СОФИЙСКИ УНИВЕРСИТЕТ
„СВ. КЛИМЕНТ ОХРИДСКИ“

ЮРИДИЧЕСКИ ФАКУЛТЕТ

КАТЕДРА „ НАКАЗАТЕЛНОПРАВНИ НАУКИ“

ГЕНТИАН ФЕТАХ КОЧИ

КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ ПО БЪЛГАРСКОТО И АЛБАНСКОТО НАКАЗАТЕЛНО ПРАВО

АВТОРЕФЕРАТ

на дисертационен труд за присъждане на образователна и научна степен

„ ДОКТОР”

ПРОФЕСИОНАЛНО НАПРАВЛЕНИЕ: 3.6 „ПРАВО“

НАУЧНА СПЕЦИАЛНОСТ: 05.05.16 - НАКАЗАТЕЛНО ПРАВО

Научен ръководител : **проф. д.ю.н. Борис Велчев**

СОФИЯ

2016 г.

Дисертационният труд е обсъден и допуснат до защита пред научно жури на заседание на катедрата по „ Наказателноправни науки‘‘ при Юридически факултет на СУ „ Св.Климент Охридски ‘‘ на 15.11.2016 г.

Авторът е зачислен, като редовен докторант към Катедра „Наказателноправни науки” на Юридически факултет при Софийският университет „Св. Климент Охридски ” .

Дисертацията е в обем от 273 страници и съдържа седем глави, включващи :
Увод, изложение на главите, заключение, научна литература - заглавия на български и чуждестранен език, интернет източници

СЪДЪРЖАНИЕ

Използвани съкращения

АПК	Административно-процесуален кодекс
ВДПЧ	Всеобща декларация за правата на човека
ВС на РБ	Върховен съд на Република България
Г8	Групата на осемте
ЕСПЧ	Европейски съд по правата на човека
ЕС	Европейски съюз
ЗАПСП	Закон за авторското право и сродните му права
ЗДДФЛ	Закон за данъците върху доходите на физическите лица
ЗДОИ	Закон за достъп до обществената информация
ЗЕДЕП	Закон за електронните документи и електронния подпис
ЗЕС	Закон за електронните съобщения
ЗОП	Закон за обществените поръчки
ИКТ	Информационни и компютърни технологии
ИТ	Информационни технологии
МПГПП	Международен пакт за граждански и политически права
МПИСКП	Международен пакт за икономически, социални и културни права
НК	Наказателен кодекс
НПК	Наказателно-процесуален кодекс
ОС на ООН	Общо събрание на Организацията на обединените нации
ОИСР	Организация за икономическо сътрудничество и развитие
ООН	Организация на обединените нации
НАТО	Организация на Северноатлантическия договор
ОЕИС	Организацията за европейско икономическо сътрудничество
ПМС	Постановление на Министерски съвет
СОИС	Световната организация по интелектуална собственост
СНПООН	Служба на ООН по наркотиците и престъпността
СЕ	Съвета на Европа
САЩ	Съединени американски щати
ССА	Споразумението за стабилизиране и асоцииране
СКТ	Съюзно командване по трансформацията на НАТО

ГЛАВА I

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Въведение

Процесите на ускорената международна интеграция и глобализацията на информационните технологии промениха значително традиционния облик на обществените отношения. В съвременното общество се наблюдава по-висока степен на обвързаност между суверенните държави, наднационалните международни организации, гражданите и бизнеса. Една от причините за нарастващата взаимозависимост между правните субекти, е прогресивното развитие на информационните и комуникационните технологии. Безспорно, този глобален феномен има положителен принос в историческото развитие на човечеството. Той предостави на гражданското общество неограничени възможности за влияние върху всички видове обществени отношения: икономически, политически, социални, религиозни и пр. От друга страна, възходът на технологиите и комуникационните системи, доведе до появата на нови форми на престъпна дейност, а именно: компютърните престъпления или т.нар. киберпрестъпност. В съвременното общество, броят на престъпните посегателства в кибернетичното пространство заплашително нараства. Престъпленията от тази категория стават все по-сложни, увеличава се участието на организирани престъпни групи в тях, те излизат извън териториалните граници на отделните държави. Киберпрестъпността е една развиваща се индустрия, която води до значително увреждане на световната икономика и търговия, накърнява правата на хората и застрашава както националната сигурност на държавите, така и световния мир. Тези негативни явления изискват нова наказателна политика[1] , която да бъде провеждана както от международната общност, в глобален аспект, така и от суверенните държави в рамките на териториалната им компетентност, да насочат политическата си воля и дейност към създаване на адекватно законодателство, което да регламентира изпреварващите обществени промени. Необходимо е синхронизиране на създадената международна и национална наказателноправна уредба, с цел предотвратяване и ограничаване на компютърните престъпления. Единствено, чрез създаването и прилагането на всеобхватна правна рамка, може да се избегне нежеланото явление, правото да изостава от технологиите. В тази връзка, становището на Професор Стойнов, че: „Развитието на наказателното право се предопределя от развитието на

[1] Велчев, Б „Проблеми на наказателната политика в Република България”. С. (2012)

обществото, но потребността от наказателноправна закрила на обществените отношения във виртуалното пространство, свързани с ползването на компютри обикновено се осъзнава от законодателите известно време след увреждането или поставянето в опасност на тези отношения[2] " отговаря изцяло на съвременната действителност.

2. Актуалност на изследването

Прогресивното развитие на информационните технологии и компютърните системи предизвика пораждането на непознати до сега престъпни деяния. Тази нова категория престъпления, налага създаването на адекватни правила за поведение, съобразени с техните техническите особености. Актуалността на настоящия дисертационен труд е обусловена от необходимостта да бъде проведено задълбочено изследване на процеса по интеграция на технологичните понятия в правната материя, както и на правната конструкция на новите престъпни състави, с оглед нарастващата киберпрестъпност.

Днес всички държави са изправени пред едно сериозно предизвикателство, а именно: създаването на наказателноправната уредба, която да съответства на нивото на развитие на компютърните технологии. Поради специфичния начин на регулиране на обществените отношения, наказателното право изостава от технологичното развитие и хармонизирането им се оказва трудно постижимо, предвид динамичното развитие на информационните и комуникационните технологии.

В анализираната материя интерес представлява и въпросът: ***Какъв ефект има хармонизирането на глобалните технически стандарти върху развитието на националното наказателно право ?***

В тази връзка, в правната доктрина е изразено следното становище: "Теоретично, развитието произтичащо от техническата стандартизация излиза далеч извън глобализацията на технологии и услуги и може да доведе до хармонизиране на националните законодателства, въпреки че те се променят много по-бавно, отколкото техническото развитие[3] ". На практика, глобалните технически стандарти осигуряват определени граници на съществуващата и бъдещата технология, което улеснява развитието на правната система, включително при изработване на глобални технически регламенти. Вътрешното законодателство на държавите единствено препраща към тези

[2] Стойнов, А. Наказателно право-Обща част. София, 2011, с.15

[3] Marco, Gercke, Understanding cybercrime: phenomena, challenges and legal response. ITU publication, 2012, стр 4

технически регламенти, като се ръководи от конституционно установените правила по прилагането им. Това обаче не осигурява необходимия синхрон между националната и международната правна уредба, като създава противоречия между правото и технологията.

3. Предмет на изследването

Дисертационният труд представлява задълбочено изследване на наказателноправната уредба на компютърните престъпления в Република България и Република Албания. Анализирани са също така основните източници в международното право, които уреждат различните видове киберпрестъпления. Представени са основните дефиниции и термини използвани при кодификацията на посочените престъпления, които представляват основата при тълкуването и практическото прилагане на правните норми. Изследвано е нивото на международната и националната закрила (в Република България и Република Албания) против компютърни престъпления, чрез всеобхватно проучване на основните органи в областта.

