, посочени в алинея 1(а), тя може в замяна на това да приеме законодателни и други мерки, които са необходими за осигуряването на събирането или на записването в реално време на данни за трафика, свързани с конкретни съобщения, предавани на нейна територия, чрез прилагането на съществуващите технически средства на тази територия.

3. Всяка страна приема такива законодателни и други мерки, които могат да се окажат необходими, за да задължи доставчик на услуги да запази в тайна съществуването и всяка

информация за изпълнението на което и да е от правомощията, предвидени в настоящия член.

4. По отношение на правата и процедурите, посочени в настоящия член, се прилагат членове 14 и 15 (от Конвенцията, Nda).

10.2. Анализ на връзката между компютърната експертиза и правните процедури

За по-доброто разбиране на изискванията, установени от Конвенцията за престъпленията в кибернетичното пространство, е важно да се определи същността на компютърната експертиза. Това е новопоявила се и бързо развиваща се област, която може да се опише като наука за електронните доказателства при инцидент или престъпление.

Компютърната експертиза, наричана също кибернетична експертиза, е прилагане на компютърно разследване и техники за анализ за събирането на доказателства, подходящи за представяне в съда. Целта на компютърната експертиза е да извърши структурирано разследване, докато поддържа документирана верига от доказателства, за да открие какво точно се е случило в дадена компютърна система и кой носи отговорност за това. Ето защо е от изключително значение за полицейските служители, консултантите и магистратите да знаят следните концепции:

1. Придобиване на доказателства без променяне или повреждане на оригинала.

2. Удостоверяване, че записаното доказателство е същото като първоначално иззетите данни.

3. Анализиране на данните, без да бъдат модифицирани.

Гореописаните фактори са фундаментални. Много съдебни процедури, в които подобни фактори не се зачитат, приключват с отхвърляне на събраните електронни доказателства.

10.2.1. Стандартна методология

„Една стандартна методология ще осигури защитата на доказателства и за някои общовалидни стъпки, които трябва да се следват в процеса на разследване" (МакМилън, 2000). Стандартната методология трябва да обхваща следните „дейности/процедури за изолиране на предполагаемото компютърно местопрестъпление [и които да включват] изключване на компютъра, регистриране на доказателство, осигуряване на серия от документаци за задържане, удостоверяване на доказателствата и тяхното пренасяне" (Грейс, 2001). Методологията също трябва да се прилага при боравене с доказателства, удостоверяване на автентичността им и съхранението им.

Липсата на прилагане на гореспоменатите принципи може отново да доведе до непризнаване на доказателствата в съда. Това не е маловажен проблем. В света (и в един исторически период, където много наказателни и граждански съдебни заседания се управляват на международно ниво), спазването на стандартната методология е задължително.

Важно е да се отбележи, че на този етап нито един местен закон не регулира техническите процедури. Важно е това да бъде разяснено, защото е по-добре да се изисква практическите процедури на гореспоменатите принципи да стоят над научната общност, както е навсякъде по света.

Важна основа на тази парадигма е разяснена от един от най-уважаваните научни документи в тази област, RFC 3227, създаден от Internet Engineering Task Force (IETF). Това е един от най-публикуваните (и признавани в съда) водещи документи и който в основата си е свързан с няколко фактора, включващи, но не ограничаващи се до:

10.2.2. Съображения, свързани с поверителността

Процедурата на компютърната експертиза трябва да зачита правилата и насоките за поверителност на физическите и юридически лица и на установената правна юрисдикция. И по-специално, оперативното лице трябва да гарантира, че никаква информация, събрана покрай събирането на доказателствата, търсени от него/нея, няма да бъде достъпна до лица, които обикновено нямат достъп до тази информация. Това включва достъп до лог-файлове (които могат да разкрият модели на поведение при потребителите), както и файлове с лична информация. Това обаче не означава, че разследването и експертизите не могат да бъдат направени поради съображения за поверителност, но оперативното лице не трябва да нарушава личното пространство без солидна обосновка. В частност, оперативното лице:

1) не трябва да събира информация за области, до които обикновено няма достъп (като файлове с лична информация), освен в случаите на наличие на достатъчни индикации, че има реален инцидент или нарушаване на сигурността;

2) да си подсигури подкрепата на установените процедури на своята организация при предприемането на стъпки по събирането на доказателства за инциденти/нарушения.

