15.33АБ

ВИСШ АДВОКАТСКИ СЪВЕТ SUPREME BAR COUNCIL

РЕПУБЛИКА БЪЛГАРИЯ
ВИСШ АДВОКАТСКИ СЪВЕТ

ул. „Цар Калоян" № 1-а, 1000 София, тел. 986-28-61, 987-55-13,
факс 987-65-14, e-mail: arch@vas.bg

ДО
КОМИСИЯТА ПО ПРАВНИ ВЪПРОСИ
НА ЧЕТИРИДЕСЕТ И ТРЕТОТО
НАРОДНО СЪБРАНИЕ

С Т А Н О В И Щ Е

НА ВИСШИЯ АДВОКАТСКИ СЪВЕТ

ОТНОСНО :
ПРОЕКТ ЗА ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА НАКАЗАТЕЛНИЯ КОДЕКС, № 702-01-10 / 01.08.2017 г.

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА НАРОДНИ ПРЕДСТАВИТЕЛИ,

С внесения законопроект се предлагат изменения и допълнения на Наказателния кодекс, като се цели въвеждане в националното законодателство на изискванията на директива 2013/40/ЕС на Европейския парламент и на Съвета от 12.08.2013 г. относно атаките срещу информационните системи и за замяна на Рамковото решение 2005/222/ПВР на Съвета; директива 2014/57/ЕС на Европейския парламент и на Съвета от 16.04.2014г. относно наказателноправните санкции за пазарна злоупотреба; директива 2014/62/ЕС на Европейския парламент и на Съвета от 15.05.2014г. относно защитата по наказателноправен ред на еврото и на другите парични знаци срещу подправяне и за замяна на Рамковото решение 2000/383/ПВР на Съвета; директива 2013/40/ЕС на Европейския парламент и на Съвета от 12.08.2013г. относно атаките срещу

информационните системи и за замяна на Рамковото решение 2005/222/ПВР на Съвета.

Висшият адвокатски съвет предлага на народните представители своето становище по законопроекта:

Констатации и препоръки /съгласно номерацията на параграфите по законопроекта/:

1. С пар. 13 ЗИД на НК се създава нова ал. 2 на чл. 251 НК /свързан с нарушаване на задълженията за деклариране на парични средства, благородни метали, скъпоценни камъни и изделия със и от тях, пренасяни през границата на страната, която е външна граница на Европейския съюз, и стойността на предмета на престъплението е в особено големи размери/ когато предметът на престъплението по ал. 1 е **„укрит по специален начин“**. Този квалифициращ признак на изпълнителното деяние е напълно неясен, дава възможност за различно и нееднозначно тълкуване и се нуждае от сериозно прецизиране. Запазването му в този вид, ще създаде изключителни затруднения при правоприлагането. Не става ясно какъв е акцентът, който се поставя - дали по-високата обществена опасност на деянието се свързва с факта на укриването или с мястото, начина, средствата на укриване и т.н. Всяко укриване е насочено към затрудняване достъпа до укритата вещ и е специфично.

2. По пар. 17, т.1 ЗИД НК

Предложен е текст за изменение на чл. 319а, ал. 1: „Който неправомерно осъществи достъп до информационна система или части от нея, в немаловажни случаи се наказва с лишаване от свобода до две години.“

По принцип необходимостта от изменение на чл. 319а е наложителен. Предложението за промяна на правилото, обаче, е непрецизно и може да се тълкува, че и при физически осъществяване на достъп до информационна система, без да е осъществен достъп до данните в нея, пак е налице обществена опасност и деецът следва да се накаже. Едва ли такава е законодателната воля при транспониране на Конвенцията за престъпленията в кибернетичното пространство и идеята на нормата в глава „Компютърни престъпления“. Тук става дума не за физически достъп до системата и помещението, в което се намира, а за достъп до данните в нея. Извън изложеното остават и хипотезите, при които чуждите данни са съхранени на външен носител, но достъп до тях се осъществява от информационна система, до която има правомерен достъп. Напр. чужди данни са записани на флашка, до които се осъществява неправомерен достъп от собствена на дееца информационна система. Понятието „части

от нея“ също е непрецизно. Съгласно определението на „информационна система“ в чл. 98 тя е съвкупност от устройства, които в изпълнение на програма осъществяват някакъв резултат. Освен това, самото изпълнително деяние на т.нар. „неактивно хакерство“ разкрива по-ниска степен на обществена опасност, отколкото активното хакерство по чл. 319б, следователно и санкцията следва да е съобразена и по-ниска.

