БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ

ИНСТИТУТ ЗА ДЪРЖАВАТА И ПРАВОТО

СЕКЦИЯ ПО ГРАЖДАНСКОПРАВНИ НАУКИ

Калоян Руменов Монев

ОТГОВОРНОСТ ЗА ВРЕДИ, ПРИЧИНЕНИ ЧРЕЗ ИЗПОЛЗВАНЕ НА КОМПЮТЪРНИ СИСТЕМИ И ГЛОБАЛНИТЕ МРЕЖИ

А В Т О Р Е Ф Е Р А Т

на дисертационен труд
за присъждане на образователната и научна степен "Доктор"

Научна област: ш.3. Социални, стопански и правни науки
Професионално направление: ш.3.6. Право
Научна специалност: Гражданско и семейно право

Научен консултант доц. д-р Вълчин Даскалов

София, 2014 г.

Дисертационният труд е обсъден и насочен за публична защита от Секцията по гражданскоправни науки на Института за държавата и правото при Българската академия на науките на 23.04.2014 г.

Докторантът е зачислен като редовен докторант в Секцията по гражданскоправни науки на Института за държавата и правото при Българската академия на науките, и е отчислен с право на защита.

Изследванията по дисертационния труд са извършени главно в Института за държавата и правото при Българската академия на науките.

Защитата на дисертационния труд ще се състои на 24 септември 2014 г. в Института за държавата и правото при Българската академия на науките (гр. София, ул. „ Сердика” № 4) пред научно жури, назначено със Заповед №РД-09-42/20.05.2014 г. на зам.директора на Института, в състав:

Членове:

проф. д-р Поля Голева

проф. д-р Венцислав Стоянов

проф. д.ю.н. Методи Марков

доц. д-р Иван Иванов

доц. д-р Вълчин Даскалов

Резервни членове:

доц. д-р Захари Торманов

Дисертационният труд и материалите по защитата са на разположение в Института за държавата и правото при Българската академия на науките (гр. София, ул. „ Сердика” № 4), както и на интернет страниците на Института и на Академията.

Съдържание

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД..... 4

II. КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД..... 11

III. ПУБЛИКАЦИИ НА АВТОРА ПО ТЕМАТА НА ДИСЕРТАЦИЯТА..... 31

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Значимост на изследването

В последните три десетилетия информационните и комуникационни технологии навлязоха изключително широко в живота на съвременния човек, улесниха неговия бит, работа и общуване. В същото време тези постижения на техническия прогрес са свързани и с някои неблагоприятни последици, в това число създават нови форми на посегателства върху личността, тайната на кореспонденцията, собствеността. С помощта на компютърните системи и технологии, съчетани с „анонимността", която предлага световната Интернет мрежа, сме свидетели на редица нови и непознати до момента случаи на непозволено увреждане:

- нарушаване на неприкосновеността на личния живот на хората, правата на собственост и свободата на изразяването в електронна среда
- злоупотреби с личните данни на потребителите, включително кражба на самоличност, кражба на електронни пари
- нарушаване тайната на електронната кореспонденция
- нарушаване на правата на интелектуална собственост при компютърното пиратство
- нови измамни схеми по Интернет обхващащи голям брой пострадали лица

При всички описани случаи може да открием сходство в начина и средствата за осъществяване на деянията, а именно – чрез използване на компютърни системи, мрежи и Интернет базираните услуги като електронна поща, социални мрежи, търсачки, блогове и форуми.

Проблемите на гражданската отговорност, на двата й подвида - договорната и деликтната, са едни от най-сложните въпроси на гражданското право. На тях са посветени голям брой научни трудове и разработки в чуждестранната и наша правна литература. Голяма част от тези разработки обаче, особено българските източници, не касаят директно проблемите на деликтното право в електронна среда. При разработката на настоящата дисертация задълбочено бе проучена относимата българска и чуждестранна литература, както и съдебната практика. Съществуващата правна регламентация в тази област на живота в повечето случаи се оказва неспособна да реагира адекватно на измененията в обществените отношения, настъпили в резултат на описаната „цифрова" революция. Вероятно ще изминат много години, преди правото като обществен регулатор да „догони" и уреди напълно обществените отношения и проблемите свързани със съвременните технологии, ако въобще е възможно да се случи. Това „изоставане" създава редица

проблеми на специалистите, работещи в сферата на информационните технологии, и изобщо на всички потребители. Те следва да познават правната регламентация на своите действия в мрежата, да са наясно с последствията и отговорностите от тях.

Вниманието към дисертационната тема се предопределя не само от актуалността на така определения предмет, но и от факта, че правната същност и особеностите на гражданската отговорност в електронна среда досега не е изследвана цялостно в българската правна доктрина, не е отделено необходимото внимание за изясняване на теоретичните и практическите проблеми, които тя поставя. Поради тези причини значимостта на изследването се определя и с оглед стремежа му да запълни тази празнота и да снабди правната теория и практика с анализ на поставените въпроси.

2. Предмет и задачи на изследването

Основен предмет на изследване в дисертационния труд е отговорността при непозволено увреждане в една особена хипотеза - чрез използване на компютърните системи и технологии. За терминологично улеснение в работата се използва фразата „отговорност в електронна среда", като се има предвид именно гражданската отговорност за вреди, причинени чрез използване на компютърните системи в глобалните мрежи и киберпространството.

Темата за дейностите в електронна среда е изключително обширна и засяга много области на живота и правото, включително гражданското, наказателното и административно право. Чести са случаите, когато електронната среда се използва за извършване на престъпления. Изследваната в дисертацията наказателно-правна теория и системата от компютърни престъпления служат единствено като база за сравнително-правен анализ, анализирайки възможностите за комбиниране на наказателната с гражданската отговорност. По същия начин стои и въпросът с очертаните хипотези на договорна отговорност. Доколкото такива разпоредби са цитирани, то е с оглед пълнотата на изследването, като подобни препратки нямат претенции за изчерпателност и задълбоченост.

Използвайки характеристиките и дефиницията на специфичните деяния при компютърните престъпления, за целите на дисертацията, се дефинира едно ново и непознато до момента за българската правна доктрина понятие – *компютърен деликт*. Дори и да не съдържа характеристиката на изцяло нов подвид деликтна отговорност, то е *приносно и знаково* за смисъла и значението което носи, а именно хипотези на непозволено

увреждане, извършени при или по повод използването на компютърните системи и глобалната мрежа. Идеята за неговото бъдещо развитие, систематизация, характеризиране и употреба е рационална и практична, отговаряща на съвременните тенденции в развитието на правото. Дисертацията има за цел да даде най-обща правна характеристика на термина и да постави началото на обособяването му като правен институт с голямо обществено и практическо значение, да предложи изходните опорни точки, да постави началото на дебат по тях сред българската юриспруденция. Подробно са изследвани въпросите и хипотезите на компютърния деликт, регулацията на дейността и отговорността на Интернет-доставчиците. Към последния въпрос има висок обществен интерес, свързан и с Международното търговско споразумение за борба с фалшифицирането между Европейския съюз и неговите държави-членки, Австралия, Канада, Япония, Република Корея, Мексиканските съединени щати, Кралство Мароко, Нова Зеландия, Република Сингапур, Конфедерация Швейцария и Съединените американски щати – АСТА, както и с Договора от Пекин приет в началото на 2014г.