4. Научни задачи на изследването

- ✓ Да анализира нивото на наказателноправна закрила на обществените отношения, свързани с използването на компютърните технологии в албанското и българското наказателно законодателство;
- ✓ Да представи в систематизиран вид комплекса от правни норми, които регламентират отделните състави на компютърните престъпления в изследваните държави;
- ✓ Да анализира правната конструкция на тези състави, както и теоретичните и практическите проблеми, свързани с прилагането им;
- ✓ Да представи изградената в международното право система от основни международни актове, които допринасят за борбата с киберпрестъпността;
- ✓ Да посочи основните международни и държавни органи, които осъществяват дейност в изследваната област;
- ✓ Да открие недостатъците на съществуващата правна уредба и да направи препоръки *de lege ferenda* за усъвършенстването ѝ.

5. Научна новост на изследването

В международната доктрина са публикувани различни научни изследвания и статии, които анализират същността на компютърните престъпления, различните им форми и отражението им върху съвременното обществено развитие. В българската и албанската правна теория в тази проблематика са публикувани малко на брой научни статии, които разглеждат отделните състави на компютърните престъпления по НК. Основният източник в областта е книгата на автора Моника Копчева -"Компютърни престъпления" издадена през 2006г. В нея авторката представя всеобхватен анализ на съществуващата международноправна уредба за компютърните престъпления, както и задълбочено теоретико-правно изследване на отделните видове компютърни престъпления. Научен принос в областта на албански език е книгата на автора Ветон Вула -"Компютърни престъпления" издадена през 2009г.

Настоящият дисертационен труд е първото българско изследване, което съдържа изчерпателен сравнително правен анализ на комплекса от правни норми в българското и албанското наказателно право, които регламентират различните видове компютърни престъпления. Задълбоченият анализ на компютърните престъпления и тяхната уредба, има за цел да открие пропуските в наказателноправната регламентация в двете държави, в контекста на усложнената международна среда.

В заключение, се представя критичен анализ на правната уредба на компютърните престъпления в двете държави, като излага аргументирани препоръки за нормативни промени. Те се заключават в необходимостта от въвеждането на по-ясни и непротиворечиви дефиниции на техническите понятия, употребени в отделните състави; в синхронизация на националното право с международното такова; в премахването или усъвършенстването на разпоредби от процесуалните закони, които препятстват ефективното разследване на киберпрестъпленията.

6. Практическо значение на изследването

Дисертационният труд може да бъде използван като практическо ръководство за правоприлагащите органи, практикуващи юристи, експерти в областта на киберпрестъпността, както и за повишаване правната култура на всички граждани.

7. Методи на изследването

За да бъдат постигнати целите на научното изследване е използван комплексен метод на проучване, който включва:

- нормативен метод;
- историческия метод;
- системен метод;
- сравнително правен метод;
- формално-логически метод

В резултат на обширното изследване, са представени в систематизиран вид основните международни актове, които съдържат юридическата регламентация на отделните видове компютърните престъпления. Представени са правните конструкции на тези престъпления, закрепени в албанското и българското наказателно право. Авторът осъществява сравнително правен анализ на правната уредба на киберпрестъпленията в двете държави, като посочва недостатъците и прави препоръки за усъвършенстването й.

8. Обем и структура на изложението

Изследването се състои от уводна част, основна част и заключение, които са структурирани в седем глави.

В глава първа от изложението е изложено въведение в проблематиката. В глава втора авторът прави кратък исторически преглед на зараждането на киберпристъпността.

Международноправната уредба на компютърните престъпления е представена в глава трета от дисертационни труд, като са разгледани и различните международни органи в областта. Със следващите две глави е представен задълбочен анализ на различните състави на компютърните престъпления в албанското и българското наказателно право. Накрая на дисертационния труд, в глава шест и седем, авторът обобщава пропуските в наказателноправната уредба на компютърните престъпления и прави препоръки за изменения *de lege ferenda* в тях.

ГЛАВА II

ЗАРАЖДАНЕ НА КОМПЮТЪРНАТА ПРЕСТЪПНОСТ. ИСТОРИЧЕСКО РАЗВИТИЕ НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ

2.1. Кратък исторически преглед на появата на компютърната престъпност

Компютърната престъпност е сравнително ново явление в развитието на съвременното общество. Нейната поява се свързва с еволюционното достижение на човешката мисъл, а именно: създаването на световната информационна мрежа интернет в края на 50-те и началото на 60-те години на миналия век. Едно от първите наименования за компютърните престъпления е жаргонното понятия "престъпления на белите яки"[4], което няколко учени, сред които Едвин Сутерланд[5] използват при проведените в началото на XX-ти век изследвания за появата на киберпрестъпленията.[6]

Зараждането на компютърните престъпления се обуславя от прогресивното развитие на информационни технологии (ИТ) и тяхното широко приложение в различни сфери на обществения живот. С тези фактори се свързват първите престъпни посегателства извършени с помощта на компютри[7]. През 60-те години на миналия век се издават и първите научни изследвания и литература, в които се анализират отделни аспекти на компютърните престъпления. С развитието на информационните и компютърните технологии през 90-те години, ръстът на компютърната престъпност значително нараства, като се появяват нови форми на злоупотреби в киберпространството.

В международноправната доктрина изследователи участвали в редица изследвания на компютърните престъпления и киберсигурността са Дон Б.Паркър, Аугуст Бекуи, Джей Блумбърг, Стеин Счйолберг, Улрич Сиебер, Хенрик В.Касперсен, Пол Кюлен, Мария Копчева. Днес различните форми на компютърните престъпления, като проникване в компютърните системи, компютърните вируси, компютърните измами, извършени чрез използване на интернет технологиите, не предизвикват изненада в обществото. Историята на компютърните престъпления се превръща в история на статистиката за растежа на криминалните атаки в глобалните информационни мрежи. Компютърните престъпления са сравнително ново явление, което все повече застрашава нормалното функциониране на

---

[4]Wasik, M. Crime and Computer. Oxford, (1991) c.24

[5] Sutherland, E H, White Collar Crime - The Uncut Version, (1983), NCJ 091976

[6]Много автори определят компютърните престъпления като синоним на киберпрестъпления, вж Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing. и Копчева, М Компютърни престъпления. София (2006) с.13

[7] Krapac, D. Kompjutorski kriminalitet. Zagreb, (1992) c.15

обществените отношения в различните правни отрасли. В тази връзка, международната общност и суверенните държави все още не са достигнали достатъчно високо ниво на ефективна наказателноправна защита срещу нарастващите по вид и комплицираност злоупотреби в сферата на технологиите. Процесът на развитие на киберпространството и глобалната комуникация се отличава с изключителна бързина и динамика, поради което законодателят среща сериозни затруднения при създаването на адекватна правна уредба за регулиране и закрила на отношенията, възникващи в информационното пространство. За да бъдат практически приложими правните норми за компютърните престъпления, те трябва да бъдат съобразени със специфичните характеристики на тази категория престъпни посегателства, особената среда, в която те могат да бъдат извършени.

2.2. Основни понятия и термини в областта на компютърните престъпления

Развитието на компютърните технологии, освен приноса в световната икономика, доведе и до антисоциално и престъпно поведение , което се изразява в извършването на нови престъпни деяния, при които извършителите успяват да адаптират и осъществят традиционните престъпления по нетрадиционен начин, [8]в синхрон с технологичното развитие. Зависимостта на обществото от компютърните системи, води до нарастване на компютърните престъпления, които създават сериозни икономически щети и разходи по отношение на сигурността на потребителите. Това явление поставя под въпрос националната сигурност на повечето държави.

