ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 13.9.2017 г.
COM(2017) 474 final

ДОКЛАД НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

с оценка на степента, в която държавите членки са взели необходимите мерки, за да се съобразят с Директива 2013/40/ЕС относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета

Съдържание

1. Въведение

Според оценката на Европол за 2016 г. на заплахата от организирана престъпност, ползваща се от интернет (IOCTA), киберпрестъпността става все по-агресивна и търсеща конфронтация. Това е видно от различните проявления на киберпрестъпността, в това число атаки срещу информационни системи[1]. Някои от посочените от Европол тежки форми на атаки са използването на злонамерен софтуер и социално инженерство с цел инфилтриране и придобиване на контрол върху информационна система или прихващане на съобщения и провеждането на мащабни атаки срещу мрежи, в това число от критичната инфраструктура. Тези атаки се определят като ключови заплахи за обществото ни.

Поради по-голямото количество информация, което се съхранява в облак, и интензивната мобилност на информацията и правонарушителите трансграничното сътрудничество между правоприлагащите органи е придобило жизненоважно значение за повечето разследвания на киберпрестъпления.

За да се борят ефективно с тези престъпления, държавите членки трябва да определят заедно кои деяния следва да се считат за атаки срещу информационни системи. Освен това те трябва да имат приблизително еднакъв размер на санкциите и да разполагат с оперативните средства за съобщаване за престъпления и обмен на информация между органите. По тази причина на 12 август 2013 г. Съветът и Европейският парламент приеха Директива 2013/40/ЕС (наричана по-нататък „директивата“) относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета[2].

1.1. Цели и обхват на директивата

Целите на директивата са да се сближи наказателното право на държавите членки[3] в сферата на атаките срещу информационните системи и да се подобри сътрудничеството между компетентните органи. Това се постига чрез установяване на минимални правила за определянето на престъпленията и наказанията в областта на атаките срещу информационните системи и налагане на задължение за наличие на оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата.

В директивата се дават **определения** на следните относими термини:

- „Информационна система“ в член 2, буква а)[4]. Определението е близко до това на понятието „компютърна система“ в член 1, буква а) от Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство от

[1] Европол, оценка за 2016 г. на заплахата от организирана престъпност, ползваща се от интернет (IOCTA), на разположение на адрес https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:bg:pdf.

[3] Оттук нататък в текста, освен ако не е посочено друго, „държавите членки“ или „всички държави членки“ означава обвързаните от директивата държави членки, т.е. всички освен Дания, която не участва в приемането на директивата в съответствие с членове 1 и 2 от Протокола относно позицията на Дания, приложен към Договора за Европейския съюз и Договора за функционирането на Европейския съюз (ДФЕС). В съответствие с член 3 от Протокол 21 относно позицията на Обединеното кралство и Ирландия и двете държави участват в приемането на директивата и са обвързани от нея.

[4] Всички членове, на които се прави позоваване, са част от директивата, освен ако не е посочено друго.

23 ноември 2001 г. (наричана по-нататък „Конвенцията от Будапеща“) с разликата, че в директивата се обхващат изрично и компютърните данни.

- „Компютърни данни“ в член 2, буква б). Определението е съгласувано с това в член 1, буква б) от Конвенцията от Будапеща, като вместо „компютърна система“ е използвано понятието „информационна система“.
- „Юридическо лице“ в член 2, буква в). Определението има за цел да се гарантира, че наказателна отговорност носят както физическите, така и юридическите лица, като изключва държавите, публичните органи и публичните международни организации.
- „Неправомерно“ поведение в член 2, буква г). Определението е свързано с общ принцип на наказателното право и има за цел да се избегне наказателна отговорност на лица, които действат съгласно това, което е позволено по силата на националното право, или с разрешение от собственика или от друг притежател на права върху информационната система или част от нея.

Дефинирани са и следните **конкретни престъпления:**

- незаконният достъп до информационни системи като такъв (член 3);
- незаконна намеса в система (член 4), което включва всеки незаконен достъп до информационна система, който причинява сериозно възпрепятстване или спиране на функционирането ѝ;
- незаконна намеса в данни (член 5), което означава всяка неправомерна намеса в компютърни данни, която уврежда целостта или достъпността им;
- незаконно прихващане (член 6) на изпращани непублични компютърни данни и електромагнитните емисии от информационна система, пренасящи такива данни;
- незаконно предоставяне на инструменти, използвани за извършване на посочените престъпления (член 7). В тази връзка такива инструменти биха могли да са компютърна програма, компютърна парола или други данни, с чиято помощ може да се получи достъп до информационна система.