Цел на изследването е въз основа на съществуващите нормативни актове, теоретични разработки и съдебна практика /национална и чуждестранна/ да се изведе правната същност на този нов и специфичен подвид деликтна отговорност като се посочат и неговите характеристики. Работата доказва, че тази отговорност по своята същност принадлежи към категорията на гражданскоправната отговорност и към нея субсидиарно следва да се прилагат гражданскоправните норми. Наред с това, изложението анализира специфичните особености на този вид отговорност, търси нейното място в системата на гражданската отговорност и има за цел да ги подчертае и индивидуализира като самостоятелен вид отговорност и съответно да аргументира необходимостта от по-детайлна нормативна регламентация, която да съответства на обществените нужди. Тъй като правният режим на гражданската отговорност в исторически план е създаден по време, когато в българския правен мир липсват отношенията на непозволено увреждане чрез използване на компютърни системи, на договори сключвани през Интернет, изобщо на гражданскоправни отношения в електронна среда, тези правни норми не могат да отговорят напълно на спецификата на тези отношения. В тази връзка са направени и редица предложения de lege ferenda, които се опират не на последно място на богатия чуждестранен опит в тази област. Като най-честа база за сравнително-правни изследвания послужиха законодателствата на САЩ, Великобритания, Австрия и Естония. Обърнато е специално внимание също така и на общоевропейското законодателство регулиращо поведението на потребителите в Интернет.

Основна научна задача на дисертацията е да обърне специално внимание на българското законодателство и доктрина към осъвременяване законовата уредба на гражданската отговорност, в двата й основни вида към намиране на рационални начини за обезщетяване на вреди причинени в електронна среда. Изпълнението на посочената задача би допринесло за създаване на един систематичен правен режим, който да съответства на функциите на този вид отговорност. За постигане на горния резултат са изследвани и следните по – конкретни научни въпроси:

1. Да се установи какви са правно-теоретичните постановки на проблема на компютърните деликти съгласно действащото право - българското и приложимото европейско законодателство;
2. Анализирани са правните особености на субектите и обектите на отговорността;
3. Анализирани са предпоставките за възникване на отговорността с акцент върху спецификата им – вредите и деянията проявяващи се само в електронен вид;
4. Проучени са различните правни възможности за ограничаване, намаляване и изключване на отговорността, коментар на проблема за нейното трансгранично проявление;
5. Изследване на материалноправните предпоставки за възникване на отговорност за причинени вреди в електронна среда, да се посочат проблемите при реализирането й;
6. Приложението на електронните доказателства при реализация на отговорността за компютърен деликт.

3. Методи на изследване

Методологическа основа на изследването са общите и специални методи за научни изследвания каквито са историческия, системноправния, и аналитично критичния метод. Те намират съответно приложение при установяване на общата правна регламентация на тези обществени отношения, при проследяване на историческите и социално-икономическите предпоставки за пораждане и развитие на техниката и технологиите, при съпоставянето на този род отговорност със сходни правни фигури и при разглеждане на особеностите и режима им в различни правни отрасли. Особено място заема сравнително-правният метод относно теоретичните виждания и нормативна уредба на гражданската отговорност за вреди в електронна среда в чужди

законодателства от континенталната правна система и от системата на Общото право. Водещо място заема методът на индукцията, при който от конкретно проявеното се прави логически общ извод за съдържанието и характера на изследвания обект, от който проявеното е част.

4. Научна новост и приносен характер на труда

Представеният дисертационен труд съдържа следните научни приноси:

1. За пръв път в българската правна доктрина се прави опит цялостно и на монографично ниво се разгледат и изяснят въпросите, свързани с новите форми на отговорност за вреди причинени в електронна среда. Проблемът досега не е бил обект на самостоятелно научно изследване и това дава възможност да се развият тези с приносен характер в теорията на българското облигационно право относно:

- Правната същност и понятие за видовете увреждания, причинени чрез използване на компютърните системи и глобалните мрежи;
- Предложение за дефиниране на нов, специфичен подвид деликтна отговорност в електронна среда – компютърен деликт и очертаване на неговите характерни белези. Предлага се идея и поглед към разширяването й към обективната и безвиновна отговорност на определен кръг субекти - собствениците на компютърните системи и титулярите на IP адреси от които е извършено вредоносното деяние, родителите или попечителите предоставили електронно устройство на своите непълнолетни деца, от което е причинен компютърен деликт;
- Критичен анализ на възможните начини и способи за реализиране на гражданска отговорност за този род деликти, обосновка на възможните граници на отговорноста и нейния трансграничен характер;
- Предложения за определяне на справедливо обезщетение за пострадалите лица в законово определени минимални размери;
- Използване на специфичните електронни средства като електронните доказателства и компютърната съдебна експертиза в процеса на реализация на отговорността за компютърен деликт;

2. Предложено е задълбочено изследване на някои основни хипотези на компютърния деликт, като е обърнато специално внимание на тяхната специфика проявяваща се единствено в електронна среда. Разгледани са хипотези на компютърен

деликт при неправоремен достъп до чужда компютърна система, компютърните измами, нерагламентираното изпращане на СПАМ и компютърното пиратство.

3. Направено е актуално изследване на Търговското споразумение за борба с фалшифицирането – АСТА, което е опит за нов тип регулация в отношенията възникнали по повод фалшифицираното на търговски марки и нарушаването на авторски права, не само в глобалната мрежа, а по принцип. То дава една действително модерна правна уредба на отношенията по повод реализиране на гражданската отговорност за обезщетяването на вредите.

4. Направен е анализ на правната същност на дейността на Интернет доставчиците, посочена е нормативната им регулация и са дадени нужните легални дефиниции. Изложени са вероятни хипотези на възникване на гражданска отговорност в отношенията между потребителите и Интернет-доставчиците, разгледан е режима на приемане на Общи условия и последствията от това. Очертани са случаите при които законът предвижда неотговорност на тези лица за причинени вреди на потребителите. Отделно като екскурс е разработен актуалния проблем за защита на потребителите при сключването на сделки в Интернет.

5. Практическо значение на труда

Разгледаните в изследването въпроси имат не само своето теоретично значение за разбиране същността на гражданската отговорност в електронна среда, но и практическа стойност. Съобразно това предложените изводи биха могли да послужат за усъвършенстване на правната уредба на разглежданите явления. Същевременно систематизираната и анализирана в изследването практика и направените въз основа на това предложения за решаването на реално възникващи или възможни проблеми във връзка с изследваните явления, биха могли да послужат, както на практикуващите юристи и на студентите по право, така и на всички, които проявяват интерес към разглежданите актуални на съвремието ни проблеми.

Правят се редица предложения за допълване и усъвършенстване на законодателството, които ако бъдат възприети ще се достигне до ясното, точно и непротиворечиво уреждане на един самостоятелн правен режим на нов подвид деликтна отговорност – компютърния деликт. Предложенията *de lege ferenda* могат да се обособят в три категории: предложения за запълване на празнини със структурно значение, които имат за задача да придадат систематичен характер на правния режим (напр.

регламентиране на компютърния деликт в Закона за задълженията и договорите, законовата забрана за изпращане на СПАМ, нови задължения на Интернет доставчиците по отношение предотвратяване на компютърните измами и др.). Към втората категория спадат предложения, които имат за цел да подчертаят и засилят обезщетителната функция на отговорността (напр. въвеждане на обективна отговорност на собствениците на компютърните системи, включително родителите, от които е причинено деянието, твърди размери на обезщетенията при СПАМа, компютърното пиратство и др.). Към третата категория спадат предложения, имащи чисто технически характер или отнасящи се до други, сходни правни фигури (напр. нови законови възможности за използване на електронните доказателства в съдебния процес, правна регламентация на компютърната съдебна експертиза, разширяване на обхвата на представяните пред съда електронни доказателства др.).

6. Обем и структура на дисертацията

Дисертацията е с обем 176 страници самостоятелен текст, допълнително съдържание, приложения и списък на използваната литература. Общия обем е 199 страници. Направени са общо 274 бележки под линия. Като библиография са цитирани 57 български и 23 чужди литературни източника. В приложение към дисертацията има 10 фигури и диаграми, както и допълнително разработен проблем по темата в екскурс.

