IV. ПРАВНИ ОТНОШЕНИЯ ВЪВ ВИРТУАЛНОТО ПРОСТРАНСТВО

1. Правонарушения във виртуалното пространство

Правните отношения придобиват реална характеристика тогава, когато бъдат установени гаранции за това, че задълженията по тях ще бъдат изпълнени от субектите, а така също и ако е установена отговорност за тяхното неизпълнение или ненадлежно изпълнение.

Основание за възникване на юридическа отговорност във виртуалното пространство, както и в традиционните правни отношения е правонарушението, извършено от субектите. Т. е. противообществено, противоправно, виновно извършено деяние на конкретен субект , забранено с юридически санкции. [1] Юридическата отговорност произтича от нарушение на нормативно установени правила на поведение.

За реализацията на юридическата отговорност във виртуалното пространство също е важно да се установи наличието на причинно – следствена връзка между негативните последици и извършените действия, нарушаващи правните предписания за дължимо поведение, действащи в Интернет. Характерът на юридическата отговорност, главната цел на нейното прилагане не може да бъде сведена само до наказването на виновното лице. Водещата цел на прилагането и е поддържане на ред и сигурност във виртуалното пространство, основано на следването от субектите на установени норми на материалното право. В този смисъл установяването на юридическата отговорност има още факултативно, нравствено – възпитателно въздействие.

В разглежданата сфера отговорността също може да бъде разграничена по видове, в зависимост от характера на извършеното правонарушение -административна, гражданска, наказателна отговорност.

Във връзка с характеристиката на обществените отношения, осъществявани чрез Интернет, може да се направи извод, че най- често към правонарушителите (и може би най- адекватна към спецификите на тези отношения) се прилагат мерките на гражданската отговорност, като

[1] Бойчев, Г. Правонарушение, 1998, трето преработено и допълнено издание

тя може да бъде реализирана и в двата си вида – договорна и деликтна отговорност, произтичаща от общото задължение да не се вреди другиму.

Да бъдат разгледани всички видове правонарушения в Интернет на практика е невъзможно. Поради това, при изследване особеностите на юридическата отговорност на информационните посредници във виртуалното пространство следва да се постави акцента върху тези видове правонарушения, които са най- съществени и характерни на този етап на развитие на правните отношения в Интернет.

Техническите характеристики на Мрежата правят въпросите, свързани с контрола върху информацията до голяма степен условни. При специфичния начин, по който могат да се пренасочват съобщенията, контролът върху тях може да бъде упражняван само на точките вход и изход на мрежата (сървъра, чрез който потребителя има достъп или терминала, използван за четене или сваляне на информация и сървъра, на който е публикуван документът). Дори и да се премахне даден публикуван документ от един сървър, той може бързо и лесно да се прекопира, така че да продължи да бъде достъпен, ако и докато тези места не бъдат също блокирани. Това обаче не е основание въпросите, свързани с отговорността да не бъдат поставяни.

При използването на услугите в Мрежата, потребителят носи отговорност за съдържанието на предаваната от него информация, за нейната достоверност, чистота с оглед претенции за права на трети лица и правилата за нейното разпространение. Той отговаря за вредите , които могат да настъпят от неговите действия върху личността или имуществото на други лица или нравствените принципи на обществото.

Могат да бъдат приведени различни примери за неправомерни действия в Интернет. Такива могат да бъдат: нарушаване от страна на ползвателите на общо приетите правилата за използване на услугите, на общоприетите норми на използване на Интернет (правилата за използване на общодостъпните ресурси се определят от притежателите или администраторите на тези ресурси и са задължителни за всички ползватели), използване за достъп до мрежата на компютърно оборудване , програмно обезпечение, което не е сертифицирано по надлежния ред; разпространяване на материали, оскърбяващи човешкото достойнство , за

пропаганда на насилие, расова или национална вражда, с хулигански цели; използване на предоставените услуги за предаване по мрежата на информация, която противоречи на действащото българско или международно законодателство; публикуване, предаване, изпращане или използване на информация или програми, които съдържат в себе си компютърни “вируси” или могат да нарушат нормалното функциониране на компютрите, достъпни чрез мрежата; публикуване, изпращане, предаване, възпроизвеждане или разпространяване ,независимо от способа, посредством достъпа до Мрежата на програмно обезпечение или други материали, защитени от авторски права без съответното разрешение за това; използване на предоставения достъп до мрежата за създаване на т. нар. спам, който може да се изразява в:

