КОМПЮТЪРНИТЕ ПРЕСТЪПЛЕНИЯ И НАКАЗАТЕЛНАТА ИМ РЕГУЛАЦИЯ В БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО

Николай Атанасов Николов, студент в програма "Право" , НБУ

Many country are reception a legislation against computer crimes. Changes in Criminal Code is increse capacity the authorities

Всяко законодателство чрез правните си норми рамкира съществуващи обществени отношения, като по този начин регулира правилното им развитие и определя санкциите за действията, които са в нарушение на правата на отделния правен субект при възникнали отклонения от предписанието на тези норми. Законодателството има задължението да обхване новопоявилите се обществени отношения като по този начин то се осъвременява и е в такт с правната действителност в държавата. Такива нови отношения "обхванати" от нашето законодателство се явяват тези, които са свързани пряко с все по-голямото и по-бързо навлизане на компютрите в ежедневието на хората. Поради измененията в почти всички области на човешките отношения, предизвикани от въвеждането на цифровите технологии и постоянната глобализация на компютърните мрежи, Съветът на Европа прие редица важни актове в борбата с престъпленията, извършвани чрез използване на компютърни системи и мрежи или електронна информация, както и злоупотребата с тях, от които особено съществено значение имат:

1. КОНВЕНЦИЯТА ЗА ПРЕСТЪПЛЕНИЯ В КИБЕРНЕТИЧНОТО ПРОСТРАНСТВО от 23 ноември 2001г., подписана от нашата страна и влязла в сила;
2. ПРЕПОРЪКА № R (89) 9 относно ПРЕСТЪПНОСТТА СВЪРЗАНА С КОМПЮТРИТЕ;
3. ПРЕПОРЪКА № R (95) 13 за НАКАЗАТЕЛНИТЕ ПРОИЗВОДСТВА, СВЪРЗАНИ С КОМПЮТЪРНИТЕ ТЕХНОЛОГИИ.

На своето 50-о заседание през юни 2001 г. Европейският комитет по проблемите на престъпността - междуправителствен орган от експерти към Комитета на министрите на Съвета на Европа - прие окончателния проект на Конвенцията за престъпления в кибернетичното пространство. Тази конвенция е първият международен договор за престъпления, извършени по Интернет и други компютърни мрежи. Тя регламентира

главно правонарушения, свързани с авторските права, компютърната измама, детската порнография, както и правонарушения, свързани със сигурността на мрежите. Конвенцията съдържа правна уредба и на редица процедурни правомощия, като претърсване на компютърните мрежи и прихващане на информация. Основната цел на Конвенцията за престъпленията в кибернетичното пространство, обявена в преамбюла, е постигането на "обща наказателна политика, насочена към закрила на обществото срещу кибернетичните престъпления, включително и чрез прилагане на съответното законодателство и поощряване на международното сътрудничество". Търсенето на наказателна отговорност за предвидените в конвенцията правонарушения е обусловено от наличието на две кумулативно дадени общи условия - инкриминираното поведение трябва да бъде извършено с умисъл и "без законно основание". Правонарушенията са обособени в четири големи категории, а именно:

- правонарушения, свързани с тайната, неприкосновеността и осигуряването на достъп до данните и системите: незаконен достъп, незаконно прихващане, посегателство срещу неприкосновеността на данни, посегателство срещу неприкосновеността на системата, злоупотреба с устройства;
- компютърни престъпления: компютърна фалшификация и компютърна измама;
- правонарушения, свързани със съдържанието: производството, разпространението и притежаването на детската порнография;
- правонарушения, свързани с авторските и сродните им права: масово разпространение в големи мащаби на незаконни копия от произведения, закриляни от авторското право.