В структурно отношение изследването включва увод, четири глави и заключение. В структурата на всяка глава са обособени отделни параграфи. Параграфите съдържат отделни тематично структурирани заглавия, означени с арабски цифри и подзаглавия, означени с арабски цифри.

II. КРАТКО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава I. ПРАВНА СЪЩНОСТ НА ОТГОВОРНОСТТА ЗА ВРЕДИ И НЕЙНАТА СПЕЦИФИКА В ЕЛЕКТРОННА СРЕДА.

Във встъпителната глава най-общо са очертани правната характеристика на гражданската отговорност, нейните видове, правен режим и тенденции. Подходът към изследването на гражданската отговорност за вреди чрез използване на компютърните системи и мрежи, изисква като начало да се разкрият общите признаци с юридическата отговорност и на тази основа да се търсят и изследват нейните специфични признаци. Последните следва да се търсят в начина, съдържанието и обекта на възникващите правоотношения. Прилагането на такъв структурен подход към изследването се предопределя от сложния строеж на юридическата отговорност като система от правоотношения. Именно характерните белези на нейните начин на възникване, съдържание и обект на закрила съставляват основа на специфични характеристики, които позволяват да се търси видовата ѝ принадлежност и конкретни особености. За да може да се дефинира спецификата на отговорността за вреди в електронна среда, с оглед пълнота и въвод в §1 са разгледани някои общи теоретични постановки. Посочени са приложимите към поставения проблем норми de lege lata като Закона за задълженията и договорите, Закона за отговорността на държавата и общините за вреди, Закона за защита на потребителите и др. Даден е кратък анализ на въпросите свързани с хармонизацията на българското с европейското право по повод случаи на непозволено увреждане при: отговорност за вреди причинени от стоки, обективна отговорност в областта на обработката на лични данни, включително и в електронна среда, отговорност при дискриминация по пол, защита на конкуренцията и отговорност на държавата за вреди. Посочени са конкретни европейски нормативни актове свързани с посочената проблематика като ДИРЕКТИВА 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ДИРЕКТИВА 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации, ДИРЕКТИВА 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи.

От съществено значение за правното регулиране на хипотезите на непозволено увреждане е и съдебната практика. Без да е източник на правни норми тя, по пътя на правоприлагането, е натрупала богат опит, конкретизирала е и правно е интерпретирала законовите правила. За целите на дисертацията са проучени и анализирани стотици съдебни актове, на най-различни по ранг съдилища в България, Съдът на Европа, някои съдебни решения от САЩ, Естония, Австрия и Великобритания. Следва да отбележим, че именно съдебната практика е важен показател за развитието на цитирания правен институт, защото посочените законови норми обективирани в ЗЗД, не са изменяни от влизането в сила на закона през 1950г. Независимо от богатата обща практика обаче, както и при договорната отговорност и тук, български съдебни решения по казуси за търсене на обезщетения и реализиране на имуществени права, свързани с вреди причинени по електронен път, чрез използване на компютърните системи и мрежи, са изключително малко. В този смисъл, няма и изградено единно становище на правоприлагащите и съдебните органите по въпросите за обезщетяване на вреди причинени в електронна среда. Констатира се, че именно случаи на засегнати неимуществени субективни права, права на интелектуална собственост, неприкосновенност на електронната кореспондеция, на електронната идентичност, преобладават при вредите от непозволено увреждане нанесени по електронен път. Относно вида на репарираните вреди, интерес представлява разгледаното ТР №4/2012г на ОСГТК на ВКС, в което съдът за първи път приема, че е допустимо присъждане на обезщетение за неимуществени вреди при договорна отговорност. По натам в изложението се спирам на общата характеристика на отговорността за вреди, нейните функции, момент на възникване, видове.

В §2 се разглежда спецификата на отговорността за вреди в областта на компютърните системи и Интернет, именно тук се дава предложение за дефиниране на нов подвид деликтна отговорност наречена компютърен деликт. За изясняване на специфичната материя в областта на компютърната техника и компютърното право използвани в разработката се анализират легалните дефиниции в областта на компютърно-информационните технологии / компютърна система, компютърни данни и компютърна мрежа/, а след това фактическия състав за възникване на отговорността, неговото съдържание, общи и специфични елементи. Използвайки характеристиките и дефиницията на специфичните деяния при компютърните престъпления, в т.2, се дефинира едно ново и непознато до момента за българската правна доктрина понятие – *компютърен деликт*. Посочва се, че дори и да не съдържа характеристиката на изцяло нов подвид деликтна отговорност, то е *знаково* за смисъла и значението което носи, а именно хипотези на непозволено увреждане, извършени при или по повод използването на компютърните

системи и глобалната мрежа. Идеята за неговото бъдещо развитие, систематизация, характеризиране и употреба е актуална, необходима и отговаряща на съвременните тенденции в развитието на правото. Дисертацията има за цел да даде най-обща правна характеристика на термина и да постави началото на обособяването му като правен институт с голямо обществено и практическо значение, да предложи изходните опорни точки, да постави началото на дебат по тях сред българската юриспруденция.

Дефинирайки компютърния деликт в най-широк смисъл, се посочва че това са хипотези на деликти, които по един или друг начин са свързани с употребата на компютри, компютърни мрежи и изобщо на съвременните информационни технологии. По своята правна същност компютърният деликт се явява специфична хипотеза на общия гражданско-правен деликт. Общия фактически състав на отговорноста за непозволено увреждане включва пет елемента: деяние, противоправност, вина, възникнали вреди, причинна връзка между деянието и вредите. При компютърния деликт те не се различават, но всеки един от тях, малко или много е повлиян от изследваните по-горе общи особености свързани с електронния характер и среда в която се проявяват. Част от елементите на фактическия му състав имат спецификата и особеността, че се развиват, проявяват и характеризират *само* в електронна виртуална компютърна среда – това са *деянието* и *вредите*. *Деянията* при този вид деликти, се осъществяват само и единствено с помощтта и чрез използване на компютърна система /десктоп или лаптоп компютър/ или комуникационно устройство снабдено с мини компютърна система /например смартфон или таблет/. Осъществяване на *вредоносния резултат* по друг начин е обективно невъзможно. Посочва се, че увреждането също се осъществява обективно върху хардуера и/или софтуера на компютърен терминал, върху цифров електронен носител, база данни, елекронна потребителска информация. *Вредите* в голямата си част са свързани с промяната, унищожаването или нерегламентираното използване /разпространение/ на цифрова електронна информация. Обобщавайки горното, когато компютърно електронно устройство е необходимото средство и предмет на определено посегателство от което са причинени вреди, когато този вид посегателство не може да бъде извършено с друго средство или спрямо друг предмет, тогава е налице компютърен деликт.

От дадената характеристика е видно, че средството на извършване на деянието, както и предмета на посегателство при компютърния деликт е винаги компютърно електронно устройство - настолна или преносима компютърна система, смартфон, таблет или друго устройство което може да се управлява чрез операционна система или директни машинни команди. Ако средството или предмета, обекта на посегателство не е компютърно електронно устройство, то не е налице компютърен деликт. На следващо

място двете електронни устройства е необходимо да са свързани с цифров електронен канал за предаване на данни и команди – с кабел, през локална компютърна мрежа, през безжична мрежа или по друг начин. Самото деяние, посегателство, се изразява в предаване през създадения цифров електронен канал на данни или команди, които причиняват неблагоприятни последици, вреди, на собственика или ползвателя на потребителското електронно устройство. Посочва се, че компютърния деликт вече е познат в чуждата правна литература и че за компютърни деликти в САЩ се приемат клеветата и измамата в Интернет-пространството, нарушаване на правата на интелектуална собственост, злоупотребата с лична информация и файлове като снимки, видео и документи, действия или бездействия, нарушаващи Интернет етиката, морала или нанасящи вреди на лица, свързани към Интернет, изпращане на нежелана поща (непоискани търговски съобщения), препълване на каналите (flood), получаване на достъп до ресурси с чужди права и пароли, използване на недостатъци в системите с цел собствена облага или добиване на информация (hack), извършване на действия, които могат да бъдат квалифицирани като компютърен шпионаж или саботаж, повреждане или разрушаване на системи или информационни масиви (crack), изпращане на "троянски коне" или предизвикване инсталация на вируси или системи за отдалечен контрол, смущаване нормалната работа на останалите потребители на Интернет.

