Сигурност и защита при работа в локална и мрежова среда
1 част

доц. д-р инж. мат. М. Брусева

Компютърни престъпления

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.

Компютърни престъпления

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.

Компютърни престъпления

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.

Компютърни престъпления

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.

Компютърни престъпления

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.

Компютърни престъпления

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.

Компютърни престъпления

Броят на компютърните престъпления в една държава е правопропорционален на степента на използване на компютри и броя на ползвателите на интернет. Колкото по-голям е броят на лицата, ползващи интернет, толкова по-голям е и броят на престъпленията в кибернетичното пространство.

В България определено се забелязва тенденция на увеличаване, още повече че интернет не е национално явление и има много престъпления, които се извършват оттук, но потърпевшите лица са в чужбина, и обратно – такива, които се извършват от чужди граждани, но са насочени към ресурси в България.

Компютърни престъпления

Това, което предстои в сферата на правораздаването за успешна борба с киберпрестъпността, е работа за повишаване капацитета на магистратите и адвокатите. Все още няма специализирани програми за обучение на магистрати и адвокати, свързани с правните аспекти на информационните технологии. А както адвокатът, който трябва да защити правата и интересите на клиентите си, така и разследващите органи, прокурорите и съдиите трябва да имат знания за това какъв смисъл е вложил законодателят, като е използвал един или друг технически термин в дадена правна норма. От друга страна е необходимо да се работи в посока създаване на знания и умения относно нови методи на разследване на тези киберпрестъпления у разследващите органи.

Компютърни престъпления

Ясно е, че претърсването и изземването, в класическия смисъл на думата, не може да бъде приложимо към един компютър. Претърсването и изземването на данни в компютърна система като методология и практически стъпки няма нищо общо с претърсването на едно помещение и изземване на веществени доказателства. Използването на конвенционалните методи е неприложимо, защото, както се вижда от практиката, понякога се увреждат непоправимо правата и интересите на стотици пазарни агенти, когато се изземват компютърните им конфигурации като веществени доказателства. Именно повишаването на знанията на разследващите органи би помогнало да се създадат такива механизми за разследване на компютърни престъпления, които ще подпомогнат тяхното разкриване.

Компютърни престъпления

И не на последно място, когато се идентифицира нужда от промяна в законодателството именно поради факта, че възникват нови ИТ и следователно нови обществени отношения, тя трябва да се адресира към държавата. Например, ако ваш съсед е оставил отворена безжичната си домашна мрежа за достъп до интернет (WiFi) по някаква причина, а вие имате инструмент, с който да използвате неговата мрежа, очевидно нарушавате интересите му, но това не е престъпление по нашия закон.

Компютърни престъпления

При използването на информационните технологии въпросите са много деликатни. Правото е изправено пред огромно изпитание: **До каква степен и как трябва да регулира използването на ИКТ, така че от една страна да се запази свободата при използването им, а от друга да постави някаква граница за защита на правата и интересите на гражданите.**

Компютърни престъпления - НПК

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 /неправомерен 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.

Компютърни престъпления - НПК

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).

Компютърни престъпления - НПК

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.

Компютърни престъпления - НПК

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.

Компютърни престъпления - НПК

Задълженията на доставчика на удостоверителни услуги са предвидени в чл.22 точки 1-8 от Закона за електронния документ и електронния подпис (ЗЕДЕП)4. 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 комуника-ционна 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 страна е необходим умисъл, а предвиденото наказание е глоба до пет хиляди лева, ако не подлежи на по-тежко наказание.

Компютърни престъпления - НПК

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).

Компютърни престъпления - НПК

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".

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 увеличават капацитета на правораздавателните органи за противодействие на посочените престъпления и спомагат за ограничаване и контролиране на престъпната дейност.

Неправомерен достъп до ПК

Неправомерния достъп е опасен не само за четене на лична информация, но също така представлява и възможност за външен контрол върху компютърната системата с помощта на управлявани програмни отметки. Няма да се отрече фактът, че за по-сериозна защита на компютъра вградените в операционната система средства не са достатъчни. Ето защо, заедно със стандартните средства за защита няма да пречи и използването на специални инструменти. Те са разделени на два вида: средствата за ограничаване на физическия достъп, и средства за ограничаване на достъпа до мрежата.

www.vfu.bg

Варненски свободен университет

Благодаря!