Предлагаме следната редакция:

„(1) Който неправомерно осъществи достъп до компютърни данни в информационна система или до такива, съхранени на електронен носител, в немаловажни случаи се наказва с лишаване от свобода до една година“

3. По пар. 18, т.1 ЗИД НК

Предложен е текст за изменение на чл. 319б, ал. 1: „Който неправомерно добави, копира, използва, промени, пренесе, изтрие, повреди, влоши, скрие, унищожи компютърни данни в информационна система или спре достъпа до такива данни, в немаловажни случаи се наказва с лишаване от свобода до две години и глоба до три хиляди лева.“

По принцип необходимостта от изменение на чл. 319б е наложителен. Предложението за промяна на правилото, обаче, е непрецизно. На първо място изпълнително деяние „пренесе“ се дублира с деянието „копира“. Самото копиране е пренасяне на данни. На следващо място понятието „влоши“ и „повреди“ не може да се използва по отношение на компютърни данни, а за качествените функции на вещи от материалния свят. На трето място „скрие“ касае деяние по отношение на обекти от физическия свят. То се обхваща от деянието „промени“, защото се извършва промяна по отношение на данни за логическа адресация на други данни.

Предлагаме следната редакция:

„Който неправомерно добави, копира, използва, промени, изтрие или унищожи компютърни данни в информационна система или записани на електронен носител, или спре достъпа до такива данни, в немаловажни случаи се наказва с лишаване от свобода до две години и глоба до три хиляди лева.“

4. По пар. 18, т.3 ЗИД НК

Предложено е създаване на нова ал. 4 към чл. 319б със следното съдържание:

„(4) Ако деянието по ал. 1 е извършено чрез компютърна програма, парола, код за достъп или други данни за достъп до информационна система или до част от нея, предназначени да засегнат повече от една информационна система, и са настъпили последиците по ал. 2, наказанието

е лишаване от свобода от една до четири години и глоба до шест хиляди лева.“

Така формулираното правило е непрецизно. На първо място буди недоумение защо се въвежда квалифициран състав на правилото по ал. 1, когато деянието е извършено чрез друга програма, парола или код за достъп. Каква по-висока степен на обществена опасност се разкрива от общото правило по ал. 1? Нима има значение дали е имало защита или е нямало, за да се осъществи достъп до чуждите данни? Резултатът е един и същ – осъществяване на деянието по ал. 1. Също така непрецизност разкрива използване на думите „други данни от информационна система или до част от нея“. Непонятно е как ще се използват други данни от информационна система (а за „част от нея“ по-горе е обосновано, че не носи никакъв смисъл, предвид логическата унитарност на понятието „информационна система“ като единство от взаимосвързани устройства). Ако целта на нормата е била въобще да се установи квалифициран състав на случаите, при които се осъществява деянието по ал. 1 касае повече от една информационни системи, това отново буди сериозни несъвършенства. На първо място какво отношение имат от обективна страна начините на осъществяване на деянията по ал. 1 – „извършване чрез компютърна програма, парола или кодове за достъп или други данни“. Какви утежняващи средства за осъществяване на деянията са това и каква по-висока степен на обществена опасност се разкрива? Важното е от деянието да настъпил престъпният резултат – деяние по ал. 1. Освен това какво означава „и са настъпили последиците по ал. 2“. Всички деяния по глава IXа са резултатни. **Предлагаме правилото въобще да отпадне**. Но ако въпреки това се прецени, че следва да се установи такъв квалифициран състав, **предлагаме следната редакция**:

„(4) Ако деянието по ал. 1 е извършено по отношение на данни от повече от една информационна система или електронни носители, наказанието е лишаване от свобода от една до четири години и глоба до шест хиляди лева.“

5. По пар. 21, т. 1 ЗИД НК

Предложен е нов текст на ал. 1 към чл. 319д със следното съдържание:

„(1) Който създава, набавя за себе си или за другиго, внася или по друг начин разпространява компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или част от нея с цел да се извърши престъпление по чл. 171, ал. 3, чл. 319а, чл. 319б, чл. 319 в или чл. 319г, се наказва с лишаване от свобода до две години.“

Освен аргументите, които бяха споделени по-горе по отношение на непрецизността на думите „или части от нея“ (информационна система), извън правилото са останали случаите на използване на програми, пароли, кодове и т.н. за достъп до данни, записани на електронен носител.

В тази връзка предлагаме следната редакция:

„(1) Който създава, набавя за себе си или за другиго, внася или по друг начин разпространява компютърни програми, пароли, кодове или други подобни данни за достъп до информационна система или до електронни носители с цел да се извърши престъпление по чл. 171, ал. 3, чл. 319а, чл. 319б, чл. 319 в или чл. 319г, се наказва с лишаване от свобода до две години.“.

6. По пар. 21, т. 2 ЗИД НК

Предложен е нов текст на ал. 1 към чл. 319д със следното съдържание:

“(2) Когато с деянието по ал. 1 са разкрити лични данни, класифицирана информация или друга защитена от закона тайна, доколкото извършеното не съставлява по-тежко престъпление, наказанието е лишаване от свобода до три години.“

Правилото е редактирано, но в него като квалифициран състав отново е включено разкриването на „лични данни“, като престъпен резултат, вследствие на предстъплението по чл. 319Д. Обръщаме внимание, че личните данни не са защитена от закон тайна, за разлика от квалифицираната информация (държавната тайна), осигурителната тайна, банковата тайна, медицинската тайна и т.н. Законът за защита на личните данни (както и влизащия в сила Общ регламент за защита на личните данни GDPR) в нито една разпоредба не правят личните данни тайна, а само създават права и задължения във връзка със събирането, обработването предоставянето и т.н. на лични данни.

