

МЕХАНИЗМИ НА МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

Драгомир Кръстев

*Докторант в Института за държавата и правото
към Българска академия на науките*

MECHANISMS OF INTERNATIONAL COOPERATION AGAINST CYBERCRIME

Dragomir Krastev

*PhD student at the Institute of State and Law
at the Bulgarian Academy of Sciences*

Резюме: В доклада се разгледани специфичните проблеми, свързани с международното сътрудничество при разследване на киберпрестъпления. Акцентът е поставен върху действащата нормативна база на международни организации и отделни държави, които имат голям опит и реализирана практика в тази сфера на борба с престъпността.

Ключови думи: *киберсигурност, киберпрестъпления, международни организации, разследване*

Abstract: The manuscript examines specific issues related to international cooperation in the investigation of cybercrime. Emphasis is placed on the current regulatory framework of international organizations and individual countries that have extensive experience and practice in this area in the fight against crime.

Key words: *cybersecurity, cybercrime, international organizations, investigation*

Doi: <https://doi.org/10.36997/PPDD2022.70>

Въведение

Успехът на международното сътрудничество при разследване на киберпрестъпления зависи от съществуването на унифицирани национални материални закони за киберпрестъпления, които да ги криминализират, и национални процесуални закони, които да установяват правила за тяхното доказване и за провеждане на наказателно производство.

Изложение

Международното сътрудничество може да се подобри чрез подписване на двустранни, регионални и многостранни договори за борба с киберпрестъпленията, при условие че тези деяния са двойно инкриминирани (т.е. да има клауза в договорите, съгласно която деянията трябва да се считат за незаконни в сътрудническите си държави). При липсата на двойно инкриминиране и хармонизирано законодателство се създават „убежища“ за киберпрестъпници, където те не могат да бъдат преследвани. Такъв например е случаят със създателя и разпространителя на компютърния вирус „Love bug“ през 2000 г., който не може да бъде съден, тъй като към момента на извършване, действията му не се считат за престъпление в страната му на пребиваване (Филипините).

Съществуват и изключения от изискването за двойна наказуемост. Така например чл. 29, §3 от Конвенцията на Съвета на Европа за компютърни престъпления от 2001 г. не изисква съответното деяние да бъде двойно инкриминирано, когато има нужда от своевременно осигуряване на компютърни данни, *„съхранявани в компютърна система, намираща се на територията на тази друга страна, и по повод на които молящата страна има намерение да изпрати молба за взаимопомощ за извършване на претърсване или за достъп по сходен начин, за изземване или за получаване по подобен начин или за разкриване на посочените по-горе данни“*¹.

В областта на международното сътрудничество за противодействие на престъпленията в кибернетичното пространство страните по Конвенцията са обвързани от система права и задължения, уредени в Дял III от Глава I и в Глава II на Конвенцията. Пряко отношение към темата обезпечаване на доказателства и имущество имат правилата относно взаимната правна помощ. Следва да се отбележи обаче, че още с представянето на общите принципи на международно сътрудничество (чл. 23 и чл. 25 от Конвенцията), страните по нея са приели да се подпомагат във възможно най-широка степен. Прието е това да

¹ Конвенция за престъпленията в кибернетичното пространство, приета на 109-ото заседание на Комитета на министрите на Съвета на Европа и открита за подписване в Будапеща на 23 ноември 2001 г. Ратифицирана със закон, приет от 39-тото НС на 1.04.2005 г. – ДВ, бр. 29 от 5.04.2005 г. Издадена от Министерството на правосъдието, обн. ДВ, бр. 76 от 15.09.2006 г., в сила за Република България от 1.08.2005 г.

се случва на основата на всички приложими международни актове и реципрочни институти от вътрешното им право с цел провеждане на разследване на престъпленията, свързани с компютърните системи, и с цел събиране на доказателства в електронна форма.

По-конкретно въпросите с обезпечаването на доказателства са разгледани в специалните разпоредби на Глава II от Конвенцията, които уреждат процедури относно:

а) Взаимната помощ при изпълнението на временни мерки. Такава мярка се явява изпращането и изпълнението на молби за бързо запазване на данни, съхранявани в компютърна система на територията на замолената страна, за които молещата държава има намерение да изпрати молба за достъп, претърсване и изземване по линия на международната правна помощ. Молбите за запазване имат превантивен характер и основанията да бъде отказано изпълнението им са силно ограничени – при опасност от накърняване суверенитета, сигурността или други важни интереси на замолената държава, при основания да се счита, че разследването се води за политическо престъпление. Двойното инкриминиране на деянието не е задължително условие, за да реагира на молба за запазване. Част от запазените данни относно трафика подлежат и на бързо разкриване, ако замолената страна установи, че в предаването на съобщение е участвал доставчик на услуги от трета страна. Тогава тя разкрива на молещата страна тази информация, за да бъдат идентифицирани доставчикът и пътят на съобщението.