10.2.3. Правни съображения

Според Мъркюри (2005), ако не е налице достъп до електронни доказателства от орган с права за конфискуване, може да са необходими съдебни заповеди за придобиването на данни, както и за използването на инструменти за извличане, за да се определи дали протоколите са били приложени правилно. И обратно, разследващият екип или екипът на защитата може да забранят разкриването на доказателства, ако смятат, че те могат да навредят на делото. Именно тук времеотнемащите аспекти на експертизното изследване могат да влязат в употреба. Обикновено не е възможно да се осъществи изчерпателно раздробяване и разглеждане на всички материали (като например съдържанието на всеки сектор от харддиск с големина 1 терабайт или хиляди часове видео материал от камера за наблюдение), така че може да се използва подхода „разрови и подуши” *("scratch-and-sniff")* за откриването на желаната информация. Въпреки че са рентабилни, тактическите решения за продължаване само с частично разследване може да се окажат грешни на по-късен етап, ако последващ изчерпателен анализ покаже, че е могло да има алтернативен подход.

При всички случаи, компютърните доказателства трябва да бъдат:

- допустими: трябва да съответстват на законовите разпоредби, преди да бъдат представени на съда;
- автентични: трябва да е възможно доказателственият материал да бъде недвусмислено свързан с инцидента.
- пълни: трябва да са цялостни, а не да отразяват само определен аспект на случая.
- надеждни: нищо от начините, по които доказателствата са събрани и впоследствие обработвани, не трябва да поражда съмнения относно тяхната автентичност и правдивост.
- правдоподобни: трябва да бъдат правдоподобни и разбираеми за съда.

10.2.4. Процедура по събиране на доказателства

Процедурите по събиране на доказателства трябва да са колкото е възможно по-детайлни. Те трябва да са недвусмислени и да минимизират нуждата от взимане на решения по време на процеса по събирането им. Методите, които се използват при натрупването на доказателства, трябва да са прозрачни и възпроизводими. Оперативното лице трябва да е подготвено да възстанови точно използваните методи и те да бъдат тествани от независими експерти.

Има няколко стъпки в процеса на събиране на доказателства, които трябва да бъдат направени:

- Къде са доказателствата? Важно е да се изброят системите, свързани с инцидента, и от които ще бъдат събирани доказателства.
- Трябва да се установи кои доказателства ще бъдат от значение и ще са приемливи. Когато се съмнявате, избегнете по-голямата грешка и събирайте повече от необходимите доказателства, вместо по-малко.
- За всяка система трябва да се открие приложимата скала на променливост.
- Трябва да се премахнат външните възможности за промяна.
- Следвайки скалата на променливост, съберете доказателствата посредством инструменти, които са надеждни и одобрени от съответните специалисти.
- Трябва да се запише отклонението на системния часовник.
- По време на работата по стъпките за събиране на доказателства, трябва да се изпитва всичко друго, което може да бъде доказателство.
- Трябва да се документира всяка стъпка.
- Не бива да се забравят замесените в случая хора. Трябва да се водят бележки за това кой е присъствал, какво е правил, какво е наблюдавал и как е реагирал.
- Където е възможно, трябва се вземе в предвид генерирането на контролни суми и шифрирано обозначаване на събраните доказателства, тъй като това може да улесни запазването на една силна поредица от доказателства. В този процес не бива да се променят самите доказателства.

10.2.5. Процедура по архивиране и управление на доказателства

Доказателствата трябва да бъдат строго охранявани. Освен това, процедурата по събирането им трябва да бъде ясно документирана. В частност, оперативното лице трябва да може ясно да опише как е било намерено съответното доказателство, как е третирано и всички действия, на които е било подложено. Трябва да бъдат описани следните неща:

- къде, кога и от кого е открито и събрано доказателството;
- къде, кога и от кого с доказателството е било боравено или е било изследвано;
- кой е бил отговорен за доказателството през този период и как то е било съхранявано;
- кога се е сменило отговорното лице за доказателството, кога и как е било прехвърлено (включително транспортни номера и др.).

Важно е също да се знае къде и как да се архивира електронното доказателство. Ако е възможно, трябва да е посредством общо използвана среда (вместо някои по-неясни среди за съхранение). Достъпът до доказателствата трябва да е изключително ограничен и трябва да бъде ясно документиран. Трябва да е възможно да бъде засечен всеки неправомерен достъп до тях.

10.3. Квалификация на експертите по компютърна експертиза (*computer forensic operators*)

В литературата има множество препратки и карти, свързани с това доколко един човек може да бъде технически обучен, за да извършва електронни разследвания и в частност компютърна експертиза.

Първото нещо, което правителството и съдебните власти трябва да направят, е да разделят държавния и частния сектор. Докато последните имат широка дискреционна власт относно това как да избират своите консултанти, държавният сектор (включително полицията и съдебните власти) трябва да следва точни критерии, за да избегне много проблеми в съда.