В допълнение към това директивата **предвижда наказателна отговорност** и при подбудителство, помагачество и опит от страна на физически и/или юридически лица за извършване на някое от гореизброените престъпления (член 8). Подбудителството и помагачеството са обвързани с престъпленията по членове 3—7, а опитът за извършване се отнася само до членове 4 и 5.

Минималният размер на максималните **наказания** за посочените в директивата престъпления е предвиден в член 9:

- Като основа за всички престъпления освен посочените в член 8 се предвижда максимално наказание лишаване от свобода не по-малко от две години (член 9, параграф 2).
- Лишаване от свобода с максимален срок не по-малко от три години се предвижда за престъпленията, посочени в членове 4 и 5, когато са били засегнати значителен брой информационни системи (по принцип това са престъпленията с използване на така наречените „ботнети“; член 9, параграф 3).
- Лишаване от свобода с максимален срок не по-малко от пет години се предвижда за престъпленията, посочени в членове 4 и 5, когато са извършени от престъпна организация (член 9, параграф 4, буква а), причинили са сериозни

вреди (член 9, параграф 4, буква б) или са извършени срещу информационна система, която е част от критична инфраструктура (член 9, параграф 4, буква в).
- Когато престъпленията, посочени в членове 4 и 5, са извършени чрез злоупотреба с лични данни на друго лице, държавите членки следва да гарантират, че това може да се разглежда като квалифициращо обстоятелство, освен ако тези обстоятелства не са вече част от друго престъпление (член 9, параграф 5).

В по-нататъшните членове се определят минималните условия за ангажиране на **отговорността на юридическите лица** (член 10) и се предоставя примерен списък с възможните санкции спрямо тях (член 11).

Признава се, че горепосочените престъпления могат да бъдат извършени (в смисъл „осъществени“) на място, където извършителят осъществява самото деяние, докато ефектът му върху атакуваната информационна система може да се прояви на друго място, поради което в член 12 се предвиждат задължения за установяване на **компетентността**, като се прави разграничение между:

- мястото, където извършителят се намира физически, когато осъществява деянието;
- местоположението на атакуваната информационна система;
- гражданството на извършителя;
- неговото обичайно местопребиваване; и
- мястото, където е установено юридическо лице, в чиято полза е извършено престъплението.

По отношение на обмена на информация в член 13, параграф 1 се предвижда задължение за държавите членки да осигурят наличието на оперативни национални **звена за контакт**, които са на разположение 24 часа в денонощието и седем дни в седмицата, за да са в състояние да отговорят на спешно искане от друга държава в рамките на осем часа.

Освен това държавите членки трябва да предприемат необходимите мерки за **улесняване на докладването** на компетентните национални органи за горепосочените престъпления (член 13, параграф 3) и за събиране и споделяне на минимум от **статистически данни** относно тези престъпления (член 14).

1.2 Цел и методология на доклада

В член 16 от директивата от държавите членки се изисква до 4 септември 2015 г. да въведат в сила законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с директивата, и да ги съобщят на Комисията.

С настоящия доклад се изпълнява изискването съгласно член 17 от директивата Комисията да докладва на Европейския парламент и на Съвета, като оценява степента, в която държавите членки са предприели необходимите мерки, за да се съобразят с директивата. В тази връзка докладът има за цел да предостави кратък, но информативен преглед на основните мерки за транспониране, предприети от държавите членки.

Транспонирането от държавите членки включи събиране на информация за съответното законодателство и административни мерки, анализ на информацията, изготвяне на ново законодателство или в повечето случаи изменение на съществуващите актове, процеса до приемането им и накрая докладването им към Комисията.

До крайния срок за транспониране 22 държави членки са уведомили Комисията, че са завършили изцяло транспонирането на директивата. През ноември 2015 г. Комисията откри производства за установяване на неизпълнение на задължения за непредоставяне на информация относно националните мерки за транспониране спрямо останалите пет държави членки: BE, BG, EL, IE и SI[5]. Към 31 май 2017 г. все още бяха в ход производствата за установяване на неизпълнение на задължения за непредоставяне на информация относно националните мерки за транспониране спрямо BE, BG и IE[6].

