ЗАКОНОДАТЕЛНА РАМКА В ОБЛАСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ ТЕХНОЛОГИИ В БЪЛГАРИЯ – СЪСТОЯНИЕ И ПЕРСПЕКТИВИ

ноември 2002
София

Съдържание

Съкращения

ДР	Допълнителни разпоредби
БИС	Български институт по стандартизация
БТК	Българска телекомуникационна компания
ЕКС	Европейски комитет по стандартизация
ЕКЕС	Европейски комитет по електронна стандартизация
МС	Министерски съвет
КРС	Комисия за регулиране на съобщенията
ЗЕДЕП	Закон за електронния документ и електронния подпис
ЕИСТ	Европейски институт по стандартизация в телекомуникациите
ЕС	Европейски съюз
ИКТ	Информационни и комуникационни технологии
МКЕ	Международна комисия по електротехника
ISO	Международна организация по стандартизация
ISP	Internet Service Providers - Доставчици на Интернет
СНРС	Съвет по националния радиочестотен спектър
OSP	Доставчици на онлайн услуги
ЗЗЛД	Закон за защита на личните данни
СС	Съвет по стандартизация
ДВ	Държавен вестник
ДКД	Държавна комисия по далекосъобщения
ЗД	Закон за далекосъобщенията
ЗТИП	Закон за техническите изисквания към продуктите

ЗАКОНОДАТЕЛНА РАМКА В ОБЛАСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ ТЕХНОЛОГИИ В БЪЛГАРИЯ – СЪСТОЯНИЕ И ПЕРСПЕКТИВИ.

I. Законодателна рамка на телекомуникационния сектор. Статус на телекомуникационните оператори. Начини за контрол

1. Общи условия

Правната рамка, която регулира информационните мрежи, електронните комуникации и електронната търговия в България се състои от значителен брой нормативни актове. Някои от тях контролират взаимоотношенията в сектора в общ план (такива са Закон за задълженията и договорите, Търговският закон, Наказателният кодекс, Закон за защита на личната информация, Закон за стандартизацията, данъчните и процесуалните закони и др.), а други осигуряват специфични регулации (например Законът за далекосъобщенията (ДВ №93, 11 август 1998 г.), Законът за електронния документ и електронния подпис (ДВ №34, 6 април 2001 г.), както и подзаконовите нормативни актове за тяхното прилагане, и др.).

Основните играчи на пазара за информационни и комуникационни технологии (ИКТ) в страната са телекомуникационните оператори според определението на Закона за далекосъобщенията. Това са икономическите субекти, които изграждат и притежават телекомуникационните мрежи, (като операторите на фиксирани мрежи, мобилните оператори, сателитните оператори и др.), както и компаниите, които осигуряват ИК услуги чрез тези мрежи без да са собственици на инфраструктурата. Следователно телекомуникационните оператори могат да бъдат разделени на мрежови оператори и оператори на услуги (доставчици на услуги).

Мрежовите оператори инсталират, управляват и поддържат собствена (фиксирана или безжична) телекомуникационна мрежа с цел доставка на обществени гласови услуги или обществени мрежови услуги. Доставчиците на услуги от друга страна са оператори, които предлагат телекомуникационни услуги, като използват основно мрежи на трета страна. Сред тези оператори специално внимание трябва да се отдели на тези, които осигуряват достъп до глобалната мрежа Интернет – *Доставчици на Интернет достъп (IAP – Internet Access Providers)*.

Важни играчи на пазара са *Доставчиците на интернет услуги (ISP)*. Терминът ISP има по-широк смисъл, тъй като той включва компаниите, предоставящи

различни Интернет-базирани услуги. За да се наблегне на факта, че се предлагат предимно услуги, различни от достъп до Интернет, тези оператори се наричат също и *Доставчици на онлайн услуги (OSPs)*. За целите на настоящия документ терминът OSP ще се използва в по-широк смисъл, като ще включва доставчиците на Интернет, както и на различни типове Интернет-базирани услуги.

OSP са част от кръга лица, чиято дейност се регулира от гореспоменатите актове. Според спецификата на извършваната дейност, те могат да се квалифицират като телекомуникационни оператори според Закона за далекосъобщенията, посредник на електронни изявления по ЗЕДЕП, администратори на лични данни по ЗЗЛИ и др.

2. Правен статут на далекосъобщителните оператори

Законът за далекосъобщенията (ЗД) и наредбите, приети във връзка с неговото прилагане съставляват основната рамка, която определя правния статут на OSP, които експлоатират цифрови мрежи. Такива OSP са телекомуникационните оператори по смисъла на ЗД. Този извод може да се направи на базата на определенията дадени в текста на ЗД. Според определението в §1 т. 17 от Допълнителните разпоредби на ЗД – "Далекосъобщителен оператор е всяко лице, което осъществява далекосъобщения въз основа на лицензия, регистрация или свободен режим". Според чл. 3 (1) от ЗД, "Далекосъобщения са пренасяне, предаване или приемане на знаци, сигнали, писмен текст, изображения, звук или информация от всякакъв вид чрез проводник, радиовълни, оптична или друга електромагнитна среда". Доколкото предоставянето на онлайн усуги включва предаване на знаци, сигнали и друга информация през кабели, радиовълни, оптика или друга електромагнитна среда, то може да се разглежда като далекосъобщение според значението на ял. 3 (1) от ЗД и съответно да се счита като далекосъобщителна услуга.

ЗД предлага три режима за осъществяване на далекосъобщителна дейност - индивидуална лицензия, регистриране по обща лицензия или свободен режим. Чл. 39 ЗД дава основната рамка осъществяването на съответната далекосъобщтелна дейност, а детайлно въпросите се разглеждат от Наредба 13 за определяне на далекосъобщителните дейности, подлежащи на индивидуално лицензиране, регистриране по обща лицензия и свободен режим (02 юли 2002 г.). Според специфичната дейност на далекосъобщителния оператор той може да попадне във всеки един от трите режима.

2.1. Индивидуално лицензиране на далекосъобщителните оператори

Според настоящото българско законодателство, далекосъобщителните оператори (ДО) имат нужда от индивидуален лиценз за предоставяне на услуги в някой от следните случаи:

2.1.1. Когато на ДО се предоставя индивидуално определен ограничен ресурс за изграждане, поддържане и използване на далекосъобщителна мрежа;

Случаите, в които ДО са обект на индивидуално лицензиране за използване на радиочестотния спектър – индивидидуално определен ресурс - са описани в детайли в Наредба 13, където са посочени следните хипотези, имащи отношение към дейността на ДО:

- Изграждане, поддръжка и използване на обществени или обособени далекосъобщителни мрежи от неподвижната радиослужба

- Изграждане, поддържане и използване на обществени или обособени далекосъобщителни мрежи от неподвижната спътникова радиослужба

- Изграждане, поддържане и използване на обществени и обособени далекосъобщителни мрежи за пренос на данни..

2.1.2.Индивидуално лицензиране на ДО когато се изгражда, поддържа и използва обществена далекосъобщителна мрежа и се предоставят обществени далекосъобщителни услуги чрез нея (чл. 39, ал. 3, т. 2 ЗД)

За издаването на индивидуална лицензия при споменатите хипотези трябва да са налични кумулативно следните условия: Изграждане, поддръжка и използване на далекосъобщителни мрежи; мрежата трябва да е обществена (т.е. да бъде предназначена за предоставяне на обществени далекосъобщителни услуги и/или за далекосъобщения между ограничен кръг потребители) и, освен това, през нея трябва да се предоставят обществени далекосъобщителни услуги.

Клаузите от чл. 32, ал.3, т.2 императивно указват случаите, в които според ЗД от ДО се изисква да имат индивидуална лицензия за да предлагат Интернет достъп до неограничен кръг от потребители без да използват индивидуално определен ограничен ресурс - а именно, когато те самите изграждат и притежават обществена далекосъобщителна мрежа. Наредба 13 дава по-подробно определение на типовете даейност, подлежаща на лицензиране – "изграждане, поддържане и използване на обществени далекосъобщителни мрежи за пренос на данни" (чл. 3, т. 2, Наредба 13).

Лицензиите се издават от Комисията за регулиране на съобщенията (КРС) без търгове или конкурс при поискване от ДО, който отговаря на поставените изисквания. Въпреки че процедурата по регистриране не е много усложнена, проверката в публичния регистър поддържан от КРС показва, че към момента много малка част от българските ISP са получили такъв лиценз. Това означава, че при текущите условия на все още съществуващия монопол за голяма част от далекосъобщителната дейност повечето от ISP не изграждат и не притежават далекосъобщителни мрежи.

2.2. Специфични задължения на лицензираните ДО

В случаите, когато ДО изграждат, поддържат и експлоатират обществена далекосъобщителна мрежа и/или предлагат обществени далекосъобщителни услуги с индивидуална лицензия, те работят като ДО по смисъла на т.18 от Допълнителните разпоредби на ЗД. Като такива, тези ДО са натоварени с някои допълнителни задължения в сравнение останалите ДО. Например, според т.11 от ДР на ЗД до отпадането на монопола на БТК в края на 2002 г., всички обществени

ДО са задължени да изграждат наземните части от своята мрежа чрез наети линии от БТК. На обществените ДО е забранено до 31.12.2002 г. да предлагат на трети страни наети линии, както и да преотстъпват линии наети от БТК - § 10, ал. 1б и § 11а, ал. 2 от Преходните и заключителни разпоредби на ЗД. Обществените ДО с индивидуални лицензии са обвързани също и със задължения от индивидуалната лицензия, влючващи подготовката на "Общи условия" за връзката им с потребителите, които са обект на координиране с КРС. някои по-общи условия също се прилагат - публикуване на цените на далекосъобщителните услуги и предаването на тези цени на КРС преди тяхното публикуване (чл. 111, ал. 1 и ал. 3 ЗД), предлагане на равни и обществено известни условия за предоставяните далекосъобщителни услуги, осигуряване на достъп и взаимосвързаност с други обществени ДО и др.

2.3. Регистрация според обща лицензия и свободен режим

Както бе упоменато по-горе, при използването на индивидуално определен ограничен източник ДО могат да изграждат ДМ – обществени или обособени – само след индивидуална лицензия от КРС.

Когато използват радиочестотния спектър определен за обща употреба в съответствие с *Националния план за разпределение на радиочестотния спектър на радиочестоти и радиочестотни ленти за граждански нужди, за нуждите на отбраната и на сигурността, както и за съвместно ползване между тях (ДВ №56/2002),* след регистрацията с общ лиценз ДО могат да изграждат обособени далекосъобщителни мрежи за обмен на данни, където съобщенията ще се предават за собствени цели (чл. 39, ал. 4, т. 1 и чл. 81, ал. 2 ЗД; чл. 7, ал. 2, чл. 9, ал. 2 и чл. 8, ал. 4, т. 4 Наредба 13).