В правната доктрина се срещат различни концепции за същността на понятието „компютърно престъпление".В литературата термините, които се използват за описание на компютърните престъпления са толкова много на брой, колкото са и самите престъпления. Първите от тях са: "компютърни престъпления", "престъпления свързани с компютри" или "престъпление извършени от компютър"[9]. Често в научната литература, като синоним на термина компютърно престъпление, се използва понятието "киберпрестъпление". Следва да се има предвид , че между тях има някои различия. При компютърното престъпление, изпълнителното деяние се осъществява чрез компютъра, а при киберпрестъплението се използват компютърните системи за връзка към глобалната мрежа (Интернет). Киберпрестъпността е общо понятие, което обхваща всички форми на

[8] Vula.V. Kriminaliteti kompjuterik. Prishtina, (2009)c.26

[9] House Of Commons Standing Committee On Justice And Legal Affairs, Computer Crime, Final Report (1983), c.12

престъпност, извършени с помощта на компютърни мрежи. В правната доктрина се срещат различни концепции за същността на понятието "компютърно престъпление". При дефиниране на термина "киберпрестъпление" се изхожда от целта на използване на термина. Дори Европейската комисия по проблемите на престъпността към Съвета на Европа, не успява да изработи такова определение и предпочита да остави на отделните държави да тълкуват понятието и да го адаптират съобразно особеностите на техните правни системи и исторически традиции.

2.3 Кибернетично пространство (Виртуална правна реалност)

Кибернетичното пространство променя традиционното разбиране досежно значението на географските граници в общуването на хората, и поставя нова ера в комуникацията.

За престъпленията в кибернетичното пространство е характерно, че те са зараждат и еволюират в резултат на технологичното развитие в широка интерактивна среда, наречена "виртуално пространство". Те са генерирани от компютърна връзка с широко достъпната международна мрежа за обмен на информация и засягат всички правни отрасли и аспекти на обществените отношения. Основната проблема при изследването на престъпленията в кибернетичното пространство, е липсата на точни и адекватни дефиниции на различните форми на престъпни прояви и техните специфични елементи, както от вътрешното наказателно право, така и от международното право. В българската правна доктрина, Проф. Кискинов използва редица специфични термини като: „виртуалнопространство"[10];„правна реалност"[11]; „виртуална правна реалност"[12]; „виртуална среда"[13]. Той разглежда „ виртуалната правна реалност" като теоретичен модел, анализирайки я първоначално чрез езиковото тълкуване. Също така авторът преминава през философската хипотеза на "трансцендентната идеална реалност като абсолютно независима и неизразима, приближавайки до нейните качества на виртуалната

[10] Кискинов, В. Правна система. Онтодология и методология. (2006) с. 227-231 и Цакова, Ирина. Интернет право. бг . София, (2014) с.43

[11] Кискинов, В. „Правна информатика". София, V издание, (2012), с.63 - 69

[12] Кискинов,В. Към понятието за виртуална правна реалност – Съвременно право, № 3 (2014), с.7 - 25

[13] Кискинов, Вихър. Юридически модел на действие на правната система във виртуалната среда – Юридически свят. № 2 (2013), с.23 - 56

реалност в настоящото си битие, но далеч от божествените черти". Авторът Хаген[14] пък прави по- широко тълкуване на понятието виртуалната реалност като счита, че то: "*включва всички компютърно генерирани светове, в които зрителят може да влезе и да ги промени чрез въображението си*."

Предвид становищата на различните български и чужди автори, виртуалната реалност може да бъде определена като: *среда, в която се обединяват различните сетивни възприятия, като зрение, слух, допир, като те се симулират, за да се пресъздаде реалността, в която потребителят само частично контролира*[15] *компютъра, и в която самия той привидно има "естествено" участие.*

2.4. Действие на правната система във виртуалната среда

Действието на правната система протича в материалната и във виртуалната среда, като то се осъществява чрез социални, психологически и специални юридически механизми [16].Виртуалната среда или виртуалната реалност се определя като нефизическа реалност, създадена посредством информационни и комуникационни технологии. Тя е относително независима от материалната действителност, защото има нематериални основи[17] .Действието на правната система във виртуалната среда се осъществява, чрез електронната форма на правните волеизявления, като участващите правни субекти нямат непосредствен контакт. Различните форми на престъпна дейност, осъществявани в областта на информационните технологии, изискват законодателят да въведе адекватни правни норми, които да регулират правните отношения възникнали във виртуална среда и да предоставят необходимата закрила. Правните разпоредби, чрез предвидените в тях наказателни санкции , влияят върху поведението на правните субектите във виртуалното пространство и са основна предпоставка за осъществяване на правомерни юридически действия.

2.5. Етиологични характеристики на компютърните престъпления

---

[14] Hagen, Charles. New York Times. July 5, 1992. Section 2, c. 19

[15] Spring, Michael B. "Informating with Virtual Reality" in S. Helsel & J. Roth. (ed.) Virtual Reality: Theory, Practice, and Promise Meckler Publishing, (1991) c. 7-9

[16] Цит Кискинов, Вихър. Юридически модел на действие на правната система във виртуалната среда – Юридически свят. № 2 (2013), стр 23

[17] Пак там с.27

За да се извърши едно компютърно престъпление е необходимо да се изпълняват кумулативно три предпоставки, които са:

1.**Мотивация**, която формира в съзнанието на извършителя желание и воля да извърши престъпното действия. Като цяло мотивацията може да бъде породена от: *финансови* причини (нелоялна конкуренция, финансова несъстоятелност); *идеологически* причини (политически, религиозни); *психически* (синдром на милостта, заболяване)

2.**Готовност** на извършителя да приеме последиците от неговите престъпни действия.

3.**Възможност** на извършителя да осъществи криминалното деяние. Възможността е свързана не само с физическите способности на субекта, но и с неговата професионалната подготовка в областта на информационните и компютърните технологии.

Криминалистичната характеристика на компютърните престъпления обхваща три групи обстоятелства, а именно:

1.способ на извършване;

2.обстановка на извършване на деянието (място и време);

3.способ на укриване на престъплението (обичайни способи и програмно-технически способи).

ГЛАВА III

ПРАВНА УРЕДБА НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ В МЕЖДУНАРОДНОТО ПРАВО.МЕЖДУНАРОДНИ ОРГАНИ С КОМПЕТЕНТНОСТ В ОБЛАСТТА.

3.1. Въведение

Информационните и компютърните технологии са средство за общуване, което по своя териториален обхват и приложимост отдавна е надхвърлило границите на държавите. Компютърните престъпления, предвид глобалните им измерения, не могат да бъдат предмет единствено на наказателноправната уредба на националните държави. Множеството инициативи и политики от страна на международната общност, усилията, които тя полага за насърчаване борбата с киберпрестъпленията, взаимното сътрудничество и обмяната на информация , водят до по-ефективни резултати.

Суверенните държави, от своя страна, трябва да хармонизират националните си законодателства, в съответствие с юридическа уредба в международното право. Киберсигурността се очертава като основен, глобален проблем, който засяга цялата световна общност. Познатият до сега международен ред се променя драстично под влияние на прогресивното информационното развитие.

3.2 Организацията на обединените нации и нейната дейност в областта на компютърните престъпления

След като се сблъсква със сериозните последици, които нанасят киберпрестъпленията, международната общност насочва усилията си към създаване на глобална култура по киберсигурността. В тази връзка, през 2013 г. генералният секретар на Организацията на обединените нации , Бан Ки-Мун заяви, че: "кибератаките имат потенциал да доведат до дестабилизация в глобален мащаб”. Организацията на обединените нации стига до извода, че киберсигурността има глобално значение, поради което международната общност трябва да предприеме необходимите мерки за ограничаване на киберпрестъпленията. ООН насърчава диалога и сътрудничеството между държавите-членки, за да се гарантира сигурна, спокойна и достъпна информационна и комуникационна среда. Общото събрание на ООН макар и не така видимо, повече от десетилетие обсъжда активно въпросите по киберсигурността. ООН винаги е била ключов орган и източник на легитимност в международното право.

3.2.1 Конференции на ООН

В съвременните международни отношения, една от най-важните форми на многостранна дипломация, са международните конференции. По своята същност, международната конференция е временен, колективен международен орган, организиран от субекти на международното право, в рамките на който се осъществява международно общуване. Организацията на обединените нации като най-значимата международна организация, организира и провежда редица международни конференции, на които се обсъждат проблемите на киберпрестъпността.