Една от най-успешните истории по случая идва от английски проект, наречен *умения за правосъдието.* Според тяхната литература, за да отговаря на стандартите, експертът трябва да знае и да разбира следното:

10.3.1. Правни и организационни изисквания

1. съответното законодателство, политики, процедури, професионални кодекси и насоки за изследване на електронни доказателства;
2. съответното законодателство и организационни изисквания във връзка с расата, различията и човешките права;
3. съответното законодателство и организационни изисквания във връзка със здравето и безопасността;
4. ситуации и обстоятелства, за които се изисква притежаване на определени права, и как се придобиват тези права;
5. как се извършват оценки на рисковете и защо те са необходими;
6. ограниченията на вашата отговорност и ниво на компетентност;

10.3.2. Изследване на електронни доказателства

7. как да се изследват електронни доказателства;
8. научните принципи, подкрепящи изследването на електронни доказателства;
9. нуждата да се установи поле на изследването;
10. параметрите и целите на тези видове изследвания;
11. ограниченията на тези видове изследвания;
12. видове налично оборудване за изследване на електронни доказателства;
13. как да се използва оборудването за изследване на електронни доказателства;
14. значението на доказателствено солидни съдебни инструменти и техники и как те се прилагат;
15. как да се провежда кръстосана обоснованост на резултатите и защо това е необходимо;
16. силните и слабите страни на различните инструменти за изследване на електронни доказателства;
17. третите страни, с които може да е необходимо да се консултират;
18. как да се консултират с трети страни, за да се получи допълнителна информация;
19. как да провеждат проучвателни дейности, за да получат допълнителна информация;
20. как да създадат работещ продукт, включващ подразделения на информацията, и междинни доклади;
21. как да документират изследването на електронните доказателства;
22. причините, поради които е важно да се документира изследването;
23. видовете проблеми, които може да се появят, и как може да се разрешат;
24. как да се прави устно представяне на изводите.

Докато този проект е добър при интерпретирането на нуждата от умения, той е по-малко показателен относно вида образование, което експертът по компютърна експертиза

трябва да има. Общата практика предполага следното:

1) Поне диплома от университет (еквивалентът на степен „специалист”) в областта на компютърните науки или сходна област. Това трябва да даде на експерта минимални умения за компютрите/системите, които той/тя ще разследва.
2) Последваща сертификация в областта на дейността. Много важно да се познава така наречената „сертификационна дилема”. Най-добрите практики предлагат да обучават хора, които да получат сертификати в областта, въпреки продавача на технологии, използвани при разследването. Общите практики предполагат също да се продължи с второ сертифициране, свързано със самата технология.
3) Притежаването на международно признат сертификат е абсолютно задължително. Разбира се, може да се организира местно обучение всяка година.

Също така се предлага да се изгради лаборатория за компютърна експертиза, която да е научно структурирана. Всяка лаборатория трябва да е оборудвана с последните технологии и в нея да работят няколко експерти. Всеки един от тях трябва да се е специализирал в някакви вертикални области (напр. мобилни телефони, лог-анализ и т.н.)

10.4. Финансови и технически аспекти

Областта на компютърната експертиза нараства и включва няколко различни подобласти. По отношение на инвестициите, те не са малки и трябва да се правят постепенно. По-специално, въпреки че има някои магистрати, които предпочитат да наемат оборудването, добрите практики съветват то да се закупува. Критериите, които обикновено се следват, са:

1) Поле на действие. Ако една лаборатория е с вход от първо ниво (*entry level one*) (например, за разследване на детска порнография и малки/средни случаи), предлагаме да се започне със съдебен хардуер и с изследване на областта на електронната експертиза с отворен код. Областта на електронната експертиза с отворен код (The Open Source Digital Forensics) е препратка към употребата на софтуер с отворен код при електронните разследвания (също известни като електронна експертиза, компютърна експертиза, реагиране при инциденти). Инструментите с отворен код са безплатни и могат да имат правно предимство пред инструментите със затворен код (частни и търговски), защото имат документирана процедура и позволяват на разследващия орган да провери дали инструментът прави това, което се твърди, че прави. Докато е важно да се отбележи, че инструментите и със затворен и с отворен код са широко признати в съда, експертизата на отворения код е важна новопоявила се област. Броят на хората, работещи в тази област, нараства, и поради финансови причини, и поради признаването на съда. PTK е нов проект, зародил се в IRItaly (http://ptk.dflabs.com), и е бил пуснат в края на март 2008 г. Броят на сваляния на този софтуер, който позволява ефективни и паралелни електронни разследвания на много ниска цена, достига 10 000 по целия свят. PTK е на английски език, но може да бъде локализиран на няколко езика.

2) Брой и сложност на разрешените случаи. Ако броят на разрешените случаи за една година надхвърля 200, е по-добре да се осъществи по-задълбочено инвестиране. За да се направи това, трябва да се проведе предварително проучване, за да се класифицира типа лаборатория и технологиите, които ще се използват. По правило е по-добре да се избягват технологии, които не са били използвани преди това от общността. Това ще предотврати отрицателните последици в съда.