За целите на доказване, че компютърния деликт може да се обособи като нов подвид деликтна отговорност, в т.3, са разгледани и контретните специфични белези на елементите от фактическия му състав, в това число – специфика на деянието, противоправност, вината, видовете вреди и начините за причиняването им, особените начини на доказване на причинната връзка между тях. Посочва се, че при специалните деликтни състави, които разглеждаме, противоправността се изразява в самото извършване на забраненото поведение. Така на пострадалите лица се нанасят вреди и се нарушават правата им в най-различни сфери – лични данни, авторско право, унищожение или разпространение на потребителска информация, изтриване на софтуер или повреда на хардуера на компютърната инсталация. Разгледани са случаите, когато не е налице противоправност на деянието. Обсъдена е невъзможността за приложение на институтите на неизбежна отбрана и крайна необходимост.

При разглеждане на елемента за вината е посочено, че най-характерни са деянията извършени недобросъвестно, т.е. умишлено и целенасочено – неправомерно използване на компютърни данни, нарушаване на права на интелектуална собственост, целево заразяване на компютърна система с вирус, публикуване на невярна и клеветническа информация в социална мрежа, форум или блог. Интерес представлява разгледания въпрос възможни ли

са хипотези на небрежно причинени вреди в електронна среда? Считам, че отговорът е по-скоро положителен. Пример за такова деяние е създаването на компютърен вирус с научна експериментална цел за нуждите на антивирусните софтуерни компании и единствено за подобряване на антивирусната защита, който вирус бива инсталиран случайно или по погрешка на потребителски компютър и с това унищожава съхраняваната на него потребителска информация. Незнанието или пропуските в знанията, уменията и опита не оневиняват дееца. Виновно ще действа и компютърният специалист, който не притежава необходимата подготовка и знания за боравенето с определена компютърна програма или хардуер и поради своята самонадеяност причини вреди на трети лица.

По отношение на характера на вредите е посочено, че основно са свързани с нарушаване на личната неприкосновенност и злоупотреба с придобитите лични данни /при електронна кореспонденция, електронни потребителски профили/, нарушаване на правото на личен живот и самоопределяне, включително и виртуални такива /в електронни сайтове, блогове, форуми, социални мрежи и други/, накърняване тайната на електронната кореспонденция, накърняване или отнемане правото на собственост върху пари и вещи, в това число електронни пари, компютърни данни, програми, права на интелектуална собственост и унищожаване или повреждане на потребителския софтуер и хардуер, нарушаване целостта и годността за работа на компютърната система.

В т.4 е разгледан проблема за субектите на отговорността и възможните според българското законодателство случаи на обективна отговорност. Посочва се, че с използване на съвременните електронни технологии, е възможно „проследяването" на електронните следи на дееца, и от там характера на намеренията му. Идентификацията обаче на конкретния извършител и доказването на вината му в редица практически случаи е невъзможно. В този смисъл, актуален е въпроса за разширяване на хипотезите на обективна безвиновна отговорност, както и за ангажиране на отговорността на юридическите лица в един по-голям обем при компютърните деликти. В рамките на гаранционно-обезпечителна отговорност работодателите например могат да бъдат имуществено отговорни за действия на своите работници или служители, там където тези действия са свързани с използване на фирмени електронни ресурси и по повод възложената работа /използване на корпоративен e-mail сървър за изпращане на измамни електронни съобщения, СПАМ или вируси, за достъп до отдалечени компютърни ресурси използвайки фирменият IP адрес, с цел заблуда на проследяващите програми и т.н/. При сега действащото гражданско законодателство подобен род отговорност от предприятията може да се ангажира, само ако се цитира виновно поведение на конкретения работник или служител, съгласно разпоредбата на чл.49 от ЗЗД. В този смисъл, законовата уредба на

непозволеното увреждане и в частност в областта на гаранционната отговорност се счита, че следва да бъде разширена по подобие на страните от англо-саксонската правна система. Като предложение de lege ferenda се предлага да се обмисли създаването на законова разпоредба в ЗЗД, примерно чл. 48а, относно нова специална, обективна, отговорност на родителя ако вредите от компютърен деликт са причинени чрез използване на домашен или мобилен компютърен терминал, включително таблет и смартфон, предоставен за ползване от родителя на непълнолетното му дете. Отговорността ще бъде за недостатъчно упражнено възпитание и надзор, което е довело и позволило извършването на противоправни действия. Подчертава се, че такава отговорност би допринесла и за повече контрол върху достъпа, и използването на КИС.

На следващо място, в т.6, акцент в работата се поставя и върху проблема за трансграничността на компютърния деликт, а именно че голяма част от вредоносните деяния, причинени в електронна среда, чрез използване на компютърни системи и глобалната мрежа, се извършват „дистанционно", т.е. без физическото присъствие на дееца и механично взаимодействие с КИС. Така актуален става въпроса за териториалната подсъдност и компетентната съдебна институция за реализиране на отговорноста. Международния характер на компютърния деликт може да се прояви във всички възможни хипотези на чуждестранност, на който и да е от елементите на фактическия състав като:

- вреда чрез използване на КИС извън територията на страната;
- вреда върху КИС или мрежа на територията на страната, която е местна или чужда;
- деликвент – български гражданин и увреден чужденец;
- увреден български гражданин, съответно фирма със седалище в България и деликвент чужденец;

При всички посочени и други възможни хипотези обединяващото обстоятелство е, че деликтът като юридически факт, като поведение, изразяващо се в действие или бездействие, се проявява на територията на страната ни. Стълкновителната норма определя като приложим закон Lex loci delicti commisi и това е местният, български закон за деликта. Що се касае до компютърни деликти свързани с нарушаване на авторски и сродни права, чл.110 от КМЧП е категоричен, че те се уреждат от правото на държавата, в която се търси закрила. Чл.8 от Регламент "Рим II" също указва, че правото, приложимо към извъндоговорни задължения, произтичащи от нарушаване на права върху обекти на интелектуална собственост, е правото на държавата, в която се търси закрилата на тези права /lex loci protectionis/. В случай на извъндоговорни отношения, произтичащи от нарушаване на единното общностно право върху обекти на интелектуална собственост,

приложимото право за всеки неуреден от съответен акт на Общността въпрос е правото на държавата, в която е извършено нарушението . Така на българския съд са подведомствени всички дела срещу ответници, които имат в Република България обичайно местопребиваване, седалище или местонахождение на действителното си управление.

В края на Първа Глава, в т.7 на §2 се прави и кратък анализ на Компютърните престъпления като допълнителен източник на гражданска отговорност за вреди в електронна среда. Посочва се, че в българското законодателство вече съществува правно регламентиран, конкретен, систематизиран и своеобразен каталог на редица деяния чрез използване на компютърни системи и мрежи, които закона вече е определил за противоправни, а именно – компютърните престъпления в специалната част на Наказателния кодекс. При осъществяването им неминуемо възникват и граждански вреди, които следва да бъдат обезщетени – или по реда на гражданския иск в наказателния процес или в отделно гражданско производство. Прави се констатация, че независимо от вече над десетгодишното съществуване на тези състави съдебна практика по тях почти липсва.