Не се изисква лицензия за изграждане, поддръжка и използване на обособени далекосъобщителни мрежи за обмен на данни без използване на радиочестотния спектър – чл. 9, ал. 4, т. 3 Наредба 13. Общото между всички гореспоменати хипотези е, че те са приложими само за изграждането на обособени ДМ. Според определението на т. 3 от Допълнителните разпореднби на ЗД обособена далекосъобщителна мрежа е *"далекосъобщителна мрежа, предназначена за осъществяване на далекосъобщения, по нетърговски начин, за вътрешните нужди на обособения далекосъобщителен оператор, включително в и/или между неговите поделения, клонове или дъщерни дружества.*". Това означава, че при изграждането и експлоатацията на ДМ регистрирани по обща лицензия или свободен режим, без значение дали това става с или без използването на радиочестотен спектър, ДО няма право да предоставя далекосъобщителни услуги на клиентите си, и единствено ще може да пренася съобщения за собствени цели в обособената си ДМ.

Не се изисква лицензия за осъществяване на далекосъобщителни услуги, когато ДО не изгражда собствена ДМ, а използва мрежата на друг ДО и предоставя на крайни потребители Интернет достъп и други Интернет услуги.

3. Методи за контрол на далекосъобщителния сектор

ЗД въвежда разделения на функциите на държавно управление (изпълнявани от Министерството на транспорта и съобщенията (МТС), Министерски съвет (МС) и Съвета по националния радиочестотен спектър (СНРС)) от тези по регулиране на далекосъобщителния пазар (изпълнявани от КРС).

В изпълнение на задълженията си за управление на далекосъобщителната дейност МС приема Секторна политка за далекосъобщенията, която определя държавната политика в тази сфера. Актуализираната секторна политика беше публикуван в ДВ №62, 25 юни 2002. Тя подчертава основните насоки и конкретните етапи и условия за развитието на телекомуникационния сектор и неговото регулиране в България.

СНРС към МС изпълнява националната политика по отношение на радиочестотния спектър. Съвета подготвя и периодично аклтуализаира *Националния план за разпределение на радиочестотния спектър на радиочестоти и радиочестотни ленти за граждански нужди, за нуждите на отбраната и на сигурността, както и за съвместно ползване между тях*, който се одобрява от МС.

Министъра на транспорта и съобщенията изпълнява далекосъобщителната политика на базата на ЗД и Секторната политика приета от МС. Министърът подготвя, представя за одобрение пред МС и изпълнява секторната политика в сферата на телекомуникациите. Той изпълнява ролята на единствен собственик на капитала в едноличните търговски дружества и в компаниите от сектор "Съобщения" в които държавата е акционер или съдружник.

Регулацията и контрола на далекосъобщителната дейност в момента се изпълнява от Комисията за регулиране на съобщенията (наричана по-надолу "Комисията" или КРС). Комисията беше основана преди няколко месеца като наследник на Държавната комисия по далекосъобщенията (ДКД) с промяна на закона от декември 2001 г.

Новата комисия се различава съществено от закритата ДКД по отношвние на нейнта независимост, състав и мандат. Въведени са и нови функции на КРС - регулиране и контррол върху предоставянето на пощенски услуги, регистрация и контрол върху дейностите по предоставяне на удостоверителни услуги свързани с електронния подпис и т.н.

Създаването на КРС е стъпка напред в посока въвеждане на европейското законодателство по отношение на националните регулаторни органи. Комисията е независим специализиран държавен орган, който изпълнява секторната политика в далекосъобщенията и секторната пощенска политика приемани от МС като се спазва обществения интерес, държавния суверенитет и националната сигурност. Комисията регулира и контролира далекосъобщенията по реда определен в закона и регистрира и контролира дейностите по предоставяне на удостоверителни услуги свързани с електронния подпис по реда определен от ЗЕДЕП.

Комисията е колегиален орган съставен от пет членове, включително председател и заместник-председател. Основната й дейност в определена в чл. 27 ЗД и предполага: подготовка на документите и извършване на необходимите действия

за издаване на лицензии в областта на далекосъобщенията; тя има правото да издава, изменя, допълва, спира, прекратява и отнема лицензии за далекосъобщителна дейност и изграждане, поддържане и използване на нови ДМ; да регистрира и заличава регистрацията при обща лицензия за далекосъобщителна дейност; подготвя и управлява Националния номерационен план и разпределя номерата и адресите за далекосъобщителни мрежи между операторите, съобразно утвърдените принципи.

Комисията също така изпълнява определени дейности свързани с управлението на радиочестотния спектър, като: изработване и публикуване на принципи на управление и разпределение на на радиочестотния спектър, предоставяне за използване на радиочестоти и радиочестотни ленти на ДО лицензирани според този закон; издаване на разрешения за въвеждане на пазара на радиосъоръжения използващо нехармонизирани честотни ленти за граждански нужди, оползотворяване на радиосъоръженията за осигуряване на ефективно използване на радиочестотния спектър за граждански нужди и др. Комисията контролира съблюдаването на нормативните актове в сферата на далекосъобщенията, принципите на формиране на цената, качеството на услугите, условията определени в лицензиите и др.

II. Регулиране на далекосъобщителните мрежи и услуги – бъдещо развитие. Либерализация и хармонизация

Законът за далекосъобщенията е в сила от 15 август 1998 и е една от най-важните стъпки в преоцеса на хармонизация на българското заонодателство в сферата на телекомуникациите със съответното европейско законодателство.

Основната цел при приемането на ЗД бе създаването на необходимите правни и регулаторни рамки за развитие на далекосъобщенията и за задоволяване на обществените нужди за висококачествени и достъпни телекомуникационни услуги.

Според ЗД, далекосъобщителната дейност и услуги са частично либерализирани с изключение на предоставянето на гласови услуги (местни, междуградски, международни и транзитни между терминалните точки на фикдираната телефонна мрежа, предоставянето на наети линии и презграничното предаване на глас в реално време с цел осигуряване на международни гласови услуги от обществените ДО. Върху тези дейности има установен монопол до 31 декември 2002.

През 2002 г. беше направен и подробен преглед на законодателната рамка в сферата на телекомуникациите. През май МС прие Актуализираната стратегия за развитие на далекосъобщенията. В изпълнение на основните й цели и с оглед на пълната либерализация на телекомуникационния сектор след 31 декември 2002 г. МТС подготви проект за изцяло нов Закон за далекосъобщенията, който беше предоставен за одобрение от Народното събрание и МС. Актуализираната стратегия, както и проектозакона за далекосъобщенията осигуряват:

- прекратяване на монопола на БТК,
- пълна либерализация на пазара,
- въвеждане на регулаторни инструменти, които принуждават операторите със значително пазарно въздействие да изпълняват изискванията за конкурентна среда,
- определяне на обхвата на универсалната далекосъобщителна услуга и въвеждане на механизми за компенсиране на операторите, които я предлагат при икономически неизгодни условия,
- определяне на условията за взаимосвързаност на мрежите и достъп до последната миля (терминът последна миля се използва за означаване на физическата връзка, обикновено меден кабел, в локалната мрежа, свързваща обекта на клиента с принадлежащия на ДО локален суич, концентратор или подобно оборудване,
- развързване на последната миля, т.е. предоставяне на възможност на други ДО да осигуряват услуги за клиентите без задължително да използват други далекосъобщителни услуги от собственика на последната миля,

- определяне на правата за пренос през държавна и общинска собственост,

- напълно разделяне на регулаторните функции от управлението на собствеността,

- намаляване на лицензионните режими и процедури, осигуряване на предвидимост, прозрачност и предварително консултиране по отношение на лицензионната политика.

1. Либерализация на телекомуникационния пазар

Процеса на либерализация на телекомуникационния пазар в България започна през 1992 г. Той следва европейската политика и в частност, препоръките от Директива 90/388/ЕЕС за конкуренция на пазарите на тлекомуникационни услуги, и нейните последващи промени водещи до постепенното отваряне на телекомуникационните пазари. Либерализацията е част от процесите на настоящата структурна реформа в сектора. Тя следва правната и регулаторна рамка, отразена в ЗД и в съществуващото вторично законодателство.

В резултат на това към момента всички далекосъобщителни услуги, освен фиксираната гласова услуга и наетите линии са либерализирани. Според политиката за либерализация, отразена в ЗД, и задълженията поети в преговорите за присъединяване към ЕС според Глава 19, пълната либерализация ще се въведе след 31 декември 2002 г., и ще включва фиксираните гласови услуги, наетите линии и презграничното предаване на глас в реално време. В общи линии, въвеждането на пълна либерализация предполага, че всяко лице (физическо или юридическо), което желае да предлага някаква услуга на пазара, има правото да получи сътветното разрешение в зависимост от типа услуга. Това означава, че всички ограничения за достъп до пазара ще бъдат премахнати, освен на базата на обективни, прозрачни, пропорционални и недискриминационни критерии, свързани с използването на изчерпаеми ресурси. Отказът може да се направи само при обществено известни условия, определени в нормативен акт.

В сегашното законодателство – ЗД и Наредба 13 преобладават индивидуалните лицензии. Причината за това е ранната фаза на саморегулирането и неефективно действащите механизми на конкуренцията. В бъдеще лицензирането ще следва линия на пълно опростяване на режима по издаване на разрешения без да се пропуска надзора и контрола на пазара. Основната регулаторна рамка за издаването на лицензии за далекосъобщителна дейност в България следва насоките на директивите на ЕС. Основните принципи на лицензирането при условие на пълна либерализация са:

- премахване на ограниченията за брой на пазарните участници с изключение на случаите на използване на ограничени ресурси;

- даване на приоритет на регистрационните режими с обща лицензия пред режима на индивидуалното лицензиране;

- определяне на принципи, процедури и документи, свързани с лицензирането, включително създаването на прецедурата “едно гише”.

Въвеждането на пълна либерализация на пазара изисква приемането на редица законодателни мерки за насърчаване влизането на нови играчи и поддържането на честна конкуренция при спазване на насоките на ЕС по отнопение на политиката на конкуренция в телекомуникациите. Необходимо е да се създадат ясни правила за нужното съдържание на договорите за взаимосвързаност и достъп до инфраструктурата на ДО, които се конкурират на пазара; да се използват схемите за финансиране на универсалната далекосъобщителна услуга; да се осигури нормативно достъп до правата на пренос през държавна и общинска собственост и обща собственост върху различните мрежи и споделеното предоставяне на мрежи и услуги.

2. Хармонизация

Очаква се в началото на 2003 г. в България да бъдат направени значителни промени в регулаторната рамка по отношение на електронните мрежи и предоставянето на електронни услуги.

През септември 2002 г. МС представи на НС проектозакон за нов ЗД. Приемането на изцяло нов закон се налага не само от необходимостта за хармонизация на законодателството в областта на далекосъобщенията със законите на страните членки на ЕС, но и поради изтичането на срока за монопол в сектора. На 31 декември 2002 г. изтича монопола на най-големия ДО в страната - БТК, над определен брой далекосъобщителни услуги, като предлагането на фиксирана гласова услуга между крайните точки на фиксираната телефонна мрежа, наетите линии и презграничното пренасяне на глас в реално време. Целта на приемането на нов ЗД е да се подготвят условията за ефективна конкуренция в съответствие с тенденциите за либерализация на телекомуникационните услуги в Европа.