Въвеждането на процесуалноправни разпоредби от конвенцията във вътрешното право същевременно трябва да бъде подчинено на условията, предвидени в законодателството на държавите - страни по конвенцията[1], като се гарантира спазването на правата на човека и прилагането на принципа на пропорционалността. В този смисъл процедурите могат да се прилагат само при определени условия, като например, според случая, с предварително разрешение от съдебен или от друг независим орган.

[1] Тя е открита за подпис на 23 ноември 2001 г., като в деня на откриването е подписана от 30 държави, включително и от България

При изработването на конвенцията са взети предвид традиционните форми на международно сътрудничество в наказателноправната област, включително тези, предвидени в Европейската конвенция за екстрадицията и в Европейската конвенция за взаимопомощ по наказателноправни въпроси. Наред с това обаче конвенцията въвежда и нови форми на международно сътрудничество, съответстващи на правомощията, залегнали в нейните разпоредби. Така например съдебните органи и службите по издирване на доказателства в електронна форма могат да действат по молба на държава - страна по конвенцията, без да водят самостоятелно разследване или трансгранично претърсване. Получените данни трябва да бъдат предавани бързо.

Едно от предимствата на конвенцията е създаването на контактна мрежа между държавите, която е на разположение 24 часа в денонощието и 7 дни в седмицата. Във връзка с това се обсъжда възможността то да бъде създадено като структурно обособено звено в рамките на Министерството на вътрешните работи с цел оказване на незабавна помощ при започналото разследване. Предвид сложността на наказателно-процесуалните норми, свързани с прилагането на конвенцията, продължава работата по изработването на измененията на Наказателно-процесуалния кодекс относно задълбочаването на международното сътрудничество между полицейските и съдебните органи.

Ратифицирането на конвенцията се обуславя, от една страна, от универсалния й характер, и от друга, от нейното изключително голямо значение за предотвратяване на тероризма чрез Интернет. Важно значение има и фактът, че този международноправен договор предоставя адекватните средства за защита и предотвратяване на престъпленията, извършвани чрез компютърните системи и по компютърен път. Ратифицирането и обвързването с конвенцията е в съответствие с Резолюцията, приета на 24-ата среща на министрите на правосъдието от европейските страни (Москва, октомври 2001 г.) за укрепване на превенцията и наказването на терористични актове, извършени срещу или чрез компютърни и телекомуникационни системи (кибертероризъм). С тази Конвенцията се дават определения на редица общи понятия и се очертани различните видове компютърни престъпления, които са възприети и в нашия Наказателен кодекс (НК) с промените от 13 септември 2002 г.[2]

Борбата с престъпността предполага подобряване на някои текстове от НК с цел улесняване на наказателното съдопроизводство. Процесите на евроинтеграция налагат във вътрешното законодателство да бъдат предприети необходимите мерки за защита.

[2] ДВ, бр. 92 от 2002 г

Престъпните състави предвиждат защитата на обществените отношения, свързани със създаването, използването, разпространението и съхранението на компютърна информация. Бързото развитие в областта на информационните технологии и телекомуникациите създава големи възможности за извършване на деяния с висока степен на обществена опасност.

Компютърно престъпление, в най-широк смисъл, е всяко престъпление, което по един или друг начин е свързано с използването на компютри и информационни технологии. В света съществува голяма терминологична разлика относно това, кое деяние съставлява компютърно престъпление. Термините "компютърно престъпление" (computer crime), "престъпление, свързано с компютри" (computer-related crime), "престъпление в сферата на високите технологии" (hi-tech crime) и "кибер-престъпление" (cybercrime) често се използват като взаимозаменяеми. Може да се направи разлика между компютърни престъпления в строгия смисъл на думата и традиционни престъпления, извършвани с помощта на компютърна технология. Компютърните престъпления в строгия смисъл изискват нови състави в националните наказателни закони, докато конвенционалните престъпления, извършени с помощта на компютри, изискват в съответните закони създаване на квалифицирани състави за улесняване на практиката и с оглед превенция. Тези престъпления са улеснени от съществуването на информационни и съобщителни мрежи, които не познават граници, и от движението на данни, които са неосезаеми и извънредно неустойчиви.