- поместване в различни форуми или електронни списъци на статии, които не съответстват на зададената тематика (off topic), поместване на реклами в същите, освен в случаите когато тя е разрешена с конкретни правила;
- масово разпращане на несъгласувани предварително електронни писма, (mass mailing) превишаващи по обем 10 Кб и/или съдържащи приложени файлове. Под масово разпращане се разбира както разпращане към множество получатели, така и масирано изпращане на съобщени към един получател;
- несъгласувано изпращане на електронни съобщения с рекламен или агитационен характер, а така също и писма , съдържащи груби и оскърбителни изрази и предложения;
- изпращане на информация към получатели, изразили несъгласие за получаване на такава;
- използване на собствени и/или предоставени информационни ресурси (адреси на електронна поща, уеб- страници ит. н.) в качеството на координати за контакт при извършване на гореописаните действия;
- използване на несъществуващи адреси за обратна електронна пощ, извън случаите когато е разрешена анонимността.

Осъществяване на опити за несанкциониран достъп до ресурсите на доставчика и други системи, достъпни чрез мрежата. Тези действия могат да се изразяват в :

- използването на специални средства , насочени към нарушаване на нормалното функциониране на елементи в мрежата , непринадлежащи на ползвателя;
- използване на специални средства , за неправомерно получаване на достъп, а така също и последващо използване на вече осъществен такъв достъп;
- предаване чрез Мрежата на безсмислена или безполезна информация, създаващи паразитна натовареност на компютрите или оборудването;
- унищожение или модификация на програмно обезпечение или данни, които не принадлежат на ползвателя, без съгласието на притежателя или администратора на това програмно обезпечениеили данни;
- неправомерна промяна на собствен IP адрес при предаване на данни в Мрежата, а така също и на информация за контакт с ползвателя;
- използване на псевдоними или анонимност , извън случаите, когато правилата на ползване на съответните ресурси разрешават анонимността при при тяхното използване;
- Подправяне на служебна информация в заглавията на съобщенията,отправени например посредством електронна поща, ICQ, и други подобни средства за личен обмен на информация;

Трябва да се отбележи, че съдилищата са поставени пред определени трудности при решаването на спорове относно указаните нарушения, свързани с Интернет. Сред множеството проблеми, които се очертават пред съдебната практика могат да се отделят два, непосредствено отнасящи се до механизмите на разпространение на информацията:

На първо място това е сложността при определяне на кръга от лица, които трябва да носят юридическа отговорност и са задължени да обезщетят нанесените морални и материални вреди. И на второ , въпросите за събиране и представяне на доказателствата, тяхната допустимост и достоверност.

Процесът на разпространение на информацията в този случай може да се опише като процес , в който участват основно два субекта – собственика на сайта (наричан още доставчик на информационен ресурс, доставчик на съдържание) и собственик на сървъра (хост – доставчик). В

тази хипотеза потенциални ответници в евентуално съдебно производство могат да бъдат както хост – доставчиците, разположили информационния ресурс на своя сървър, така и собствениците на ресурса.

Възможността за анонимен достъп до Мрежата обаче, позволява да остане скрито истинското име на автора, източника и лицето , поместило информацията. В тази връзка проблема се усложнява и от наднационалния характер на виртуалното пространство, позволяващ да се разполага незаконна информация на територията на друга държава (например като се сключи договор за хостинг с доставчик , намиращ се извън пределите на дадената държава).

Това прави необходимо да се уточнят понятията “български сегмент в Интернет” и “българскоезичен информационен ресурс”.

Под първото в практиката е възприето да се разбира съвкупността от информационните ресурси на сървърите, намиращи се на територията на една страна (регистрацията в зоната “bg”е указание , но не и доказателство).

Под българоезични ресурси следва да се разбира съвкупността от информационни потоци, предоставени на български език, независимо от мястото на разположение и регистрацията на съдържащите ги сървъри.