Описанието и анализът в настоящия доклад се основават на предоставената от държавите членки информация към 31 май 2017 г.[7] Нотификациите, получени след тази дата, не са взети предвид. Всички нотифицирани мерки, позоваващи се на национално законодателство, бяха взети под внимание, както и съдебни решения и по целесъобразност общата правна теория. Освен това в хода на анализа Комисията се свърза пряко с държавите членки по необходимост и целесъобразност, за да получи допълнителна информация или пояснения. Цялата събрана информация е взета под внимание в анализа.

Освен установените в настоящия доклад проблеми може да има допълнителни предизвикателства при транспонирането и други разпоредби, които не са докладвани на Комисията, или възникнали впоследствие законодателни и незаконодателни развития. Следователно настоящият доклад не пречи на Комисията допълнително да оцени някои разпоредби и да продължи да подкрепя държавите членки при транспонирането и прилагането на директивата.

2. Мерки за транспониране

2.1 Законови определения (член 2 от директивата)

В член 2 от директивата се дават законови определения на понятията „информационна система“ (буква а), „компютърни данни“ (буква б), „юридическо лице“ (буква в) и „неправомерно“ поведение (буква г). Единствено CY и UK (Гибралтар) са въвели законодателство, което обхваща всички аспекти на горепосочените определения. В по-големи подробности това означава следното:

а) Информационна система

Определението в директивата се основава на определението на понятието „компютърна система“ в член 1, буква а) от Конвенцията от Будапеща, като добавя самите компютърни данни като част от информационната система. CY, EL, IE, FI, HR, MT, PT и UK (Гибралтар) са въвели законови разпоредби, съдържащи определението за

[5] В настоящия документ държавите членки са посочени със съкращения в съответствие със списъка на адрес: http://publications.europa.eu/code/bg/bg-5000600.htm.

[6] Информация за решенията на Комисията относно производствата за установяване на неизпълнение на задължения е налична на адрес http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=bg.

[7] IE съобщи за пълното транспониране на директивата на 31 май 2017 г.

информационна система, а предоставената от DE, ES, FR, LU, LV, PL, SE и SK информация не беше изчерпателна. При останалите държави членки, т.е. AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI и UK (с изключение на Гибралтар), съответните законови определения не съдържат изрично понятието „компютърни данни“. Това предполага позоваване на член 1, буква а) от Конвенцията от Будапеща и идентичен обхват с този на определението за „компютърна система“.

б) Компютърни данни
Понятието „компютърни данни“ е предвидено в законодателството на AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO и UK (Гибралтар), а предоставената от ES, FR, IT, LU, LV, PL, SE, SK и UK (с изключение на Гибралтар) информация не беше изчерпателна. В случая на SE обаче специфичната организация на позоваващите се членове правят това определение излишно. По отношение на останалите държави членки HU обвързва определението на „компютърни данни“ единствено с престъпленията по членове 4 и 5 от директивата, докато BE и SI пропускат да включат в определението на „компютърни данни“ частта „програма, която е в състояние да направи така, че дадена информационна система да изпълни определена функция“.

в) Юридическо лице
С изключение на LU, който не предостави изчерпателна информация относно транспонирането на член 2, буква в), транспонирането на определението на „юридическо лице“ не предизвика никакви проблеми. Причината е, че по принцип то вече присъства най-вече в разпоредбите на гражданското или търговското право на държавите членки. Единствено CY въвежда конкретна разпоредба в рамките на мерките, приети за транспониране на директивата.

г) Неправомерно поведение
По отношение на определението на понятието „неправомерно“ поведение в член 2, буква г) единствено CY, IE, RO и UK (Гибралтар) съобщиха за транспониране, което означава, че в останалите 23 държави членки няма никакви мерки за транспониране на това определение. Трябва да се отбележи обаче, че във всички държави членки съществува общият принцип, че наказателна отговорност не се носи за действия, когато за извършването им са налице съответните права.

2.2 Конкретни престъпления (членове 3—7 от директивата)

а) Незаконен достъп до информационни системи
Във връзка с незаконния достъп до информационни системи член 3 от директивата е транспониран в националното законодателство на AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE и SK.

Във всички останали държави членки, т.е. BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI и UK, в съответното национално описание на престъплението не се прави разлика между придобиването на достъп до цялата информационна система, от една страна, и до част от нея, от друга, макар това да е предвидено изрично в директивата. Освен това при транспонирането в DE не се обхваща достъпът до компютърен хардуер сам по себе си, в AT и LU са предвидени допълнителни изисквания относно конкретен умисъл (умисъл за придобиване на информация, причиняване на загуба или умисъл за измама), а в LV — относно причиняването на съществена вреда. В BE, BG, FR, HR, LU, MT, PT, RO, SI и UK обхватът на националните разпоредби е по-широк от този в директивата, тъй като за да се установи наказателна отговорност в тях, не е нужно да е налице заобикаляне на каквито и да е мерки за сигурност. Останалите държави членки се

позовават буквално на престъпление, извършено чрез нарушаване на мярка за сигурност (CY, EL и SK), или използват сходна терминология, за да опишат този аспект (AT, CZ, DE, EE, ES, FI, HU, IT, LT, LV, NL, PL и SE).