ГЛАВА ВТОРА - ХИПОТЕЗИ НА КОМПЮТЪРНИЯ ДЕЛИКТ

В глава II са анализирани няколко основни групи хипотези за компютърни деликти, които в определени случаи са взаимосвързани, а в други имат самостоятелно проявление. Това са случаите на неправомерен достъп и манипулация на електронни данни в чужда компютърна система, компютърните измами, разпространяването на множество непоискани рекламни или злоумишлени съобщения /СПАМ/ и нарушаване на правата на интелектуална собственост в Интернет или т.нар. Интернет пиратство.

В §1. Отговорност за вреди, причинени от неправомерен достъп до компютърни информационни системи и мрежи, и последваща манипулация с данните в тях, са описани техническите начини за причиняване на вредите, дадени са необходимите легални и технически дефиниции на използваните понятия. Посочва се, че достъпът до потребителска компютърна информационна система или мрежа е свързан винаги с активно поведение от страна на външен за системата потребител, чрез технически хардуерни и/или/ софтуерни средства. Веднъж осъществен, той дава възможност за последващи действия върху КИС свързани с манипулации на данните. Сам по себе си осъществения достъп не е вредоносен, но последващите манипулации са такива. В този смисъл, именно манипулацията с данните е онова вторично действие свързано с достъпа, което причинява вредите. Така под неправомерен достъп, за целите на компютърният

деликт, може да разбираме онзи достъп или намеса, който не е разрешен от собственика или правомерния ползвател на КИС. Неправомерна намеса в компютърна система следва да се разбира всяко спиране или възпрепятстване на функционирането на информационна система чрез неправомерно въвеждане, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни. Неправомерна намеса в компютърни данни би било всяко непозволено изтриване, увреждане, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни в дадена информационна система. Описват се спецификите на елементите от състава на деликта, а именно деянието и вредите. Деянието в повечето случаи има комплексен характер и съдържа два или три елемента неправомерен достъп, манипулация с данните и тяхното последващо използване. Посочва се, че има два основни подвида последващи действия след осъществяване на достъпа - А. Нерегламентирано копиране или използване на компютърни данни и Б. Фалшификация или унищожаване на компютърна програма или данни. Въвеждане на компютърен вирус в компютър или информационна мрежа.

Относно вредите при този компютърен деликт се посочва, че най-често те са свързани с:

- нарушаване на личната неприкосновеност във виртуалното пространство
- злоупотребата с лични данни от виртуалния живот на потребителя, негови снимки, видео, документи намиращи се в компютърната система, личен блог, форум, профил в социална мрежа
- нарушаване на правото на личен живот, включително и във виртуална среда, право да се самоопределя и показва така както желае
- накърняване на тайната на електронната кореспонденция – електронна поща, чатове, съобщения и постове във форуми, блогове, социални мрежи
- нарушаване на правото на собственост върху пари и вещи, в това число компютърни данни, програми, права на интелектуална собственост, електронни пари, кодове за електронно банкиране
- унищожаване или повреждане на потребителския хардуер /компютърни системи, мрежови устройства и други/ чрез зловредни програми или вируси.

В същия параграф, се поставя въпроса дали генералната клауза в ЗЗД при разгледаните компютърните деликти дава в достатъчна степен защита на пострадалите лица, дали покрива всички хипотези на отговорност в електронна среда и гарантира справедливо и навременно обезщетение на причинените вреди. Въпреки че има универсално приложение, отговорът на тези въпроси е отрицателен. Достатъчно

показателен е фактът, че липсва съдебна практика и реално разгледани от съда случаи на търсене на отговорност за вреди причинени чрез компютърните системи и глобалните мрежи. В тази връзка се прави и конкретно предложение de lege ferenda за нов специфичен състав в съответния раздел на ЗЗД касаещ специфичните състави на компютърните деликти. В частност се предлага създаването на чл.50а /нов/ на ЗЗД със следния текст:

“(1) Който, използвайки електронни технически средства, осъществи неправомерен достъп до компютърна система или мрежа, и използва, копира, фалшифицира или унищожи компютърни данни дължи обезщетение на техния собственик и/или ползвател.

(2) Съдът определя справедливо обезщетение зависещо от реално претърпените вреди. При определяне размера на обезщетението съдът взема предвид и всички обстоятелства, свързани с нарушението, пропуснатите ползи и неимуществените вреди.

(3) В случаите, когато размерът на вредите не може да бъде обективно установен, съдът определя обезщетение по справедливост .

(4) Когато не може да бъде установен конкретният извършител на деянието, обезщетението се дължи от собственика на компютърната информационна система и/или титуляра на IP адреса, от който е осъществен достъпа, освен ако същият е направил всичко възможно за недопускане или ограничаване на последиците от деянието.”

Систематично новата разпоредба е предложено да бъде след хипотезите на обективна отговорност за непозволено увреждане по чл.49 и чл.50 от ЗЗД с оглед специфичния характер, който има. Предложението включва описателно изброяване на противоправните деяния, особения елемент на развитието им само и единствено в електронна среда /от една КИС в друга/. Създава се също право на обезщетение и на субект различен от собственика на КИС, а именно на временния ползвател ако собственика докаже че не е бил във владение на КИС по време на увреждането и посочи конкретен ползвател. Въведеното законодателно предложение за разширяване на кръга от засегнати лица считам, че отговоря на практическата насоченост на проблема, свързано с честото предоставяне от собственика на трети лица на КИС за ползване, било по повод служебно или трудово правоотношение или правна сделка. В случаите когато, не може да бъде установена точната граница на отговорност, обема и размера на вредите, тяхната относителна стойност, се предлага да се въведе принципа за обезщетяване по справедливост. В разширение на предложението за обезщетяване по справедливост може да са помисли и за посочване на негов минимален размер свързан например с минималната работна заплата. От изключително голямо значение за успешно провеждане на процедурата по реализиране на отговорността считам предложението по ал.4, а именно при невъзможност да бъде установен конкретният нарушител, обезщетението да бъде

търсено на принципа на обективната отговорност от собственика на КИС и/или титуляра на IP адреса, от който е осъществен достъпът. Отговорността тук е за неосъществен в достатъчна степен контрол върху използването на КИС, с което са причинени вреди другимо. В същия смисъл е и направеното вече предложение de lege ferenda за създаването на законова разпоредба в ЗЗД, относно специална, обективна, отговорност на родителя, ако вредите от компютърен деликт са причинени чрез използване на домашен или мобилен компютърен терминал, включително таблет и смартфон, предоставен за ползване от родителя на непълнолетното му дете.

Като съпътстващо предложение de lege ferenda се посочва за уместно да се добавят в Допълнителните разпоредби на ЗЗД легалните дефиниции за Неправомерен достъп до КИС, Неправомерна намеса в компютърна система и Неправомерна намеса в компютърни данни.

В § 2 се разглежда отговорността за вреди причинени чрез компютърни измами. Посочва се, че ръстът и обемът на нанесените чрез тях вреди в последните години е значителен. Основното разграничение между тях и другите видове измамни схеми е ролята на компютърната система и глобалната мрежа за извършване на увреждането. КИС може да бъде както средството, чрез което се осъществява измамата, така и среда за нейното извършване. Компютърната измама може да се определи като измама, извършена с помощта КИС в голяма част от случаите свързани с глобалната мрежа Интернет. Дава се описание и характеристика на най-популярните измамни схеми в глобалната мрежа - търговски онлайн измами , измамни схеми, които използват механизмите на финансовия пазар , мними онлайн търгове , фишинга , фарминга и т.нар. нигерийски измами. Посочва се спецификата на елементите от състава на деликта, както и се разглежда престъплението компютърна измама по НК като допълнителен източник на гражданска отговорност за вреди. За намаляване на посочения вид правонарушения се правят предложения de lege ferenda относно засилване на контрола върху поведението на потребителите в Интернет от страна на доставчиците на Интернет съдържание и услуги в това число чрез промени в:

- Закона за електронната търговия в частта му за отговорността на Интернет доставчиците – Глава Четвърта, чрез включване на разпоредби за задължителни действия от страна доставчика при сигнализиране за извършена измамна схема чрез предлаганите от него услуги на информационното общество;
- Закона за електронните съобщения в Глава петнадесета - Сигурност и цялост на електронните съобщителни мрежи и услуги, конфиденциалност на съобщенията и

защита на данните на потребителите чрез включване на разпоредби за превантивен контрол върху съдържанието на електронните съобщения и

- Закона за защита на потребителите в Глава Четвърта, Раздел II в частта касаеща уреждане на отношенията на продажбите от разстояние чрез включване на допълнителни разпоредби гарантиращи правата на потребителите при случаи на измама.