Ако приемем,че субекта на определено отношение , разпространяващ незаконната информация е установен, то пред ищеца по евентуален съдебен спор възниква проблема за събирането и предоставянето в съда на необходимите доказателства.

Възприемайки, че сървъра, в паметта на който е разположена незаконната информация е идеалното веществено доказателство в съда, следва да бъдат отчетени следните трудности. Да бъде прегледан целият обем от съхраняваната в сървъра информация е сложно поради големият обем на неговата памет, защото при изземване на сървъра ще бъдат нарушени правата на третите ползватели и практически ще бъде нарушена цялата работа на доставчика.

Такива възможности на доставчика като въвеждане на протоколи за достъп, отчетни записи, а така също и ползването на лог- файл, позволяващ да се фиксират всички осъществявани на него действия, могат да бъдат използвани в помощ на правосъдието. Затова е

необходимо доставчикът да бъде обвързан регулярно да копира информацията от лог- файла, надлежно да я съхранява и да я предоставя при първо поискване от компетентните държавни органи.
Такива доказателства се считат допустими и в съответствие с гражданско – процесуалното законодателство се приемат в съда в качествотона писмени .

Европейското законодателство възприема идеята, записана в Директива 1999/93ЕС (Директива за електронния подпис), че съдът не може да откаже допускането като доказателства в съдебния процес на електронни документи , на основание на това, че са представени в електронен вид.

Счита се, че в качеството на обезпечаване на такива искове, на основата на съдебен акт, може да бъде блокиран достъпа от страна на доставчика с т. н. филтри (програми за филтриране, съдържащи списък от интернет адреси, към които не може да бъде осъществен достъп)

Като група във виртуалното пространство могат да бъдат обособени правонарушенията, свързани с качеството на информацията, представяна в рамките на електронната търговия.

Сделките, осъществявани по електронен път стават все по – популярни. Търговията чрез Интернет по своята природа е интернационална.

На този етап България няма собствен опит в развитието на широкомащабна електронна търговия, но за това има редица причини, една от които е отсъствието доскоро на собствена правна база.

Към момента търговската информация в Интернет се разполага в две форми: във вид на общи сведения за продавача и стоките(услугите) , които той предлага, или във вид на конкретни сведения за стоката (количество, цена, условия на доставка и заплащане) с предложение в случай на съгласие с указаните условия да бъде попълнен формуляр за поръчка . Т. е. разликата между тях се състои в това, че в първия случай конкретната сделка се състои извън рамките на Мрежата. Във втория информацията се разглежда като публична оферта за сключване на договор и затова тя е обвързваща за предложителя.

Възниква въпроса за правната природа на тази информация и последиците за нейната недостоверност.

Разглеждането на тази тематика може да стане в контекста на разпоредбите, относящи се до защитата на потребителските договори в Интернет, попадащи под дефиницията на чл. 69, ал.1 ЗЗППТ.

Въпреки, че приложното поле на закона по отношение на субектния състав е ограничен и влиза в рамките на легалните определения, той съдържа редица гаранции за правата на потребителите при осъществяване на сделки дистанционно, посредством електронен обмен на данни и използване на поместена в Интернет информация за продажба на стоки и услуги.

В два самостоятелни раздела законът отделя внимание на разпространяваната информация в Интернет под формата на реклама, като се посочват случаите обхванати от понятията заблуждаваща и непочтена реклама.

Тези общи разпоредби по отношение на рекламата могат да се отнесат към първият от посочените форми на предоставяне на търговска информация, с уговорката че те не са достатъчна гаранция за търсене и подвеждане под отговорност .

Що се отнася до втората форма, към нея могат да бъдат приложени правилата установени в чл.69 ЗЗППТ по отношение на съдържанието на предложението за сключване на потребителски договор. Офертата трябва да съдържа гаранции за адекватна защита на потребителя. В този смисъл тя трябва да съдържа като минимум информация за търговеца, за основните характеристики на стоката(услугата), въпросите за доставката ,за времето в което предложителя се счита обвързан с офертата и т.н. Съгласно чл.3 посочената информация трябва да бъде вярна, точна и ясна.