10.5. Бъдещето

Съгласни сме с ISACA, които наскоро публикуваха писмено становище за бъдещето на тази дисциплина. Изглежда, че за науката за компютърната експертиза има неограничено бъдеще и с напредването на технологиите полето ще продължи да се разширява. С такива доказателства трябва да се борави по подходящ начин и те трябва да се документират, за да могат да се ползват в съда. Всяко прекъсване на методиката, процеса или процедурите при приложението на компютърната експертиза може да застраши случаите.

Организациите – правителствата и частния сектор – започват да разчитат на заключенията, които правят специалистите по компютърна експертиза, когато е извършено кибернетично престъпление. Компютърната експертиза бързо се превръща в стандартен протокол при корпоративните и съдебните разследвания, като се разширява извън областта на специализираните екипи за реагиране при компютърни престъпления. Тъй като по-голямата част от документацията сега се съхранява в електронна форма, е трудно да си представим какъвто и да е тип разследване, което не използва компютърната експертиза. Така компютърната експертиза се превръща в стандарт при разследването на електронни престъпления. Обаче докато корпоративният сектор ще я използва „само" за разрешаване на проблеми със сигурността, съдебните власти ще я използват за широк обхват от престъпления – от детска порнография до измами, тероризъм и организирана престъпност.

Компютърната експертиза не се използва само в случаите на кибернетични престъпления, а техниките и методите се използват също и за цели, различни от разследването. Примерите включват картографирането на бази данни с цел оценка на риска относно сигурността и неприкосновеността и търсенето на интелектуална собственост при защитата на данните.

Компютърната експертиза преминава от механизъм за разследване и реагиране към такъв за превенция, съгласуване и сигурност. Чрез използването на техники за компютърна експертиза, компаниите могат по-добре да се защитят от потенциални заплахи от хакери и недоволни служители. Освен това, схемите на компютърната експертиза могат да се използват, когато по невнимание или при хардуерен срив се изтрият критични файлове. Така, има няколко допълнителни приложения, принадлежащи на науката за компютърната експертиза, освен използването на методите й за разследване на компютърни престъпления.

III. ЗАКЛЮЧЕНИЯ И ПРЕПОРЪКИ

1. Общи насоки за реформата

1.1. Методология

Интернет се развива с толкова бързи темпове, че е невъзможно всички предизвикателства, които възникват във връзка с него, да бъдат разрешени със създаването на един единствен нормативен акт. От голяма важност при изработването на национална правна рамка е да се осигури достатъчно технологично-неутрална гъвкавост, за да има оптимален баланс между интересите на носителите на авторските права (при законодателството за интелектуалната собственост), тези на обществото като цяло (при законодателството за интелектуалната собственост и това за компютърните престъпления), както и на Интернет потребителите.

1.2. Технологично-неутрален език

Бързите промени в сферата на технологиите скоро ще направят така, че всеки технологично-специализиран език ще бъде остарял към определен момент. Въпреки, че именно новите технологии са причината за създаването на Интернет договорите от Световната организация за интелектуална собственост (WIPO) през 1996 година, в техните преамбюли, при обобщаването на разгледаните от Договорите въпроси, технологичният аспект се поставя едва на четвърто място след „икономическите, социалните и културните" аспекти. Според разясненията на Михаил Фиксор, един от създателите на Договорите, изборът не е случаен. Целта е да се наблегне, че фокусът на усилията за реформа, не трябва бъде от технологично естество. Клаузите „не трябва да бъдат специализирани технологично, а по-скоро абстрактни, така че да покриват икономическите, социалните и културните въпроси, които се повдигат от технологиите".[1]

1.3. Категоризация на аспектите

Правните проблеми, възникнали във връзка с Интернет са многобройни, но техният анализ и поставянето им в отделни категории може да улесни създаването на адекватен юридически отговор. Полезна е следната модифицирана класификация, направена през 1998 година от професор Тротър Харди, направена в изследването му:

(а) нови въпроси по темата;
(б) нови употреби; и
(в) децентрализирани правни нарушения.[2]

1.4. Цената на прехода

Всяка правна реформа изисква ресурси от време, пари и кадри. Нужни са добре осведомени и обучени хора, които да изготвят правните норми. Наложително е също единство и експедитивност сред законодателите, както и воля от страна на институциите за промяна на ежедневния им начин на работа. Преди да се вземе решение да се тръгне по пътя на промяната, важно е да се преценят последиците от провеждането или непровеждането й. Фредерик Шоуер отбелязва, че „някой от преходите в правото, които при други обстоятелства биха могли да бъдат оптимални, трябва да се изключат или да бъдат

максимално забавени в услуга на устойчивостта, стабилността и спокойствието”.[3] При една децентрализирана и саморегулираща се медия, каквато е Интернет, юридическите преходи са най-ползотворни, когато други по-икономически методи не могат да разрешат възникналите въпроси и има всеобщ консенсус сред заинтересованите лица как да се продължи напред. В противен случай е по-безопасно законодателството да остане непроменено, а пропуските да бъдат запълвани съобразно възникващите казуси чрез договори и тълкуване на правните норми. Като се вземе предвид, че юридическите процеси съответстват на поставените задачи, „интерпретиращият” метод може да се окаже по-икономичен от цялостната юридическа реформа това трябва да се има предвид, преди да се премине към изработване на радикално нов законодателен акт.

