ДИРЕКТИВА 2013/40/ЕС НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 12 август 2013 година

относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 83, параграф 1 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет ([1]),

в съответствие с обикновената законодателна процедура ([2]),

като имат предвид, че:

(1) Целите на настоящата директива са да се сближи наказателното право на държавите членки в сферата на атаките срещу информационните системи посредством установяването на минимални правила относно определението на престъпленията и определянето на съответните наказания и да подобри сътрудничеството между компетентните органи, включително полицията и други специализирани правоприлагащи органи на държавите членки, както и компетентните специализирани агенции и органи на Съюза, като Евроюст, Европол и Европейския център по киберпрестъпност към него, както и Европейската агенция за мрежова и информационна сигурност (ENISA).

(2) Информационните системи представляват ключов елемент от политическото, социалното и икономическото взаимодействие в Съюза. Все по-често и в по-голяма степен обществото зависи от тези системи. Безпроблемното функциониране и сигурността на тези системи в Съюза са от жизненоважно значение за развитието на вътрешния пазар и на конкурентоспособна и иновационна икономика. Осигуряването на подходящи равнища на защита на информационните системи следва да бъде част от цялостна ефективна рамка за превантивни мерки, съпътстваща реакцията на наказателното право спрямо киберпрестъпността.

(3) Атаките срещу информационните системи, и по-специално атаките, свързани с организираната престъпност, представляват засилваща се опасност както в Съюза, така и в световен мащаб, а съществува и растяща загриженост от вероятни атаки по терористични или политически подбуди срещу информационните системи, които са част от критичната инфраструктура на държавите членки и на Съюза. Това представлява заплаха за постигането на едно по-безопасно информационно общество и за изграждането на пространство на свобода, сигурност и правосъдие, и следователно налага ответна реакция на равнището на Съюза, а също така и по-добра координация и сътрудничество на международно равнище.

(4) В Съюза съществува определен брой критични инфраструктури, чието нарушаване или унищожаване би имало значителни трансгранични последици. От необходимостта да се подобрят способностите за защита на критичните инфраструктури в Съюза става ясно, че мерките срещу кибератаките следва да бъдат допълнени от строги наказателни санкции, отразяващи тежестта на подобни атаки. Като критична инфраструктура могат да се разглеждат разположени в държавите членки елемент, система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението. като електроцентрали, транспортни мрежи или правителствени мрежи, и чието нарушаване или унищожаване би имало значителни последици в дадената държава членка в резултат на невъзможността да се запазят тези функции.

(5) Има доказателства за наличието на тенденция към все по-опасни и повтарящи се широкомащабни атаки срещу информационните системи, които често могат да бъдат от решаващо значение за държавите членки или за определени функции в публичния или частния сектор. Тази тенденция е придружена от разработката на все по-усъвършенствани методи, като например създаването и използването на така наречените „ботнети“, които се състоят от няколко етапа на престъпното деяние, при които всеки етап поотделно би могъл да създаде сериозен риск за обществения интерес. Настоящата директива има за цел, *inter alia*, да въведе наказания за създаването на ботнет, по-конкретно за акта на установяване на контрол от разстояние върху значителен брой компютри посредством заразяването им със зловреден софтуер чрез целенасочени кибератаки. 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 е в състояние да причини сериозни вреди, както е посочено в настоящата директива. Държавите членки следва да могат да определят кое представлява сериозна вреда съгласно националното право и практика, като например нарушаване на системни услуги от важно обществено значение или причиняване на сериозни финансови разходи или загуба на лични данни или чувствителна информация.

(6) Широкомащабните кибератаки могат да предизвикат съществени икономически вреди както поради прекъсването на информационните системи и комуникации, така и поради загуба или промяна на важна от търговска гледна точка поверителна информация или други данни. Особено внимание следва да се обърне на повишаването на осведомеността на иновативните малки и средни предприятия за заплахи, свързани с подобни атаки, и тяхната уязвимост на такива атаки, тъй като тези предприятия зависят във все по-голяма степен от правилното функциониране и наличност на информационните системи и често разполагат с ограничени ресурси за информационна сигурност.