Може да се обособи и проблема за отговорността за разпространяването на информация, нарушаваща авторските права.
Известно е, че въпросът за правното регулиране и защита на изключителните права в Интернет в последно време придобива особена актуалност, тъй като Мрежата е препълнена с материали, нарушаващи авторските права. Всяка една държава се стреми да защити интелектуалния си потенциал , тъй като това е залог за

конкурентоспособността на нейната икономика и в този смисъл са създадени редица законодателни актове на международно и национално ниво.

Правонарушенията в тази област могат да бъдат представени в две форми:

На първо място е преобразуването на произведение в електронна версия и последващо публикуване в Интернет без съгласието на неговия автор;

На второ е копирането на материали от даден сайт за разпространение или поместване в друг сайт без уведомлението и съгласието за това на автора на материала.

2. Юридическа отговорност на доставчиците и защита на личните данни

На съвременния етап от развитие на законодателството в областта на обществените отношения, развиващи се във виртуалното пространство, проблемите свързани с отговорността за разпространяваната в Мрежата информация се разглеждат не в общ вид, а в контекста на дейността на информационните посредници като основни доставчици на услуги.

Обикновено доставчика не инициира информационното отношение, не избира съдържанието на предаваната информация и нейния получател, не влияе на съдържанието на информацията и осъщесвява съхранение на същата за време , определено от техническите стандарти и протоколи с оглед нуждитена предаване на информацията.

В този смисъл, доколкото Интернет е доброволно обединение на различни мрежи, доставчикът не носи отговорност за нормалното функциониране и достъпност на отделните сегменти в мрежата.

Доставчикът не може да гарантира възможността за нормалнен информационен обмен с тези сървъри, които временно или постоянно са недостъпни. Също така той не може да носи отговорност за неизправности по време на работа, произтичащи пряко или косвено извън сферата на разумния контрол от страна на доставчика.

Изучаването на законодателството в различните страни показва, че в тях проблема за отговорността на информационните посредници се решава различно , като могат да бъдат отделени три основни подхода:

Според първият от тях доставчикът във всички случаи носи отговорност за действията на ползвателите, независимо от това дали е знаел за тях;

Съгласно втория подход доставчикът не носи отговорност в случаите, когато е изпълнил определени условия, свързани с характера на предоставяната услуга, взаимодействието със субектите на информационния обмен и третите лица, чиито права са нарушени;

И на трето място доставчикът не отговаря за действията на ползвателите.

Първият подход се използва в Китай и страните от Близкия Изток където интернет доставчиците носят отговорност за всички действия на ползвателите, без значение за това дали са знаели за извършените действия или биха могли да знаят за тях.

Вторият подход е най – възприетия в европейското законодателство.

В европейската Директива за електронна търговия 2000/31/EC(Directive on electronic commerce, Council of European Union . Brussels,28 February 2000), са предписани указания към страните членки по въпросите за задълженията на интернет доставчиците (service provider) и границите на тяхната отговорност по отношение информационния поток като са разработени детайлно решения на основните проблеми. Подходът в Директивата съчетава два елемента: 1) установяване на гаранции за свободно предоставяне на услугите на информационното общество (ст.3), отсъствие на общи задължения за мониторинг върху информацията от страна на доставчиците (ст.15); и 2) възможност за въвеждане на ограничения на национално равнище.

Спрямо интернет доставчиците не е наложено общо задължение за наблюдение на информацията, която те прехвърлят или складират, нито да следят за факти или обстоятелства, указващи наличие на незаконна дейност, с изключение на временни и изрично посочени дейности по

наблюдение, инициирани от съответните държавни органи, съгласно националното законодателство.

Основанията за отговорност на доставчиците са формулирани с оглед видът на извършваната от тях дейност : просто предаване на информация , “кеширане”, “хостинг”.