3.2.2 Резолюции на ОС на ООН

Резолюциите на Общото събрание, по съществото на дейността на ООН, имат характер на препоръки. Тези актове формулират правила за поведение, които имат нормативно въздействие, и могат да влияят на международните отношения и на поведението на отделни държави, без да се третират като право в същинския смисъл на думата. В правната доктрина, актове от тази категория са известни под родовия термин "меко право"(от англ.език *soft law*). В тази връзка, категорията soft law обхваща и резолюциите приети от Общото събрание на ООН в областта на киберсигурността, които съдържат правна регламентация на отделните видови компютърните престъпления. По-надолу ще бъдат представени най-важните от тях, които са структурирани с оглед предмета на регулиране:

3.2.2.1 Резолюции за създаване на глобална култура на киберсигурност и защита на критичната информационна инфраструктура.

- Резолюция 57/239 от 20 декември 2002г. относно създаване на глобална култура на киберсигурност
- Резолюция 58/199 от 23 Декември 2003 г. относно създаване на глобална култура на киберсигурност и защита на критичната информационна инфраструктура
- Резолюция 64/211 от 21 Декември 2009 г. за създаване на глобална култура на киберсигурност и национална самооценка на защитата на критичната информационна инфраструктура

3.2.2.2 Резолюции относно развитието в областта на информацията и далекосъобщенията в контекста на международната сигурност.

- Резолюция 53/70 от 4 декември1998 г.;

- Резолюция 54/49 от 1декември 1999 г.;
- Резолюция 55/28 от 20 ноември 2000 г.;
- Резолюция 56/19 от 29 ноември 2001 г.;
- Резолюция 57/53 от 22 ноември 2002 г.;
- Резолюция 58/32 от 8 декември 2003 г.;
- Резолюция 59/61 от 3 декември 2004 г.;
- Резолюция 60/45 от 8 декември 2005 г.;
- Резолюция 61/54 от 6 декември 2006 г.;
- Резолюция 62/17 от 5 декември 2007 г.;
- Резолюция 63/37 от 2 декември 2008 г.;
- Резолюция 64/25 на 2 декември 2009 г.;
- Резолюция 65/41 от 8 декември 2010 г.;
- Резолюция 66/24 от 2 декември 2011 г.;
- Резолюция 67/27 на 03 декември 2012 г.;
- Резолюция 68/243 от 27 декември 2013 г.;
- Резолюция 69/28 от 2 декември 2014 г.

Големият брой приети резолюции, сам по себе си, е достатъчен показател за съществено значение, което отдава световната организация на сигурността в този аспект.

3.2.2.3 Резолюции относно борбата с престъпната злоупотреба синформационни технологии.

- ✓ Резолюция 55/63 от 4 Декември 2000 г. ;
- ✓ Резолюция 56/121 от 19Декември 2001 г.

Двете резолюции на ООН акцентират върху необходимостта от засилена координация и сътрудничество между държавите-членки в борбата с престъпните злоупотреби с информационни технологии.

3.2.2.4 Резолюция65/230 от 21 Декември 2010г.за превенция на престъпността и наказателно правосъдие.

В посочената резолюция, Общото събрание на ООН отправя апел към специализираната Комисия по превенция на престъпността и наказателното правосъдие, в съответствие с параграф 42 от Салвадорската резолюция, да инициира задълбочено проучване по различните аспекти на киберпрестъпността.

3.2.2.5 Резолюция A/HRC/20/L.13 относно насърчаването, защитата и упражняването на правата на човека в интернет, приета на 20 юни 2012г. от Съвета на ООН по правата на човека

Съветът на ООН по правата на човека, като се ръководи от международно утвърдените стандарти за правата на човека и основните свободи, възприети във ВДПЧ, МПГПП и МПИСКП, както и останалите международни договори за правата на човека, потвърждава позицията на международната общност, че правата на човека трябва да се защитават и прилагат еднакво, както във физическия свят, така и във виртуалното пространство.

3.3. Други международни организации с правомощия в областта на компютърните престъпления

- Организацията на Северноатлантическия договор (НАТО)
- Съюзно командване по трансформация на НАТО
- Центъра за киберзащита на НАТО
- Европейския съюз (ЕС)
- Европейски център за борба с киберпрестъпността (ЕС3)
- Съветът на Европа
- Международна асоциация по наказателно право
- Организацията за икономическо сътрудничество и развитие (ОИСР)
- Интерпол
- Групата на осемте- Г8

ГЛАВА IV

ПРАВНА УРЕДБА НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ В РЕПУБЛИКА АЛБАНИЯ

4.1. Историческо развитие на правната уредба

Република Албания е една от първите държави, присъединили се към Конвенцията за престъпленията в кибернетичното пространство (ETS No.185). Тя ратифицира Конвенцията на 25.04.2002г. чрез нарочния Закон №.8888 "За ратифициране на Конвенцията в областта на престъпленията в кибернетичното пространство". През 2004г. Република Албания ратифицира и Допълнителния протокол към Конвенцията за престъпления в кибернетичното пространство досежно криминализирането на действия с расистки и ксенофобски характер, извършени чрез компютърни системи (ETS No.189). Законодателят при ревизията на НК, пресъздаде редица от нормите на Конвенцията във вътрешното право. Така например чл. 2 от Конвенцията намери израз в новия чл.192/б от НК, озаглавен „Нерегламентиран достъп до компютър“.

На следващо място се създадоха следните нови разпоредби:

- ✓ чл.293/а НК -„Незаконно прихващане на компютърни данни“;
- ✓ чл.293/б НК -„Посегателство срещу неприкосновеността на компютърни данни“; чл.293/ц НК-„посегателство срещу неприкосновеността на компютърни системи“;
- ✓ чл.293/ч НК -„злоупотреба с устройства“;
- ✓ чл. 186/а НК-„компютърна фалшификация;
- ✓ чл. 143/б НК -„компютърна измама“;
- ✓ В съответствие с чл.3 от допълнителния протокол се добави новата разпоредба на чл.74/а НК „компютърно разпространение на материали, които благоприятстват геноцид или престъпления срещу човечеството“;
- ✓ чл. 84/а НК „заплаха с мотиви на расизъм и ксенофобия посредством компютърни системи“;
- ✓ чл.119/а НК “разпространение на расистки или ксенофобски материали чрез компютърна система“.
- ✓ чл. 119/б НК „расистки и ксенофобски обиди чрез компютърна система“ ;

4.2. Правна уредба на новите технологии в Република Албания

С цел синхронизиране на националното законодателство с международното такова , в частност с европейското законодателство, беше създаден комплекс от нови закони, които да обхващат отношенията в областта на информационното общество, както и развитието на информационните и комуникационните технологии.

Правната уредба, която регламентира компютърните престъпления в Р. Албания, може да бъде обособена в две категории:

- първична правна уредба;
-вторична правна уредба.

