EUROPEAN LEGISLATION TO FIGHT CYBERCRIME

Nadezhda Krasteva
South-West University "Neofit Rilski", Blagoevgrad, Bulgaria nkrusteva@law.swu.bg

Abstract: Globally, over the last few years, there has been a rapid development of Internet technologies. This, in turn, favors the discovery of new educational, intellectual and social opportunities. The Internet has become an integral part of the lives of each and every one of us. However, the Internet hides serious risks and threats. Unfortunately, the evolution of Internet technologies also serves the expansion of the relevant criminal activity. It can even be said that cybercrime is the "hit" of the criminal world since the beginning of the 21st century. It is a borderless crime that does not meet the usual limitations and obstacles. Individuals and / or groups of people around the world use the Internet to commit various illegal acts – financial frauds; theft of virtual identity; violation of copyright and related rights; production, possession and distribution of pornographic material with minors; arranging games of chance; recruitment of terrorists; and lately people are even talking about cyberwar.
Modern society is becoming increasingly dependent on electronic networks and information systems. Such dependence makes individual citizens, businesses and governments particularly vulnerable. In view of the serious threats posed by the spread of cybercrime and the need for adequate protection, the European Union has a continuing policy of fighting cybercrime. In 2013, the European Commission adopts the Cybersecurity Strategy "An Open, Safe and Secure Cyberspace", which presents the EU's vision on how best to prevent cyber disruptions and attacks and how best to respond to them. The strategy is followed by several legislation actions which main task is to ensure safety on the Internet – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA; Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. This theoretical and legal research aims to explore the European Union's actions to the fight against cybercrime and to find out the improvement of the Bulgarian legislation in this specific area.
Keywords: cybercrime, protection, European legislation

ЕВРОПЕЙСКО ЗАКОНОДАТЕЛСТВО СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

Надежда Кръстева
Югозападен университет „Неофит Рилски", гр. Благоевград, България nkrusteva@swu.law.bg

Резюме: В световен мащаб през последните няколко години се наблюдава бързо развитие на интернет технологиите. Това от своя страна благоприятства за откриването на нови образователни, интелектуални и социални възможности. Интернет се превърна в неразделна част от живота на всеки един от нас. Интернет пространството крие обаче сериозни рискове и заплахи. За съжаление, еволюцията на интернет технологиите обслужва и разрастването на съответната престъпна дейност. Може дори да се каже, че киберпрестъпността е „шлагерът" на престъпния свят от началото на XXI в. Това е престъпност без граници, която не среща обичайните ограничения и препятствия пред себе си. Отделни хора и/или групи от хора по света използват интернет за извършването на различни неправомерни деяния – финансови измами; кражба на виртуална самоличност; нарушаване на авторски и сродни права; производство, държане и разпространение на порнографски материали с непълнолетни лица; устройване на хазартни игри; набиране на терористи; а напоследък дори се говори и за кибер-войни.
Съвременното общество става все по-зависимо от електронните мрежи и информационни системи. Именно подобна зависимост прави отделните граждани, бизнеса, правителствата особено уязвими. С оглед на сериозните заплахи от разрастването на киберпрестъпността и необходимостта от адекватна защита, Европейския съюз провежда постоянна политика в борбата с престъпленията в кибернетичното пространство. През 2013 г. Европейската комисия приема Стратегия за киберсигурност „Отворено, безопасно и сигурно киберпространство", която представя визията на ЕС за това как най-добре следва да се предотвратяват кибернетични смущения и атаки и как най-адекватно да се отговаря на тях. Стратегията е

последвана от няколко законодателни актове, чиято основна задача е да осигурят безопасност в интернет пространството – Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза; Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета; Директива 2011/92/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета. Настоящата теоретично-правна разработка има за цел да изследва стъпките на Европейския съюз в борбата с киберпрестъпността и да констатира подобряването на българското законодателство в изследваната област.
Ключови думи: киберпрестъпност, защита, европейско законодателство