В сравнение с настоящия закон, проектозаконът за далекосъобщенията предлага редица решения непознати в българската съдебна система до момента. Той регулира: обхватът и основните изисквания за предоставяне на универсална далекосъобщителна услуга и компенсиране на разходите за предоставянето й; определението за "оператор със значително въздействие върху пазара" и неговите основни задължения; защитата на личните данни в телекомуникациите; достъпът до далекосъобщителните мрежи и взаимосвързаността; предоставянето на наети линиии използването на далекосъобщителни мрежи; основни права на потребителите на пазара; принципи на формиране на държавните такси и цените.

Проектозаконът е съобразен със задълженията поети при затваряне на Глава 19 при преговорите за присъединяване към ЕС - "Телекомуникационни и информационни технологии". Прие се тезата, че в предпресъединителния период законодателството ще бъде съобразено с *acquis communitaire* в сила към 2000 г. и до 01.01.2007 България трябва напълно да хармонизира законите си с европейските. Това е причината проектозакона да е съобразен с актовете действащи в ЕС в периода 2000-2001.

Не са взети под внимание директивите приети през 2002 г. - Директива 2002/21/ЕС за обща регулаторна рамка за електронните телекомуникационни мрежи и услуги (Рамкова директива), Директива 2002/19/ЕС за достъпа и взаимосвързаността на електронните телекомуникационни мрежи и оборудване (Access Directive), Директива 2002/20/ЕС за оторизацията на електронните

телекомуникационни мрежи и услуги (Authorisation Directive), Директива 2002/22/ЕС за универсалната далекосъобщителна услуга и правата на потребителите свързани с електронните телекомуникационни мрежи и услуги (Universal Service Directive), Директива 2002/58/ЕС по отношение на обработката на лични данни и защитата на личната информация в сферата на електронните комуникации (Directive on privacy and electronic communications) и Директива 2002/77/ЕС за конкуренцията на пазарите на електронните телекомуникационни мрежи и услуги.

Шестте нови директиви съдържат унифицираната регулаторина рамка за всички съобщителни мрежи и услугите, свързани с тях, като термините "електронни телекомуникационни мрежи и услуги" се използват вместо "далекосъобщителни мрежи и услуги". Приемането на новите директиви се наложи поради необходимостта от по-нататъшна либерализация на телекомуникационния сектор, повишената конкуренция и възможността за избор на услугите, което е и в основата за унифицирането на регулаторната рамка.

Новата регулаторна рамка на ЕС обхваща електронните комуникационни мрежи и тяхната взаимосвързаността за предоставянето на електронни комуникационни услуги. Определението електронни комуникационни мрежи и услуги до голяма степен е независимо от бързо развиващите се технологии в сектора. Мрежите, които се визират в новите документи включват всички комуникационни мрежи предоставящи обществено достъпни комуникационни услуги, като фиксираните и мобилните мрежи, кабелните телевизии, наземните излъчващи мрежи, сателитните мрежи, Интернет, независимо дали се използва за глас, факс, данни или изображения. Мерките в тези директиви целят да се създаде рамка, която да насърчава конкурентните мрежови инфраструктури и взаимносвързаността на услугите предлагани през тези инфраструктури, което е в полза на потребителите.

Проектозаконът за далекосъобщенията е съобразен с правната рамка, която ще бъде отменена от новите европейски директиви от 25 юли 2003 г. (датата, в която повечето от по-старите директиви ще бъдат отменени). Изборът направен от авторите на проекта изглежда логичен, като се вземе предвид етапа на развитие на пазара на телекомуникационни услуги в България, който се характеризира с прехода от държавен монопол към свободен режим. Именно този етап в ЕС бе регулиран от директивите, които ще бъдат отменени през 2003 г. От друга страна, избраният подход означава, че през 2007 г. (годината за очакваното присъединяване на България) ще трябва да се подготвя и приема трети, изцяло нов ЗД, който ще следва предписанията на европейските директиви от 2002 г.

III. Конкуренция в телекомуникациите и специфични въпроси – взаимосвързаност на мрежите, достъп до последната миля, предлагане на универсална далекосъобщителна услуга, оператори със значително въздействие върху пазара

В резултат на сериозните промени в глобалната телекомуникационна индустрия светът бе залят от вълна от про-конкурентни и дерегулационни политики. Тези процеси наложиха връзката между темите за либерализация на телекомуникациите и свободната конкуренция на пазара на електронни комуникационии услуги.

Сред най-важните мерки, които трябва да се предприемат за засилване на конкуренцията и долиберализирането на телекомуникационния сектор е развитието на регулаторна рамка за:

- Взаимосвързаност на мрежите, достъпа, наетите линии;
- Колокация и достъп до последната миля;
- Предоставянето на универсална далекосъобщителна услуга;
- Задължения на операторите със значително пазарно въздействие.

1. *Взаимосвързаност на мрежите*

Условията за предоставяне на отворени мрежи (open networks provision) в модерния либерализиран телекомуникационен пазар гарантират свободен и ефикасен достъп до далекосъобщителните мрежи в съответствие с хармонизираните условия в ЕС по отношение на технически интерфейс, условия за използване, принципи за тарифиране и достъп до честоти и номера/адреси/имена.

С оглед на гореспоменатото взаимосвързаността на далекосъобщителните мрежи се смята за един от ключовите фактори за предоставянето на отворени мрежи. Взаимосвързаността изисква прилагане на принципите на отворените мрежи - прозрачност, обективност, равнопоставеност, пропорционалност и дава приоритет на търговските споразумения между страните, взаимосвързване на мрежите им, според правила, определени от национален регулаторен орган. Ефективната система за взаимосвързаност е предпоставка за инвестиции, особено при условията на пълна либерализация на телекомуникационния пазар.

2. Достъп до далекосъобщителните мрежи. Наети линии.

В европейското законодателство "достъп" е общ термин, който включва всички форми на достъп до далекосъобщителните мрежи и услуги, предлагани от ДО или доставчиците на услуги, които използват мрежите като транспортна среда. Смята се, че взаимосвързаността е специфичен тип достъп, който осигурява връзка (физическа или логическа) между две далекосъобщителни мрежи. В директивите на ЕС "достъп" предполага да са налични съоръженията и/или услугите, за други задачи, при определени условия, с цел предлагане на електронни комуникационни услуги. Терминът включва например: достъп до елементи от мрежата (точки за достъп, точки на присъствие), както и, че услугите, свързани с тях, които могат да включват вкръзката с оборудването през кабели или безжично; достъп до физическата инфраструктура, включително сгради, канали (за прокарване на кабелите), и др.; достъп до софтуерни системи, заедно с оперативната им поддръжка; достъп до системи за транслиране на номера или системи със сходна функционалност и др. Достъпът до далекосъобщителните мрежи може също да се извършва и чрез наети линии.

Регулирането на поставените въпроси според в момента действащото законодателство на България все още е недостатъчно и не е изцяло съвместимо с предписанията на законите на ЕС. Чл. 84 от ЗД гласи, че обществените ДО са задължени да създават мрежите си по такъв начин, че да имат възможност да осигуряват достъп и взаимосвързаност помежду си. Те не могат да откажат на молба за свърване, ако тя е обоснована и технически необходима. В случай, че това е невъзможно, операторите са задължени да обяснят своя отказ писмено.

Достъпът до далекосъобщителната мрежа на обществен ДО се дава на базата на договори за взаимосвързаност, подписани от операторите, в които се определят техническите и финансовите параметри и които се представят на КРС. Обществените ДО са задължени също така да изграждат наземната част от своите мрежи чрез наети линии от БТК до 31 декември 2002 г. Те могат да отдават под наем линии при публично обявени условия в съответствие с принципите за равнопоставеност на наемателите. Въпреки това тази дейност до края на 2002 г. е държавен монопол и може да се осъществява единствено и само от БТК. Само при отказ от страна на БТК да осигури линии на даден ДО той може да поиска от КРС да му бъде разрешено изграждането на собствени линии (§11, Преходни и заккючителни разпоредби, ЗД)

Във връзка с въпросите за взаимосвързаността и нейното влияние върху телекомуникационния пазар трябва да се спомене и новият Проектозакон за далекосъобщенията. Според неговите предписания, правилата свързани с правата и задълженията на ДО по отношение на взаимосвързаността влизат в действие преди тези, които определят задължението на операторите със значително пазарно въздействие да осигурят справка за взаимосвързаността и нейната цена. Заради този пропуск в условията определени в проектозакона се появява предпоставка за отказ за свързване или за искане на необосновано висока цена. В резултат на това в случай на отказ клиентие на ДО няма да имат възможност да осъществяват повиквания към клиентите на ДО със значително въздействие върху пазара. Или в случай на необосновано висока цена клиентите на този оператор ще трябва да използват изключително скъпа услуга, защото повечето от техните повиквания ще

бъдат до клиентите на ДО със значително пазарно въздействие. И двете възможности водят до невъзможност на новопоявилите се играчи на пазара да предлагат конкурентни цени на крайните потребители, което е пречка за развитието на конкурентен пазар през преходния период.

3. Колокация и развързване на последната миля

По принцип, договорите за специфичен достъп до мрежа са въпрос на търговски и технически преговори между заинтересованите страни. В процеса на либерализация и влизане на нови играчи на пазара, колокацията (co-location) следва да бъде насърчавана с случаите, при които липсва технически капацитет за индивидуална експлоатация, има необходимост от запазване на околната среда, здравето или безопасността на хората или причината е съобразяване с целите и изискванията на обществената инфраструктура. Националният регулаторен орган (КРС?) следва да определи условията за колокация при ДО така че:

- трети страни да получат достъп до определени елементи или възможности на далекосъобщителната мрежа;
- да не бъдат нарушавани съществуващи права;
- да се предлага пре-продажба на определени услуги;
- да се осигури отворен достъп до технически интерфейси, протоколи и други ключови технологии, които се необходими за функционалната свързаност на услугите;
- да се осигурят възможности за колокация, включително колокация на подземни съоръжения (напр. тръби за полагане на кабели), сгради или кули;
- да се осигурят специфични услуги, необходими за фукционалната свързаност на услугите за потребителите, включително възможности за изграждане на интелигентни мрежи или роуминг на мобили мрежи;
- да се осигури достъп до системи за оперативна поддръжка или подобни софтуерни системи, необходими за гарантирането на справедлива конкуренция в предлагането на далекосъобщителни услуги;
- да се предлага взаимосвързаност или достатъчен капацитет на далекосъобщителната мрежа.

В условията на пълна либерализация е изключително важно да бъдат създадени условия множество ДО да имат достъп до крайните потребители на базата на вече изградената последна миля, собственост на разполагащата преди с монопол в тази сфера БТК. Тази услуга трябва да се предлага от ДО със значително пазарно въздействие и се нарича “развързване на последната миля” (Local Loop Unbundling). Според Разпоредба No. 2887/2000 на Европейския Парламент и Съвета на ЕС развързването на последната миля включва пълен или споделен достъп до потребителите (абонатите) през кабелите, свързващи техните помещения с устройствата на ДО със значително пазарно въздействие. Предлагат

се два варианта за развързване на последната миля – пълна или споделен достъп до кабелите.