1. Доставчикът на достъп до комуникационна мрежа не носи отговорност за прехвърлената информация при условие,че:
   - не инициира прехвърлянето;
   - не избира получателя на прехвърлената информация;и
   - не избира и не изменя информацията , която се прехвърля.
2. Когато услугата на доставчика включва прехвърляне в комуникационната мрежа на информация, той не носи отговорност за временно и автоматично складиране на информацията, с оглед целите на прехвърлянето(кеширане), направено по молба на получателя на услугата, при условие, че:
   - не изменя информацията;
   - съблюдава изискванията за достъп до информацията;
   - не се намесва в технологии, съответстващи на индустриалните стандарти, използвани за придобиване на данни за употреба на информацията;
   - действа незабавно за отстраняване или установяване на забрана за достъпа до информацията при узнаване на следното:
     - информацията при първоначалния източник на прехвърляне е била отстранена от мрежата;
     - достъпът до информацията е бил забранен;
     - компетентна организация е наредила такова отстраняване или забрана.
3. Когато доставчикът на достъп предоставя услуги по складиране на информация (hosting) на получателя на услугата, той не носи отговорност, ако:
   - не знае, че дейността е незаконна и не са му известни факти и обстоятелства, от които да е видно, че дейността е незаконна;
   - доставчикът, при узнаване на това действа незабавно за отстраняване или прекратяване на достъпа до информация;

- получателя на услугата не е под контрола на доставчика.

Визираните задължения на доставчика кореспондират с основно извършваната от него дейност в качеството му на посредник при осъществяване на електронна комуникация в мрежата. Доставчикът не носи отговорност за съдържанието на информацията, предоставена от трети лица, но при узнаване за такава той е задължен да предприеме съответните действия, ако това е технически възможно, като отстрани на дадената информация или достъпа до нея.

Подобно е решението и в редица предметни закони, отнасящи се до отговорността на доставчиците.

На практика съществува възможност за "узнаване"(откриване) на незаконни материали, но тя не може да бъде абсолютизирана.Това може да стане като се използват различни критични материали от ползватели, наблюдение на най- често посещаваните страници и на пряко свързаните с тях сайтове, автоматично откриване на подозрителни думи (използване на програмни продукти , наречени"crawiers")

Законодателно тези въпроси се свързват преди всичко със задълженията на доставчиците да съхраняват комуникационни данни за определен период от време. Този подход е възпроизведен в приетия във Великобритания Закон за противодействие на тероризма, престъпността и безопасността (Anti- terrorism, Crime and Security Act 2001) от 14.12.2001г., които съдържа специална част 11 " Съхранение на комуникационните данни".

Нейните положения се отнасят до задълженията спрямо доставчиците за съхраняване на комуникационни данни, направено на основание кодекс, споразумение или разпореждане от страна на Държавния секретар.

Тези задължения могат да се отнасят както до всички доставчици , така и до определен тип или даже до конкретен доставчик. Неспазването на тези задължения не носи само по себе си отговорност на доставчика, но независимо от това, така съхранените данни се признават в качеството на доказателства в съдебното производство(чл.102).

Възможно е този подход да бъде възприет в европейското право, където е започнало разработването на директиви, предвиждащи

задължения на доставчиците на услуги , свързани с електронните комуникации, да съхраняват записи на всички съобщения в течение на 12-14 месеца, по искане на правоохранителните органи. Съхраняваните данни следва да бъдат достъпни от всяка точка на територията на ЕС.

След събитията от 11 септември в американското право също се забелязва тенденция към засилване на държавния контрол по отношение задължията на доставчиците. Характерен пример за това е приетия на 26 октомври 2001г. USA Patriot Act (предвиждащ редица предохранителни мерки за пресичане и възпрепятстване на тероризма) и по- точно неговия Раздел II" Усилени процедури за наблюдение". Съгласно чл.210 на доставчиците се възлага задължението да съхраняват подробни записи на електронните съобщения включително име, адрес, тип и продължителност на услугата, средства за заплащане на услугата, номера на кредитната карта или банковата сметка. Тази информация може да бъде разкрита по реда на чл.112, с цел защита на живота и здравето доброволно – ако доставчика обосновано предполага, че разкриването на информацията е оправдано , или по искане на държавен орган.

Санкциите по този закон могат да бъдат налагани от съдилищата на цялата територия на САЩ без оглед пределите на териториалната юрисдикция. Тези мерки имат временен характер и са установени за период от четири години.

На този етап в българското законодателство не е определена в яснота границата на юридическата отговорност на информационните посредници. За съдебна практика в тази област все още не може да се говори. Затова са необходими редица законодателни решения.