1. ВЪВЕДЕНИЕ

През последните години дигиталните технологии се превърнаха в неразделна част от живота на хората, като имат и съществена роля в осъществяването и развитието на икономиката в Европа и останалата част от света. Колкото и привлекателни, впечатляващи и улесняващи да са тези технологии, те крият сериозни рискове и заплахи. Появилата се зависимост и тясната връзка между ежедневните ни потребности и работа, значително увеличават възможностите за различни злоупотреби. А с това идват и непознати трудности, с които сякаш не можем или поне все още не знаем как да се справим. Сериозността на проблемите се подчертава неведнъж от Европейската комисия, която съобщава, че през 2016 година е имало над 4000 атаки на ден от Ransomware (рансъмуер)[288], а 80% от европейските компании са имали поне един инцидент, свързан с киберпрестъпността. Наред с това Европейската комисия изразява своята загриженост и по отношение на обстоятелството, че икономическото влияние на киберпрестъпността се е увеличило многократно само през последните няколко години. Комисар Аврамопулос, отговарящ за миграцията, вътрешните работи и гражданството, заявява: „Киберпрестъпниците нарушават основните права на гражданите на ЕС и вредят на нашата икономика. Потребителите имат право да се чувстват сигурни онлайн и извършителите не трябва да чувстват, че могат да действат безнаказано. Трябва да се засили доверието в онлайн услугите…“.

Едно от основните работни понятия в настоящата разработка е понятието „киберпрестъпност“. Оттук се поражда и нуждата от неговото изясняване. Приема се, че киберпрестъпността включва разнообразни престъпни деяния, които са извършени онлайн чрез използване на електронни съобщителни мрежи и информационни системи[289]. Като се осъзнават дълбоките изменения, предизвикани от въвеждането на цифровите технологии, от постоянната глобализация на компютърните мрежи, за компетентните органи е ясно, че е необходимо предприемане на мерки, които да са насочени към противодействие на разрастващата се киберпрестъпност. Затова на преден план излиза потребността от провеждането на обща наказателна политика, насочена към закрилата на обществото от престъпността в кибернетичното пространство, чрез приемане на съответно законодателство и чрез укрепване на международното сътрудничество. В тази връзка е важно да се отбележат предприетите вече европейски законодателни инициативи в тази посока.

Настоящата теоретично-правна разработка има за *цел* да изследва именно законодателните решения на европейско ниво по пътя на създаване на единна рамка за защита на гражданите от многобройните престъпни прояви, включени в термина „киберпрестъпност“. Също така следва да се констатира и влиянието му върху усъвършенстването на българското законодателство.

[288] Ransomware е съкращение от Ransom и Software и означава софтуер, който иска откуп. Ransomware е вид зловреден софтуер (malware), ограничаващ достъпа до компютърната система, която е поразил и изисква определена сума като откуп изплатен към създателя му, за да бъде премахната рестрикцията. Някои Ransomware-а криптират файловете на хардиска, докато други просто заключват екрана и показват съобщения, целящи да излъжат жертвата да плати (http://geakom.net/index.php/en/25-news/18-ransomware).
[289] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime.

2. ЕВРОПЕЙСКА ЗАКОНОДАТЕЛНА РАМКА ЗА ПРОТИВОДЕЙСТВИЕ НА КИБЕРПРЕСТЪПНОСТТА

Ефективната борба срещу престъпленията в кибернетичното пространство изисква провеждането на мащабно, бързо и ефикасно международно сътрудничество. Първата стъпка в тази посока е предприета от Съвета на Европа през 2001 г., когато е приета *Конвенцията за престъпления в кибернетичното пространство*. Това е първи опит за създаване на обща законодателна рамка за борба с киберпрестъпността. Конвенцията изяснява същността на редица важни определения („компютърна система“, „компютърни данни“, „доставчик на услуги“ и др.). Съществен принос на международноправния акт е определянето на отделни деяния като престъпления: правонарушенията срещу тайната, неприкосновеността и възможността за ползване на компютърните данни и системи; компютърните престъпления; правонарушенията, свързани със съдържанието; престъпленията, свързани с посегателствата срещу авторското право и сродните му права. Наред с въпросите в областта на материалното наказателно право, Конвенцията урежда и редица процесуални правила и гаранции – претърсване и изземване на съхраняваните компютърни данни; събиране в реално време на компютърни данни; компетентност и др. Показателно за необходимостта от подобен международноправен акт за защита на всички граждани от посегателства в кибернетичното пространство е обстоятелството, че Конвенцията е подписана и ратифицирана и от държави, които не са членове на Съвета на Европа, а именно САЩ, Япония и Канада.