В § 3 се разглежда отговорността за вреди причинени от изпращане на множество непоискани търговски съобщения /СПАМ/. Дадена е обща характеристика и дефиниция на СПАМа. Посочени са характерните му елементи:

- нежелано или неочаквано съобщение (т.е. липсва съгласие за получаването му, изрично изразено или подразбиращо се)

- липса на предварително установени отношения с изпращача.

- досадно или оскърбително съобщение (напр. "верижни" писма, заблуждаващи съобщения, порнография, духовни послания, личностно самоизтъкване);

- има маркетингов /търговски/ характер;

- възможно незаконно или измамническо съобщение (напр. детска порнография, схеми за "бързо забогатяване", подвеждаща реклама).

- невъзможност да се установи изпращача или пътя, който е изминало съобщението;

- липсват данни за физически компютърен адрес и други подробности за изпращача.

- не дава възможност или е трудно да се "отпишеш" от получаването на следващи съобщения;

- изпратено е в големи количества (масово) (напр. чрез автоматизирана система или нецелево, безразборно);

- методът, използван за събирането на електронните адреси на получателите;

Обсъдени са специфичните елементи от фактечския състав – деяние, противоправност, вреда. Посочено е, че деянието при спама, като компютърен деликт, също е комплексно и се състои от няколко елемента:

- Подготовка етап 1– създаване, написване на текста на съобщението или компютърен алгоритим, програма за неговото автоматично генериране;
- Подготовка етап 2 - създаване на компютърен алгоритим, програма за неговото изпращане и препращане;
- Изпращане – ръчно или автоматизирано в предварително определени обем, съдържание, списък получатели, период и други

Относно противоправността е посочено, че в България изпращането на СПАМ е частично забранено от закона, който го разглежда като непоискани рекламни /търговски/ съобщения. По смисъла на Закона за електронната търговия, търговски съобщения са рекламни или други съобщения, представящи пряко или косвено стоките, услугите или репутацията на лицето, извършващо търговска или занаятчийска дейност или упражняващо регулирана професия. Търговските съобщения, които са част от или представляват услуга на информационното общество, следва да отговарят на изброени в закона изисквания: те трябва да бъдат лесно разпознавани като търговски, да позволяват ясна идентификация на физическите или юридическите лица, от името на които са направени, да определят ясно и недвусмислено условията за ползване на промоционни предложения като отстъпки, премии и подаръци и т.н. Доставчик на услуги, изпращащ непоискани търговски съобщения по електронната поща без предварително съгласие на получателя, е длъжен да осигури ясното и недвусмислено разпознаване на търговското съобщение като непоискано. Правен абсурд е обаче фактът, че Република България е една от страните, която е легализирала изпращането на спам. Според чл. 5 и чл. 6 от ЗЕТ се узаконява изпращането на спам до адреси на юридически лица, стига в текста на съобщението да е включено предупреждение, че то може да представлява непоискано търговско съобщение. Комисията за защита на потребителите се задължава да води публичен регистър на фирмените електронни пощенски адреси, които не желаят да получават непоискани търговски съобщения. Съгласно чл.3 от Наредбата за водене на електронен регистър на електронните адреси на юридическите лица, които не желаят да получават непоискани търговски съобщения се вписват единствено български и чуждестранни юридически лица. Per argumentum a contrario следва, че регистърът не е за индивидуални електронни пощенски адреси на физически лица и изпращането на спам до тях е разрешено !?! Относно вредите е посочено, че възможните вредоносни и негативни последици от получаване на множество спам съобщения може да се опишат така:

- намалена пропускателна способност на електронните канали за комуникация и от там затрудняването й;
- повишени разходи за обработка и съхраняване на електронните съобщения
- загуби в производителността на труда на работещите с електронна поща
- загуби от измами и други незаконни действия;
- загуби поради причиненото забавяне /или пропускане/ недоставяне на полезни електронни съобщения.

От друга страна спамът може да доведе и до:

- подбуда към криминално действие на пълнолетни и непълнолетни лица;

- рекламиране, водещо до покупка на стоки с несигурно или вредно съдържание за човешкото здраве;
- разпространение и осигуряване лесен достъп до порнографски материали на непълнолетни лица;
- разпространение на информация за лесен достъп до адреси, съхраняващи и популяризиращи расова нетърпимост или подтикващи към форми на нарушаване на човешките права и свободи;
- нарушаване на правото на личен избор при получаване на нежелана информация ;
- възможно разпространение или използуване на застрашаващи личното електронно съдържание и пространство или личните данни, програми, вируси и др.

Направени са и няколко обосновани предложения de lege ferenda - за въвеждане на обективна, безвиновна, отговорност за лицата, в чиято полза и/или с чието съдействие се изпращат съобщенията, както и твърдо определен размер на обезщетението за всяко изпратено непоискано съобщение по подобие на САЩ. Размерът може да се свърже с минималната работна заплата за страната. С оглед противоправността на деянието може да се помисли като предложение de lege ferenda, за изменение и допълнение на ЗЕТ за още по-тясно дефиниране на непоисканите търговски съобщения, като всички останали да се считат за незаконосъобразни и увреждащи, причиняващи компютърен деликт. Най-малкото нещо, което може да направи законодателят е да премахне двойния режим регулиращ непоисканите рекламни съобщения, като забрани тяхното изпращане без предварително съгласие на всички получатели било то физически или юридически лица. В този смисъл е предложена редакция на чл.6 от ЗЕТ като се премахне регистъра на адресите и остане само и единствено текстът на сегашната ал.4, а именно: “Чл.6, ал. Единствена - Забранява се изпращането на непоискани търговски съобщения на потребители без предварителното им съгласие.”

§ 4 касае нарушаването на правата на интелектулна собственост в Интернет като форма на компютърен деликт. Посочено е, че това са едни от най-сериозните нарушения на субективни права при използване на КИС и Интернет - противоправното разпространение и използване на музикални, графични и видео произведения, на компютърни програми. Дава се най-обща характеристика, че Компютърното пиратство се изразява в неоторизираното придобиване, копиране, възпроизвеждане, разпространие и/или/ използване на компютърни електронни данни, които са обект на авторско право. Тези неправомерни действия нанасят значителни вреди на авторите и дистрибуторите им,

поради невъзможността да печелят от своя авторски труд. Прави се заключение, че Компютърното пиратство е особена хипотеза на проявление на компютърния деликт и следва да намери систематично място в разработката с оглед мащабите и сериозността на проблема. Допълнително основание е и фактът, че гражданскоправната защита на носителите на авторски права по Закона за авторското право и сродните му права също е уредена като специфичен деликтен състав.