б) Взаимната помощ относно правомощията за разследване. По отношение осигуряване достъпа до съхраняваните данни, наред със стандартния механизъм за изпълнение на молба за правна помощ, Конвенцията предвижда молбата за претърсването, изземването или осигуряването по друг сходен начин на достъп до данните, съхранявани в компютърна информационна система, да се удовлетворява по най-бърз начин, когато:

- има основание да се смята, че данните са изложени на сериозна опасност от изгубване или изменение;

- приложими актове, споразумение или законодателни разпоредби от националното право изрично предвиждат бързо сътрудничество.

В допълнение към изискването за двойна наказуемост друго съществено изискване за международно сътрудничество е спазване-

то на международните задължения в областта на правата на човека. Молба за международна помощ може да бъде отхвърлена, ако в резултат на удовлетворяването на молбата замолената държава наруши своите международни задължения за правата на човека (UNODC 2013: 229).

Официалните механизми за международно сътрудничество включват двустранни, регионални и многостранни договори в областта на борбата с киберпрестъпността. Въпросите за сътрудничество заемат видно място в тези договори. Например Споразумението от 2001 г. за сътрудничество между държавите – членки на Общността на независимите държави, в борбата с престъпленията в областта на компютърната информация съдържа няколко разпоредби за международно сътрудничество (чл. 5-7), които изброяват формите на сътрудничество, обхванати от това споразумение (а именно: обмен на информация; предоставяне на правна помощ в съответствие с международните инструменти; предотвратяване, разкриване, пресичане и разследване на престъпления в областта на компютърната информация и др.), както и начините, по които държавите членки могат да поискат съдействие и насоки за държавите членки относно изпълнението на исканията. Чл. 8 от това споразумение определя обстоятелствата, при които искането за помощ може да бъде отказано (а именно – когато изпълнението на молбата противоречи на националното законодателство на замолената държава), както и изискването държавата да откаже да изпълни изискванията на искането и е длъжна да уведоми молящата държава писмено за отказ, като посочи причините за отказа².

Освен това чл. 32 и 34 от Конвенцията на Арабската лига за престъпленията в областта на информационните технологии от 2010 г. съдържат разпоредби относно взаимната помощ, процедурите за сътрудничество и исканията за взаимна помощ³. Също така чл. 28 от Конвенцията на Африканския съюз за киберсигурност и защита на личните данни от 2014 г. включва разпоредби относно хармонизацията, взаимната правна помощ по дела, свързани с киберпрестъпленията и обмена на информация. В разпоредбите за споделяне на инфор-

² Commonwealth of Independent States. Agreement on Cooperation in Combating Offences related to Computer Information, Date of Adoption: June 1, 2001.

³ League of Arab States. Arab Convention on Combating Information Technology Offences. Date of Adoption: December 12, 2010.

мация се призовава държавите да създадат институции, които могат да улеснят споделянето на информация за заплахи и уязвимости за киберсигурността, като екипи за реагиране при киберинциденти (CERT) или екипи за реагиране при инциденти с киберсигурността (CSIRT). Чл. 28, §4 изисква държавите да *„използват съществуващите механизми за международно сътрудничество“*, които могат да включват *„международни, междуправителствени, регионални или... публично-частни партньорства“*, за да реагират на киберпрестъпленията⁴.

Договорите за взаимна правна помощ и екстрадиция са другите механизми, които насърчават международното сътрудничество при разследване на киберпрестъпления и наказателно преследване на киберпрестъпниците. Договорите за взаимна правна помощ представляват споразумения между държавите, които се прилагат за престъпления, изброени в тях, и определят видовете помощ, която всяка страна предоставя при разследвания (Maras 2016: 78). Подходът, основан на списък с престъпления, е много остарял и не отчита еволюиращия характер на киберпрестъпността. Предвид променящия се характер на престъпленията (вкл. и киберпрестъпленията) в някои договори за взаимна правна помощ, вместо да предоставят списъци с престъпления, държавите решават да си сътрудничат в разследването и наказателното преследване на всички престъпления, считани за такива съгласно националното им законодателство, с някои изключения.

Молбите за взаимна правна помощ могат да бъдат отхвърлени, ако например искането *„се отнася за престъпление, считано от замолената страна за политическо престъпление или престъпление, свързано с политическо престъпление“* (чл. 25, §4 от Конвенцията за престъпленията в кибернетичното пространство)⁵. Искането за данни може също да бъде отказано, ако изпълнението на искането или разкриването на данни би довело до нарушаване на международните задължения по правата на човека от запитаната държава (UNODC 2013: 228).

4 African Union Convention on Cyber Security and Personal Data Protection, Date of Adoption: June 27, 2014.

5 Конвенция за престъпленията в кибернетичното пространство, приета на 109-ото заседание на Комитета на министрите на Съвета на Европа и открита за подписване в Будапеща на 23 ноември 2001 г. Ратифицирана със закон, приет от 39-тото НС на 1.04.2005 г. – ДВ, бр. 29 от 5.04.2005 г. Издадена от Министерството на правосъдието, обн. ДВ, бр. 76 от 15.09.2006 г., в сила за Република България от 1.08.2005 г.