Развързването на последната миля позволява на новите ДО да предлагат на потребителите достъп до нови услуги, посредством нови технологии като xDSL (Digital Subscriber Lines), работещи върху съществуващата в момента преносна среда (медни чифтове). Алтернатива на тази среда е използването на радиовръзка между абоната и базовата станция, която е част от далекосъобщителна мрежа, използваща честоти в обхвата на 2.6GHz, 3.5GHz, 26GHz и др. Условията за създаване на конкуренция при последната миля са споменати в посочената по-горе Разпоредба на Европейския Парламент и Съвета на ЕС. Важен елемент от нея е задължението на ДО със значително пазарно въздействие да осигурят достъп (пълен или споделен) на други ДО при условията, които важат за самия ДО със значително пазарно въздействие или неговите дъщерни дружества. След координиране с КРС, ДО със значително пазарно въздействие е длъжен да обяви и актуализира референтно предложение за условията за развързване на последната миля при разходно-ориентирани цени.

Новият проектозакон за далекосъобщенията третира темата за развързването на последната миля поради факта, че целта на развързването е намаляване на икономическите и техническите бариери за новите играчи на далекосъобщителния пазар. Като правило конкуриращите се ДО не са склонни да финансират изграждането на дублиращи (т.е. нови) мрежи поради необходимите значителни инвестиции и време. В същото време съществуващите ДО със значително пазарно въздействие не са склонни да осигурят на своите конкуренто достъп до неразвързани компоненти на мрежата, освен ако не за задължени да направят това. Именно поради това задължителното развързване на последната миля е залегнало в проектозакона.

4. Универсална услуга

Осигуряването на универсална услуга (предлагане на определен минимален комплект услуги на всички крайни потребители на достъпна цена) може да включва осигуряване на някои услуги на част от крайните клиенти на цени, които се различават от нормално определените на пазара. Усилията, които са направени за предлагането на тези услуги се компенсират според предписанието на закона, който описва също и поддръжката и развитието на универсалната услуга в съответствие с принципите на прозрачност, пропорционалност и липса на дискриминация.

Основно изискване към универсалната услуга е тя да предлага на потребителите (при желание от тяхна страна) връзка към обществената телефонна мрежа на определено място и на достъпна цена. Обхватът на универсалната услуга може да бъде разширен с предлагане на безплатно повикване за населението (спешна медицинска помощ, пожарна и аварийна безопасност, полиция), услуги за търсене на номер на абонат, достъп до гласови услуги през обществените телефони, специални услуги, които позволяват на индивидите да използват услугите от обхвата на универсалната услуга - всичко това е изключително важно с оглед на обществения интерес. В съответствие с изискванията на европейските норми, КРС отговаря за определяне на начинанията, които са задължени да предлагат

универсалната услуга според методологията, одобрена от Министерски съвет. В §10 от Проектозакона за далекосъобщенията, БТК е задължена да предлага универсална услуга за 9 месеца след влизането на закона. Това гарантира правата на потребителите и плавния преход към разпределение на задълженията за универсална услуга сред всички конкуренти на пазара.

5. Оператори със значително пазарно въздействие (ЗПВ)

Терминът "значително пазарно въздействие (significant market power)" е определен за първи път в Директива 97/13/ЕС (отменена), а след това в Директива 2002/22/ЕС (от 7 март 2002 г.). Основните формулировки от настоящото европейско законодателстство предполагат, че ДО има ЗПВ в случай, че индивидуално или в съдружие с други, заема доминираща позиция, или позиция с икономическа сила, която му дава възможност да влияе върху конкуренцията, клиентите и крайните потребители.

Новият проектозакон за далекосъобщенията следва горната дефиниция. Според неговите предписания се смята, че ДО има ЗПВ, ако притежава над 25 на сто от съответния телекомуникационен пазар в географския регион, където той има разрешение за работа. Националният регулаторен орган може да реши, че ДО с пазарен дял под 25 на сто от съответния пазар има ЗПВ, както и обратно - че ДО с над 25 на сто от пазара не е оператор със ЗПВ.

Тъй като основният въпрос е определението за пазара на продукти и услуги в далекосъобщенията, в проектозакона е записано, че националният регулаторен орган анализира пазара на продукти и услуги според методология, подготвена от КРС и одобрена от МС. Методологията определя принципите, които регулаторните органи трябва да следват, когато оценяват ефективната конкуренция на пазара или наличието на значително пазарно влияние. Изготвеният анализ на всеки пазар трябва да се публикува. На базата на анализите, подготвени по тази методология, националните регулаторни органи изразяват своето мнение дали пазарът в определен район е наистина конкурентен.

Задълженията наложени на ДО със ЗПВ са дефинирани в законодателството на ЕС за да се осигури предлагането на универсалната услуга и взаимносвързаност чрез прилагането на принципите за отворената мрежа, които са базирани на прозрачност, липса на дискриминация, отделни сметки; достъп до инфреструктурата на мрежата; контрол на цените, включително условия за ориентация на цените и системи за отчитане. Някои от тези задължения могат да се обобщят както следва: осигуряване на достъп на определено място, предлагане на специални мерки за инвалиди, качество на услугите и т.н.

IV. Стандартизация в сферата на ИКТ

За да може да се определи текущото състояние и да се прогнозират насоките за развитие на ИКТ пазара трябва да се вземат под внимание процесите на стандартизация в телекомуникациите. Този въпрос има отношение към възможностите за бързо и сигурно разгръщане и прилагане на последните технологии и висококачествени информационни и комуникационни услуги. Основните аргументи за развитието на стандарти в сферата на далекосъобщенията са необходимостта от ясни технически критерии по правните въпроси и договорите, осигуряването на бази за оценяване на продуктите, процесите или услугите, главно с оглед безопастност, както и нуждата за глобално познаване и използване.

1. Определение

Стандартът може да бъде определен като техническа спецификация, одобрена от официално признат орган и предназначена за обща и многократна употреба. Според юридическото определение в чл. 3 от Закона за националните стандарти всеки стандарт трябва да бъде одобрен и разпространяван според процедурите зададени в закона, а името на стандарта, номера и регистрационния му номер трябва да бъдат публикувани в Официалния бюлетин на Българския институт по стандартизация (БИС). В момента, стандартизирането е доброволна процедура, която се базира на консенсуса между различни икономически и социално обвързани субекти – производители, потребители, обществени институции и др. заинтересовани страни. При все това, само стандарти съобразени с характеристиките в чл. 3 могат да влизат в сила и да се смятат за официални български стандарти.

Към момента, стандартизацията в далекосъобщителната сфера се регулира от Закона за националната стандартизация и Закона за техническите изисквания за продуктите, както и от предписанията на чл. 30 на ЗД, според който КРС се определя като "*национална стандартизационна организация пред Европейския институт по стандартизация в телекомуникациите*". Правният режим работещ в момента се допълва от няколко наредби и процедури, издадени от БИС. Някои от тези актове са: Наредба за етикетирането във връзка с техническите изисквания към продуктите; Процедура, определяща стандартизационните дейности за включването на техническите комитети в Регистъра на техническите комитети по стандартизация за одобряване и гласуване на стандартите и др. Република България е член на ISO, IEC, CEN, CENELEC и други организации по стандартизация. Въпреки това няма международен или европейски стандарт в сферата на телекомуникациите, за който да се смята, че е официално в сила според българското законодателство, освен ако не е въведен като Български национален стандарт.

2. Институции и органи участващи в развитието и прилагането на стандарти

Процесът по стандартизация в областта на далекосъобщенията е дейност, която се организира и управлява от БИС и Съвета по стандартизация (СС) към института.

2.1. Български институт по стандартизация

БСИ е националния орган по стандартизация в РБългария, който представлява държавата пред междунартодните и европейските организации по стандартизация (ISO, IEC, CEN, CENELEC и др.). Неговите правомощия са определени в чл. 6а от Закона за националната стандартизация, като най-важните от тях са организацията на изработването и подготовката за одобрение на българските стандарти, както и осигуряването на единството и липсата на противоречие между съществуващите стандарти. Въпреки това трябва да наблегнем, че на базата на изричните предписания на чл. 30 от ЗД статус на национална организация по стандартизация по отношение на ETSI има КРС.

2.2. Съвет по стандартизация

Съветът по стандартизация подпомага председателя на БСИ при определяне на приоритетите при работа над националната стандартизация в съответствие с развитието на телекомуниакционните пазари и одобрява програма по стандартизация. Той се състои от 11 членове, представители на институции, оказващи вличние върху сферата на телекомуникациите като Българската търговско-промишлена палата, Българска стопанска камара, Българска академия на науките, Асоциация на националните застрахователи и др.

2.3. Технически комитети

Хората, които се интересуват от създаването на българските стандарти в сферата на далекосъобщенията могат да се организират в технически комитет, които са отговорни за приемането на проекти за български стандарти в съответните области. Според предписанията на чл.12, ал.2 статут на "технически комитет" се постига след като той се запише в Регистъра на техническите комитети по стандартизация на базата на заповед, издадена от председателя на БИС в случай, че няма друга регистрирана комисия, която да работи в същата сфера. В момента има три технически комитети към БИС, които от близо се занимават с дейността на ДО. Тези комисии са: Технически комитет по радиокомуникационните системи и радио оборудването, Технически комитет по ИКТ, и Технически комитет за електронната обмяна на комуникации в индустрията и администрацията. Последната отговаря на ISO/TC 154 и ISO/TC 184.

3. Процедури за развитие на стандартите

Заради изискванията за хармонизация на телекомуникационното законодателство с европейските стандарти е необходимо да се въведат като български стандартите, свързани с радио-оборудването и терминалното телекомуникационно оборудване, както и съответните стандарти по отношение на изискванията за безопастност при работа с електричество и електромагнитна сигурност. С оглед на тези изисквания трябва да споменем, че Законът за националните стандарти определя две процедури за създаване на стандарти – първата е според Раздел II, който е

посветен на създаването и прилагането на българските стандарти, и тази според Раздел III, който излага процеса на въвеждане на международните и европейските стандарти.

Ако техническите спецификации в стандарта са ясни и добре описани, ако той е технически реализируем, има множество независими приложения със значителен оперативен опит, получава значителна обществена подкрепа, и е очевидно полезен за някои или всички сфери на телекомуникациите, тогава конкретни предложения за изработване на български стандарти могат да се подават и от отделни хора или юридически лица пред БИС, както е описано в чл.24 и следващите.

Европейските стандарти в сферите, които по принцип не се регулират (например международните етикети на продуктите) стават официални за България, ако е спазена процедурата според Закона за националните стандарти. В него са описани две процедури за въвеждане на международен или европейски стандарт – публикуване на текста на стандарта в превод на български език или чрез утвърждаване на прилагането му като български стандарт.