Към категорията на първичната правна уредба спадат следните източници:

- Наказателен кодекс
- Наказателно процесуален кодекс
- Закон за защита на личните данни
- Закон за обществените поръчки
- Закон за електронните съобщения в Република Албания
- Закон за електронната идентификация и доверителни услуги
- Закон за електронния подпис
- Закон за електронния документ
- Закон за електронна търговия
- Закон за класифицираната информация „Държавна тайна“
- Закон за „Държавна база данни“

Към вторичната правна уредба се включват следните източници:

- ПМС относно „Документ за политиката за електронните съобщения в Република Албания“;
- Правилник относно „Управление на електронния документ в Република Албания“;
- Инструкция относно „ Удостоверение на копие в хартиен вид на електронния документ от публични институции;
- ПМС относно „Сигурността на класифицираната информация, "държавната тайна", които се създават , съхраняват, обработван или предават в комуникационните системи (INFOSEC);
- Правилник относно„ Администриране на системата за държавни база данни;

- ПМС относно "Създаване на регулаторен координационен орган на държавните бази данни "
- Стратегия за национална сигурност на Република Албания;
- Междуведомствена стратегия за информационно общество;
- ПМС относно „Създаване и функциониране на системи за съхранение на информация, непрекъснатост на труда и споразумения за нивото на обслужване“;
- ПМС относно „Документ за политиката относно кибер сигурността“;
- Заповед на министър-председателя за „Укрепване на прозрачността, чрез увеличаване използването на интернет и усъвършенстването на съществуващи интернет сайтове“;
- ПМС относно „Създаване на ведомства на информационни технологии и съобщения в отрасловите министерства и подчинени институции“;
- ПМС относно „Одобряване на общите минимални стандарти на персонала от ведомства на информационни технологии и съобщения (ВИТС) относно структуриране на организационни единици на ВИТС";
- Заповед на министър-председателя за „Администриране на онлайн портал за отказ на достъп до уеб страница с незаконно съдържание“;
- ПМС относно „Създаване на единна система за регистрация, удостоверяване и идентификация на потребителя при вземане на услуги“

4.3. Държавни органи с правомощия в областта на компютърни престъпления

Прогресивното развитие на информационните технологии , както и задълженията на Република Албания към европейските партньори в областта на киберпрестъпността, са едни от факторите, които доведоха до усъвършенстване на съществуващите държавни органи и до създаването на нови специализирани органи за борба с киберпрестъпността. Тяхната дейност е свързана с ефективното изпълнението на стратегическите политически документи и законите, които пряко се отнасят към защитата на комуникационните технологии и информация. Тези структури са:

- Главна дирекция „Национала полиция“
- Национална агенция за компютърна сигурност (ALCIRT)
- Национална агенция за информационно общество (AKSHI)
- Национален Електронно-Сертифициращ орган (AKCE)
- Орган по електронни и пощенски съобщения (AKEP)
- Дирекция по сигурността на класифицираната информация (DSIK)

- Главна прокуратура на Република Албания
- Държавна Агенция Национална Сигурност (SHISH)
- Министерството на отбраната (ММ)
- Генерален щаб на Въоръжените сили
- Цифрова Дирекция (DSH)
- Агенция за военното разузнаване и сигурност (AISM)
- Комисия за регулиране на електронните и пощенските съобщения(AKEP)
- Комисионера за защита на личните данни и правото на информация

4.4. Система и видове компютърни престъпления регулирани от албанското наказателно право.

В албанския наказателен кодекс е въведена диференциация на компютърните престъпления, в зависимост от ролята и начина на използване на информационната и компютърната технология. В албанското наказателно право, както и в българското право , компютърните престъпления са обособени в две основни групи:

1. същински компютърни престъпления (в тесен смисъл) и
2. несъщински престъпления (в широк смисъл)

Към тези две групи *de lege ferenda* следва да се добави трета група престъпни посегателства, към която да се отнасят онези престъпления уредени в НК, които поради развитието на информационни и компютърни технологии, биха се осъществили и посредством компютърна система, мрежа или интернет. Това разграничение е от съществено значение, за да се регламентира мястото на информационните и компютърните технологии при определянето на предмета на престъпното посегателство и състава на престъплението.

Според албанския НК ***към първата група*** престъпления се отнасят следните деяния:

1. нерегламентиран достъп до компютър - чл.192/б НК;
2. незаконно прехващане на компютърни данни- член 293/а НК;
3. посегателство срещу неприкосновеността на компютърни данни – чл.293/б НК ;
4. посегателство срещу неприкосновеността накомпютърнисистеми – чл.293/ц НК ;
5. злоупотреба с устройства- чл.293/ч НК ;

Във ***втората група*** са включени следните престъпленията:

1. компютърно разпространение на материали които благоприятстват геноцид или престъпления срещу човечеството – чл.74/а НК ;

2. заплаха с мотиви на расизъм и ксенофобия посредством компютърни системи – 84/а НК;
3. порнография– чл.117 НК;
4. расистки или ксенофобски материали чрез компютърната система – чл.119/а НК;
5. обида с расистки или ксенофобски подбуди чрез компютърни системи – чл.119/б НК;
6. кражба на електронни комуникационни мрежи-чл.137/а НК;
7. компютърна измама-чл.143/б НК;
8. компютърна фалшификация- чл.186/а НК;
9. нарушаване неприкосновеността на кореспонденцията чл. 255 НК;
10. неправомерно използване на телефонна комуникация- чл.275 НК;
11. незаконно използване на високите технологии-чл.286/а НК
12. сексуален тормоз- чл.108/а НК;
13. проституция (виртуална проституция)- чл.113 НК;
14. неправомерна намеса в личен живот- чл.121 НК ;
15. преследване (stalking) -чл.121/а НК;
16. разпространение на лични тайни- чл.122 НК;
17. финансиране на тероризма- чл.230/а НК;
18. заплаха заради служебното положение- чл.238 НК;
19. откриване на анонимни банкови сметки - чл.287/а НК;

В албанския НК съставите, които обхващат различните форми на престъпни действия, извършени чрез или срещу информационни и компютърни технологии, не са систематизиране в една глава от особената част на НК, а са добавени към съществуващите глави, в зависимост от предмета на посегателство.

ГЛАВА V

ПРАВНА УРЕДБА НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ В БЪЛГАРСКОТО НАКАЗАТЕЛНО ПРАВО

5.1.Създаване и развитие на правната уредба — исторически бележки

Законодателната уредба на компютърните престъпления в Република България след 1990г се сблъсква с първите компютърни престъпления, като измами с фалшиви кредитни карти, престъпни посегателства срещу електронните пощи и сайтове както на държавните органи, така и на частните субекти, разпространение на порнографски материали в интернет и пр. Това негативно явление "събуди" българския законодател, който осъзна сериозната необходимост от създаване на адекватна наказателноправна уредба на новите престъпни деяния. Това наложи въвеждането на съществени изменения в националното законодателство.Тенденциите в международното и европейското наказателно право за противодействие на компютърните престъпления поставиха българското законодателство пред необходимостта за изменение и допълнение на НК и НПК, като през различни периоди от време в парламента бяха внесени няколко законопроекта които се отнасяха до компютърните престъпления.

5.2.Система и видове компютърни престъпления по българския Наказателен кодекс

Системата на компютърните престъпления обхваща множество престъпни посегателства, предвид широкия кръг обществени отношения, които те могат да застрашат или увредят. Това са следните групи деяния:

1. Компютърни престъпления против неприкосновеността на кореспонденцията и на информацията в електронна форма (чл. 171 и чл. 319д НК);
2. Компютърни престъпления срещу икономическите отношения (чл. 216, ал. 3-6, чл.212а, чл. 246, ал. 3 , чл.319а, чл. 319 б, чл. 319в НК);
3. Компютърни престъпления против интелектуалната собственост(чл. 172а НК);
4. Компютърни престъпления, които се отнасят до създаването, предоставянето или разпространението на произведения с незаконно или неморално съдържание(чл.159 НК);
5. Специфични компютърни престъпления(чл. 313, чл.319г и чл. 319 е НК).

Уредбата на различните видове компютърни престъпления се съдържа на различни места в Особената част на НК, в зависимост от това дали са същински компютърни

престъпления или компютърни престъпления в широк смисъл. В Раздел IV, Глава 9 “а” от НК са регламентирани съставите на шест вида компютърни престъпления от т.нар. “чист вид”. Компютърните престъпления в широк смисъл са разпръснати в различни глави и раздели на НК. Същинските компютърни престъпления са нов вид престъпни деяния, породени от прогресивното развитие на компютърните и информационните технологии. Тяхната поява налага създаването на нови наказателноправни състави както на международно, така и на национално ниво, за да бъде осигурено нормалното функциониране на компютри, компютърни системи, компютърни ресурси и компютърни мрежи, както и правомерното създаване и ползване на информация.

