До

Научното жури

Утвърдено със Заповед

№ РД -09-112/02.12.2015 г. на

Зам.-директора на ИДП при БАН

Р Е Ц Е Н З И Я

От

Д.ю.н. Орлин Борисов

Професор по МПП и Право на ЕС

В ЮФ на СУ “Св. Кл. Охридски“

Относно: Защита на дисертация на Елена Иванова Стоянова за присъждане на образователната и научна степен „доктор“ на тема:

„Международноправна уредба на борбата с киберпрестъпленията“ по

Научната специалност Международно право и международни отношения,

Шифър 3.6. Право

Представената за рецензиране дисертация е в обем от 225 печатни страници, които обхващат Предговор, три глави (включващи 7 параграфа, 14 под параграфа и 41 под под параграфа), Заключение, Библиография и Декларация за оригиналност и достоверност.

I

Елена Иванова Стоянова е родена на 25.05.1982 г. в гр. София.

Средното си образование получава през 2001г. след завършване на 91.НЕГ „Проф. Константин Гълъбов“. През 2006 г. завършва като частна ученичка и Първа Английска гимназия в София.

В периода 2001-2002 е студентка в ЮФ на СУ „Св. Кл.ОХридски“, след което продължава обучението си по право в периода 2002-2007 г. като студентка в ЮФ на Университета в Манхайм.

От месец януари 2008 г. (заповед № 13/ 30.01. 2008 г) до отчисляването й през 2013 г. (заповед № РД-09-1-02/ 11.01.2013) е редовен докторанти в ИДП при БАН.

В периода от месец юни до м. септември е посещавала Еразъм програмата за докторанти, Университета в Залцбург, Австрия.

Трудовият стаж на дисертанта включва:

- 2003-2004 г. – Асистент при застрахователен фонд ВКК, Лудвихсхафен, Германия;
- Януари-септември 2004 г. – Асистент при юридическа фирма, Хайделберг, Германия;
- Септември-октомври 2005 г. – Стаж в СГС;
- Януари – април 2008г. – Експерт в борба и превенция на измами при онлайн разплащания, София; и др.
- От м. юни до сега е адвокат в САК.

II

Представената за рецензиране дисертация съдържа три глави напълно свързани с темата и анализиращи детайлно действащата на практика международноправна уредба на борбата на международната общност с киберпрестъпленията на съвременния етап.

Изследваната материя се характеризира с интердисциплинарен подход при научното анализиране на проблемите.

ПЪРВА глава е посветена на историята и развитието на интернет и киберпрестъпността, като в първи параграф е анализирано развитието на интернет и киберпространството. Авторът научно-обосновано приема, че „В наши дни киберпространството неправилно се идентифицира с понятието Интернет“ (анализ на разграничаването по начин на функциониране).

В дисертационния труд мотивирано се приема, че Интернет се появява през 1968 г. първоначално в доклад на Министерството на отбраната на САЩ, а с термина Итернет се описва единна глобална компютърна мрежа съгласно създадения през 1980 г. модел TCP/!P.

В труда се приема, че ролята на Интернет в международен план нараства, а броя на потребителите непрекъснато се увеличава (напр. от 300 млн. през 1999 г. до 600 млн през 2002 г. (а през 2012г. според Световната Итернет статистика вече са над 2 млрд), т.е. в периода 2000г. до 2008г. броят на потребителите се увеличава с 290%). В тази връзка в труда обосновано се приема, че електронната кореспонденция вече е заместила традиционните писма, електронната търговия е на път да достигне обеми, конкурентни на традиционното

пазаруване, а Онлайн представянето вече е от решаващо значение в бизнесредите и като цяло електронните услуги спомагат значително за намаляване на размера на разходите за същите услуги извън мрежата и т.н.

Авторът научно-обосновано прима извода, че „Междувременно световната информационна мрежа непрекъснато се променя, като предоставя на потребителите все повече нови услуги и възможности“ и се присъединява към общоприето становище, че Интернет се превръща от глобално информационно и комуникационно пространство в икономическа, културна и социална среда.

Във втори параграф е изследвано развитието на престъпленията в кибернетичното пространство, върху което според труда, силно революционно влияние оказва развитието на технологиите, което наред създаваните комуникации, предоставя възможност за развитието на нов вид престъпления – киберпрестъпления. Според автора „Интернет пространството представлява лесно уязвима среда за криминални прояви главно поради две причини: дава възможност за анонимност и надхвърля географските граници“.