2. Привеждане в действие

Независимо колко добри са материално правните норми, те не значат нищо, ако не е подсигурено прилагането им на практика. Нужни са не само отделни добре изготвени правни норми за интелектуалната собственост и за наказателно право, но също и адекватна и съгласувана процесуална уредба, позволяваща на потребителите успешно да защитят правата и интересите си, както и независими правни институции и организации, занимаващи се с популяризирането, разясняването и спазването на правото.

2.1. Привеждане в действие чрез законодателни мерки

Член 14 (Обезпечаване привеждане в действие на правата) на Спогодбата за авторското право на Световната организация за интелектуална собственост (WIPO) от 1996 година изрично изисква договарящите страни да „подсигурят свободното прилагане на процедурите според вътрешното им законодателство, така че да могат да бъдат предприети успешни действия срещу всякакви посегателства срещу права, защитени от Спогодбата, включително бързо удовлетворение на загубите, което би възпряло по-нататъшни нарушения”. Това задължение отразява и изискванията на Споразумението ТРИПС (чл. 14).

През април 2004 година, ЕС прие отделна Директива за прилагането правата на интелектуалната собственост. В чл. 1 на тази Директива се набляга на факта, че мерките, процедурите и средствата необходими, за да се подсигури прилагането на практика на тези права следва да бъдат честни и съразмерни, без излишни усложнения и оскъпявания, както и пропорционални и мотивирани.[4] Директивата изисква достъпът до въпросните мерки да бъде подсигурен за всички заинтересовани лица, включително:

а) носителите на авторски права;

б) всички лица, упълномощени да се ползват от тези права, и по-специално притежателите на лицензи;

в) организации за колективно управление на авторските права; и

---

[1] Mihaly Ficsor, The Law of Copyright and the Internet, Oxford University Press, 2002, p. 413.

[2] Проект стремящ се към очертаване бъдещето на авторските права в мрежовия свят, май 1998 г., Финален доклад от И. Тротър Харди, достъпен на http://www.copyright.gov/reports/thardy.pdf.

[3] Frederick Schauer, Legal Transitions: Is There an Ideal Way to Deal with the Non-Ideal World of Legal Change?: Legal Development and the Problem of Systemic Transition, 13 J. Contemp. Legal Issues 261, 265 (2003).

[4] Директива на Европейския парламент и на Съвета относно действието на правата на интелектуална собственост (IP Enforcement Directive) 2004/48/ЕО от 29 април 2004 г., достъпна на http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf.

[5] *Виж* отново там в чл. 4

г) професионални защитни организации, имащи право да представляват притежателите на права на интелектуалната собственост.[5]

С цел опростяване достъпа до подобни мерки за защита в Директивата е предвидена презумпция за авторство.[6] С оглед на възможните материално правни мерки за защита, се предвиждат следните инструменти за прилагането им:

- съдебни предписания;[7]
- парични компенсации;[8] и
- присъждане на съдебни разходи.[9]

2.2. Привеждане в действие чрез процесуални мерки

Звукозаписните компании в САЩ водят бдителна процесуална кампания. Тя е доказала ползата от привеждането в действие на тези мерки. След като Американската асоциация за звукозаписна индустрия (RIAA) завежда няколко стотин дела срещу отделни лица, обменящи файлове (file swappers) през юни 2003 година, броят им в KaZaa спада от 6.2 милиона през май на 4.3 милиона през август, според изследване на уеб потока осъществено от Nielsen/NetRatings.[10] Според друга компания за проучване на пазара, NPD Group, до края на август са се сваляли от Интернет с 30% по-малко песни, отколкото през пролетта. Forrester Research направи проучване сред хора на възраст между 10 и 22 години, като им зададе въпроса дали биха спрели да свалят нелегални копия на защитени от авторското право творби, ако има сериозен риск от затвор или глоба и 68% от запитаните отговарят „да".