Някои държави, като Бразилия, Япония и Украйна, предоставят взаимна правна помощ, ако молещата държава гарантира реципрочност, т.е. ако подобно искане от замолената държава бъде удовлетворено от молещата държава в бъдеще. Освен това Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство от 2001 г. действа като договор за взаимна правна помощ за държави, които нямат такова споразумение с молещата държава. При липса на договори и споразумения, писма за искане (т.е. писмени искания от национални съдилища, които включват информация за случая, описание на изискваните доказателства, с указание защо са необходими и обещание за спазване на принципа на реципрочност в бъдеще) може също да се използват за получаване на помощ при случаи на киберпрестъпления (Bell 2007).

Значителни закъснения във времето, обикновено от около няколко месеца, възникват и при използване на други официални механизми за сътрудничество, например механизми за екстрадиция (UNODC 2013, р. 230). Такива закъснения са много проблематични предвид нестабилността на цифровите доказателства.

Европейската заповед за арест предоставя възможност за задържане на извършители на престъпления, свързани с използването на компютър, които са *„наказуеми в издаващата държава с наказание или мярка за неотклонение „лишаване от свобода“ с горна граница от най-малко три години... без проверка за двойната наказуемост на деянието“* (чл. 2, §2 от Рамковото решение на Съвета на Европейския съюз 2002/584/ПВР от 13 юни 2002 г. относно Европейската заповед за арест и относно процедурите за прехвърляне на лица между държави членки) са изявления, направени от някои държави членки във връзка с приемането на рамковото решение⁶.

Наличието на договор за екстрадиция не гарантира, че дадено лице ще бъде екстрадирано в молещата държава. Това се наблюдава в случая с Лаури Лав – британски хакер, чиято екстрадиция е отказана от САЩ, въпреки съществуването на договор за екстрадиция, подписан през 2003 г. между Обединеното кралство и САЩ (Parkin 2017).

Освен това договорите за екстрадиция включват условия, при които не се извършва такава. Например съгласно Междумерикан-

⁶ Рамково решение на Съвета от 13 юни 2002 г. относно европейската заповед за арест и процедурите за предаване между държавите членки (2002/584/ПВР).

ската конвенция на американските държави за екстрадиция „исканията за екстрадиция се отхвърлят, когато наказанието за престъплението е доживотен затвор или смъртно наказание“ (чл. 9)⁷. Екстрадиция ще бъде отказана и в случаите, когато лицето, което трябва да бъде екстрадирано, е подложено на нечовешко или унижително отношение или наказание⁸. Исканията за екстрадиция могат да бъдат отхвърлени и по други причини, като липса на достатъчно доказателства за оправдаване на екстрадицията, когато искането включва престъпление, което не подлежи на екстрадиция, или когато се иска екстрадиция на лице, което е гражданин на замолената държава. По отношение на екстрадицията на граждани на замолените държави принципът за неекстрадиция на собствените граждани е залегнал в конституциите на някои държави, като например Бразилия и Алжир, както и в регионални и международни договори. Независимо от този принцип международното публично право налага правно задължение на държавите да екстрадират или преследват *aut dedere aut judicare*⁹ извършители на тежки международни престъпления.

Заклучение

Ефективността на международното сътрудничество, при разследване на киберпрестъпления, зависи от способността на държавите да изпълняват искания за предоставяне на цифрови доказателства по начин, който гарантира, че те ще бъдат годни в съда. Това изисква наличието на квалифицирани експерти по разкриване на киберпрестъпления, които могат да извличат цифрови доказателства в съответствие с националните наказателно-процесуални закони. Към момента съществува дефицит на достатъчно такива специалисти. Освен това на държавите липсва национален капацитет, необходим за борба с киберпрестъпността. Тази липса е налице в резултат от комплекс от различни фактори с негативен характер, сред които можем да отворим следните:

На първо място, в голям брой държави няма достатъчно квалифицирани специалисти за провеждане на разследвания на киберпре-

⁷ Inter-American Convention on Extradition. OAS, 1981, Entry into force: March 28, 1992.

⁸ Ibid.

⁹ Да се екстрадира или преследва наказателно (бел. авт.).

стъпления, както и за наказателно преследване на киберпрестъпници и разглеждане на искания за съдействие чрез международно сътрудничество по дела, свързани с киберпрестъпления.

На второ място, на национално ниво липсват финансови ресурси, необходими за набиране и задържане на квалифициран персонал, както и за осигуряване на редовно и актуално обучение за разследващи киберпрестъпления и други специалисти.

На трето място, държавите нямат необходимите финансови средства за анализ на цифрови доказателства, както и за закупуване на необходимото цифрово криминалистично оборудване за качествено провеждане на разследвания на киберпрестъпления.

Използвана литература

1. Bell, A. Investigating International Cybercrimes. // Police Chief Magazine, 2007, Vol. 74, №3.
2. Maras, M.-H. Cybercriminology. Oxford University Press, 2016, p. 78.
3. Parkin, S. Keyboard warrior: the British hacker fighting for his life. // The Guardian, №8, September 2017.
4. UNODC. Draft Comprehensive Study on Cybercrime, 2013, p. 228-230.

За контакти:

Драгомир Кръстев

Докторант в Института за държавата и правото
към Българска академия на науките

E-mail: drago.krastev@gmail.com