б) Незаконна намеса в система

Член 4 от директивата се отнася за незаконната намеса в система. В директивата се изброяват осем възможни деяния (въвеждане на компютърни данни, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или спиране на достъпа до такива данни) и две възможни последици от тях (сериозно възпрепятстване или спиране на функционирането на информационна система). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE и UK (с изключение на Гибралтар) са въвели съответни законодателни мерки. BG включва единствено въвеждането на вирус, а останалите държави членки (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK и UK) не посочват изрично от едно до четири от възможните деяния. В тази връзка може да се отбележи, че повечето проблеми възникнаха по отношение на понятията „влошаване“ (отсъства в осем случая) и „спиране на достъпа“ (отсъства в девет случая).

в) Незаконна намеса в данни

В член 5 от директивата се разглежда незаконната намеса в данни и се изброяват следните шест възможни деяния: изтриване, увреждане, влошаване, променяне, скриване или спиране на достъпа до данни. CY, EL, IE и MT са транспонирали разпоредбата буквално; BE, CZ, LT, PT и SE са използвали по-общи термини, за да обхванат всички възможни деяния. Мерките за транспониране във всички останали държави членки не обхващат всяка от възможностите, а по-скоро се позовават на пет от тях (FI и SK) или по-малко (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI и UK). Повечето проблеми възникнаха по отношение на понятията „увреждане“ (отсъства в осем случая), „влошаване“ (13 случая), „скриване на данни“ (11 случая) и „спиране на достъпа до данни“ (13 случая). В допълнение към текста на директивата във FI се изисква наличието на „умисъл за причиняване на вреда или финансова загуба“, а в LT и LV — „деянието да е нанесло голяма щета или съществена вреда“, за да се ангажира наказателна отговорност.

г) Незаконно прихващане

В член 6 се разглежда незаконното прихващане и се обхващат изпращането на непублични компютърни данни и електромагнитните емисии от информационна система, пренасящи такива компютърни данни. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK и UK (Гибралтар) са въвели законодателство, което изцяло транспонира член 6. В някои държави членки общият обхват на директивата във връзка с прихващането на компютърни данни е ограничен до съобщения (AT и BG), наблюдение на лице (EE) или кореспонденция (FR и HU). Освен това мерките за транспониране на следните държави членки не включват прихващането на електромагнитни емисии: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI и UK (с изключение на Гибралтар). Освен това в някои държави членки се изисква конкретен умисъл (като придобиване на информация или икономическа изгода или причиняване на загуба — вж. AT, EL, HU) или конкретни допълнителни действия (като записване на прихванатото съдържание или узнаване за него — вж. BG и HU).

д) Инструменти, използвани за извършване на престъпления

В член 7 се криминализират няколко деяния, свързани с инструменти като компютърни програми или кодове за достъп, които се използват за извършване на престъпленията по членове 3—6: производство, продажба, набавяне за употреба, внос,

разпространяване или друга форма на предоставяне на такива инструменти. AT, BE, CY, DE, EL, IE и SK са въвели съответно национално законодателство. Някои държави членки не обхващат всички посочени престъпления (EE, IT, MT, PL и SI). Някои не правят разграничение между извършителя на деянията по член 7 и извършителя на деянията по членове 3—6 (CZ и SI). Други изискват конкретен умисъл (увреждане или измама — вж. FI, IT и LU), конкретно следствие, като нарушаване на тайната (BG), или престъпленията да са най-малко на етап на подготовка (SE). Накрая, съществуват разминавания между член 7 и националните мерки, тай като не са транспонирани всички изброени възможни деяния. Случаят е такъв в BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI и UK. Сред тях в законодателството на LU изрично се споменават пет от шестте възможни деяния, изброени в директивата, докато останалите държави членки се позовават изрично на едва четири или на по-малко.

Единствено ES е транспонирала текста за „набавяне за употреба“.