2.3. Привеждане в действие чрез промени в културата

За да се води ефективна борба с нарушаването на закона онлайн, както и навсякъде другаде, е нужно да има предвидени както наказания, така и поощрения. Европейската Директива за авторското право набляга на методи за борба като кодекси за поведение, разработени от професионални сдружения[11] и даване на голяма публичност на съдебни решения относно дела по авторско право.[12]

От голямо значение е и да се създадат ефикасни обществени кампании, които да разяснят на обикновените Интернет потребители защо защитата на авторското право е важна за самите тях. Полезно би било да се направят изследвания, оценяващи икономическото и социалното влияние на подобни посегателства върху лица извън заинтересованата индустрия. Трябва също така да се разясни засилващата се връзка между пиратството в областта на авторското право и организираната престъпност. Тази връзка е естествена, като се има предвид, че рисковете, свързани с пиратството в тази област, са значително по-ниски от свързаните с наркодилърството, а печалбите са пропорционално по-високи. Докато със сумата от 47 000$

---

[6] *Виж* отново там в чл. 5.
[7] *Виж* отново там в чл. 11.
[8] *Виж* отново там в чл. 12 и 13.
[9] *Виж* отново там в чл. 14.

[10] *Виж* Jefferson Graham et al., Hammering Away at Privacy, USA Today (Sept. 11, 2003), at D1.
[11] *Виж* IP Enforcement Directive, чл. 17.
[12] *Виж* отново там в чл. 15.

може да се закупи един килограм кокаин, който може да се продаде с печалба от 100%, със същата сума може да се закупят 1 500 пиратски копия на Microsoft Office и да се генерира печалба от 900%.[13]

Като цяло могат да се приложат множество от мерки - от телевизионни реклами и до конкурси за писане на есета на тази тема, които да убедят обществото да изисква адекватна система за защита на интелектуалната собственост, вместо да я пренебрегва. На края, но не на последно място, производителите в тази сфера трябва да предложат алтернативи: лесно достъпни и легални средства за сваляне на материали на разумна цена.

[13] *Виж* Jennifer L. Schenker, Busting Software Pirates, Time (Nov. 18, 2002), at 54.

IV. БИБЛИОГРАФИЯ

Правна уредба на компютърните престъпления в Румъния

Престъпления, предвидени в специални закони (съдържа компютърните престъпления)/Михай Адриан Хоця, 2007

Компютърно право и права/ Йоана Васиу, 2007 г.

10 юридически съвета за електронната търговия /Богдан Маноля, 2007 г.

Няколко аспекта на престъпленията за неправомерен достъп до компютърните системи /Богдан Маноля, 2007 г.

Престъпления в компютърната сфера / Максим Добриною, 2006 г.

Юридически проблеми на злоупотреби с малолетни по интерент – *др. Хорациу Димитру* - август - октомври 2006г. – публикувано с списание "Pandectele Romane", бр. 2/2006г. и бр. 4/2006 г.

Предотвратяване на компютърните престъпления / Йоана Васиу, Личян Васиу, 2006 г.

„Наказателно регламентиране и криминално разследване на компютърните престъпления"- др. Георге Алеку , др. Алексей Барбанеагра, 2006 г.

Въведение за прилагане на законовите разпоредби по отношение на компютърните престъпления, RITI dot-Gov, 2004 г.

Използване на компютрите и електронните услуги: ръководство за обществено функциониране , RITI dot-Gov , 2004 г.

Компютърна престъпност / Тудор Амза, Космин Петронел Амза, 2003 г.

Юридически проблеми по отношение на негативното съдържание в Интернет – *др.. Хорациу Дан Думитру* - (статията е излязла в списание "Pandectele Romane" Nr.3/2003 г., 4/2003, 5/2003, 6 /2003 si 1/2004)

Компютърни измами

Council of Europe, (2001) Convention on Cybercrime (ETS 185)
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

De Hert, P. González Fuster, G. & Koops, B-J. (2006) Fighting Cybercrime in the Two Europes: The added value of the EU Framework Decision and the Council of Europe Convention, Revue Internationale de droit pénal 77(3-4): 503-524.
<http://www.vub.ac.be/LSTS/pub/Dehert/260.pdf>

European Union, Safer Internet plus programme
<http://ec.europa.eu/information_society/activities/sip/index_en.htm>

European Union, (2001) Council Recommendation on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime (OJ 2001/C 187/02: 5–6.)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2001:187:0005:0006:EN:PDF>

--, (2004) Regulation 2006/2004/EC on cooperation between national authorities responsible for the enforcement of consumer protection law (OJ 2004 L 364/1-11).
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:364:0001:0011:EN:PDF>

--, (2005) Council Framework Decision 2005/222/JHA on attacks against information systems (OJ 2005 L 69/67-71)
<http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf>

International Consumer Protection and Enforcement Network (ICPEN)
<http://www.icpen.org/operation.htm>

OECD – Consumer Policy Committee
<http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html>

OECD, (1999) Guidelines for Consumer Protection in the context of Electronic Commerce
<http://www.oecd.org/dataoecd/18/13/34023235.pdf>

--, (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders
<http://www.oecd.org/dataoecd/24/33/2956464.pdf>

--, (2006) Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders
<http://www.oecd.org/dataoecd/45/53/37125909.pdf>

Savirimuthu, J. (2008) Identity Theft and the Gullible Computer User: What Sun Tzu in The Art of War Might Teach, Journal of International Commercial Law and Technology 3(2): 120-128.
<http://www.jiclt.com/index.php/JICLT/article/view/65/51>

Smith, R. G. & Urbas G. (2001) Controlling Fraud on the Internet: A CAPA Perspective, Australian Institute of Criminology Research and Public Policy Series No. 39.
<http://www.aic.gov.au/publications/rpp/39/RPP39.pdf>

Smith, R.G. (2008) Coordinating individual and organizational responses to fraud, Crime, Law and Social Change (2008) 49(5): 379–396.