В тази връзка предлагаме следната редакция:

“(2) Когато с деянието по ал. 1 са разкрити класифицирана информация или друга защитена от закона тайна, доколкото извършеното не съставлява по-тежко престъпление, наказанието е лишаване от свобода до три години.“

7. Правилото на чл. 319е ЗИД НК трябва да отпадне.

Аргументите за това са следните:

Непосредствен обект на престъплението по чл. 319е НК са обществените отношения, осигуряващи нормалното изпращане, получаване, записване и съхраняване на електронни изявления. Тези обществени отношения са регламентирани в ЗЕДЕП. Нормата на чл. 319е

НК е бланкетна норма, защото препраща за един от елементите на престъплението (изпълнителното деяние) към друг нормативен акт – Закона за електронния документ и електронния подпис (чл. 6, ал. 2, т. 5 ЗЕДЕП). От обективна страна изпълнителното деяние се изразява в нарушаване на задължението за съхраняване на информацията за времето и източника на предаваните електронни изявления за срок от 1 година. То може да бъде осъществено чрез бездействие - непредприемане на необходимите действия за запазване на информацията, което на практика прави разпоредбата неприложима. На първо място определянето на субекта на престъплението по чл. 319е НК следва да се има предвид основният наказателно-правен принцип, че наказателната отговорност е лична и наказателно-отговорни могат да бъдат само физически лица. Следователно субект на престъплението по чл. 319е НК може да бъде посредникът - физическо лице. Такива посредници няма. Когато посредникът при електронното изявление е юридическо лице (например доставчик на услуги на информационното общество), субект на престъплението по чл. 319е НК ще бъде физическото лице – служител на доставчика, което съгласно вътрешните правила на доставчика е задължено да осигури съхраняването на посочената информация. Такава отговорност на може да се обоснове. Въобще доколкото престъплението е резулатно, следва да се докаже от субективна страна умисъл в несъхраняването на информацията – деецът е знаел, че не съхранява информацията, осъзнавал е настъпването на последиците от непазенето, но е искал или допускал настъпването на неблагоприятните последици – непазенето. Обосноваването на такава отговорност не кореспондира на обществената опасност на това деяние. На практика това е мъртва разпоредба – по нея няма нито едно повдигнато обвинение и нито една постановена присъда. Извън изложеното, Конституционният съд със свое Решение № 2 от 2015 г. - ДВ, бр. 23 от 2015 г.отмени аналогичните разпоредби в Закона за електронните съобщения (чл. 250а, 250б, 250в, 250г, 250д, 250е, 251, 251а) по отношение на задължението на предприятията, предоставящи електронни съобщителни услуги да съхраняват трафичните данни за ползваните електронни съобщителни услуги.

Предлагаме следния текст:

„§21а. Отменя се чл. 319е“

8. Необходимо е да се предвиди създаване на нов състав на престъпление, свързано с компютърните престъпления, при което деянието разкрива висока степен на обществена опасност и на този етап не е криминализирано.

Става сума за т.нар. **„деперсонификация“** – лъжливо представяне на едно в интернет за друго лице. Случаите са многобройни – създаване на фалшиви профили във Фейсбук и социалните мрежи от името на лица, които не предполагат, организиране на мними партита чрез социалните мрежи с от името на лица, с цел нарушаване на личния им живот, поръчване на артикули с плащане на доставка от чуждо името и без знанието на лица чрез интернет с цел компроментиране и т.н. Случаите в практиката са много. Липсва престъпен състав, по който тези опасни деяния, засягащи личната неприкосновеност на гражданите да бъдат подвеждани и извършителите наказвани. Тези престъпления са същински компютърни престъпления – с особен обект на посегателство, средства за извършване и с по-висока степен на обществена опасност. Винаги са резултатни. Примери за криминализиране на такива деяния в другите законодателства има множество.[1]

Предлагаме следния текст:

§21б. Създава се чл. 319ж

„Чл. 319ж. Който използва компютърни данни, за да се представи за другиго без негово знание или съгласие при предоставянето на услуги на информационното общество, сключване на сделки по електронен път или при извършване на електронни съобщения, се наказа с лишаване от свобода до две години.“

ПРЕДСЕДАТЕЛ НА
ВИСШИЯ АДВОКАТСКИ СЪВЕТ:

РАЛИЦА НЕГЕНЦОВА

ВИСШ АДВОКАТСКИ СЪВЕТ * РБългария *

[1] Виж. *САЩ*: The Identity Theft and Assumption Deterrence Act, последван от The Theft Penalty Enhancement Act от 2004;

Индия: The Information Technology Act (2000) - Чл. 417A и 419 A.
Великобритания: Data Protection Act 1998
Австралия: Criminal Law Consolidation (Identity Theft) Amendment Act 2003
Канада: Canadian Personal Information Protection and Electronic Documents Act
Франция: The Information Technology Act, чл. 66A и 66D.