2.3 Общи правила за разглежданите престъпления (членове 8—12 от директивата)

а) Подбудителство, помагачество

В член 8, параграф 1 от държавите членки се изисква да гарантират, че подбудителството или помагачеството за извършване на някое от престъпленията, посочени в членове 3—7, е наказуемо като престъпление. Всички държави членки са транспонирали тази разпоредба.

б) Опит за извършване на престъпление

Съгласно член 8, параграф 2 опитът за извършване на престъпление, посочено в членове 4 и 5, трябва да е наказуем като престъпление. Всички държави членки разполагат със законодателство, което транспонира тази разпоредба, освен PT, където не са обхванати всички видове опити за извършване на престъпленията по член 4, и SE, където не се търси наказателна отговорност за опит за извършване на престъплението „нарушаване на тайната на съобщенията“.

в) Наказания

аа) Обща разпоредба

В член 9, параграф 1 от държавите членки по принцип се изисква да осигурят ефективни, пропорционални и възпиращи наказания за престъпленията, обхванати от директивата. Макар да се предполага, че това е така във всички държави членки, в AT, BE, BG, IT, PT, SE и SI минималният размер на максималните наказания, посочен в член 9, параграф 2 (вж. точка 1.1 по-горе), не е спазен във всички случаи. Това засяга транспонирането на член 9, параграф 1, тъй като може да се изведе заключението, че минималните изисквания по член 9, параграф 2 са най-малкото, което трябва да бъде въведено, за да се допусне, че е налице ефективно, пропорционално и възпиращо наказание.

бб) Общ минимален размер на максималното наказание

Съгласно член 9, параграф 2 минималният размер на максималното наказание за стандартните престъпления, посочени в членове 3—7, е две години лишаване от свобода. Повечето държави членки спазват тази разпоредба. Само в шест държави членки се наблюдават известни разминавания: AT (шестмесечен максимален срок на лишаване от свобода), BG (максимум една година лишаване от свобода за всички престъпления с изключение на незаконното прихващане), IT (максимум една година лишаване от свобода за престъплението по член 7, буква б), PT (максимум една година

лишаване от свобода за престъплението по член 3), SE (максимум една година лишаване от свобода за престъплението „увреждане“) и SI (максимум една година лишаване от свобода за престъпленията по членове 3, 6 и 7). В случая на BE минималният размер на максималното наказание за престъпленията по членове 3, 6 и 7 се налага само когато те са извършени с намерение за измама.

вв) Значителен брой засегнати информационни системи

В член 9, параграф 3 минималният размер на максималното наказание се повишава на три години лишаване от свобода, когато значителен брой информационни системи са били засегнати от посочените в членове 4 и 5 престъпления. Като цяло държавите членки са въвели съответно законодателство; DE се позовава единствено на информационни системи, „които са от съществено значение за други“; FI изисква престъплението да бъде преценено „като едно цяло“, за да се приложи по-голямата продължителност на наказанието, а LV не се позовава на значителен брой информационни системи (или подобна формулировка), а единствено на причиняването на „съществена вреда“. Предоставената от BG и SI информация не беше изчерпателна.

гг) Престъпни организации

Съгласно член 9, параграф 4, буква а) престъпленията, посочени в членове 4 и 5, се наказват с лишаване от свобода с максимален срок не по-малко от пет години, когато са извършени от престъпна организация съгласно определението в Рамково решение 2008/841/ПВР.

И тук повечето държави членки спазват разпоредбата на член 9, параграф 4, буква а). В наказателното право на LU и SI разпоредбите за престъпления, извършени от престъпна организация, не обхващат киберпрестъпленията. В законодателството на BE се предвижда максимално наказание едва три години лишаване от свобода за престъпленията по член 5; в законодателството на DE не се обхващат физическите лица като жертви на престъпленията; в законодателството на FI се изисква допълнителна преценка на престъплението „като едно цяло“, а в законодателството на SE се предвижда максимално наказание четири години лишаване от свобода за „грубо нанасяне на вреда“.

дд) Причинени сериозни вреди

Съгласно член 9, параграф 4, буква б) престъпленията, посочени в членове 4 и 5, се наказват с лишаване от свобода с максимален срок не по-малко от пет години, когато са причинили сериозни вреди. Въпреки че не е налице определение за „сериозни вреди“, всички държави членки с изключение на BG, DE, FI, HU, LU и SE са въвели законодателство, което съответства на директивата. Предоставената от HU информация не беше изчерпателна. В BG не се достига минималният петгодишен размер на максималното наказание, а LU се позовава на обща наказателна разпоредба при причиняване на сериозна вреда, в която не се обхваща нито едно от киберпрестъпленията. Съществуват несъществени разминавания в DE (не са обхванати физическите лица като жертви на престъпленията), FI (за да се наложи по-голямо наказание, се изисква допълнителна преценка на престъплението „като едно цяло“) и SE (максимум четири години лишаване от свобода за „грубо нанасяне на вреда“).