Отделни положения, засягащи тези въпроси се съдържат в Закона за електронния документ и електронен подпис от 2001г., където в чл.6, ал.2 са визирани основни задължения на посредника при електронно изявление. Той е длъжен да разполага с техническо и технологично оборудване, което да осигурява надеждност на използваните системи ; да поддържа персонал ,притежаващ необходимите експертни знания, опит и квалификация; да осигури условия за точно определяне на времето и източника на предаваните електронни изявления; да използва надеждни системи за съхраняване на тази информация в срок от шест месеца.

Посредникът отговаря за причинените вреди от неизпълнение на задълженията му. Той ще носи наказателна отговорност, съгласно новите текстове в НК, отнасящи се до компютърните престъпления.

Положенията в ЗЕДЕП са твърде принципни, тъй като текстовете ясно визират задължения на доставчика по създаване на условия и използване на надеждни системи за съхраняване на информацията, но в разпоредбите липсват указания в кои случаи доставчикът извършва тези действия и кой е органът който може да ги инициира. Така създадените текстове не дават правомощия на доставчиците в тази насока и предприемането на действия от тяхна страна може да наруши основни конституционни права на ползвателите. В този смисъл тези текстове е необходимо да бъдат законодателно допълнени и прецизирани.

Текстовете на посочената Директива 2000/31/ЕС, отнасящи се до въпросите за отговорността на информационните посредници са пряко транспонирани в смислово и структурно отношение от българския законодател в приетия Закон за електронната търговия (обн. ДВ.бр.51,изм.доп.ДВ. бр.105/2006г., в сила от 24.12.2006г.)

Въпросите, свързани с незаконната информация и контрола върху нейното разпространение са регулаторни въпроси, засягащи информационното общество като цяло, които трябва да бъдат уредени на базата на административно сътрудничество както между страните – членки на ЕС , така и на международно равнище , при възприемани на принципа за баланс между свободата на информацията и нейното придвижване и защитата на обществените интереси.

От съществено значение за характеристиката на юридическата отговорност на информацинните посредници са въпросите , свързани със защитата на личните данни и неприкосновеността на личността.

В тази посока е издаденото Проекто- ръководство на Работна група по защита на данните към Съвета на Европа във връзка със защитата на личната неприкосновеност по Интернет. [2]

Документът поставя началото на “справедлива практика във връзка с личната неприкосновеност по отношение на потребителите и

[2] http: //europa.eu/int.eur _lex/en /com/pdf/en_599PC0348.pdf

доставчиците на услуги по Интернет”. В него е отбелязано, че договора за доставка на интернет услуги е необходимо да бъдат отбелязано какви данни на своите абонати събира, обработва и съхранява доставчика, по какъв начин и с каква цел. Той трябва да използва наличните технологии за защита на личната неприкосновеност, чрез осигуряване на неделимост на данните и конфиденциалност, както и физическа и логическа защита на мрежата. Доставчикът носи отговорност за правилното използване на личните данни. Той не може да използва такива данни за собствени рекламни или маркетингови цели, освен ако лицето , което е засегнато е дало явно съгласие за това.

Задълженията на доставчика в качеството му на администратор на лични данни, по тяхното правомерно обработване се съдържат и в българския Закон за защита на личните данни. Законът изисква обработваните данни : да са получени законосъобразно; да са събрани за определените в закон цели и да се използват само за изпълнението им; да съпътстват по обхват целите , за които се обработват; да са точни и актуални; да се съхраняват за период, не по- дълъг от необходимия, съгласно целите, за които се обработват.

Правото на информационните посредници да обработват лични данни на потребителите се предпоставя от тяхното изрично съгласие или изпълнение на клаузите на договор между страните (например при сключване на договор за откриване на електронна поща).

Основните разпоредби на ЗЗЛД са взаимствани от текстовете на Конвенция 108 от 1981г. на Съвета на Европа за защита на лицата при автоматизирана обработка на лични данни и Директива 95/46 на Европейската общност за защита на личността срещу обработка на лични данни и свободното движение на тези данни. Тези актове са допълнени от Директива 2002/58/ЕС на ЕП и ЕС за обработване на личните данни и защита неприкосновеността в електронно съобщителния сектор, която унифицира разпоредбите в областта на защитата на личните данни, като ги хармонизира в съответствие с Общата релаторна рамка на общността за електронните съобщителни мрежи и услуги.