През последните години законово бе уредено използването на информационни и компютърни технологии за пренасяне, съхраняване или обработка на данни. Това налага криминализиране с общ, бланкетен текст на случаите, при които чрез определени манипулации на данните се засягат обществените отношения в отделни важни сфери - социално осигуряване, данъчно облагане, търговия с ценни книжа и др. (чл. 319в). За да се прилага в практиката електронния подпис и електронния документ е необходима допълнителна правна защита и гаранции срещу злоупотреби с тях уредени с текстовете на чл. 319б и 319е НК.

Престъпленията по чл. 319а до чл. 319е от Наказателния кодекс (НК) могат да бъдат определени като същински компютърни престъпления. При тях се засягат обществените отношения, осигуряващи нормално функциониране на компютри, компютърни системи, компютърни ресурси и компютърни мрежи, както и правомерното създаване и ползване на информация. Към тях се включват нерегламентирания достъп, промяна, повреда,

унищожаване на данни или програми, въвеждането на "вирус" или разпространение на пароли.

Друга група компютърни престъпления условно могат да бъдат определени като извършвани чрез компютър и засягащи различни обществени отношения. Такива са компютърната измама по чл. 212а, особената форма на унищожаване и повреждане по чл. 216, ал. 2, специфичния начин на нарушаване на тайната на кореспонденцията по чл. 171. Специално се криминализира и детската порнография.

Поради промяната застъпена в глава девета “а” на НК се наложи да се направят и промени в чл. 93, в който се обясняват основните понятия залегнали при създаването на кодекса. Създават се т. 21, 22, 23, 24 и 25:

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

22. "Компютърни информационни данни" е всяко представяне на факти, информации или понятия във форма, поддаваща се на автоматична обработка, включително такава програма, която е в състояние да направи така, че дадена компютърна система да изпълни определена функция.

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

За т. 24 в комисията се взе решение да отпадне, понеже терминът "данни за трафика" не се употребява в останалата част на Наказателния кодекс.

25. "Платежен инструмент" е веществено средство, различно от законно платежно средство (банкнота или монета), позволяващо, поради специфичната си природа самостоятелно или във връзка с друго средство, на държателя да прехвърля пари или парична стойност, като например дебитна карта, кредитна карта, електронно портмоне или друга карта, издадена от финансова институция, чек или пътнически чек."

Новите състави за шест вида компютърни престъпления се съдържат в Глава девета “а” от Наказателния кодекс. Първият от тях се отнася за копиране или използване на компютърни данни без разрешение чрез осъществяване на нерегламентиран достъп до

ресурсите на компютър (чл. 319а ал.1 от НК). Изпълнителното деяние се изразява в две форми:

А) копира компютърни данни и

Б) използва тези данни.

Престъплението е свързано с начина на неговото осъществяване – чрез нерегламентиран достъп до ресурсите на компютър. От обективна страна е необходимо още тази дейност да се извършва без разрешение, когато се изисква това. Престъплението е умишлено – деецът съзнава, че копира или използва компютърните данни, чрез осъществяване на нерегламентиран достъп до ресурсите на компютър, както и че прави това без разрешение. Предвиденото наказание е глоба до три хиляди лева. Предвидени са два квалифицирани случая:

А) когато деянието е извършено от две или повече лица, сговорили се предварително, при което наказанието е лишаване от свобода до една година или глоба до три хиляди лева (чл. 319а, ал. 2 от НК);

Б) ако деянието е извършено "повторно" по смисъла на чл. 28 от НК, за което наказанието е лишаване от свобода до три години или глоба до пет хиляди лева (чл. 319а, ал.3 от НК). По-тежко квалифициран е случаят, когато това престъпление по основния или двата квалифицирани състави е извършено по отношение на сведения, съставляващи държавна тайна. Наказанието е лишаване от свобода от една до три години, ако не подлежи на по-тежко наказание (чл. 319а, ал.4 от НК). Най – тежка е квалификацията за последния случай, ако са настъпили тежки последици. Наказанието е от една до осем години без да е посочен изрично вида на наказанието, макар и да се разбира, че то е лишаване от свобода (чл. 319а, ал.5 от НК).