В случай на одобрено предложение за въвеждане на международен или европейски стандарт чрез публикуване на текста на стандарта в превод на български език, работните групи към техническите комисии са длъжни да проверят техническата терминология на превода и проведат оформянето му като стандарт. Ако предложението за въвеждане на международен или европейски стандарт чрез утвърждаване на прилагането като български стандарт се одобри, БИС издава документ за потвърждение.

Гореспоменатите процедури за въвеждане на стандарти са от изключително значение за прилагане на европейските стандарти от серии BSS EN ISO 9000 и BSS EN 45000, BSS EN ISO/IEC 17025, които са много важни за хармонизацията на българската сертификационна система с европейската. Те са необходима предпоставка за подписваните договори с ЕС за взаимно признаване на съгласувания резултат от оценката на оборудването и услугите в областта на телекомуникациите с изискванията изложени в хармонизирания стандарт.

С оглед на премахването на монопола на БТК след 31.12.2002 г. и влизането на нови ДО на пазара приоритет в процеса по стандартизация трябва да бъде транспонирането на европейските стандарти свързани с предоставянето на отворени мрежи, аналогови и цифрови наети линии, взаимосвързаността на мрежите и пакетните услуги за данни.

4. Технически изисквания за продуктите

Докато ЗНС определя етапите на процеса по стандартизация, изискванията за движението на документите между етапите и типовете документи използвани по време на процеса, Законът за техническите изисквания за продуктите съдържа задълженията на ДО по отношение на продуктите и оборудването, които те използват, както и надзора за тяхното съответствие с техническите изисквания.

Въвеждане на продукти в употреба, според Допълнителните разпоредби на ЗТИП, представлява моментът в който продуктът преминава на етап първа употреба от крайния потребител. Дейността на ДО, свързана с продукти, за които има определени съществени изисквания може да се упражнява от тях легално

само след оценяване на съответствието на продукта на тези изисквания. Те са определени в наредби, издавани от Министрите след одобрение от МС и задават нормите, които продуктът покрива или рисковете, които трябва да се избягват за да се осигури защита на живота и здравето на хората, безопасността на домашните животни и защитата на околната среда и собствеността. Задълженията на ДО са определени в чл.4, ал.2 от ЗТИП, които гласят, че задължението за оценка на качествата на продукта са на този, който ги пуска в употреба – производител, вносител или този, който ги сглобява, инсталира или осъществява друга дейност, която може да окаже влияние върху съвместимостта на продукта със съществените изисквания. Оценките за тях могат да се правят от хората, които пускат продукта в употреба или от лица, които са получили разрешение за провеждане на такива тестове.

Единственото изключение от задължението за оценяване е описано в чл. 5 от ЗТИП, според който продуктите проектирани и произведени по изискванията на български стандарти, следващи приблизително европейски стандарти ще се смятат за съвместими с основните изисквания определени в съответната приложима наредба.

Либерализацията на далекосъобщенията и глобализацията, съсредоточаването на технологии, миграцията на мрежата към ATM и IP, както и усилията за все повече мобилност при телекомуникациите водят до засилване на ролята на стандартизацията като техническа нормативна база за регулиране и предоставяне на услуги в конкурентна среда. Ето защо въвеждането на стандарти за услуги, терминално и мрежово оборудване е от изключително значение за да се улеснят търговските преговори между ДО и потребителите на достъпа и услугите.

V. Правни аспекти на електронната търговия. Електронен документ, електронен подпис и услуги, свързани с него. Инициативи за Електронно правителство

1. Преглед на правната рамка на електронната търговия

Във времето на постоянното и бързо развитие на информационните технологии електронните комуникации между правните субекти са станали един от обичайните и предпочитани начини за комуникация. Съдебната система в много страни (България не е изключение) се сблъсква с трудности при регулиране на специфичните проблеми, произтичащи от използването на електронни средства за комуникация и обмяната на стоки и услуги през Интернет.

С оглед необходимостта от създаването на модерна законодателна рамка за развитието на електронна търговия от една страна, и стратегическото ударение на процеса по хармонизация на българското законодателство с това на Европейския съюз от друга, Министерският съвет прие с Решение №679/29.10.1999 г. Стратегия за развитие на информационното общество и Национална програма за развитие на информационното общество на РБ. В последствие Програмата беше обновена с Решение №213 от 4 октомври 2001 г. Един от основните елементи на програмата е развитието на регулаторна рамка за електронния подпис и електронната търговия, която да следва европейските директиви в областта, както и други подобни международни документи.

В резултат на работата по тези въпроси през април 2001 беше поставена основата за развитие на електронната търговия - приет бе нов Закон за електронния документ и електронния подпис (ЗЕДЕП - ДВ 34, 6 април 2001 г.). Законът влезе в сила шест месеца по-късно - на 7 октомври 2001 г. ЗЕДЕП е подготвен на базата на Директива 1999/93/ЕС за Обществена рамка за електронен подпис. Малко по-късно бяха приети от МС и три наредби за прилагането на закона - Наредба за дейността на доставчиците на удостоверителни услуги, реда за нейното прекратяване и за изискванията при предоставяне на удостоверителни услуги; Наредба за реда за регистрация на доставчиците на удостоверителни услуги и Наредба за изискванията за алгоритмите за усъвършенстван електронен подпис (ДВ №15, 08.02.2002 г.).
Трябва да се има предвид, че дори и преди влизането на ЗЕДЕП в сила, взаимодействията в сферата на електронната търговия се регулираха от останалите закони, регламентиращи търговските взаимоотношения като цяло. Част от тези закони са: Търговският закон и Законът за задълженията и договорите, Законът за защита на потребителите и за правилата за търговия, Законът за защита на конкуренцията, специалните закони регулиращи банковата и застрахователната дейност, и др. Основната цел на ЗЕДЕП е да създаде основата на специфичната законодателна рамка за електронна търговия в България, която да отрази всички особености на сектора.

Въпреки това, дейностите свързани с електронната търговия са много повече от това, което обхваща ЗЕДЕП – например, те включват осъществяване на отдалечени договори за продажби на стоки онлайн; предоставяне на достъп, използване на

търсене, достъп и обработка на данни, осигуряване на достъп до обикновен и защитен пренос на информация през комуникационни мрежи и предоставяне на достъп до такива мрежи, предлагане на хостинг, особености при набиране на информация от ползвателя на услугата, установяване на ясни и точни изисквания за необходимите мерки за контрол на Интернет доставчиците и др. Регулирането на всички тези въпроси излиза много извън обхвата на приложение на ЗЕДЕП.

Приемането на закон, който да регулира отношенията при електронната търговия е необходимо заради изискванията на Директива 2000/31/ЕС за определени правни аспекти на услугите за информационното общество, и по-специално електронната търговия (Директива за електронна търговия), другите Европейски директиви, към които тя препраща по отношение на е-търговията, както и Закона-модел за електронна търговия на УНСИТРАЛ. В момента има две работни групи, които се занимават с подготовката на такъв закон за България. Първата група е организирана от Министъра на държавната администрация, а втората е между-институционална, водена от Министъра на икономиката.

2. Цели на ЗЕДЕП. Сфери на приложение.

Основният проблем, който играчите на пазара срещат при комуникацията си при използване на частни или обществени мрежи е създаването на бърз и сравнително сигурен метод и инфраструктура за обмен на информация. Наличието на тези неща ще благоприятства за увеличаване на доверието във възможността да се идентифицира автора на съобщенията и да се потвърди тяхната цялост.

По цял свят електронният подпис, базиран на инфраструктурата на публичния ключ е основно използвано средство за сигурност при комуникациите. Доставчиците на доверителни услуги свързани с е-подписите играят важна роля в тази структура. Дали чрез издаване на сертификати, или чрез използване на удостоверителни и други спомагателни услуги, те са тези, на които играчите на пазара имат доверие и поверяват защитата на електронно подписаните документи.

Ето защо е необходимо да се въведат правила за юридическо признаване на ЕП, както и за дейността по предлагане на удостоверителни услуги.

Както вече беше споменато, ЗЕДЕП влезе в сила на 7 октомври 2001 г. Целта на закона е да се уреди правният статут на електронния документ и електронния подпис и условията и реда за предоставяне на удостоверителни услуги. Разпоредбите на закона не се прилагат относно сделки, за които законът изисква квалифицирана писмена форма или когато държането на документа или на екземпляр от него има правно значение (ценни книжа, товарителници и други)..

За разлика от директивата, според българския закон и двата основни типа електронен подпис (квалифициран и неквалифициран) са равни по отношение на правните последствия, които предизвикват в сравнение с ръкописния подпис, освен в случаите, когато подписващия или адресата на електронното изявление е държавата, държавен или общински орган. Универсалният електронен подпис, като разновидност на квалифицирания подпис има силата на ръкописен подпис по отношение на всички.

Не е необходимо да се прави специална промяна на процесуалните закони, която да позволява приемането на документ подписан с усъвършенстван е-подпис. В процесуалните закони вече са определени ясни правила за приемането на писмените доказателства, от което следва, че електронният документ (който е приравнен на писмения), трябва да бъде приет.

Обхватът на закона не е ограничен само до регулиране на използването на електронни подписи в частния сектор, а също така и в обществената сфера. Българският законодател е възприел няколко особености в това отношение. Всички граждани и организации могат да подписват документи до държавните и общински власти само с универсален електронен подпис, и *обратно*, за да може тези подписи да бъдат смятани и юридически признати като ръкописни. Универсален е-подпис ще се използва от STC, регистрираните доставчици на удостоверителни услуги, всички държавни органи, и др. В изключение на това правило, законът гласи, чеМинистерски съвет ще определя държавните органи, които могат да използват друг тип е-подпис в своите взаимоотношения.

Министерски съвет ще определи органите, които не могат да отказват приемането на електронни документи, подписани с универсален е-подпис, и не могат да отказват издаването на разрешения, лицензи, одобрения, и други административни актове във формата на електронен документ, подписан с универсален електронен подпис. Вторичното законодателство в това отношение все още не е прието.

Приемането и издаването на електронни документи, подписани с е-подпис в съдебната система ще се определя в закон. В момента такъв закон се подготвя от работна група от юридически консултанти.

Приемането и издаването на електронни документи, подписани с е-подпис от други държавни органи освен описаните по-горе и освен местните органи за самоуправление ще се определя от техни собствени актове. Процедурата и формата за представянето и съхраняването електронните документи на се определя от вътрешни правила. Все още няма издадени подобни актове.

3. Пазар на удостоверителни услуги

Към момента няма развит пазар за удостоверителни услуги в България.

Причината за това се крие в липсата на ясни процедури по регистриране на доставчиците в КРС, липса на органите, които трябва да извършват техническата и организационната проверка на доставчиците на удостоверителни услуги (УУ), липса на развит електронен регистър в КРС и т.н. Факт е, че все още няма регистрирани доставчици на УУ.

Има няколко компании, които се подготвят да работят като доставчици на УУ.

Единствените официално подадени документи до момента са на фирма Информационно обслужване АД. Компанията е подписала с Utimaco Safeware договор за 1.6 милиона евро за създаване на инфраструктура за сигурността за приложенията на електронното правителство, планирана от Министерството на финансите. Партньор по изпълнението на проекта е компанията GlobalSign.