В нея европейския законодател въвежда понятието “ трафични данни”, за означаване на всякакви данни, обработени за целите на

преноса на съобщения посредством електронна съобщителна мрежа или за съответно таксуване.

Едно съобщение може да включва информация за име, номер или адрес, предоставени от изпращача на съобщения. Трафичните данни могат да се състоят от данни за маршрута, продължителността, времето и обема на съобщенията, за използвания протокол, за местоположението на крайното съоръжение, за началото, края и продължителността на връзката.

Доставчиците на услуги трябва да предприемат необходимите мерки за защита сигурността на своите услуги и да информират абонатите за всеки специфичен риск от нарушаване сигурността на мрежата, особено за тези рискове, които са извън обхвата на възможните обезщетения от доставчиците на услуги. Доставчиците трябва да разяснят възможността за използване на специфични видове софтуер или технологии за криптографиране. Изискването за информиране на абонатите не освобождава доставчика от задължението да предприеме за своя сметка подходящи мерки за осигуряване на ниво на “ нормална сигурност на услугата”.

Доставчиците на услуги трябва да предприемат и мерки по защита тайната на съобщенията, както на тяхното съдържание, така и на данните свързани с тези съобщения. Директивата допуска автоматично, междинно или транзитно съхраняване на такива данни от доставчиците на услуги и без изричното съгласие на потребителите доколкото това става единствено с цел осъществяване на преноса и при условие , че:

- информацията се съхранява за период не по- дълъг от необходимото за преноса и за целите на управление на трафика;
- през времето на съхранение тайната остава гарантирана.

Момента на завършване на преноса на съобщение, след което трафичните данни трябва да бъдат изтрити, освен за целите на таксуването зависи от вида на предоставената електронна съобщителна услуга. При електронната поща , например, преносът завършва в момента, в който получателят изтегли съобщението от сървъра на своя доставчик на услуги.

Доставчиците на услуги могат да обработват трафични данни за абонати и потребители, когато е необходимо в определени случаи, за да установят технически недостатъци или грешки в преноса на съобщенията.

Директива 2002/58/ЕС съдържа и текст, визиращ условията за съхраняване на съобщения в хода на бизнес практиката. Когато е необходимо и законосъобразно такива съобщения могат да се записват с цел предоставяне на доказателство за търговска сделка . Необходимо е страните на съобщението да бъдат информирани за записа, неговата цел и родължителността на неговото съхраннение още преди записването. Записаните съобщения трябва да бъдат изтрити най- късно до изтичане на времето, през което сделката може да бъде оспорена.

Посочените положения на Директивата , е уместно да бъдат възприети от българския законодател по отношение регулиране на отношенията, свързани с защитата на данните в електронните съобщителни мрежи и в частност допълване и конкретизиране на текстовете на чл.6, ал.1 на ЗЕДЕП , в смисъла, отбелязан по- горе, с оглед синхронизирането им с нормите на европейското законодателство и внасяне на яснота по посочените въпроси.

В този смисъл са и принципите, записани в Декларацията на Съвета на Европа за свободата на съобщенията по Интернет , приета от Комитета на министрите на заседание на постоянните представители(Страсбург, 28.05.2003г.).

Възприема се позицията за ограничена отговорност на доставчиците на услуги по Интернет в смисъл ,че страните – членки не следва да налагат общо задължение за наблюдаване съдържанието на Интернет, до който осигуряват достъп, което пренасят или съхраняват, нито да търсят активно факти и обстоятелства, указващи за незаконна дейност.

Отговорността на доставчиците се определя съобразно характеристиките на техните функции. Изразената принципна позиция е , че страните – членки ни трябва да подвеждат под отговорност за съдържанието на информацията в Интернет доставчиците на услуги , когато тяхната функция се свежда до пренасяне на информация или доставка на достъп.

В случаите, когато техните функции са по- широки и включват услуги по съхраняване на съдържание, те следва да носят солидарна отговорност, ако не свалят информацията или деактивират достъпа до нея веднага щом научат за незаконния и характер.

Във всички случаи ограниченията на отговорността не трябва да се отразяват на възможността за налагане на възбрани, когато от доставчиците на услуги бъде поискано да прекратят или предотвратят до възможната степен нарушаване на закона.