През този период Европейския съюз предприема сериозна инициатива за защита на европейските граждани от измами, включващи каквато и да е форма на платежни средства, различни от парите в брой (напр. кредитен превод, директен дебит, плащане с карта). За тази цел, Съвета на ЕС приема *Рамково решение 2001/413/ПВР относно борбата с измамата и подправянето на платежни средства*, различни от парите в брой. В Рамковото решение са описани различни действия, свързани с измамата и с подправянето на платежни средства, различни от парите в брой. Посочените правонарушения са разделени в три групи: правонарушения, свързани с платежните инструменти (напр. кражба на дебитна карта или чек); правонарушения, свързани с използването на информационни технологии и правонарушения, свързани със специално приспособено оборудване. Рамковото решение изисква всички посочени видове деяния да бъдат обявени за престъпления в националните законодателства на отделните държави. Държавите от своя страна следва да определят адекватни санкции за извършителите.

Видно е, че Рамково решение 2001/413/ПВР има тясно приложно поле. Затова е необходимо осигуряването на пълна защита от различните форми на посегателства чрез интернет технологиите. В тази връзка ЕС предприема важна стъпка в борбата с киберпрестъпността. През 2005 г. Съвета на ЕС приема *Рамково решение 2005/222/ПВР относно атаките срещу информационните системи*, което следва да осигури една по-всеобхватна наказателноправна защита от престъпленията в кибернетичното пространство. В сравнение с Конвенцията за престъпления в кибернетичното пространство, Рамковото решение от 2005 г. урежда само въпроси от естеството на материалното наказателно право. Наред с това то е насочено единствено към държавите-членки на ЕС. Съществен принос на посоченото решение е въвеждането на изискване за обмен на информация между държавите-членки, за което следва да се използва съществуващата мрежа от оперативни точки за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата.

Въпреки предприетите законодателни инициативи, киберпрестъпността продължава да се разраства и да придобива нови проявни форми. Лицата, използващи интернет технологиите с престъпни намерения и за постигането на престъпни цели, лесно и бързо се приспособяват към новостите на средата и трансформират дейността си в друга, вероятно по-печаливша и трудно разкриваема. Така например се появяват ботнет атаките[290], кражбата на онлайн самоличност, различните форми на онлайн сексуално посегателство спрямо деца, кражбата на пароли и др. Всички тези обстоятелства са предпоставка за необходимостта от изготвянето на нови, допълнителни законодателни мерки за борба с киберпрестъпността.

[290] Ботнет (botnet) е мрежа от софтуерни приложения или компютри, които работят в автономен режим и имат за цел кражба на лични данни. Botnet се състои от думите „робот“ и „мрежа“. Киберпрестъпниците използват специални троянски вируси, за да нарушат сигурността на компютрите на няколко потребители, да поемат контрола над всеки компютър и да организират всички заразени машини в мрежа от „ботове“, които престъпникът може да управлява от разстояние (https://www.kaspersky.com/resource-center/threats/botnet-attacks).

Един от сериозните проблеми, който създава киберпрестъпността, е свързан с осигуряване на адекватна защита на децата в интернет пространството. Интернет пространството осигурява уникална анонимност на своите потребителите, защото те могат спокойно да прикрият истинската си самоличност, личностните си особености и характеристики. Напредъкът на информационните и комуникационните технологии, за съжаление, улесни и т.нар. „сприятеляване“ с деца. Вече съществуват и се използват нови начини за установяване на контакт с малолетни и непълнолетни лица, например социалните мрежи, Skype, чат стаите и др. Тук извършителите не се притесняват, че може лесно да бъде разкрита тяхната самоличност, защото е възможно да се представят за всеки. Така интернет пространството се превръща в истинска опасност за всички онези деца, които имат нужда да бъдат чути, да споделят с някого своята болка и радост, да разкрият своите емоции и мечти. Всяко едно от тези деца е потенциална жертва.

Проблемът със сексуалните посегателства над деца е изключително сериозен. Неговите измерения са трудна, а понякога и непосилна задача. През 2010 г. Съвета на Европа посочва, че едно на пет деца в Европа е жертва на някаква форма на сексуална експлоатация. През същата година Европейската комисия предприема сериозни мерки в борба срещу тежките посегателства спрямо половата неприкосновеност на децата. Направено е предложение за Директива за борба със сексуалното насилие, сексуалната експлоатация и детската порнография, която да замени действащото Рамково решение 2004/68/ПВР на Съвета. През 2011 г. Съветът приема предложената Директива, с която се сближават националните законодателства на държавите-членки по отношение на 20 престъпления и се определят високи размери на наказанията за тях.