Към тях се включват нерегламентираният достъп, промяна, повреда, унищожаване на данни или програми, въвеждането на "вирус" или разпространение на пароли В българското наказателно право към същински компютърни престъпления спадат изброените в Глава 9 “а” НК основни и квалифицирани състави, а именно:

1. *Член 319а НК- Престъпно копиране или използване на компютърни данни;*
2. *Член 319б НК- добавянето, промяната, изтриването или унищожаването на компютърна програма или данни ;*
3. *Член 319в- т.нар. “компютърен саботаж”;*
4. *Чл. 319 г НК-Престъпно разпространение на компютърни вируси в компютър или информационна мрежа;*
5. *Член 319д НК- Разпространение на компютърни или системни пароли*
6. *Член 319е НК - престъпното нарушаване на Закона за електронния документ и електронния подпис.*

Наказателен процесуален кодекс

В Глава четиринадесета, Раздел VIII на НПК е регламентиран процесуалния ред за използване на специални разузнавателни средства, които имат изключително важно значение при разследването на компютърните престъпления. Относимите норми към компютърните престъпления са: -чл. 172-чл.177 НПК

5.3 Правен анализ на процесуалните норми

Най- съществения недостатък на българското процесуално право, по отношение на компютърните престъпления, се съдържа не в материалното наказателно право, а в НПК. Както бе посочено по-горе в чл.172, ал.1 от НПК сред посочените специални разузнавателни средства, като технически средства и оперативни способи - наблюдение, проследяване, проникване, и проверка на кореспонденция и компютърна

информация,могат да бъдат използвани само при разследване на тежки умишлени престъпления.

Легална дефиниция на понятието "тежко престъпление" се съдържа в чл. 93, т. 7 от НК, според който*: " тежко престъпление е това, за което по закона е предвидено наказание лишаване от свобода повече от пет години, доживотен затвор или доживотен затвор без замяна".*

В чл. 172, ал. 2 НПК са изчерпателно изброени престъпленията от българския НК, при разследването на които могат да се използват СРС. Сред тях фигурира и Глава 9 "а" от НК, която съдържа повечето състави на компютърните престъпления. От друга страна, обаче, дори и посочени в разпоредбата на чл. 172, ал.2 НПК , тези престъпления не отговорят на критерия за "тежко престъпление" по смисъла на чл. 93,т. 7 НК, защото за тях се предвиждат наказания лишаване от свобода, които не надвишават пет години.

От тук следва, че е налице съществено противоречие между разпоредбите на НК и НПК и по отношение на тези престъпления не могат да бъдат използвани специални разузнавателни средства. Това от своя страна прави разследването на този вид престъпни посегателства почти невъзможно, защото те се извършват посредством компютърни системи и мрежи, а също се осъществяват в интернет средата. Посочените специфични особености на компютърните престъпления налагат използването на СРС, както при установяване на престъпната дейност по време на извършването й , така и за разследването й, след като вече е довършена. На практика обаче, разследващите органи и прокуратурата са ограничени от самия законодател , защото те нямат законово основание при да поискат издаване на разрешение за използване на СРС при разследване на компютърните престъпления. Дори и да поискат от съда такова, последният ще им откаже и то напълно законосъобразно.

Това налага законодателят в най-кратък срок да предвиди *de lege ferenda* изменения на относимите норми, които на този етап правят разследването на компютърните престъпления невъзможно, или значително затруднено.

5.4. Специална правна уредба на РБ относима към компютърните престъпления

- Закон за защита на личните данни и релевантни актове от Европейското законодателство във връзка със защита и неприкосновеността на личните данни
- Закон за електронните съобщения и релевантни актове от Европейското законодателство

- Закон за електронния документ и електронния подпис и релевантни актове от Европейското законодателство
- Закон за електронната търговия
- Закон за платежните услуги и платежните системи

5.5 Сравнително-правен анализ на правния режим на компютърните престъпления в Република Албания и Република България

Представеният, в предходните глави, последователен анализ на правната уредба на компютърните престъпления в законодателствата на Република Албания и Република България показва, че и двете държави са положили сериозни усилия да приведат вътрешното си право, в съответствие с международноправните норми в областта на компютърните престъпления. Двете държави са ратифицирали основните международни договори, които поставят основите в борбата с киберсигурността, имплементирали са съдържанието на тези актове и съдържащите се в тях дефиниции за основни понятия, свързани с компютърните престъпления.

На следващо място, те са създали специализирани държавни органи, чиято главна цел е противодействие и превенция на киберпрестъпността.

Достатъчни ли са обаче тези действия и осигурява ли вътрешното наказателно право на двете държави, адекватна наказателноправна закрила срещу новите форми на престъпна дейност ?

Към настоящия момент, отговорът и за двете държави е отрицателен. Това е така, защото те не провеждат последователна политика в областта на киберпрестъпността, която се проявява в честите изменения на наказателноправните норми, които в повечето случаи предизвикват не усъвършенстване на правната уредба, а напротив съществени противоречия в съществуващото законодателство. Като основен недостатък се откроява подходът на двете държави, да въвеждат относимите международноправни норми във вътрешното си право чрез буквалния им превод, без да отчитат специфичните езикови несъответствия, както и техническите особености на тези престъпления.

От сравнително-правния анализ на релевантното законодателство на двете държави, прави впечатление, че в Република Албания, независимо от посочените по-горе недостатъци на правната уредба, е създадена по-всеобхватна правна рамка за компютърните престъпления. Така например, в албанския НК са закрепени повече състави на компютърни престъпления, от предвидените такива в българското право. Някои от текстовете в албанското законодателство изобщо не присъстват в българския

НК. Такива са: компютърно разпространение на материали които благоприятстват геноцид или престъпления срещу човечеството; заплаха с мотиви на расизъм и ксенофобия посредством компютърни системи; обида с расистки или ксенофобски подбуди чрез компютърни системи; кражба на електронни комуникационни мрежи; неправомерно използване на телефонна комуникация; незаконно използване на високите технологии; сексуален тормоз ; проституция (онлайн)-; неправомерна намеса в личен живот ; преследване (stalking); финансиране на тероризма; откриване на анонимни банкови сметки. На следващо място, албанският НК, в сравнение с българския НК предвижда много по-тежка наказателна репресия за извършване на компютърните престъпления. Докато у нас, повечето наказания са глоби или лишаване от свобода в размер до максимум осем години, като преимуществено размерът е от една до три години, то албанският НК предвижда много по-висок размер на наказанието до максимум петнадесет години лишаване от свобода. По отношение на процесуалната уредба, албанският НПК отново съдържа повече процесуални правила, които имат приложение към компютърните престъпления и тяхното разследване. Разбира се, не бива са се отчита само количествения показател, защото в наказателното право е изключително важно правните разпоредби да бъдат качествено изработени и да осигуряват една практически реална приложимост и ефективност. Това може да бъде постигнато, когато законодателят създава ясни, непротиворечиви и съобразени с особеностите на престъпната дейност. Противния подход изпразва от съдържание наказателноправните състави и ги превръща в едни "кухи" конструкции без възможност за прилагане. Във връзка с процесуалните норми, съществен недостатък е анализираното в предходната глава несъответствие между НК и НПК досежно прилагането на СРС при компютърните престъпления. На практика, тези престъпления трудно могат да бъдат разкрити, ако разследващите органи и прокуратурата са лишени от възможността да използват този способ на доказване. Това "недоглеждане" при създаването и измененията на наказателното законодателство е типичен пример за липса на ясна политика и изобщо за разбиране на материята от законодателя. Представените по-горе положения сочат, че албанският законодател възприема много по-сериозно компютърните престъпления, третирайки ги като сериозна заплаха за сигурността на държавата, обществения ред и за правата на гражданите.

В България обаче, законодателят подценява високата обществена опасност на тези нови престъпни прояви, тяхната изключителна комплицираност и фактът, че те всъщност те са престъпленията на бъдещето. Тези престъпни прояви ще се модифицират и усложняват, тяхното осъществяване непрекъснато ще нараства, защото бъдещето са

информационните и комуникационните технологии. Ето защо, българската държава, още повечето като част от европейската общност, следва да преосмисли своя подход в борбата с киберпрестъпността и то своевременно, защото съществуващата наказателноправна уредба не осигурява необходимото ниво на закрила.