Българската стопанска камара е действащ в момента представител на GlobalSign за страната. БСК също възнамерява да подаде документи за доставчик на УУ.

Освен това в България има няколко Web-Of-Trust нотариуса, които предлагат услуги от името на Thawte.

4. Прогноза за използването на електронен подпис в България

Очаква се, че след влизането в сила на закона и определянето на доставчиците на удостоверителни услуги, в рамките на една година ще бъдат издадени 60 000 сертификата. Те ще дадат на компаниите и индивидуалните потребители възможност да изпращат данъчни и митнически декларации, молби към определени държавни институции и т.н.

Правителството има намерение да въведе система за електронен документ за лична идентификация за всеки български жител, за целите на която трябва да се издават сертификати от национален доверителен център. Най-вероятно той ще се базира на финландския модел.

Трябва да се има предвид обаче, че осъществяването на гореспоменатите прогнози до голяма степен зависи от успешния изход и ефективното изпълнение на организационните и технологичните цели, залегнали в инициативите за електронно правителство на МС.

5. Електронно правителство

Електронното правителство включва използването на информационни технологии от държавните органи с цел улесняване и автоматизиране на предоставянето на услуги от администрацията към гражданите, бизнеса и не на последно място между държавните ведомства. Създаването му ще се отрази в няколко различни насоки: по-добро взаимодействие с гражданите и бизнеса, разширяване на достъпа до информация, и по-успешно управление на държавата. Естествените резултати от това ще са намаляване на корупцията, по-голяма прозрачност, повече удобства при работа с държавната администрация, повишаване на приходите и намаляване на разходите.

Съобразно ангажиментите поети от българското правителство във връзка с изискванията за хармонизация на националното законодателство с европейското, България бе включена в Паневропейски проект за създаване на Електронно правителство. Инициативата стартира през юли 2002 г., когато беше изготвен и първият вариант на Стратегия за електронно правителство в страната. Според документа, до края на 2005 г. правителството ще предлага 12 различни типа услуги, които ще бъдат достъпни през Интернет за гражданите и фирмите.

По принцип, взаимоотношенията между гражданите и компаниите от една страна, и държавните органи от друга, се осъществяват в определени за целта места. С появата и усъвършенстването на информационните и комуникационните технологии става възможно да се намали до голяма степен тази зависимост и да се

улесни достъпът на потребителите. Според стратегията за е-правителство услуги като подаване на данъчни декларации, плащане на социални осигуровки или попълване на различни документи (за издаване на лични карти и др.).

В Стратегията за електронно правителство, аналогично на процесите при е-търговията, са определени няколко типа взаимоотношения, които целят да направят връзките правителство-граждани (G2C), правителство-бизнес (G2B), и вътрешноведомствените връзки (G2G) по-лесни, удобни, прозрачни и евтини. Там са дефинирани и четири етапа: 1) публикуване, 2) интерактивност, 3) завършване на транзакцията, и 4) доставка. Към момента, повечето от дейността на правителството е концентрирана върху публикуването. До сега 150 от 260-те общини имат присъствие в Интернет, както и близо от 80 на сто от държавните институции притежават уеб-страница.

Като се вземат предвид гореспоменатите факти, ясно е, че българското правителство оценява важността на прехода от традиционните начини за взаимодействие към електронните. Въпреки това трябва да се има предвид, че електронното правителство включва дългосрочна програма за развитие на съвременен мениджмънт и технологични мерки, с цел подобряване на взаимодействието между държавната администрация, гражданите и бизнеса.

VI. Електронно банкиране. Системи за електронно разплащане

1. Електронно банкиране

Развитието на електронната търговия доведе до необходимостта от адекватни начини за разплащане в Интернет. Банките, финансовите институции и останалите участници в електронната търговия установиха този факт с въвеждането на нов тип банков продукт - електронното банкиране (е-банкиране) или използване на информационните и комуникационните технологии с оглед улесняване на достъпа на клиентите до услугите, предлагани от дадената банка. Въпреки че кешовите разплащания в България са доминиращи, има сериозна липса на законодателни рамки и на навици в потребителите да използват безналични разплащания, българските банки вече направиха първите опити за разширяване на обхвата на своите продукти с включване на е-банкирането.

Българското законодателство не съдържа специални норми за регулиране на е-банкирането. Тази услуга дори не е включена в списъка на лицензираните банкови сделки в чл.1, ал.2 от Закона за банките, в който са описани 16 типа такива сделки. Различните форми на е-банкиране са свързани основно с достъп до справочна информация за банковите сметки, както и с възможността да се нареждат плащания през телекомуникационните мрежи. Тези услуги се базират на вече съществуващи връзки между банката и нейните клиенти, които в отсъствието на изрични регулации могат да се класифицират като допълнителни услуги, които разширяват дейността на банката.

Нареждането на парични преводи през телекомуникационните мрежи е част от безналичните разплащания или плащанията, осъществявани посредством задължаване или заверяване на банкови сметки, според чл.1, ал.2 от Наредба №3 за безналичните плащания и националната платежна система(ДВ бр.75, 2 август 2002 г.). С оглед на това определение новите промени на Закона за банките от 25 септември 2002 г. (ДВ бр.91) имат ключово значение. Тези промени се отнасят до участието на банките в националната платежна система и особено дейността им по отношение на операциите, свързани с безналични трансгранични плащания. Наредба №3 (чл.8, ал. 2) дава следното определение на национална платежна система: "…*система, в която сетълментът на плащанията в левове на територията на страната се извършва незабавно и индивидуално за всяко нареждане за плащане в съответствие с операционни правила и процедури, изготвени от БНБ.*." Според новите разпоредби на чл. 45, ал.1 от ЗБ търговските банки имат право да извършват не само безналични плащания на територията на РБ, а също така и трансгранични, според наредбите, издадени от БНБ. Въпреки че към момента няма такива наредби, тези промени са една неизбежна стъпка. Те ще окажат влияние върху онлайн активността и особено върху е-банкирането по отношение на международните разплащания, които са честа практика, когато става въпрос за бизнес в Интернет. Поради изискванията за хармонизация на българските закони с европейското законодателство предписанията на Директива 97/5/ЕС за трансграничните кредитни плащания трябва да се прилагат в няколко аспекта: връзките между участниците в трансграничните плащания и особено за информацията, която трябва да се осигури за клиента относно плащането; условията за изпълнение на сделката, които трябва да се имат предвид от всяка от

страните; отговорността на банките при проблем с извършването на плащането и осигуряването на подходящи инструменти за решаване на спорове между банката и клиента.

В резултат на новите промени разпространението на е-банкирането няма да бъде възпирано от ограничения в законодателството. Въпреки това фактори като състояние на телекомуникационната инфраструктура, навиците на потребителите по отношение на приемане на онлайн услугите на банките ще са определящи за действията на банките в мрежата. Фактите сочат, че към момента само 29 банки имат собствен уебсайт и само няколко предлагат онлайн услуги.

2. Виртуални клонове на банки

При сегашното състояние на банковите услуги в Интернет единствено Първа Инвестиционна Банка има работещ виртуален клон. Е-банкирането и услугите, предлагани чрез виртуалния клон са две различни неща, затова и едновременното им съществуване може лесно да се обясни. Докато е-банкирането е свързано с използването на информационни технологии, виртуалният клон предлага по висока степен на интеграция на ИКТ в дейността на банката като цяло, а именно извършване на цялата електронна транзакция чрез комуникационните технологии. Всъщност той предоставя инструментите за реализация на тези дейности, които обикновено се извършват при личното присъствие на клиента.

Както и при електронното банкиране, правната уредба на виртуалните клонове на банките не е разгледана в ЗБ. При все това, докато е-банкирането обикновено се разглежда като допълнителна услуга, дейността на виртуалния клон е по-сложна. Според предписанията на чл.1, ал.3 от ЗБ българското законодателство изисква лицензиране за законовото извършване на банкова дейност. Но той не регулира дейността на виртуалните клонове, така че към момента те работят без лиценз или изрично разрешение. Още повече те не само са толерирани от БНБ, а централната банка дори стимулира тяхната дейност. Тези обстоятелства показват, че действащия ЗБ не взема предвид особеностите на онлайн услугите на банките, които се характеризират с включване на международен елемент и необходимост от защита на платежната система, както и държавен контрол и надзор за да се гарантира защитата на потребителите. Българското законодателство изисква изрично първоначално разрешение на БНБ за работа на клонове извън България. Фактът, че всеки виртуален клон може да използва TCP/IP протокол и уеб сървъри дава възможност за международни плащания, които не попадат под юриздикцията на БНБ. Поради това е изключително важно да се въведе правната рамка за дейността и основаването на виртуални клонове.

Поради факта, че банковата сделка се случва в Интернет, виртуалните клонове са зависими от законовите правила по отношение на идентификацията на човека, иницииращ или приемащ плащането, потвърждаване на подписа или волята и сигурността на процесите, през които се преминава. В резултат на влизането в сила на ЗЕДЕП от септември 2001 г., както и на развитието на вторичното законодателство, което допълва гореспоменатия закон, решаването на тези въпроси не може да търпи дълго отлагане. Следва да се има предвид, че такива услуги все още не са добили голяма популярност заради факта, че повечето потребители не са запознати с тях.

3. Системи за електронно разплащане

Към момента плащанията инициирани и осъществявани с банкови карти са една от малкото широкоразпространени онлайн услуги на банките. Засега съществуват две системи за онлайн разплащания - ePay.bg, която включва 18 търговски банки и BgPay, в която участва само ОББ. Разплащанията в мрежата, които се осъществяват на основата на банковите карти се извършват на базата на система от договори. Те регламентират отношенията между следните участници в системата за електронни плащания:

- Клиент - собственик на кредитна или дебитна карта, който желае да закупи стоки или услуги от търговец в Интернет и който е дал съгласието си в нарочен договор с Оператора на системата, че за негова сметка могат да се извършват онлайн авторизация и плащане на стоки и услуги.

- Търговец е физическо или юридическо лице, което предлага стоки и услуи в Интернет, и което според договора си с Оператора е задължено да приема онлайн плащания реализирани с банкови карти.

- Оператор на система е юридическо лице, което има право да регистрира всички клиенти и търговци, желаещи да осъществяват разплащания в Интернет с помощта на дебитни или кредитни карти. Освен това операторът обезпечава тези плащания от информационна и технологична гледна точка, както е определено в технологията на процеса, създадена от него и потвърдена от участващите банки.

- Банките не участват директно в платежната система организирана от Оператора. Въпреки това те са важен елемент от веригата, доколкото те са издателите на средството за електронното разплащане (картата), която се използва за осъществяване на транзакцията.

- С изключение на договора за издаване на банкова карта, описан в Наредба №16 за плащанията с банкови карти, договорите, които се сключват при организиране на онлайн системата за разплащане не са изрично регулирани от закона. Все пак те трябва да са съобразени с изискванията на чл.9 от Закона за задълженията и договорите "*Страните могат свободно да определят съдържанието на договора, доколкото то не противоречи на повелителните норми на закона и на добрите нрави*".