В точка втора на параграфа е дадена правната регламентация по защита на правата на интелектуална собственост в електронна среда. Посочено е, че международноправни разпоредби, регламентиращи правото на интелектуална собственост в контекста на развитието на глобалната мрежа Интернет, има в чл.8 от Договора на СОИС за авторското право и чл.10-14 от Договора на СОИС за изпълненията и звукозаписите. Визираните два международни договора, касаещи Интернет-пространството са познати като „договорите на Интернет". И двата договора съдържат императивни правила, които налагат взимането на мерки за технологична закрила и предотвратяване на непозволеното копиране, касаещо представената в електронна форма информация. Държавите членки по тези договори (включително и България) са поели ангажимент да изградят необходимите законодателни механизми, с цел създаване на защитни системи по отношение на авторските творби, разпространявани в Интернет пространството. Договорите гарантират на авторите изключителното право да разрешават разгласяването на произведенията им, включително чрез кабел и по безжичен път и предлагат достъп на неограничен брой лица, позволяващ този достъп да бъде осъществен от място и по време индивидуално избрани от всеки от тях. Именно в него е регламентирана уредбата на т. нар. on-line използване на произведението. Посочено е и националното законодателство регулиращо въпроса, а именно съответните текстове от ЗАПСП. Направен е и сравнително-правен анализ на деликтния състав по чл. 94 от ЗАПСП. Прави се извод, че той засега е единствената възможност за търсене на обезщетение за вреди в електронна среда свързани с компютърното пиратство. Съгласно цитираната норма, при нарушение на авторски права се дължи обезщетение за всички причинени вреди. Искът има деликтен характер, защото се основава на правото на автора да иска обезщетение за причинените му вреди от лицето, което неправомерно, в нарушение на нормите на ЗАПСП, ползва произведението, принадлежащо на автор или ползвател, без да е сключен договор или без да е заплатено за ползването на автора. Разпоредбата на чл. 94, ал. 1 от ЗАПСП следва да се разглежда като специална в областта на авторското право по отношение на общия принцип на чл. 45 от ЗЗД . Елементите на специалния фактически състав на иска са: противоправно нарушаване на авторско право, вината на нарушителя, вредата и причинно- следствена връзка между

нарушението и вредата. Тяхното наличие е предпоставка за уважаването на иска. По нататък са дадени спецификите от елементите на състава, разгледан е въпроса за законосъобразността на торент системите.

В края на цитирания параграф е направен кратък анализ на Търговско споразумение за борба с фалшифицирането – АСТА. Посочва се, че то съдържа изключително модерен законодателен подход към регулиране на Интернет потока данни, съдържа съобразени с актуалната ситуация разпоредби за правоприлагане в областта на правата на интелектуална собственост, включително и разпоредби за прилагане на мерки от гражданското и наказателното право във връзка с границите на цифровата среда. Посочено е, че АСТА поставя нови хоризонти на правната уредба на проблемите свързани с нарушаване на правата на интелектуална собственост, с контрола върху глобалната мрежа, със задължението към Интернет-доставчиците да следят поведението ни пред компютърния терминал. Поставените проблеми правят бъдещето на разглежданото споразумение повече от неясно въпреки неговата актуалност. За пълнота на изследването е посочен и един друг международен договор, който предстои процедура по ратификация от Народното събрание на Р България с решение на МС от 29.01.2014г. Става дума за т.нар. Пекински договор. Документът е приет от Дипломатическата конференция за защита на аудиовизуалните изпълнения на Световната организация по интелектуална собственост през юни 2012г. и предвижда всяка от присъединилите се страни да предоставя на гражданите на други страни третирането, което предоставя на своите собствени граждани по отношение на аудиовизуалните изпълнения, както и правото на справедливо възнаграждение. Съгласно клаузите му, на артистите-изпълнители се предоставят морални права, като например да бъдат идентифицирани при всяко изпълнение, както и да могат да се противопоставят на всяко изопачаване или опорочаване на техните изпълнения. Интересен анонс е направен, че посочените права съгласно Договора от Пекин вече са приложими в най-големия Интернет портал за видеосподеляне – Youtube.

ГЛАВА ТРЕТА - ПРАВНА РЕГЛАМЕНТАЦИЯ И ОТГОВОРНОСТ ЗА ВРЕДИ НА ИНТЕРНЕТ-ДОСТАВЧИЦИТЕ.

В § 1 се дава обща правна регламентация на дейността на Интернет-доставчиците, дадени са необходимите легални и технически дефиниции на използваните термини. Прави се извод, че в живота и разговорния език се е наложило обобщеното понятие Интернет-доставчик. По същността си, тези лица предлагат както достъп до Интернет

съдържание, така и услуги на информационното общество като електронна поща, хостинг на файлове, а някои и комплексни услуги "3 в 1", представляващи

1. достъп до Интернет и услуги на информационното общество
2. радио и телевизионно съдържание и
3. Интернет-телефония.

В §2 са дадени някои хипотези на гражданска отговорност в отношенията между потребителите и Интернет-доставчиците, направен е анализ относно пораждане на договорните правоотношения помежду им, обсъден е въпроса с приемането от страна на потребителите на Общите условия на доставчика, често с един клик на мишката. На практика всички доставчици на услуги на информационното общество преди ползването на услугата изискват регистрация и приемане на Общи условия. И това е разбираемо с оглед големия брой потребители и затрудненията по сключване на индивидуални договори. Чрез Общите условия страните се освобождават от необходимостта да уговарят елементите на всяка отделна сделка и по този начин се ускорява сключването на договора. Посочва се, че в Общите условия често са срещани уговорки за неотговорност на доставчика по повод:

– Липса на умения от страна на Потребителя да използва Услугата;

– Претенции от трети лица срещу Потребителя при и по повод ползване на Услугата;

– Вреди, причинени от лошо или неправилно поддържане или експлоатация от страна на Потребителя на техническите ресурси на доставчика;

– Повреди по съединителните електронни мрежи, които правят технически невъзможно предоставянето на Услугата;

– Вреди, причинени върху софтуера, хардуера или телекомуникационните съоръжения, или за загуба на данни, произтекли от материали или ресурси, търсени, заредени или използвани по какъвто и да било начин посредством предоставяните Услуги.

– Съдържанието на предаваната информация посредством предоставяните от него Услуги, както и за дейността на Потребителя.

В §3 са обсъдени някои законови ограничения и специфични основания за освобождаване от гражданска отговорност на Интернет доставчиците при услуги по достъп и пренос на електронна информация, при услуги за търсене на електронна информация, при междинни запаметявания, при хостинг и препращане към информация. Поставя се актуалния въпрос - следва ли доставчикът да следи и контролира трафика и съдържанието на електронната информация, която преминава през неговите сървъри ? Еднозначно законодателно решение се открива в разпоредбата на чл. 17 от ЗЕТ, според

която доставчикът на услуги не е длъжен да извършва наблюдение на информацията, която съхранява, пренася или прави достъпна при предоставяне на услуги на информационното общество, нито да търси факти и обстоятелства, указващи извършването на неправомерна дейност. От една страна, идеята на законодателя е да даде свобода на Интернет, на онлайн-общуването, на публикуването и размяната на електронна информация. От друга страна тази клауза за пълна липса на ангажираност е смущаваща. В тази връзка е направено предложение de lege ferenda за създаването на нова разпоредба в цитираната Глава IV на ЗЕТ, примерно чл.17а даваща допълнително уреждане на задълженията и отговорностите на Интернет-доставчиците. Предлага се също така създаването на Гаранционен фонд за обезщетяване на пострадали лица при или по повод неосъществен или зле осъществен контрол и управление на трафика на електронна информация от Интернет-доставчик.

ГЛАВА ЧЕТВЪРТА - ОСОБЕНОСТИ ПРИ ДОКАЗВАНЕ НА ФАКТИЧЕСКИЯ СЪСТАВ НА КОМПЮТЪРНИЯ ДЕЛИКТ

В последната глава на дисертацията се разглеждат основно въпроси свързани с практическата реализация на отговорността в един реален съдебен процес. Посочва се, че без съответните процесуално-охранителни правоотношения юридическата отговорност не може да съществува в обективната действителност. Тези специфичните черти от системата за реализация на отговорността са предмет на завършващата глава от изследването. Без тях разработката не би била пълна, няма да се разкрие характерът на функционално взаимодействие между материалноправните отношения и начините за реализацията им, няма да се открояят особености характерни именно за електронната природа на разглеждания вид гражданска отговороност. Такива са електронните следи, електронните доказателства, характеристиката и значението на електронния подпис, на компютърната експертиза.