Директива 2011/92/ЕС на Европейския парламент и на Съвета от 13.12.2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета е иновативен законодателен инструмент, който има съществена роля в борбата с посочените престъпни посегателства върху правилното физическо, психическо и емоционално развитие на децата. Директивата унифицира националните законодателства в целия Европейски съюз в разглежданата област. Поради обхвата и последиците от разглежданите посегателства, подобен подход сякаш е единствената възможност за реална превенция и противопоставяне. Ролята на Директивата е съществена и по отношение защита на децата в интернет пространството. Директивата изисква от държавите-членки предприемането на необходимите мерки за криминализиране на прояви като: склоняването или наемането на дете за участие в порнографски представления[291]; използването на принуда или сила спрямо дете с цел участие в порнографски представления; съзнателното получаване на достъп до детска порнография посредством информационни и комуникационни технологии; предложението, посредством информационни и комуникационни технологии, от страна на възрастен да се срещне с дете, което не е навършило възрастта за изразяване на съгласие за сексуални действия, с цел извършване на някое от престъпленията, посочени в Директивата[292] и др. Една от силните страни на разглежданата Директива са предвидените в нея квалифициращи обстоятелства, които се отнасят до *жертвата на престъплението* (напр. дете в особено уязвимо положение); до *субекта на престъплението* (престъплението е извършено от член на семейството; от лице, което съжителства с детето и др.); до *начина на извършване на престъплението* (когато престъплението включва тежка проява на насилие и др.) (чл. 9). Наред с това Директивата посочва, че лице, осъдено на някое от посочените в нея престъпления, може временно или постоянно да бъде лишено най-малко от правото да упражнява професионални дейности, които включват преки и редовни контакти с деца. Това се налага с оглед по-ефективната защита на децата, защото рецидивът сред извършителите на сексуални престъпления е често срещан.

Директива 2011/92/ЕС предвижда да се оказва помощ и подкрепа в по-голяма степен на децата, жертви на сексуално посегателство. Поради характера на причинената вреда, оказваната помощ и подкрепа следва да продължат толкова време, колкото е необходимо за пълното физическо и психическо възстановяване на малолетното и непълнолетно лице. Директивата излага различни превантивни мерки, които е нужно да се предприемат от държавите-членки с цел предотвратяване сексуалното посегателство над деца. Предвидено е някои от мерките да се прилагат *по отношение на извършителите* – включването им в специални програми, чиято цел е да се сведе до минимум опасността от рецидив. Други от мерките са

[291] Съгласно Директива 2011/92/ЕС „порнографско представление“ означава „представяне на живо, предназначено за публика, включително посредством *информационни и комуникационни технологии*, на дете, участващо в прояви на реално или симулирано открито сексуално поведение...“.
[292] Това поведение е известно като on-line grooming – *„сприятеляване“ с деца онлайн за сексуални цели*.

насочени към обществото – програми за научни изследвания, образователни програми, провеждането на кампании за повишаване на осведомеността относно проблема и др.

Навременното уведомяване на компетентните органи за подозрения за сексуални посегателства спрямо деца е основна част от превенцията. В тази връзка, Директивата изисква от държавите-членки да предприемат мерки, с които да насърчат обществото към активно участие[293].

Следващата важна стъпка на ЕС за защита на кибернетичното пространство е предложението през 2010 г., което е окончателно прието на 22 юли 2013 г. и влиза в сила на 4 септември 2013 г. като *Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи.* Посочената Директива заменя Рамково решение 2005/222/ПВР на Съвета, което е разгледано по-горе в текста. Директивата запазва доста от разпоредбите, посочени в Рамковото решение, но наред с това въвежда и нова по-строги правила. Така например Директива въвежда наказания за създаването на ботнет – акт на установяване на контрол от разстояние върху значителен брой компютри посредством заразяването им със зловреден софтуер чрез целенасочени кибератаки. Както е посочено и в самата Директива, веднъж създадена, заразената мрежа от компютри, която представлява ботнетът, може да бъде активирана без знанието на потребителите на компютрите, за да извърши широкомащабна кибератака, която обикновено може да причини сериозни вреди.

Държавите-членки следва да предприемат мерки, които да осигурят предвиждането на наказание лишаване от свобода за извършено престъпление, посочено в Директива 2013/40/ЕС. По-тежко наказуеми са случаите, когато деянието е извършено от престъпна организация, причинило е сериозни вреди или е извършено чрез информационна система, която е част от критична инфраструктура. Като квалифициращо обстоятелство съгласно националното право може да се разглежда и деянието, което е извършено чрез злоупотреба с лични данни на друго лице, за да се спечели доверието на трето лице, и по този начин да са нанесени вреди на законния собственик на самоличността.