3. Изводи

Законодателството, регулиращо банковата дейност свързана с Интернет банкирането в България, все още не е адекватно на особеностите на средата, в която се извършват електронните плащания. Още повече онлайн дейността на банките изисква значителни инвестиции, техническа инфраструктура, маркетинг и стратегическо планиране, които трябва да се подготвят и извършат от банката. Тези изисквания, в комбинация с ниската активност на потребителите по отношение на стоките и услугите в Интернет в страната възспира навлизането на банковите услуги в мрежата.

VII. Защита на личните данни и информацията при електронната комуникация

Един от основните фактори за развитие на ИКТ пазара е наличието на ясни правила и гаранции по отношение на защитата на личните данни и информация. ета защо е необходимо да се разгледа настоящото състояние на законодателството реглиращо тези важни теми.

1. Правна рамка за защита на личните данни

До началото на 2002 г. в страната нямаше специални закони, регулиращи проблемите свързани със защитата на личната информация в сферата на електронните комуникации. На 01.01.2002 г. в сила влезе Закон за защита на личните данни (ЗЗЛД, публ. в брой 1 на ДВ, 4 януари 2002 г.), който разглежда защитата на хората по отношение използването и обработката на лични данни и правото на достъп до събраната и обработена информация.

С приемането на закона се цели хармонизация на българското с европейското законодателство в областта на защитата на правата на човека. Въвеждането на нормите на Европейския съюз за осигуряване на достъп до информация при гарантиране на сигурността на данните и основните човешки права е посочено като основен приоритет в Актуализираната национална програма за развитие на информационното общество в Република България.
Законът за защита на личните данни (ЗЗЛД) въвежда в българската правна система основните положения на Конвенция 108 от 1981 г. на Съвета на Европа за защита на лицата при автоматизирана обработка на лични данни (Конвенция 108 от 1981 г.) и на Директива 95/46 на Европейската общност за защита на личността срещу обработка на лични данни и свободното движение на тези данни (Директива 95/46). Стремежът на законодателя е бил да съобрази разпоредбите на закона с европейското законодателство, като по този начин направи възможно ратифицирането от Народното събрание на Конвенция 108 от 1981 г. за защита на лицата при автоматизирана обработка на лични данни.

2. Администратори на лични данни

Към настоящия момент защитата на личните данни и правото на неприкосновеност на личния живот в електронната търговия се регулират изцяло от общата законова рамка, създадена чрез разпоредбите на ЗЗЛД. Ето защо един доставчик на Интернет услуги например, ако желае да обработва личните данни на своите клиенти, трябва да се съобразява изцяло с въведените със ЗЗЛД изисквания и ограничения. Той е администратор на лични данни по смисъла на закона и дейността по обработка на лични данни на клиентите му следва да отговаря на изискванията, посочени в чл. 17.
Администраторът на лични данни може да обработва тези данни само при условие, че е изпълнено едно от следните изисквания:

- изпълнение на нормативно задължение;

- изричното съгласие на физическото лице;
- необходимост да се защити животът или здравето на физическото лице;
- изпълнение на клаузите на договор между администратора на лични данни и физическото лице;
- законен интерес на администратора на лични данни, на трето лице или на лице, на което се разкриват данните и това не нарушава правото на защита по този закон на съответното физическо лице.

В случай, че администраторите на лични данни са и доставчици на Интернет услуги, най-широко приложно поле биха имали т. 2 и т. 4 - наличие на изрично съгласие на физическото лице или изпълнение на клаузите на договор между страните. Самото предоставяне на лични данни на потребителя - физическо лице (точно име, ЕГН, адрес и пр.) е необходимо с оглед индивидуализиране на страните по договора още преди неговото сключване. Ето защо в чл. 7 на Директива 95/46 е предвидено, че лични данни могат да се събират и в случай, когато това е необходимо за предприемане на действия по молба на потребителя преди влизане в сила на договора - едно решение, пропуснато от българския законодател при приемане на иначе буквално преведения в тази му част текст на директивата.
Като реципрочно задължение за администратора на лични данни е предвидено задължението за предоставянето на информацията, посочена в чл. 19, ал. 2 от ЗЗЛД преди обработването на личните данни, а именно информацията касаеща целта и средствата за обработката на личните данни; задължителния или доброволния характер на предоставяне на данните и последиците от отказ за предоставяне; получателите или категориите получатели, на които могат да бъдат предоставени данните, и сферата на ползването им; правото на достъп и на поправка на събраните данни, наименованието и адреса на администратора на личните данни и на обработващия данни.

Защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на този закон се осъществява от независим държавен орган наречен Комисия за защита на личните данни (Комисията). Тя осъществява цялостен контрол за спазване на нормативните актове в областта на защита на личните данни, води регистър и извършва проверки на администраторите на лични данни, изразява становища и дава разрешения в определените от закона случаи и разглежда жалби на физическите лица във връзка с правата им по този закон. Първият управителен съвет на комисията бе избран от парламента по предложение на МС с решение от 23 май 2002 г. (ДВ бр.54, 31май 2002 г.).

След нейното създаване, комисията прие предвидените в закона наредби за дейността и администрацията си (ДВ бр.71, 23 юли, 2002 г.). Шест месеца след влизането в сила на наредбите (в края на януари 2003), лицата, водещи регистрите с личните данни трябва да ги приведат в съответствие с изискванията на закона и да уведомят комисията. В тримесечен срок след приемане на информацията и след провеждане на предварително проучване, комисията трябва да регистрира (или да откаже регистрация) тези лица като администратори.

Що се отнася до осигуряване на неприкосновеността и сигурността на обработваните лични данни, администраторът е длъжен да предприеме необходимите технически и организационни мерки, за да защити данните от случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, както и от всички други незаконни форми на обработване на лични данни. Администраторът е длъжен да предприеме специални мерки за защита, когато обработването предвижда предаване на данните по електронен път. Комисията за защита на личните данни следва да определи с наредба минимално необходимите технически и организационни мерки, както и за допустимия вид защита.

3. Достъп до лични данни. Разкриване на информация пред трети лица

Законът за защита на личните данни урежда и реда за предоставяне на достъп до личните данни, както на субектите на тези лични данни - физически лица, така и на трети лица. Заинтересуваните лица подават до администратора на лични данни писмено заявление, съдържащо реквизитите и по реда, предвидени в закона. Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.
Предоставянето на достъп до регистри на лични данни и прехвърлянето на лични данни от един администратор на друг се извършва при спазване изискванията на закона и след разрешение на Комисията за защита на личните данни. В тези случаи следва да бъде налице поне едно от следните условия:

- съответното физическо лице изрично да е дало съгласието си;
- източниците на данни да са публични регистри или документи, съдържащи обществена информация, за която е осигурен достъп, по ред, определен в закон;
- предоставянето е във връзка със защитата на живота или здравето на съответното физическо лице, както и когато неговото състояние не му позволява да даде съгласие или съществуват законни пречки за това;
- предоставянето е необходимо на органите на съдебната и изпълнителната власт и за защита на конкуренцията и потребителите и това е установено в закон;
- те са необходими за целите на научни изследвания или за статистически цели и данните са анонимни.

4. Специални правила за защита на личните данни при комуникациите

Освен Директива 95/46/ЕС, която съдържа основните правила касаещи разглеждания сектор, защитата на личните данни в сферата на е-търговията и далекосъобщенията са регулирани в законите на ЕС от Директива 97/66/ЕС, разглеждаща обработката на лични данни и защитата на личната информация в

телекомуникационния сектор. От 31 октомври 2003 г. тази директива ще бъде заменена от ново приетата Директива 2002/58/ЕС, която третира обработването на лични данни и защитата на личната информация в електронните комуникации (Директива за личната информация и електронните комуникации). ЗЗЛД в България прилага само основните правила на Директива 95/46/ЕС; той нито прилага Директива 97/66/ЕС, нито Директива 2002/58/ЕС и техните специални предписания по отношение на личната информация и телекомуникациите/електронните комуникации. Към момента, единствената регулация в това отношение е чл.57, ал.1, т.19 от ЗД, според който единствено в индивидуалните лицензии за ДО могат да бъдат заложени изисквания за гарантиране тайната на съобщенията.

Актуализираната секторна политика в далекосъобщенията на Република България изрично посочва, че с оглед на бързо развиващия се процес на либерализация е важно да се оформи една цялостна правна и регулаторна рамка, която да бъде съобразена с възприетите с Директива 97/66 изисквания за събирането, обработването и използването на личните данни от оператори, предоставящи далекосъобщителни услуги.

Проектозаконът за далекосъобщенията във вида, в който беше представен на МС на 23 септември 2002 г. предлага изрично включване в текста на ЗД на правила, които регулират обработката на личните данни и защитата на личната информация в сектора. В Глава 14 от проекта - "Конфиденциалност на съобщенията и защита на личните данни за целите на далекосъобщенията" са въведени специални мерки, които целят прилагане на правилата на Директива 97/66/ЕС. Не са включени препоръките на Директива 2002/58/ЕС. Следните основни нови права и задължения на ДО и абонатите са залегнали в проекта:

- задължение на операторите да гарантират сигурността на комуникациите и да не разкриват информация или данни, които са им станали известни в процеса на тяхната работа;

- задължение за предприемане на съответни технически мерки за осигуряване на защитеност на мрежите и услугите от страна на доставчиците на далекосъобщителни услуги и информиране на потребителите при наличието на риск за сигурността;

- гарантиране на конфиденциалността на съобщенията и забрана за подслушване или други форми на надзор на комуникациите;

- ограничаване на обхвата на обработката и времето за съхраняване на данни за трафика и таксуването;

- предоставяне на функциите "идентификация на повикването" и "идентификация на линията";

- даване на право на потребителите да не се включват в обществено достъпни печатни или електронни телефонни указатели или да бъде пропусната част от техния адрес, като за това не им се налага да заплащат допълнителна цена.

VIII. Компютърни престъпления

Промените в българския Наказателен кодекс свързани с компютърните престъпления бяха публикувани в ДВ бр.2 от 27 септември 2002 г. С тях бе въведена изцяло нова глава "Компютърни престъпления", която влезе между Глава IX "Документни престъпления" и Глава X "Престъпления срещу реда и общественото спокойствие". Основната цел на тези мерки беше да се въведе наказателна политика целяща да защити обществото срещу компютърните престъпления. Промените влязоха в сила три дни по-късно.