Следващият вид компютърно престъпление е фалшификация или унищожаване на компютърна програма или данни (чл. 319б от НК). Изпълнителното деяние фалшификация се изразява в добавяне, променяне или изтриване на компютърна програма или компютърни данни, което ги прави неавтентични или несъответстващи на първоначалните и действителните програми и данни. Унищожаването е ликвидиране на съответната програма или данни. От обективна страна е необходимо деянието да е извършено без разрешение на лицето, което администрира или ползва компютъра, както и да се отнася за немаловажни случаи. Престъплението се характеризира с умисъл – деецът съзнава, че добавя, променя, изтрива или унищожава компютърна програма или данни без разрешение на лицето, което

администрира или ползва компютъра, както и че случаят е немаловажен. Наказанието в случая е лишаване от свобода до една година или глоба да две хиляди лева (чл. 319б, ал.1 от НК). В чл. 319б, ал.2 от НК са предвидени два квалифицирани случая когато:

А) са причинени значителни вреди;

Б) са настъпили други тежки последици.

Престъплението е квалифицирано по-тежко, когато е с цел имотна облага (чл.319б, ал.3 от НК). Наказанието е лишаване от свобода от една до три години и глоба до пет хиляди лева. Тази по-тежка квалификация обаче се отнася само за деяние по ал.1, но не и за квалифицираните случаи по ал.2, където наказанието е по-леко – лишаване от свобода до две години и глоба до три хиляди лева.

В чл. 319б, ал.1 от НК се визира случая, когато фалшификацията или унищожаването е по отношение на данни, които се дават по силата на закон по електронен път или електронен носител. Всъщност този състав е друг квалифициран състав на престъплението по чл. 319б, ал.1 от НК, но предвиденото наказание е еднакво с това по чл. 319б, ал.2 от НК – лишаване от свобода до две години и глоба до три хиляди лева. По тежка е квалификацията по този случай, когато деянието е извършено с цел да се осуети изпълнение на задължение (чл. 319в, ал.2 от НК). За съжаление в тази разпоредба не се посочва на кого е задължението и какъв е неговият характер. Задълженията на доставчика на удостоверителни услуги са предвидени в чл.22 точки 1-8 от Закона за електронния документ и електронния подпис (ЗЕДЕП)[3]. Доставчик на удостоверителните услуги е лице, което:

1) издава удостоверение за усъвършенстван електронен подпис;

2) предоставя на всяко трето лице достъп до публикуваните удостоверения (чл. 19 и чл. 24 от ЗЕДЕП). Понятието "Доставчик на компютърно-информационни услуги" е по-широко и включва всяко юридическо или физическо лице, което предлага възможността за комуникация чрез компютърна система или което обработва или съхранява компютърни данни за тази комуникационна услуга или за нейните ползватели (чл. 93, т. 23 от НК). С оглед на това в чл. 319е от НК е очертан специфичен състав, когато при доставяне на информационни услуги се нарушат разпоредбите на чл.6, ал.3 т.5 от ЗЕДЕП, а именно при съхраняване на информацията в срок от шест месеца не осигурява условия за точно определяне на времето и източника на предаваните електронни изявления. От субективна

[3] Обн. ДВ. бр.34 от 6 Април 2001г., изм. ДВ. бр.112 от 29 Декември 2001г., в сила от 06.10.2001 г.

страна е необходим умисъл, а предвиденото наказание е глоба до пет хиляди лева, ако не подлежи на по-тежко наказание.