Новата Директива, освен новите форми на престъпна дейност и по-строгите наказания, има за цел и да улесни предотвратяването на престъпленията в кибернетичното пространство, като подобри сътрудничеството между съдебните и останалите компетентни органи. В тази връзка държавите-членки следва да осигурят наличието на оперативно национално звено за контакт и да използват съществуващата мрежа от оперативни звена за контакт, които да са на разположение 24 часа в денонощието и седем дни в седмицата. Държавите-членки следва също така да гарантират, че разполагат с процедури, чрез които в случай на спешно искане за съдействие, компетентният орган в рамките най-много на 8 часа от получаването ще посочат най-малко дали на искането за помощ ще бъде отговорено, както и формата и приблизителното време за отговор. Това несъмнено е трудна и отговорна задача за изпълнение. Ясно е, че Директивата има за цел да подобри усилията и сътрудничеството между държавите-членки в борбата срещу киберпрестъпността.

Навярно основният законодателен акт на ЕС в борбата срещу киберпрестъпността поне засега е новата *Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза*. Тя предоставя законодателни мерки за повишаване нивото на киберсигурността в ЕС. Директивата акцентира върху осъществяването на адекватно и навременно сътрудничество на национално и международно ниво с трети държави и международни организации. В тази връзка е предвидено създаването на група за сътрудничество с цел подкрепа и улесняване на стратегическото сътрудничество и обмен на информация между държавите-членки и изграждане на доверие сред тях; създаване на мрежа на екипите за реагиране при инциденти с компютърната сигурност (наричана „мрежата на ЕРИКС“); определяне на национални компетентни органи, единни звена за контакт и ЕРИКС със задачи, свързани със сигурността на мрежите и информационните системи. Настоящата Директива следва да бъде транспонирана до 9 май 2018 г. Държавите-членки трябва да приемат всички необходими законови, подзаконови и административни мерки за съобразяване с изискванията на Директивата.

[293] Кръстева, Н. Борба със сексуалното насилие, сексуалната експлоатация на деца и детската порнография. Сб. „Правото между традицията и модерността“, В., 2014 г., стр.239-244; Krastev. V. Criminal Child Protection from Human Trafficking during Contemporary Migration. Revista Inclusiones, Vol. 4, N 1, p. 57-65 (co-author N. Krasteva).

През последните няколко години интернет технологиите се използват и за набиране на терористи или за радикализиране на младежите. В днешно време кибертероризмът представлява сериозна заплаха за всяка държава по света. По повод този изключително сериозен проблем, ЕС прие и то съвсем скоро *Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 година относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета.* В Директивата е обърнато специално внимание на борбата с тероризма в интернет. Посочено е, че едно ефективно средство за борба с този вид тероризъм е премахването или поне блокирането на достъпа до онлайн съдържание, което представлява публично подстрекаване към извършване на терористично престъпление. В тази връзка се изисква от държавите-членки да предприемат необходимите мерки, които да гарантират бързото премахване на онлайн съдържание или ако това е невъзможно да предприемат мерки за блокиране на достъпа до съдържание, което представлява публично подстрекаване към извършване на терористично престъпление. Предприетите мерки трябва да зачитат правата на крайните потребители и да спазват съществуващите правни и съдебни процедури и Хартата на основните права на Европейския съюз. Важно е да се подобрява и сътрудничеството между отделните държави, и обмена на информация между тях. Тази Директива следва да бъде транспонирана до 8 септември 2018 г. Държавите-членки трябва да предприемат необходимите законови, подзаконови и административни мерки, за да въведат изискванията на Директивата в националните си законодателства.

3. НАПРЕДЪКЪТ НА БЪЛГАРСКОТО ЗАКОНОДАТЕЛСТВО В БОРБАТА С КИБЕРПРЕСТЪПНОСТТА

Република България полага усилия за осигуряване на защита на българските граждани от престъпни посегателства в кибернетичното пространство. В тази връзка следва да се посочат предприетите мерки от страна на българската държава в борбата с киберпрестъпността.