ГЛАВА VI

УСЪВЪРШЕНСТВАНЕ НА ЮРИДИЧЕСКАТА РЕГЛАМЕНТАЦИЯ НА КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ

Представеният в настоящото научно изследване всеобхватен анализ на правната регламентация на компютърните престъпления, както на международно ниво, така и в националните законодателства на Република България и Република Албания показва, че въпреки положените усилия от международната общност и националните държави, наказателноправна уредба на този нов вид престъпни посегателства не осигурява достатъчно висока и адекватна закрила. Със сигурност може да се приеме, че първите важни стъпки в борбата с киберпрестъпността са направени от международната общност и суверенните държави. Специфичните особености на компютърните престъпления , обаче, изискват по- голяма активност и ангажираност от страна на всички правни субекти в изследваната област, с цел усъвършенстване на съществуващите правни средства и механизми за противодействие на киберпрестъпността.

На първо място, при кодификацията на тези престъпни посегателства, задължително трябва да се отчитат техническите специфики на компютърните системи и мрежи, които променят традиционните разбирания досежно средата на осъществяване на престъпното деяние, неговия териториален обхват, средствата за извършване на престъплението и пр. В повечето европейски държави, законодателят е осъзнал, че тези особености заемат основно място при криминализиране на престъпното деяния, но все още не успява да намери достатъчно адекватен подход за правилното им отразяване в състава на престъпленията. Това налага при изработване на правната уредба, да се взема предвид професионалното становище и познания на специалисти от областта на компютърните престъпления, които да характеризират възможните начини и средства за извършване на престъплението и те да бъдат включени в основни и/или квалифицираните и привилегировани наказателноправни състави

На следващо място, главно във вътрешното право на изследваните държави, трябва да се въведат легални дефиниции на редица термини и понятия от областта. По отношение на вече формулираните в законодателната уредба легални определения , е необходимо да бъдат направени изменения, които да ги направят по- прецизни и по- ясни, за да се осигури непротиворечивото тълкуване и прилагане на закрепените състави, от съответните компетентните органи.

В българската правна уредба се наблюдава една терминологична непоследователност, като част от въведените понятия са непълни, използват се различни термини в отделните съставите на компютърните престъпления, за част от които има легални дефиниции, за други няма такива, което налага те да се тълкуват като синоними на закрепените в правна уредба понятия. Така например в чл. 93, т. 21 от НК е въведена легална дефиниция на понятието "компютърна информационна система", но в отделни състава е употребено понятието "компютър", което не е легално дефинирано. Независимо, че в правната доктрина двете понятия се считат за синоними, законодателят *de lege ferenda* следва да предвиди легално определение и на термина "компютър".

По отношение на друго понятие- "компютърни информационни данни", прави впечатление, че то е използвано само в текста на чл. 212а, ал.1 и ал.2 от НК. В другите състави са употребени термините " компютърни данни "и "данни" (чл.319б НК и чл. 319а НК), които отново се приемат за синоними. В посочения случай, ще бъде подходящо да бъдат направени изменения de lege ferenda, които да въведат във всички разпоредби на НК единствено понятието "компютърни данни".

В НК липсват дефиниции на други важни понятията като: "компютърни или системни пароли "(чл.319д, ал.1 НК), "обект на авторско или сродно нему право" (чл.172а, ал.1 НК), за които също следва да бъдат приети легални определения.

Посочените по-горе несъвършенства в правната уредба са показател за непоследователната и незадълбочена наказателна политика в областта. Такъв законодателен подход е недопустим , особено при нови престъпни състави, за които все още няма достатъчно съдебна практика по прилагането им.

В съставите на отделните видове компютърни престъпление, също се наблюдават съществени недостатъци, които водят до по-трудното им прилагане, изключват от приложното им поле възможни форми на изпълнителните деяния, не отчитат възможността от настъпване на неимуществени вреди от някои престъпления и пр. Пример за това са:

- Чл.319д НК, в който за специалния предмет на посегателството, а именно: " компютърни или системни пароли" не е въведена легална дефиниция в НК. На следващо място, в алинея 2 на разпоредбата е записано, че от престъпното деяние трябва да са настъпили *"значителни вреди"*, които според съдебната практика обхващат само имуществените, но не и неимуществени вреди. Като се има предвид неразривната връзка на личните данни със самата личност на физическото лице, осъществяването на престъпното деяние би довело по-скоро до настъпване на неимуществени вреди,

отколкото на имуществени. В тази връзка разпоредбата на чл. 319д, ал.2 следва да бъде изменена *de lege ferenda* по такъв начин, че да обхване хипотезите, в които настъпват именно неимуществени вреди. Към настоящия момент, редакцията на текста неоснователно превръща потърпевшите както в жертви на престъплението, така и в жертви на законодателното бездействие.

- Чл. 319а НК, който урежда нерегламентирания достъп до ресурсите на компютър , също се нуждае от прецизиране. Независимо, че при формулиране на този състав ,българският законодател се е ръководил от Конвенцията за престъпленията в кибернетичното пространство, отново е въведен в нормата неподходящ термин, а именно: "нерегламентиран достъп". В този смисъл Конвенцията използва термина "незаконен достъп", който много по-адекватно определя това изискване от обективната страна на състава. Така формулиран съставът изключва от обхвата си хипотезите, в които достъп до ресурсите на компютърни системи или мрежи е свободен или не е предвид изричен ред за него, като например при различните интернет уеб сайтове. Фактът, че при тях, правните субекти имат свободен достъп, не означава, че те могат да извършват всякакви действия по отношение на съдържанието им, като например да го изменят, изтриват и пр. Подобно действие също би било нерегламентиран достъп, макар и да е не е предвид изричен ред в закон или правилник, но това действие при сегашната правна уредба няма да бъде съставомерно по посочения текст от наказателния кодекс.
- Чл.212а НК, който регламентира компютърната измама, не е включено като форма на изпълнителното деяние- престъпното манипулиране на самата компютърна система, което предвид съвременното ниво на компютърните технологии, е често срещано явление. При това престъпление е крайно наложително да бъдат въведени квалифицирани състави, като например: при повторното му извършване; когато причинените от него вреди са в големи или в особено големи размери; когато е извършено от особен субект, като например системните администратори. Също така текстът не предвижда хипотеза, в която престъпното деяние засяга интересите на юридическите лица, което отново налага изменения на наказателноправната уредба.
- По отношение на престъпленията против интелектуалната собственост, предвидената уредба се нуждае от осъвременяване за да бъдат отчетени новите тенденции в областта и съответно да се предвиди адекватна закрила. Наказателните състави за тези престъпления са бланкетни, което създава още повече несъответствие между различните закони, което от своя страна препятства реализираното на наказателната отговорност на субектите на престъпленията. Необходимо е да се обхванат повече форми на изпълнителните деяния

на отделните престъпления против интелектуалната собственост, да се изчистят несъответствията в употребените термини и понятия, като се изхожда от международната уредба, в която в тази област е значително по-развита.

Не на последно място, законодателят в малко от съставите на компютърните престъпления въвежда като квалифициращо обстоятелство- осъществяването на престъпното деяние по поръчение или в изпълнение на решение на организирани престъпни групи. В повечето случаи, компютърните престъпления с по-висока степен на обществена опасност, се извършват именно от престъпни сдружения и групи. Това е така, защото те разполагат с необходимите финансови ресурси, за да организират престъпни канали за клониране и източване на банкови карти; незаконно източване на парични средства от банкови сметки; изготвяне на фалшиви парични знаци; създаване и разпространение на порнографски материали и пр. Организираните престъпни групи осъществяват престъпната си дейност, не само в самите държави, но и на международно ниво. Те разполагат с разработени мрежи от посредници и преки извършители във всички държави, като в повечето случаи те са добре образовани и интелигентни лица, а тези фактори допълнително затрудняват разследващите органи. Също така българският законодател е предвидил квалифицирани състави за повторното извършване на компютърните престъпления по НК, но не е въвел като квалифициращо обстоятелство хипотезата на опасен рецидив, което практически е често срещано явения. По този начин необосновано се стеснява приложното поле на съставите и не се осигурява необходимата закрила в такива случаи. Този факт налага *de lege ferenda* да се регламентират и квалифицирани състави за извършване на анализираните престъпления при условията на опасен рецидив, което обстоятелство се характеризира с много по-висока степен на обществена опасност, в сравнение с останалите случаи.