([1]) ОВ C 218, 23.7.2011 г., стр. 130.

([2]) Позиция на Европейския парламент от 4 юли 2013 г. (все още непубликувана в Официален вестник) и решение на Съвета от 22 юли 2013 г.

(7) Приемането на общи определения в тази област е важно, за да се осигури последователен подход в държавите членки при прилагането на настоящата директива.

(8) Необходимо е да бъде постигнат общ подход към елементите, съставляващи престъпления, чрез въвеждането на общи престъпления, като незаконния достъп до информационни системи, незаконната намеса в такива системи, незаконната намеса в данни и незаконното прихващане.

(9) Прихващането включва, но не се ограничава непременно до подслушването, проследяването или наблюдението на съдържанието на съобщения и достигането до съдържанието на данни с технически средства пряко, чрез достъп до информационни системи и тяхното използване, или непряко, чрез използване на електронно подслушване или подслушвателни устройства.

(10) Държавите членки следва да предвидят наказания за атаките срещу информационните системи. Предвидените наказания следва да бъдат ефективни, пропорционални и възпиращи и следва да включват лишаване от свобода и/или глоби.

(11) Настоящата директива предвижда наказания най-малкото за случаите, които не се считат за маловажни. Държавите членки следва да могат да решат какво представлява маловажен случай в зависимост от своето национално право и практика. Даден случай може да се счете за маловажен например ако причинените от престъплението вреди и/или рискът, който то поражда за публичните или частните интереси, като например по отношение на целостта на компютърната система или компютърните данни или по отношение на неприкосновеността, правата или други интереси на дадено лице, са незначителни или от такова естество, че не е необходимо да се налага наказание в съответните предвидени в правните разпоредби предели или да се налага наказателна отговорност.

(12) Установяването и докладването на заплахи, произтичащи от кибератаки, както и на свързаната с тях уязвимост на информационните системи са важни елементи, които имат отношение към ефективната превенция и реакция на кибератаките и към повишаването на сигурността на информационните системи. Осигуряването на стимули за докладване на пропуски по отношение на сигурността би могло да допринесе допълнително за постигането на тези цели. Държавите членки следва да полагат усилия за предоставянето на възможности за откриването в правен аспект и докладването на пропуски по отношение на сигурността.

(13) Целесъобразно е да се предвидят по-строги наказания, когато атаката срещу дадена информационна система е извършена от престъпна организация съгласно определението в Рамково решение 2008/841/ПВР на Съвета от 24 октомври 2008 г. относно борбата с организираната престъпност [1], когато атаката е широкомащабна и е засегнала значителен брой информационни системи или е причинила сериозни щети, включително когато целта на атаката е създаването на ботнет или когато кибератаката е причинила сериозни вреди, включително когато е извършена посредством ботнет. Също така е целесъобразно да се предвидят по-строги наказания, когато атаката е извършена срещу критична инфраструктура на държавите членки или на Съюза.

(14) Друг съществен елемент от интегрирания подход срещу киберпрестъпността представлява установяването на ефективни мерки срещу кражбата на самоличност и други престъпления, засягащи самоличността. Евентуалната нужда от действия на Съюза във връзка с този вид престъпно поведение може да се разглежда и в контекста на оценката доколко е необходим цялостен хоризонтален инструмент на Съюза.

(15) В заключенията на Съвета от 27—28 ноември 2008 г. се посочва, че следва да се разработи нова стратегия с участието на държавите членки и Комисията, като се вземе предвид съдържанието на Конвенцията на Съвета на Европа от 2001 г. за престъпления в кибернетичното пространство. Тази конвенция е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и с атаките срещу информационните системи. Настоящата директива се основава на споменатата конвенция. Като приоритет следва да се разглежда приключването на процеса на ратификация на тази конвенция от всички държави членки във възможно най-кратък срок.