Единственият специализиран сектор, който работи за противодействие на престъпленията в кибернетичното пространство в Република България е сектор „Киберсигурност“ към ГДБОП-МВР[294]. В изпълнение изискванията на Конвенцията за престъпленията в кибернетичното пространство, от 2007 г. в сектор „Киберпрестъпност“ функционира Националния контактен пункт 24/7. Основната му цел е осъществяване на навременен и директен контакт с компетентните служители на съответните органи, пряко ангажирани в борбата с киберпрестъпността по света. За превенция и защита на гражданите, секторът създава специален сайт за борба с киберпрестъпленията[295]. Сайтът съдържа актуална информация за заплахите в интернет и съвети за защита и разпознаване на рисковете. Сайтът е специално насочен към децата и техните родители. Съдържа полезни съвети за безопасна работа в интернет и за абсолютно необходимото обучение и възпитание на децата по тези въпроси.

Наказателният кодекс на Република България (НК) претърпя известни подобрения с оглед осигуряване на защита от киберпрестъпност. Със Закона за изменение и допълнение на НК (ЗИДНК), ДВ, бр. 92 от 2002 г. се въведе нова Глава девета „а“ от Особената част на НК, озаглавена „Компютърни престъпления“. Тя регламентира престъпленията, които нарушават нормалното функциониране на компютърни системи и компютърни информационни данни. Наред с това се въведе дефиниция на понятия, свързани с предлаганата криминализация на деянията – „компютърна система“, „компютърни данни“ и „платежен инструмент“. Промените са следствие от подписаната тогава Конвенцията за престъпленията в кибернетичното пространство.

Подобренията на действаща наказателноправна уредба в областта на киберпрестъпността продължават и със ЗИДНК, ДВ, бр. 38 от 2007 г. С него се въвеждат нови понятия като „компютърна мрежа“, „компютърна програма“, „компютърен вирус“ и се допълва значението на съществуващи вече понятия като „компютърна система“ и „компютърни данни“. Това, разбира се, улесни и подобри работата на компетентните органи в борбата с киберпрестъпността. Бяха допълнени и изменени разпоредбите на Глава девета „а“ от Особената част на НК.

Република България като държава-членка на ЕС въведе в законодателството си и изискванията на разгледаната по-горе Директива 2011/92/ЕС. Българското законодателство в частта относно сексуалните

[294] Абревиатурата ГДБОП-МВР означава Главна дирекция борба с организираната престъпност към Министерство на вътрешните работи.
[295] www.cybercrime.bg

посегателства над деца е в съответствие с Конвенцията на Съвета на Европа за закрила на децата срещу сексуалната експлоатация и сексуалното насилие. По тази причина в ЗИДНК, ДВ, бр. 74 от 2015 г. са въведени само онези правила, с които Директива 2011/92/ЕС надгражда стандартите на Конвенцията. Така например се измени понятието „порнографски материал“ и се въведе ново понятие „порнографско представление“. В съответствие с изискванията на Директивата са въведоха и изменения в разпоредбите, осигуряващи закрила на децата от посегателства спрямо половата им неприкосновеност.

Налаганите европейски стандарти, които българското законодателство въведе и изпълнява имат за цел да повишат ефективността на превенцията и борбата с киберпрестъпността. Безспорно сериозната и отговорна работа тепърва предстои.

4. ЗАКЛЮЧЕНИЕ

Бързият темп, с който се развиват технологиите днес, предполага функционирането на един изцяло дигитално-зависим свят. Киберпрестъпността засяга почти всички сфери на обществения живот и това е една от предпоставките за мащабността на този вид престъпност. За получаването на качествени резултати е от особено значение съществуването на единна законодателна рамка и тясно сътрудничество между отделните държави. Усилията са продиктувани предимно от необходимостта да се осигури защита на правата и законните интереси на всички ползватели на информационните технологии. Въпреки че, настоящото изследване не претендира за изчерпателност, с него се изразява подкрепа към постигнатите резултати и загриженост за необходимостта от предприемането на нови мерки за противопоставяне на новопоявяващите се форми на престъпни прояви в кибернетичното пространство.

ЛИТЕРАТУРА И ИЗТОЧНИЦИ

[1] Копчева, М. Компютърни престъления. С., 2006.
[2] Europol Review, 2015.
[3] Krastev. V. Criminal Child Protection from Human Trafficking during Contemporary Migration. Revista Inclusiones, Vol. 4, N 1, p. 57-65 (co-author N. Krasteva).
[4] Кръстева, Н. Борба със сексуалното насилие, сексуалната експлоатация на деца и детската порнография. Сб. „Правото между традицията и модерността“, В., 2014 г., стр.239-244.
[5] www.cybercrime.bg
[6] www.eur-lex.europa.eu
[7] www.kaspersky.com