В §1 се разглеждат електронните доказателства като средство за обективиране на специфичните елементи от състава на компютърния деликт – деянието и вредите. В тази връзка се обосновава нуждата от валидни и правно регламентирани способи за доказване на извършените по електронен път противоправни деяния, причинени вреди, за изясняване на тяхната характеристика, елементи и мащаб. Прави се извод, че доказателственото значение на отразяваната, преработвана, съхранявана и възпроизвеждана с електронни средства информация за нуждите на реализация на отговорността, е от съществено значение. По нататък се описват формата и съдържанието на електронните доказателства, например:

- Електронни файлове с текст, таблици, графики, аудио-видео поток, записани върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизвеждано и /или/ разпечатвано електронното съдържание;

- Електронна поща, постове в социални мрежи, форуми, блогове, чат, SMS, MMS - електронни средства за съхраняване и пренос на електронни съобщения през Интернет мрежа чрез стандартизирани цифрови електронни протоколи за пренос на информация;

- Електронни изявления – това са словесни изявления, представени в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията. Електронното изявление може да съдържа и несловесна информация;

- Електронни следи - цифрова информация, запазена върху магнитен или оптичен носител, която може да е под формата на log файл или част от него и която съдържа запис на извършени манипулации върху дадена компютърна машина или Интернет сървър.

Изследването продължва в търсене и анализ на законодателната уредба на електронния документ и електронния подпис като част от системата на електронните доказателства. Прави се извода, че правната природа и статут на електронните доказателства поражда спорове в теорията. Така се приема, че електронните доказателства по същността си са веществени доказателства. Те съществуват чрез и върху магнитен носител или в цифрова форма и могат да бъдат събирани и изследвани със специални технически средства. Същевременно, начина на проявлението им в обективната действителност разкрива някои черти, които не са присъщи на веществените доказателства:

1. могат да се възпроизвеждат като точно, идентично копие в неограничено количество при наличието само на един единствен “оригинал” ;

2. ако бъдат направени допълнения или изменения в тях, те могат да бъдат установени по надлежния ред с нарочна компютърна експертиза

3. с използване на глобалната мрежа могат да бъдат разпространени изключително бързо към неограничен кръг лица;

4. не винаги може да удостоверят конкретната връзка между тях и извършителя и/или между тях и пострадалото лице в хипотезите на компютърните деликти и компютърните престъпления;

5. изискват специални познания относно тяхното събиране, анализиране и кредитиране по делото;

6. подлежат на архивиране и защита с нарочни програмни продукти

На следващо място се разяснява правната уредба при електронно подписване на документи, правната същност и видове на електронния подпис. Посочват се европейските и национални нормативни актове имащи отношение към въпроса. Дава се легална дефиниция на термините. Така електронното изявление е словесно изявление, представено в цифрова форма чрез общоприет стандарт за преобразуване, разчитане и визуално представяне на информацията" (чл. 2, ал. 1 от ЗЕДЕП). От тази дефиниция е видно, че всякакво съобщение, съдържащо текст, което се въвежда по определен начин в изпращащия компютър и се изпраща по мрежата до приемащия компютър, където се преобразува, разчита и представя като информация, годна да бъде възприемана, е електронно изявление по смисъла на закона. Алинея втора на посочената разпоредба разширява кръга на информацията, която се приема за електронно съобщение с варианта, че то може да съдържа и несловесна информация – примерно графики. По този начин в нашия закон е нормативно уредено общоизвестното в компютърните среди понятие за съобщение , използвано широко от потребителите на електронна поща. Всеки електронен документ съдържа електронно изявление, но наред с това съдържа и други, специфични за него характеристики. По смисъла на закона (чл. 3, ал. 1 от ЗЕДЕП) електронният документ е "електронно изявление, записано върху магнитен, оптичен или друг носител, който дава възможност да бъде възпроизвеждано". Прави се препратка към същността на писмения документ, търсят се приликите и разликите. Не на последно място се дефинира понятието електронен подпис. Той е едно от новите съвременни средства за осигуряване интегритета на данните и тяхната поверителност при предаването им в електронен вид. В чл. 13, ал. 1 от ЗЕДЕП е дадена легалната дефиниция на електронния подпис: "всяка информация в електронна форма, добавена или логически свързана с електронното изявление, за установяване на неговото авторство”. Разгледано е и приложението на електронните документи и електронния подпис в съдебния процес. Прави се предложение de lege ferenda, относно съдбата на събраните в граждански процес електронни доказатества, в това число и представените електронни документи, а именно да се създаде нормативна основа за генериране и поддържането на електронни досиета за всяко гражданско дело, достъпни на страните и съда по всяко време и място.

В §2 на Четвърта Глава се разглежда статута на Компютърната съдебна експертиза. Посочва се, че прякото използване на електронни документи, като доказателства в гражданския процес, вече е възможно поради изричната законова разпоредба на чл.184 от ГПК. Прави се извод обаче, че закона мълчи и не урежда използването на останалите форми на електронни доказателства, каквито са например компютърната информация и

файлове съхранени в дадена КИС. Тяхното удостоверяване, запазване, събиране и анализиране следва да се извършва от компетентни технически лица със специални познания в сферата на компютърните технологии. Представянето им в съда е възможно по процесуалния ред на съдебната експертиза и по-точно на компютърната съдебна експертиза /КСЕ/. Без тази форма за събиране на доказателства би било невъзможно доказването на обективните елементи от фактическия състав на компютърните деликти или установяване истинността на представените електронни доказателства. По нататък се посочват евентуалните задачи пред експертизата, механизма на извършването й, изискванията към вещите лица. че е необходимо да бъде създадена специална законова регламентация по тяхното събиране и анализиране, за провеждането на КСЕ. Прави се извод, че действащите понастоящем норми на ГПК не дават в достатъчна степен нужните гаранции за сигурността и достоверността на извършваните компютърни експертизи и изобщо при боравенето с електронни доказателства. За нуждите на наказателния процес и разкриването на компютърни престъпления, държавата прилага по-строга регламентация, обезпечаване и контрол на този род доказателствени средства. В този смисъл е и предложението за аналогично и по-строго регламентиране на събирането и оценката на електронните доказателства и в гражданския процес.

III. ПУБЛИКАЦИИ НА АВТОРА ПО ТЕМАТА НА ДИСЕРТАЦИЯТА

1. Компютърните системи и мрежи – среда за нови форми на непозволено увреждане, сп. “Правна мисъл”, кн.3/2008г, с.59
2. Отговорност на Интернет доставчиците за вреди причинени чрез предоставяните от тях услуги, сп. “Правна мисъл”, кн.2/2010г, с.98
3. Някои хипотези на гражданска отговорност за вреди причинени чрез използване на компютърните системи и Интернет, Научни трудове на Института за държавата и правото, Том VI, София 2011г, с.281
4. Търговското споразумение за борба с фалшифицирането /АСТА/ - За и против, Научни трудове на Института за държавата и правото, Том VII, София 2012г, с.263
5. Предизвикателства пред електронното управление на България, Научни трудове на Института за държавата и правото, Том VIII, София 2013г, с.268
6. Компютърните информационни системи и глобалната мрежа Интернет – среда за нови форми на непозволено увреждане, Юбилеен сборник “Развитие на правото в глобализиращия се свят” издаден по случай 100-годишнината от рождението на акад.Любен Василев и проф.дюн Живко Сталев и 90-годишнината от рождението на проф.дюн Витали Таджер, Фенея 2013, с.487