На следващо място, законодателството и в двете изследвани държави не предвижда квалифицирани състави за компютърни престъпления извършвани от особен субект- например длъжностно лице. Подобна хипотеза е напълно възможно с оглед широкото приложение на компютърните и информационните технологии във всички сфери на съвременния живот. Не бива да се подценяват сериозните негативни последици, които може да има едно компютърно престъпление извършено от такъв субект, предвид неговите функции в дадената сфера.

По отношение на режима на наказване на компютърните престъпления в българското законодателство също следва да бъдат направени изменения. Към настоящия момент, по българския НК за извършване на компютърно престъпление субектът на престъплението

се наказва най-често с наказание лишаване от свобода, кумулативно с глоба, или алтернативно на нея. Наказанието лишаване от свобода, макар и уредено в различни максимални срокове, не дава възможност повечето от тези общественоопасни деяния да се определят като тежки престъпления по смисъла на българския НК Всъщност това е най- съществено законодателно "недоразумение" в уредбата на компютърните престъпления в българското наказателно право, което се отразява както в практическото разследване и разкриване на тези престъпления, така и тяхната превенция. Както беше посочено по-горе в настоящото изследване, съществува несъответствие между нормите на НПК (чл.172, ал.2 НПК) и НК досежно прилагането на СРС за разследване на компютърните престъпления. Това на практика води до невъзможност за разследване на регламентираните в глава 9 "а" от НК компютърни престъпления, защото с предвидените в тях наказания, те не попадат в категорията " *тежко престъпление*" по смисъла на чл. 93, т. 7 НК. За практикуващите юристи е ясно , че при този специфичен вид престъпни посегателства, за да бъде предотвратено престъплението или за да бъде разкрито, разследващите органи и прокуратурата трябва да имат възможността да използват СРС, които ще им позволят правомерен достъп до компютърните системи и мрежи, законосъобразно проследяване на трафика и електронната комуникация и пр.. Тази възможност обаче е изключена от самия законодател, който въвежда противоречиви, неясни и непрецизни изменения в наказателноправната уредбата.

Ето защо, законодателят трябва да отстрани *de lege ferenda* този съществен порок, който обективно препятства разкриването на компютърните престъпления и прави неефективна битката с киберпрестъпността.

Сравнителноправният анализ на законодателствата на Република България и Република Албания показва, че във всяка от държавите е възприет опитът на международната общност в областта, като някои от разрешенията на проблематиката са по-добре уредени в албанското право, а други такива в българското законодателство. В тази връзка следва да се има предвид, че между двете държави през 2007г. е сключено споразумение за сътрудничество в областта на борбата с тероризма, организираната престъпност, незаконния трафик, както и други престъпления , включително разкриване и разследване на лица и организации, свързани с компютърни престъпления и престъпления срещу интелектуалната собственост. Този акт предоставя възможност на анализираните страни да осъществяват по-тясно сътрудничество по отношение на законодателната регламентация и прилагането на съставите за компютърни престъпления, както и обмен на нови идеи по отношение на правните механизми за закрила от киберпрестъпленията. Ето

защо, държавите следва да се възползват от този правен инструмент и своя опит , за да постигнат по-добри резултати в борбата с киберпрестъпността.

Всички представени по-горе обстоятелства имат значително негативно влияние, като затрудняват реализирането на наказателната отговорност на субектите на престъплението, стесняват неоправдано обхвата на наказателноправните състави и ощетяват пострадалите от компютърните престъпления.

ГЛАВА VII

ЗАКЛЮЧЕНИЕ

Борбата с киберпрестъпността е едно от новите и най-интересните предизвикателства пред човечеството. Тя изисква обединяване на усилията на всички правни субекти (международни и национални), за да се постигне усъвършенстване на създадените правните средства и механизми. Компютърните и информационните технологии се отличават с прекалено динамично и устойчиво възходящо развитие, което не търпи консервативен и статичен законодателен подход.

Международната общност постави основите на правната рамка за компютърните престъпления, чрез приетите международни договори и конвенции, осъзнавайки необходимостта от по-голяма ангажираност в областта. Суверените държави, в случая Република Албания и Република България, изпълниха задълженията си към международните партньори, като въведоха международноправните норми във вътрешното си законодателство. Този процес, обаче, не би могъл да бъде определен като достатъчен. Това е така, защото двете държави въведоха в материалното си право новите престъпни състави като буквален превод от международните конвенции, и при създаването на разпоредбите за компютърните престъпления не се отчитаха специфичните особености на новите престъпни посегателства. На следващо място, процесуалните правила относими към разследването на престъпленията, също не осигуряват адекватна правна рамка. Този законодателен подход, възприет в двете изследвани държави, прави наказателноправната закрила неефективна. Това от своя страна, подкопава общественото доверие към правораздавателната система и възможността й да гарантира равенство пред закона и справедливост.

Ето защо, изключително важно е двете държави да усъвършенстват вътрешното си законодателство, като изхождат от международните стандарти. Последните въвеждат по-високо ниво на закрила, в сравнение с осигуреното в националното им право.

Водещо място заема изискването двете държави да провеждат последователна политика в областта на компютърните престъпления, да въведат легални определения на основните понятия и да прецизират съществуващите такива, както и да съобразяват съставите на отделните видове престъпления със спецификите на компютърните престъпления. Това е единственият възможен и правилен подход, който ще гарантира сигурността и правата на гражданите в съвременната комуникационна и информационна глобална общност.

ПУБЛИКАЦИИ НА АВТОРА ПО ТЕМАТА НА ДИСЕРТАЦИЯТА

1. *Cybercrimein Albania, a discouse on law, policyandpractice,* Towards future sustainable development, University of Shkodër "Luigj Gurakuqi" Shkoder, Albania, 2012.
2. *Phenomenologicalaspectsofcomputer crime againstintellectualproperty,* Media & Mass Communication, International Scientific Event, Бургас,България, 2014
3. *Justice in The Digital Era - bridging the gap between law and information technology,*The State, Society and Law: Regional Cooperation, Aleksandër Moisiu University of Durrës, Albania, 2014
4. *Piracy as a special form of computer crime against intellectual property,* „102 vjet shtet shqiptar e më pastaj – Çështja shqiptare dhe Derrallaj"Center for international relationship and Balkan study Republic of Macedonia, Tetovo, Macedonia, 2014
5. *Functioning of a legal system in the virtual space,*Democracy in South Eastern Europe and Albanian factor, International Scientific Conference University of Prishtina, Kosovo, 2015
6. *Cyber terrorism as a serious threat to humanity,* V-thNational Conferenceof PhD students inthe field of legalsciences, Instituteof State and Lawat the Bulgarian Academyof Sciences, "Sunny Beach", Nessebar Municipality.Burgas – Bulgaria, 2015
7. *Modeling ethical behavior in Albanian Public Administration,* 9th Trans European Dialogue Conference-TED 9, University of Ljubljana, Slovenia, 2016
8. *Legal framework of bilateral relations Bulgaria – Albania,* Bulgaria and the Balkans in a dynamic international environment, Law Faculty of Plovdiv University, Bulgaria, 2016
9. *Ethics code in the Republic of Albania and their application,* International Seminar "Soft Law and Development of Contemporary Law", Law Faculty of Plovdiv University, Team of Researchers and European Law Student's Association – Plovdiv, Bulgaria, 2016