Според авторът след първото федерално разследване на неоторизирано проникване в компютърната мрежа на голяма банка в щата Минеаполис през 1966 г. с развитието на глобалната мрежа международните интернет престъпления се разрастват в различни форми, като напр. нелегални пробиви в системите на редица правителствени и неправителствени международни организации, появата на компютърни вируси, кибератаки и др. (Пентагонът докладва за около 6 милиона опита за пробив в системата през 2006 г. и около 360 млн. опита през 2008г.). Атаките са насочени както към кооперативни и политически организации, така и срещу частни лица (напр. в сферата на електроннните платежни документи, измамата с банкови карти, кражба на социален осигурителен номер и др. като стават сериозна заплаха за деловите инвестиции и активи).

В труда обосновано се приема, че значително е нарастването на престъпленията в мрежовата среда началото на новото хилядолетие като „ по данни на Интерпол през 2000 –та година престъпленията са се увеличили 10 пъти по сравнение с 1990 г., а през 2002 г. престъпленията са се увеличили четирикратно“. През последните години според статистиката, щетите и загубите претърпени от потребителите жертви на киберпрестъпленията през 2011 г. са на стойност 110 милиарда щатски долара (напр. средно 18 потребителя стават жертва всяка секунда).

Авторът обосновано извежда научния извод, че „ възможните щети и загуби варират от опасността за ограничен достъп до персоналния компютър до срив в системата на големи корпорации и институции, кражба на търговска конфиденциална информация, блокиране на правителствени сайтове и др.“.

Във ВТОРА глава се изследва въпроса относно понятието и видовете киберпрестъпления, в която автора приема обосновано, че интернет престъпленията са типичен пример за международни, трансгранични престъпления, но характерното за тях е, че се извършват само чрез компютърни мрежи, или са насочени към такива. Това твърдение е много точно, защото това наистина е едно от най-опасните съвременни трансгранични престъпления престъпления с международен елемент, които засягат интересите не гражданите

(потребители) само на няколко държави, а тези престъпления са с неограничен географски обхват.

Анализирайки подробно определенията давани от различни автори и приети в различни международни актове, авторът, обобщавайки ги, достига до извода, че понятието киберпрестъпление включва престъпленията, които включват компютър или компютърна мрежа.

Авторът, анализирайки международната теория и практика относно разширителното тълкуване на това престъпление, приема обосновано извода, че „понятието за киберпрестъпления понастоящем се използва за широк спектър деяния, които обхващат както „традиционни“ компютърни престъпления, така и престъпления, извършени в мрежата. Тези деяния са твърде разнообразни, за да бъдат успешно обхванати от строго и тясно определение“. В трудът се правилно се подчертава, че законодателствата на държавите съдържат различни разпореди, поради което се препоръчва разработването и приемането на широко определение за киберпрестъпление, приложимо в съответствие с конкретната държава и да отговаря на развитието на компютърните технологии.

В дисертационния труд подробно се анализират видовете киберпрестъпления според международните актове и националните законодателства. Авторът научно-обосновано приема, че като преобладаващи престъпления в електронната среда са „кражбите на интелектуална собственост, неправомерният достъп, финансовите манипулации, неоторизираното използване на компютърни ресурси, действия, свързани със съдържанието“ като подчертава, че нововъведенията в сферата на технологиите винаги води до нарастване на компютърната престъпност.

В следствие на обобщен научен анализ се приема извода, че т. нар. същински компютърни престъпления се припокриват с компютърно свързаните престъпления или различните деяния биха могли да се причислят и към едната и към другата група.

Авторът правилно подлага на много сериозен научен анализ текста на Конвенцията за престъпленията в кибернетичното пространство, по отношение на която точно отбелязва, че тя не съдържа всички проявления на престъпни деяния в киберпространството, но регламентира основните им форми.

В дисертационния труд на подробен научен анализ са подложени такива престъпления като: престъпления срещу тайната, неприкосновеността и възможността за ползване на компютърни данни и системи (като напр. възпрепятстване на функционирането на компютърни системи, незаконно прихващане на компютърни данни, компютърен саботаж, шпионаж и др.); компютърни престъпления (като напр. компютърна фалшификация и компютърна измама); престъпления свързани със съдържанието (като напр. детска порнография в Интернет, проповядване и подбуждане към расова вражда, омраза и расова дискриминация и др.); престъпления, свързани с авторското право и сродните му права (като напр. софтуерно пиратство, пиратство на интелектуални продукти и др.).