Измененията предполагат прилагане на наказателна отговорност за определени нарушения, извършени чрез употребата на компютри или включващи въздействие върху компютърна система и тяхното приемане бе дълго очаквано в страната. Те изпълняват задължението на държавата да защитава социалните и икономически отношения нарушени от престъпно поведение реализирано чрез някой от новопоявилите се типове престъпления или произтичащо от извършването на традиционно престъпление с помощта на нови технологии. Тези промени са още по-навременни с оглед на факта, че българското законодателство се сблъсква с редица нови проблеми – потокът на информация не е ограничен от съществуващите държавни граници, докато престъпниците често се намират на място, различно от това, където техните действия имат ефект. Като се има предвид гореизложеното, новите предписания по отношение на компютърните престъпления са естествен резултат от продължителен обществен дебат, задълбочената работа на редица юридически експерти, усилията на национални и международни организации и институции отдадени на целта да се защитят законните интереси при използването и развитието на информационните технологии. Те са също така и последствие от скорошните социални и икономически промени, които доведоха до неизбежността да се търсят ефективни начини за борба с подобни престъпления.

1. Причините довели до настоящите промени

През 80-те години на миналия век липсата на добра и ефективна компютърна инфраструктура в България не позволи да се разпространят компютърните престъпления до такава степен, която да предизвика намесата на законодателните органи. През този период, според данни на Националния институт по криминология могат да се категоризират само 7 регистрирани престъпни действия, при които са използвани електронни средства (това са основно измами и документни престъпления). Въпреки това, в края на 90-те и особено в периода 2000 – 2002 г. ситуацията е коренно променена. Използването на нови технологии вече става все по достъпно за българското общество. Използването на Интернет в частната и обществената сфера нараства постоянно, като предоставя възможност за достъп до огромно количество информация, знания, и съответните ползи и предимства, които могат да се извлекат от това. Според данни представени на една от работните срещи свързани с подготовката на промените в Наказателния кодекс, в резултат на тези социални промени през 2001 г. има повече от 200 нарушения, които застрашават социалните и икономическите отношения чрез използването на нови технологии. Сред най-очевидните са няколко случая на

хакерски атаки на OSP мрежи, изпращане на е-мейли със заплахи за бомби и промяна на уеб страницата на една от българските банки през 1999 г.

Докато в началото на разглеждания период повечето престъпления бяха неизменно свързани с използването на локални мрежи и локални системи, то през последните 2 години те най-често се извършат през Интернет или при наличието на няколко свързани мрежи. Тези обстоятелства увеличават възможността за нарушаване на правата и законните интереси в значително по-голяма степен отколкото в мрежи с ограничен обхват.

Законодателните промени в Наказателния кодекс са също така резултат от задълженията, приети от РБ във връзка с Конвенцията за компютърни престъпления на Съвета на подписана от България на 23.11.2001 г. Необходимо е да се отбележи, че те следват предписанията на конвенцията, както бе уговорено на 23.11.2001 г, в Будапеща. И въпреки това законодателите в страната се бавиха повече от година преди измененията да бъдат гласувани в парламента, заради широко разпространеното мнение, че компютрите са само специфичен инструмент за извършване на престъпление и няма нужда от дефиниране на нови типове престъпления.

2. Компютърни престъпления и престъпления, свързани с употребата на компютри

Трябва да се направи разграничение между компютърните престъпления, като новопоявил се тип престъпления, провокирани от развитието на ИТ и традиционните престъпления, извършвани с помощта на новите технологии. Все още няма единно мнение в българското законодателство и в правната теория по отношение на различното значение на понятията "компютърни престъпления", "кибер престъпления", "престъпления, свързани с употребата на компютри" и "високотехнологични престъпления". Тези термини се използват обикновено като синоними, без по-подробно определение при приемането им.

3. Престъпления, извършени чрез използването на компютри

Характерната черта на този тип престъпление е употребата на компютри или ИТ като средство за извършване на престъплението. Именно заради специфичните методи, които обикновено улесняват престъниците за постигане на търсения ефект, подобни действия се определят като по-опасни за обществото от някои престъпления, извършени по традиционния начин. Все пак за голяма част от тези действия беше предвидено наказание и преди промените на Наказателния кодекс. Повечето от тях могат да се квалифицират по вече съществуващите текстове като измама, документни престъпления, злоупотреба с доверие, неправилно присвояване. Дори част от извършените напоследък нарушения в Интернет могат да се квалифицират като някои традиционни престъпления (измамата при електронната търговия като измама според чл.209 "*Който с цел да набави за себе си или за другиго имотна облага възбуди или поддържа у някого заблуждение и с това причини нему или другиму имотна вреда, се наказва за измама ...*", разпространение на заплахи чрез електронна поща според чл. 326 *"Който предава*

по радио, телефон или по друг начин неверни повиквания или заблуждаващи знаци за помощ, злополука или тревога, се наказва ...").

Въпреки наличието на съществуващите възможности за налагане на наказание за тези нарушения факт е, че има голяма необходимост от засилване на защитата с помощта на адекватни текстове с цел улесняване на съдебната практика и предотвратяването на подобни престъпления. Поради тази причина след промените от септември 2002 г. някои от традиционните престъпления бяха разширени с въвеждане на смекчаващи обстоятелства и по-високи присъди при случаи с употреба на информационни технологии.

Сред традиционните престъпления, извършвани с помощта на ИТ могат да се посочат следните:

- **Престъпления срещу интелектуалната собственост.** Информационните технологии позволяват копирането и бързото разпространение на различни обекти, защитавани от правото на интелектуална собственост. Възможностт за обмяна и разпространение независимо от географските граници са допълнителни условия за увеличаването на този тип престъпления.

- **Индустриален шпионаж.** Огромният поток на информация особено във взаимносвързани мрежи в значителна степен улеснява едно от най-често срещаните престъпления в икономическата сфера. Фирмите, използващи компютърни мрежи са сериозно застрашени от индустриален шпионаж.

- Някои от останалите престъпления, които могат да се извършат чрез използването на ИТ са престъпленията срещу националната сигурност, пране на пари, особено чрез използването на електронни системи за разплащане, обида и клевета и др.

Българското законодателство към началото на октомври 2002 г. засяга четири нови нарушения, които засягат пряко компютърните системи, но фактът че при тяхното извършване са използвани ИТ води до по-големи наказания отколкото са предвидени в съществуващите текстове. Това са престъпления свързани с детска порнография, специфичните престъпления свързани с унищожаване на чуждата собственост или престъпления срещу нарушаване интегритета на личната кореспонденция.

4. Компютърни измами

Една от дългоочакваните промени е свързана с компютърните измами. През последните две години много фирми започнаха дейност в Интернет а голяма част от банките създадоха и развиха платежни системи, които изпълняват електронни разплащания. В резултат на това сметките администрирани или представени в компютърните системи стават обект на манипулация, точно както и традиционната веществена или невеществена собственост. Това е така, защото предписанията на Наказателния кодекс свързани с компютърните измами са от изключителна важност за защитата на разглежданите икономически взаимоотношения.

Целта на новия чл.212а от Наказателния кодекс е да криминализира всякаква незаконна манипулация в процеса на обработката на данни с намерение да се осъществи незаконен трансфер на собственост. Към момента няма съдебна практика свързана с този тип престъпление, както няма и точно определение, но идеята на законодателя за "*всяко внасяне, промяна, изтриване или заличаване на компютърни данни"* може да се интерпретира като действия, които включват манипулации по хардуера или такива, влияещи върху записването или предаването на данни, или последователността на работа на програми. В допълнение към това нарушението трябва да е извършено "без право" и ползите трябва да са получени "без право". Още повече нарушението трябва да е извършено не само с умисъл, но също със намерение да се извлече полза за себе си или трето лице. Последният от елементите на това престъпление предполага щета (загуба на собственост с икономическа стойност) причинена на някого освен извършителя. За разлика от традиционната измама, компютърните измами се наказват с акумулиране на присъдата – не само затвор от 1 до 6 години, но и заплащане на определена от съда глоба.

5. Компютърни престъпления

Текстовете на чл.319а до 319е от променения Наказателен кодекс са създадени с цел защита на функционирането, наличността и интегритета на компютрите, компютърните системи и мрежи, както и на законовото създаване, използване и обмяна на данни и информация. Необходимостта от подобна защита на сигурността на компютърните системи отразява интереса на организациите и идивидуалните потребители да управляват, използват и контролират своите системи по необезпокояван начин, така че да няма опасност от промяна или изтриване на данни или неоторизиран достъп до поверителни данни. Според предписанията на чл.319а "*Който осъществи нерегламентиран достъп до ресурсите на компютър, копира или използва компютърни данни без разрешение, когато се изисква такова, се наказва ..."* Най-голямото наказание, предвидено в закона се налага в случай, че нарушението е извършено от организирана група, извършено е повече от един път, ако данните се отнасят за държавна тайна и ако престъплението има сериозни последствия.

Следващите няколко текста криминализират промяната на данни и влизането в чужди системи. Ако в резултат на престъплението има значителни щети или други сериозни последствия, както и в случай, че престъплението е извършено със специални намерения на извършителя да извлече полза от действията си, то наказанията са изключително сурови. Такава е ситуацията и когато деянието е по отношение на данни, които се дават по силата на закон, по електронен път или на магнитен носител, или пък престъплението е извършено с цел да се осуети изпълнение на задължение. В разглеждания случай идеята е да се защити интегритетът и нормалното функциониране на записаните компютърни програми или данни, които могат да бъдат нарушени чрез добавяне, промяна, изтриване или заличаване.

Гореописаните деяния са наказуеми, само ако са извършени с умисъл и без разрешението на лицето, което е отговорно за компютъра или мрежата, и ако случая не е маловажен, според определението на чл.93, т. 9 от Наказателния кодекс. Напротив, ако престъплението включва компютърни данни, които се

характеризират с начина за трансфериране или запазване или начина, по който задължението за доставянето им на друг е определено, тогава поради спецификата на тези данни, намесата или промяната им се наказва с по-сурови наказия.

Промените в Наказателния кодекс криминализират също и пускането на вирус в компютърна система или мрежа, разпространението на компютърни или системни пароли, което може да доведе до разкриване на лични данни или държавна тайна, както и нарушението на задължението на удостоверителните органи да пазят информацията за времето на предаване на данните, както и техния източник.

Подробното и пълно запознаване със законодателните текстове, които въвеждат компютърните престъпления в българската правна система показва опит за приемане на решенията от Европейската конвенция за киберпрестъпленията. Въпреки това не всички престъпления, описани в конвенцията са възпрети от българските законотворци. Възможното обяснение за това е, че към момента няма социална необходимост от прилагане на всички текстове. Наказателните закони трябва да вървят в крак с технологичното развитие, което предлага изключително модерни възможности за злоупотреба с компютрите и данните, но ако няма необходимост от защита чрез тези закони, поради реална липса на някои престъпления, то подобни законови текстове могат да бъдат пропуснати.

Текстовете, приети с оглед появата на компютърните престъпления ще предлагат необходимото ниво на защита на социалните взаимоотношения по такъв начин, така че законът да може да постигне своята цел. Прилагането им от професионалистите обаче ще бъде възпрепятствано от липсата на съдебна практика, правна литература, както и от липсата на теоритични разработки в тази област. Въпреки тези трудности, основната пречка остава отсъствието на адекватни процедури адаптирани за нуждите на нововъведените престъпления. Докато не се приемат и промени в Наказателно-процесуалния кодекс, прилагането на тези текстове ще бъде ограничено.