ее) Информационни системи, които са част от критична инфраструктура

Ако престъпленията, посочени в членове 4 и 5, са били насочени към информационни системи, които са част от критична инфраструктура, това също води до лишаване от

свобода с максимален срок не по-малко от пет години, както е посочено в член 9, параграф 4, буква в).
Повечето държави членки спазват тази разпоредба, а BG не предостави конкретна информация за транспонирането. BE предвижда максимално наказание от три години за престъпленията по член 5. В DE жертвите, които са физически лица, не са обхванати. Във FI се изисква допълнителна преценка на престъплението „като едно цяло“, в IT се изисква действително да е причинено „разрушение“, в PT се изисква атаката да е била „тежка и продължителна“ и няма позоваване на член 5, а в SE се спазват изискванията на директивата само при престъплението „груб саботаж“.

жж) Кражба на самоличността и други престъпления, засягащи самоличността

В член 9, параграф 5 от държавите членки се изисква да гарантират, че когато престъпленията, посочени в членове 4 и 5, са извършени чрез злоупотреба с лични данни на друго лице, за да се спечели доверието на трето лице, и по този начин са нанесени вреди на законния собственик на самоличността, това може да се разглежда като квалифициращо обстоятелство, освен ако тези обстоятелства не са вече част от друго престъпление. Голямата свобода на преценка е довела до богато разнообразие от мерки за транспониране сред държавите членки. BE и EL не са съобщили за каквото и да е транспониране, а в наказателното законодателство на CZ няма конкретна разпоредба. Подходът на квалифициращото обстоятелство е възприет от AT, CY, ES, IE, MT, PT и SE (като в последната се посочва обстоятелството „специално предварително планиране“), а всички останали държави членки се позовават на допълнителни разпоредби за конкретното престъпление. Сред държавите, които се позовават на специални разпоредби, могат да се посочат следните проблеми при транспонирането: в BG и NL се изисква конкретен умисъл („за извличане на изгода“ и „за прикриване или злоупотреба със самоличността“); DE се позовава само на „лични данни, които не са общодостъпни“; FR се позовава само на името на лицето, без да се споменават други лични данни; в LV се изисква наличието на причинена „съществена вреда“; в RO се обхваща единствено използването на „документ“ и се изисква да е налице измама.

г) Отговорност на юридическите лица

аа) Обща отговорност

В член 10, параграф 1 се изисква юридическите лица да могат да бъдат подведени под отговорност за престъпленията, посочени в членове 3—8, ако извършителят има пълномощие да представлява юридическото лице (буква а), правомощие да взема решения от името на юридическото лице (буква б) или правомощие да упражнява контрол в рамките на юридическото лице (буква в). Всички държави членки са въвели законодателство в съответствие с този член, като се наблюдават единствено следните несъществени проблеми: в BG не е обхванато престъплението по член 6, а в HR няма позоваване относно извършителите, които имат правомощие да упражняват контрол в рамките на юридическото лице (член 10, параграф 1, буква в).

бб) За липса на надзор или контрол

В член 10, параграф 2 от държавите членки се изисква да гарантират, че юридическите лица могат да бъдат подведени под отговорност, когато липсата на надзор или контрол от страна на лице, посочено в член 10, параграф 1, е направила възможно извършването на някое от престъпленията, посочени в членове 3—8. Въпреки че почти всички държави членки спазват тази разпоредба, предоставената от LU информация не беше изчерпателна, а в BG няма позоваване на извършването на престъпление, попадащо в обхвата на член 6.

д) Санкции спрямо юридически лица

аа) Задължителни санкции

В член 11, параграф 1 от директивата от държавите членки се изисква да предвидят глоби по наказателното право или друг вид глоби, които да послужат като ефективни, пропорционални и възпиращи санкции за юридическите лица. Всички държави членки освен IE и UK са нотифицирали отговарящи на директивата национални мерки. В тези две държави максималният размер на възможните глоби остава неопределен поради липсата на конкретни законови разпоредби. Поради тази причина не е възможно да се прецени дали съответните глоби са ефективни, пропорционални и възпиращи.