Авторът наред с киберпрестъпленията, предвидени в Конвенцията за престъпленията в кибернетичното пространство, анализира и други киберпрестъпления, които според него нарастват постоянно, а същността и характерът им се изменят и адаптират според развитието на информационните технологии.

В дисертацията се анализира едно от най-опасните киберпрестъпления – кибертероризма, като имащо своето самостоятелно място в рамките на международната компютърна престъпност, което има характеристиките както на киберпрестъпление, така и на трансграничния тероризъм. Авторът го определя като „хибридна форма, при която се използват възможностите предоставяни от Интернет и компютърните системи, за извършване на политически мотивирани престъпни операции срещу компютърни данни, системи и мрежи, често с цел причиняване на икономически щети или човешки жертви“.

В дисертацията се приема, че осезателно кибертероризмът се усеща през 80-те години на XX век, когато компютърните технологии започват да се използват като оръжие от трансграничния тероризъм.

Според обосновани извод на автора кибертероризмът се проявява в киберпространството като: “ блокиране на достъпа до мрежи сайтове; интернет измами; разпространение на програми с цел унищожаване или манипулиране на информация и др.“, чрез възможност за създаване на напълно анонимен интернет адрес или интернет профил в различни платформи и да го ползва под чуждо име.

В дисертационния труд задълбочено се изследва също така и въпроса относно това, че киберпространството създава и нова област за водене на военни действия – кибервойната като една от формите на информационната война и информационния тероризъм. Авторът мотивирано приема, че „Границата между кибертероризма и войната с електронни средства или водена по електронен път понякога може да бъде трудно определима“ и че „Измеренията на кибервойната в бъдеще според експертите имат потенциал да достигнат величини, в които за 15 минути може да бъде предизвикан тотален срив в световен мащаб. Сриване на военни сървъри и данни с информация, изгубване на контрол над сателити, изпратени в космоса, злоупотреба с финансови данни“. Правилно се отбелязва, че кибероперациите обичайно се провеждат с помощта на софтуер, хардуер или комбинация на софтуер и персонал.

Авторът изследва също така конкретните проявления на кибершпионажа като напр. „извличане на поверителна информация, понякога в обичайния интернет трафик, или чрез умишлено поставяне на заразени стикове за памет на обществени места, с надеждата потребителите да ги ползват и да заразят компютрите си“. Приема се , че водещи държави в кибершпионажа са Китай и Русия, като се отбелязва, че световен лидер в това отношение са САЩ.

В труда правилно се анализира и приема, че една от новите форми на финансова престъпност е в сферата на електронните платежни инструменти (напр. с използване на банкови карти или на данни от тях), които се проявяват след внедряването на електронните средства за безналични плащания. Авторът счита, че „ с разширяване на електронната търговия и електронното банкиране се увеличават и престъпленията, извършвани по мрежов път – кражба на лични данни, номера на платежни карти, информация за състояние на банкови сметки и друга поверителна информация“. Приема се също така, че банковите транзакции в мрежата предполагат осъществяването на трансгранична престъпна дейност.

В труда освен тези престъпления на задълбочено са анализирани кражбата на самоличност (т.е. отнемането и използването на чужда самоличност чрез измама с

технически средства, онлайн и чрез Интернет), пране на пари (изпирането на престъпни капитали с банкови операции след създаването на свободни виртуални зони за финансова дейност) и други престъпления против паричната и финансовата система.

Авторът чрез научен анализ доказва, че „Световната мрежа дава възможност на терористите да осъществяват идеологическа пропаганда, да разработват планове за терористични актове, да събират информация, подпомагаща атентати. Поради тази причина може да се очаква неминуемо нарастване на тези престъпления“.

В дисертацията по отношение на трансграничния кибертероризъм се приема, че „терористичните актове засягат целия свят и застрашават мира на международно ниво“.

ТРЕТА глава очаквано анализира нормативната уредба на престъпленията в кибернетичното пространство.

В т.1 на параграф 1 са анализирани инициативите на ЕС и Съвета на Европа, които стартират през 1997 г., когато ЕС определя рисковете с Интернет, в Съобщение относно нелегалното или вредното съдържание, публикувано в мрежата.