Въвеждането на компютърен вирус в компютър или информационна мрежа е визирано от чл. 319г, ал.1 от НК. Наказанието е сравнително леко – глоба до три хиляди лева. То не е съобразено с наказанието за извършено нарушение, което е глоба от 100 до 10 000 лв., ако не съставлява престъпление. Следователно престъплението може да изключи нарушението, за което се предвижда по-строго наказание (чл.45, ал.1 ЗЕДЕП). Разбира се наказанието е по-строго, ако от това престъпление са настъпили вреди или е извършено повторно – лишаване от свобода до три години и глоба до 1000 лв. (чл. 319г, ал.3 от НК).

Най сетне самостоятелен състав е очертан в чл.319д, ал.1 от НК за разпространение на компютърни или системни пароли, когато от това последва разкриване на лични данни или лична тайна. Наказанието е лишаване от свобода до една година. Престъплението е квалифицирано по-тежко, ако е извършено с користна цел или са причинени значителни вреди. Предвиденото наказание е лишаване от свобода до три години (чл. 319д, ал.2 от НК).

Обект на посегателство при компютърните престъпления е усложнен и съчетава обществените отношения, свързани с интелектуалната и материалната собственост. В това отношение съществен интерес представлява схващането, че "обект на защита в дадени случай се явява съвкупност от обществени отношения, свързани с производството, използването, разпространението и защитата на информация и информационни ресурси"[4].

Много страни са приели законодателство за борба с компютърните престъпления. Криминализация на компютърните престъпления има в повечето европейски страни и в САЩ. Бързото развитие на съвременните технологии прави връзките ни с тези страни изключително интензивни. Сближаването на нашето законодателство с това на страните от Европа може да послужи като допълнително сериозно основание за криминализацията на посочените деяния и в България. Това ще повиши авторитета ни в областта на информационните технологии и ще създаде условия за тяхното по-широко прилагане в икономическата активност. Промените в Наказателния кодекс ще увеличат капацитета на правораздавателните органи за противодействие на посочените престъпления и ще спомогнат за ограничаване и контролиране на престъпната дейност. Те ще се отразят положително както върху хода на преговорите за членство с Европейския съюз по глава

[4] "Новое уголовное право России, Особенная част" под ред. На Кузноцова Н.Ф.,М., 1996, с. 274

двадесет и четири “Правосъдие и вътрешни работи”, така и върху решението за покана на страната за членство в НАТО.

ЛИТЕРАТУРА:

[1] Наказателен Кодекс, Обн. ДВ. бр.26 от 2 Април 1968г., изм. ДВ. бр.92 от 27 Септември 2002г.

[2] Гиргинов, А., Наказателно право на Република България, Обща част, С. 2002г.

[3] Милушев, Марио, Компютърно право

[4] СТЕНОГРАМА от обсъжданията на проектите на Закон за изменение и допълнение на Наказателния кодекс (№ 154-01-24 от 19.07.2001 г., № 202-01-22 от 19.04.2002 г., № 254-01-2 от 11.01.2002 г., № 254-01-47 от 11.06.2002 г., № 154-01-64 от 16.10.2001 г. и № 254-01-27 от 03.04.2002 г.)

[5] МОТИВИ към проекта на Закон за изменение и допълнение на Наказателния кодекс (№ 154-01-24 от 19.07.2001 г.)

[6] МОТИВИ към проекта на Закон за ратифициране на Конвенцията за престъпления в Кибернетичното пространство (№ 202-02-30 от 15.07.2002 г.)

[7] ДОКЛАД на Комисията по правни въпроси по проекта на Закон за ратифициране на Конвенцията за престъпления в кибернетичното пространство (№ 202-02-30 от 15.07.2002 г.)

[8] Михайлов, Д., Компютърни престъпления. Правноинформационна система АПИС.

[9] Кузноцова Н.Ф.,М., Новое уголовное право России, Особенная част, М. 1996