бб) Избираеми санкции

Член 11, параграф 1 продължава със списък на възможните варианти на допълнителни санкции спрямо юридическите лица. Те са: лишаване от правото на ползване на публични облаги или помощи (този вариант е избран от CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT и SK), временно или постоянно лишаване от правото на упражняване на търговска дейност (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI и SK), поставяне под съдебен надзор (CY, ES, FR, MT, PT и RO), съдебна ликвидация (CY, CZ, EL, ES, FR, HR, HU,LT, LU, LV, MT, PT, RO, SI и SK) и временно или постоянно затваряне на структури, използвани за извършване на престъплението (BE, CY, WS, FR, LT, MT, PT и RO). Това означава, че BG, DE, EE, IE, FI, NL и UK не са избрали нито един от възможните варианти.

вв) Санкции за бездействие

Съгласно член 11, параграф 2 държавите членки трябва да гарантират, че юридическите лица, подведени под отговорност за бездействие по член 10, параграф 2, подлежат на ефективни, пропорционални и възпиращи санкции. Предоставената от LU информация не беше изчерпателна. Всички останали държави членки с изключение на IE и UK са предвидили съответни законови разпоредби. В този случай при IE и UK възниква същият проблем като в член 11, параграф 1: (вж. буква аа) по-горе).

е) Компетентност

аа) Задължителни основания за компетентност

В член 12, параграфи 1 и 2 от директивата от държавите членки се изисква да определят собствената си компетентност по отношение на престъпленията, посочени в членове 3—8, когато престъплението е извършено изцяло или отчасти на тяхната територия, било то поради факта, че извършителят се е намирал физически на тяхната територия, когато е извършено престъплението, или поради това, че засегнатата информационна система се е намирала на тяхна територия, или когато престъплението е извършено в чужбина от техен гражданин. Повечето държави членки са въвели съответно национално законодателство; в законодателството на IT не се определя компетентност за основните престъпления, извършени от техни граждани в чужбина; в законодателството на LV и SI се прави позоваване на неясни разпоредби относно териториалните аспекти; компетентността на MT при извършване на престъпление отчасти на нейна територия е неясна, а UK се позовава на компютърна, а не на информационна система.

бб) Други основания за компетентност

В член 12, параграф 3 се предвижда, че когато държавите членки установяват компетентност в случаите, в които извършителят има обичайно местопребиваване на съответната им територия (този вариант е избран от AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE и SK) или престъплението е извършено в полза на юридическо лице, установено

на съответната им територия (CY, CZ, LV, PT, RO и SK), това трябва да бъде съобщено на Комисията.

2.4 Оперативни въпроси (членове 13—14 от директивата)

а) Осигуряване на оперативни национални звена за контакт
В член 13, параграф 1 държавите членки се призовават да създадат оперативни национални звена за контакт за целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8. По силата на същата разпоредба държавите членки трябва да гарантират, че разполагат с процедури, чрез които в случай на спешно искане за съдействие компетентният орган ще бъде в състояние да отговори в рамките на осем часа от получаването му. Съгласно нотифицираната информация повечето държави членки са създали необходимата инфраструктура. IE и RO са отбелязали, че съответните им звена за контакт са на разположение ограничен брой часове всеки ден, което не би дало възможност на органа да реагира в рамките на осем часа от получаването на искане във всеки отделен случай. Няколко държави членки са посочили, че използват съществуващи мрежи от оперативни звена за контакт, създадени чрез мрежата на Г7 или по силата на подписаната в Будапеща Конвенция на Съвета на Европа за престъпления в кибернетичното пространство.

б) Информация относно създадените оперативни национални звена за контакт
Съгласно член 13, параграф 2 държавите членки трябва да предоставят координатите за връзка на звената си за контакт на Комисията, която на свой ред ги съобщава на останалите държави членки. Всички държави членки са предоставили необходимата информация.

в) Канали за докладване
В член 13, параграф 3 от държавите членки се изисква да гарантират наличието на подходящи канали за докладване с цел да се улесни докладването на компетентните национални органи за престъпления, посочени в членове 3—6. Предоставената от HR, IT, IE и PT информация не беше изчерпателна. Сред останалите държави членки, изглежда, има различни подходи към прилагането на изискването за канали за докладване. Повечето държави членки (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK и UK) са нотифицирали мерки, предвиждащи канали за докладване, които улесняват докладването от страна на лицето или организацията, подаващи първоначално информацията за престъпление, например жертвата на кибератака (като в LV действителният канал за докладване остава неясен). Други държави членки обаче (AT, ES и LU) са предоставили идентична информация във връзка с прилагането на член 13, параграфи 1 и 2, от което изглежда, че мерките им ще улесняват основно общуването между органите.