Подробно се разглежда съобщение COM 687 на ЕК „Информационно общество за всички“, съгласно което е необходимо наличието на бърз и достъпен Интернет в университетските изследователски центрове, като до края на 2001 г. да има изградена компютърна мрежа поне в един университет на всяка държава-член. Авторът мотивирано приема, че „десетилетие по-късно резултатите от тази инициатива са налице дори са преизпълнени...почти няма институция или организация без собствен Интернет сайт“.

Във връзка с анализа на Съобщение COM (2000) 890 Създаване на по-сигурно информационно общество чрез подобряване на информационната сигурност и борбата с компютърната престъпност авторът мотивирано приема извода, че „ЕК набляга еднакво както на законодателните, така и на всякакви извънзаконодателни инициативи в стремежа към изграждането на единна и сигурна информационна мрежа още в началото на 21 век“.

При анализа на Съобщение COM (2007) 267 на ЕК до ЕП, Съвета и Европейския комитет на регионите „Към основна политика по отношение на борбата с престъпленията в кибернетичното пространство“ авторът научно-обосновано приема, че „Перспективите пред ЕК на този етап са насочени срещу традиционните престъпления в електронните мрежи и незаконното съдържание в интернет и конкретните мерки, които следва да бъдат приети в тази насока“.

Подробно са анализирани също така и Съобщенията COM 1996 (487) на ЕК относно „Нелегалното вредно съдържание на Интернет“; Рамковото Решение 2001/413/ПВР на Съвета относно „Измамата и подправянето на платежни средства, различни от парите в брой; Рамково решение 2004/68/ПВР на Съвета относно „Борбата със сексуалната експлоатация на деца и детска порнография“; Рамково Решение 2005/222/ПВР на Съвета относно „Атаките срещу информационните системи“; Директива 2006/24/ЕО за запазване на данни“; и др.

В т.2 на този параграф се анализира Конвенцията за престъпленията в кибернетичното пространство, която според авторът е най-значимият международен акт в областта на киберпрестъпността и посочва конкретно, че „Конвенцията за престъпленията в кибернетичното пространство е първият международен договор за престъпления, извършени по интернет и други компютърни мрежи....определяща три основни насоки, които подлежат на правна уредба: хармонизиране на националните законодателства по отношение на инкриминираните деяния, въвеждане на съответните процесуални стандарти при тяхното разследване и наказателно преследване, адаптирани към глобализацията на мрежите, както и създаването на бърза и ефикасна система за международно сътрудничество“.

Наред с европейските актове са анализирани и актовете на ООН, Актовете на Международната асоциация по наказателно право и актовете на групата на Осемте.

III

Дисертационният труд съдържа редица научни приноси, от които по-значими са следните:

- Трудът представлява първото задълбочено, изчерпателно монографично изследване в българската юридическа литература;
- Трудът има огромна практико-приложна стойност;
- В труда са разкрити и анализирани характеристиките на киберпрестъпленията;
- Причисляване на киберпрестъпленията към престъпления с международен елемент, а едновременно с това се приема, че по географски обхват, нанасянето на икономически щети и човешки жертви се приравняват към международните престъпления;
- Многобройните обобщени научно предложения de lege ferenda и др.

I V

В труда са допуснати и някои незначителни неточности, които не помрачават отличните впечатления от изложената материя като напр.:

- В Увода би допринесло малко по-точното изясняване на научно-изследователската теза;
- По правило първо се разглеждат универсалните актове преди регионалните (за това по-удачно би било размяна на т. 1 и 2 на параграф 1 на гл. III;
- Би следвало разгледаното накратко в 1.6 на парагр.2 на гл.II и т.3 на парагр. 3 на гл.III да се разгледат съвместно с други по-обемни параграфи (т.като е известно, че в рамките на 1-2 стр. не може да се направи задълбочен научен анализ).

V

В заключение бих желал да отбележа, че представената дисертация е напълно завършен научно-изследователски труд, изцяло отговарящ на Закона за развитие на академичния състав в Р. България. Монографичният труд се характеризира със значими научни приноси, изводи и анализи, поради което убедено давам своята положителна оценка и предлагам на уважаемите членове на Научното жури да присъди на Елена Иванова Стоянова образователната и научна степен „доктор“ по научната специалност „Международно право и международни отношения“.

София, февруари 2016 г.

Рецензент:

/проф. д.ю.н. Орлин Борисов/