Tally G. Thomas, R. & Van Vleck, T. (2004) Anti-Phishing: Best Practices for Institutions and Consumers, McAfee Research, Technical Report # 04-004
<http://www.antiphishing.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf>

United Nations, (1994) Manual on the Prevention and Control of Computer-Related Crime
http://www.uncjin.org/Documents/irpc4344.pdf

--, (2001) General Assembly Resolution: Combating the criminal misuse of information technologies (A/55/593)
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

Wilson, G. & Wilson S. (2007) Can the General Fraud Offence 'Get the Law Right'? Some Perspectives on the 'Problem' of Financial Crime, Journal of Criminal Law 71(1): 36-52.

Електронна порнография

Casavant, L. & Robertson, J.R. (2007) *The Evolution of Pornography Law in Canada*, Parliamentary Information and Research Service, Canada.
<http://www.parl.gc.ca/information/library/PRBpubs/843-e.htm>

Clayton, R (2005) *Anonymity and traceability in cyberspace*, Technical Report No. 653, University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf

Council of Europe, (2001) *Convention on Cybercrime* (CETS 185)
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

--, (2007) *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS 201)
<http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm>

Department for Children, Schools and Families (UK) (2008) *Byron Review – Children and New Technology - Executive Summary*
<http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf>

--, (2008) *Report of the Byron Review– Safer Children in a Digital World*
<http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

European Union, Safer Internet *plus* programme
<http://ec.europa.eu/information_society/activities/sip/index_en.htm>

---, (1996) Commission Communication on Illegal and Harmful Content on the Internet. (COM (96) 487 final)
<http://aei.pitt.edu/5895/01/001527_1.pdf>

--, (1998) *Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity* (98/560/EC)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:270:0048:0055:EN:PDF>

--, (1999)*Council Decision adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks* (276/1999/EC)
<https://www.inhope.org/system/files/siap-extension.pdf>

--, (2000) *Council Decision to combat child pornography on the Internet* (2000/375/JHA)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:138:0001:0004:EN:PDF>

--, (2004) *Council Framework Decision on combating the sexual exploitation of children and child pornography*. (2004/68/JHA)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:0048:EN:PDF

--, (2005) *Decision of the Parliament and of the Council establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies* (854/2005/EC)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0001:0013:EN:PDF

--, (2007) *Commission Report based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography* (COM(2007) 716 final)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0716:FIN:EN:PDF

ILO, (1999) *Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour*
<http://www.ilo.int/public/english/standards/relm/ilc/ilc87/com-chic.htm>

International Association of Internet Hotlines (INHOPE)
<https://www.inhope.org/>

Internet Watch Foundation (IWF)
<http://www.iwf.org.uk/>

Johnson, M. (2008) Camera Obscura - The Criminal Justice and Immigration Act 2008 and Virtual Pornography, *Justice of the Peace* 172 (29): 460-462.

Joyce, R.A. (2008) Pornography and the Internet, *IEEE Internet Computing* 12(4): 74-77.

Krause, J. (2008) The End of the Net Porn Wars, *American Bar Association Journal* 94(Feb): 52-57.
<http://abajournal.com/magazine/the_end_of_the_net_porn_wars/>

Krone, T. (2004) A Typology of Online Child Pornography Offending, *Trends & Issues in Crime and Criminal Justice*, No. 279
<http://www.aic.gov.au/publications/tandi2/tandi279.pdf>

Livingstone, S. & Bober, M. (2004) *UK Children Go Online: Surveying the experiences of young people and their parents*, Research Report, London School of Economics and Political Science

<http://www.york.ac.uk/res/e-society/projects/1/UKCGOsurveyreport.pdf>

McCabe, K.A. (2008) The Role of Internet Service Providers in Cases of Child Pornography and Child Prostitution, *Social Science Computer Review* 26(2): 247-251.