г) Събиране на статистически данни
Съгласно член 14, параграфи 1 и 2 държавите членки трябва да гарантират наличието на система за записване, производство и предоставяне на статистически данни като минимум относно броя на посочените в членове 3—7 престъпления, които са регистрирани от държавите членки, и броя на лицата, срещу които е възбудено наказателно преследване и които са осъдени за такива престъпления. Въз основа на постъпилите нотификации повечето държави членки, изглежда, са въвели както законодателни, така и административни мерки, за да гарантират събиране на информацията въз основа обикновено на обща национална електронна система. Информацията от няколко държави членки не беше изчерпателна (EL, IE, UK (Гибралтар, Северна Ирландия и Шотландия). Една от причините бе, че информацията

относно конкретни престъпления, посочени в директивата, не може да се събира отделно (BE, DE и SE) или събираната информация не може да обхване всички престъпления, посочени в директивата (RO).

д) Предаване на статистическите данни на Комисията
В член 14, параграф 3 държавите членки са призовани да предават съответните статистически данни на Комисията. Всички държави членки, които са нотифицирали мерки, с изключение на UK (Гибралтар, Северна Ирландия и Шотландия) и HU, са потвърдили въвеждането на правни или административни мерки или и двете с цел осигуряване на съответствие с това задължение. Информацията за EL, ES, LU и SI не беше изчерпателна.

3. Заключение и следващи стъпки
Директивата доведе до същински напредък при криминализирането на кибератаките на сравнимо равнище във всички държави членки, което улеснява трансграничното сътрудничество между правоприлагащите органи, разследващи този вид престъпления. Държавите членки са изменили наказателните си кодекси и друго относимо законодателство, рационализирали са процедурите си и са създали или подобрили схемите за сътрудничество. Комисията отдава дължимото на големите усилия от страна на държавите членки за транспониране на директивата.

Въпреки това все още може да се направи много с цел реализиране на пълния потенциал на директивата, ако държавите членки приложат изцяло всичките ѝ разпоредби. До момента анализът подсказва, че някои от основните подобрения, които могат да бъдат осъществени от държавите членки, включват използването на определенията (член 2), което оказва въздействие върху обхвата на престъпленията, дефинирани в националното право въз основа на директивата. Освен това изглежда, че за държавите членки е било предизвикателство да включат всички възможности, определящи деянията, свързани с престъпленията (членове 3—7), и общи стандарти за наказанията за кибератаки (член 9). Други проблеми, изглежда, са свързани с прилагането на административните разпоредби относно каналите за докладване (член 13, параграф 3) и контрола и статистиката за престъпленията, включени в директивата (член 14).

Комисията ще продължи да предоставя подкрепа на държавите членки при прилагането на директивата. С оглед потенциалния принос за трансграничното сътрудничество това се отнася по-специално за оперативните разпоредби на директивата, свързани с обмена на информация (член 13, параграфи 1 и 2), каналите за докладване (член 13, параграф 3) и контрола и статистиката (член 14). За тази цел Комисията ще даде допълнителни възможности на държавите членки да определят и обменят най-добри практики през втората половина на 2017 г.

Понастоящем Комисията не вижда необходимост от това да се предлагат изменения на директивата. В този контекст, както и за да подпомогне наказателните разследвания на атаки срещу информационните системи, на престъпления, извършвани чрез кибернетични средства, и други видове престъпления, Комисията разглежда мерки за подобряване на трансграничния достъп до електронни доказателства за наказателни

разследвания, в т.ч. предлагането на законодателни мерки до началото на 2018 г.[8] Комисията разглежда също така ролята на шифроването в разследванията на престъпления и ще докладва за констатациите си през октомври 2017 г[9].

Комисията се ангажира да гарантира, че транспонирането е завършено в целия ЕС и че разпоредбите се прилагат правилно. Това включва наблюдение дали националните мерки съответстват на разпоредбите в директивата. Когато е необходимо, Комисията ще упражнява правомощията си за принудително прилагане, които са ѝ дадени съгласно Договорите, посредством производства за установяване на неизпълнение на задължения.

[8] Оценка на въздействието от етапа на създаване на подобряването на трансграничния достъп до електронни доказателства от 4 август 2017 г., достъпна на ec.europa.eu

[9] Съобщение относно „Осми доклад за напредъка по създаването на ефективен и истински Съюз на сигурност“, COM(2017) 354 final.