McGlynn, C. & Rackley, E. (2007) Striking a Balance: Arguments for the Criminal Regulation of Extreme Pornography, *Criminal Law Review*: 677-690

UN, (2000) Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
<http://www.iin.oea.org/iin/English/observatorio/documentos/Optional%20Protocol%20to%20the%20Convention.pdf>

Wolak, J. Finkelhor, D. & Mitchell, K. J. (2005) *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study,* National Center for Missing & Exploited Children
<http://www.missingkids.com/en_US/publications/NC144.pdf>

Пране на пари по електронен път

Carroll, L. (2004) *Alternative Remittance Systems: Distinguishing Sub-Systems of Ethnic Money Laundering in Interpol Member Countries on the Asian Continent*, Lyon: Interpol General Secretariat.
<http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp>

Council of Europe, (1990) *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime* (ETS 141).
<http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm>

--, (2005) *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism*
<http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm>

European Union, (2005) Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF>

FATF, (2004) *The Forty Recommendations*, October 2004.
<http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF>

--, (2004) *Special Recommendations on Terrorist Financing*, October 2004
http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf

--, (2006) *Report on New Payment Methods*, October 2006.
<http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>

--, (2007) *БПП/БФТ Evaluations and Assessments Handbook for Countries and Assessors*, June2007
<http://www.fatf-gafi.org/dataoecd/7/42/38896285.pdf>

--, (2008) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems*, June 2008.
<http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf>

Jost, P.M. & Sandhu, H. S. (2000) *The hawala alternative remittance system and its role in money laundering*, Lyon: Interpol General Secretariat.
<http://www.treas.gov/offices/enforcement/key-issues/hawala/FinCEN-Hawala-rpt.pdf>

MONEYVAL, (2008) *Third Round Detailed Assessment Report on Bulgaria - Summary*, 3 April 2008
<http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)02Summ-BUL3_en.pdf>

--, (2008) *Third Round Detailed Assessment Report on Romania - Summary*, 11 July 2008 http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)06Summ-ROM3_en.pdf

National Drug Intelligence Center, (2008) *Money Laundering in Digital Currencies*, Product No. 2008-R0709-003, U.S. Department of Justice June 2008 <http://www.usdoj.gov/ndic/pubs28/28675/28675p.pdf>

Reuter, P. & Truman, E. M. (2004) *Chasing Dirty Money: The Fight against Money Laundering.* Washington, DC: Institute for International Economics. <http://bookstore.petersoninstitute.org/book-store/381.html>

Кибертероризъм

Forte, Dario: Assembling an Incident Response team in a Small to Medium Organization - Computer Fraud and Security - Feb 2004 Issue

Forte, Dario : Principles of Digital Evidence Collection, Publication: Network Security December 2003 issue

Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Dorothy E. Denning, Georgetown University May 23, 2000

Gabriel Weimann: Cyberterrorism: How Real Is the Threat? December 2004 | Special Report No. 119. The United States Institute of Peace, available on line: http://www.usip.org/pubs/specialreports/sr119.html

Richard Power and Dario Forte: War & Peace in Cyberspace, Stalking “cyber terrorists” in Sofia – event report, Computer Fraud & Security. Volume 2006, Issue 11, November 2006, Pages 4-8

Richard Power and Dario Forte: War & Peace in Cyberspace, Ten years in the wilderness — a retrospective Part I: Nine false notions and nine steps to success,Computer Fraud & Security. Volume 2006, Issue 1, January 2006, Pages 8-13

Richard Power and Dario Forte: War & Peace in Cyberspace, Case Study: a bold new approach to awareness and education, and how it met an ignoble fate, Computer Fraud & Security, Volume 2006, Issue 5, May 2006, Pages 7-10

Компютърна експертиза

Armstrong, Illena. “Windows vs. Linux: Taking Security Seriously.” 2001. http://www.securityfocus.com/library/3446 (2 November 2001).

Computer Forensics: An Overview By Frederick Gallegos, CISA, CDE, CGFM Volume 6, 2005, the ISACA control journal.

Farmer, Dan and Venema, Wietse. “Forensic Computer Analysis: An Introduction.” Dr. Dobb’s Journal. September, 2000. http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm (1 November 2001).

Grace, Scott. “Computer Incident Response and Computer Forensics Overview.” March 2001. http://www.sans.org/infosecFAQ/incident/IRCF.htm

Kruse, Warren G. and Jay G. Heiser. Computer Forensics: incident response essentials. Indianapolis: Addison-Wesley, 2002.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime. Berkeley: McGraw-Hill, 2001.

McMillian, Jim. “Importance of a Standard Methodology in Computer Forensics.” May 2000. http://www.sans.org/infosecFAQ/incident/methodology.htm

Romig, Steve. “Forensic Computer Investigations.” October 2001. http://www.net.ohio-state.edu/security/talks/2001-10_forensic-computer-investigations/6up-pdf/ (2 November 2001)

Challenges in Forensic Computing Rebecca T. Mercuri Communications of the ACM, Volume 48, Number 12 (2005), Pages 17-21

Scambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 2001.