(16) Като се имат предвид различните начини, по които могат да бъдат извършени атаките, и с оглед на бързите промени в хардуера и софтуера, в настоящата директива се съдържа позоваване на „инструментите“, които могат да бъдат използвани за извършване на престъпленията, изброени в нея. Тези инструменти включват зловредния софтуер, включително този, с който могат да се създават ботнети, използвани за извършване на кибератаки. Макар и даден инструмент да бъде подходящ или дори да бъде особено подходящ за извършването на някое от престъпленията, предвидени в настоящата директива, възможно е той да е бил произведен със законна цел, като например за изпитване на надеждността на продукти на информационните технологии или на сигурността на информационни системи. В подобен случай не е достатъчно дадено лице да има общ умисъл за осъществяване на обективните критерии на някое от престъпленията, предвидени в настоящата директива, а то трябва да има пряк умисъл да използва инструментите за извършването на едно или повече от престъпленията, предвидени в настоящата директива.

(17) Настоящата директива не налага наказателна отговорност в случаите, когато са изпълнени обективните критерии за престъпленията, изброени в настоящата директива, но деянията са извършени без престъпно намерение, като например при незнание, че достъпът не е разрешен, или при възложено изпитване или защита на информационните системи, например когато дружество или продавач възложи на дадено лице изпитването на устойчивостта на системата му за сигурност. В контекста на настоящата директива договорните задължения или споразуменията за ограничаване на достъпа до информационни системи посредством правила за потребителите или условия за използване на услугата, както и трудовите спорове във връзка с достъпа до информационни системи на работодателя и използването им за лични цели не следва да водят до наказателна отговорност, когато достъпът при такива обстоятелства се счита за неразрешен и това представлява единственото основание за наказателно производство. Настоящата директива не засяга правото на достъп до информация, установено в националното законодателство и законодателството на Съюза, като същевременно тя не може да се използва като оправдание за незаконен или произволен достъп до информация.

[1] ОВ L 300, 11.11.2008 г., стр. 42.

(18) Редица обстоятелства могат да улеснят извършването на кибератаки, като например случаите, когато извършителят, в рамките на своята трудова заетост, има достъп до системите за сигурност, които са част от засегнатите информационни системи. В контекста на националното право такива обстоятелства следва да бъдат отчетени в подходяща степен в хода на наказателното производство.

(19) Държавите членки следва да предвидят в националното си право квалифициращи обстоятелства в съответствие с приложимите правила, предвидени в техните правни системи относно квалифициращите обстоятелства. Те следва да гарантират, че съдиите разполагат с възможност да разглеждат тези квалифициращи обстоятелства при осъждането на извършителите. Съдията по своя преценка оценява тези обстоятелства заедно с останалите факти по конкретния случай.

(20) Настоящата директива не урежда условията за упражняване на компетентност над което и да било от посочените в нея престъпления, например съобщаване от страна на жертвата на мястото, където е извършено престъплението, съобщаване от страна на държавата на мястото, където е извършено престъплението, или факта, че извършителят не е наказателно преследван на мястото, където е извършено престъплението.

(21) В контекста на настоящата директива държавите членки и третите държави, както и техните публичните органи продължават в пълна степен да бъдат задължени да гарантират зачитането на правата на човека и основните свободи в съответствие със съществуващите задължения в Съюза и международни задължения.

(22) С настоящата директива се засилва значението на мрежите, като мрежите на Г-8 или Съвета на Европа, съставени от звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. Тези звена за контакт следва да бъдат в състояние да осигуряват ефективна помощ и по този начин да улесняват например обмена на подходяща налична информация и предоставянето на технически съвети или правна информация за целите на разследванията или производствата по престъпления, отнасящи се до информационните системи, и свързаните данни, с участието на молещата държава членка. За да се осигури гладкото функциониране на мрежите, всяко звено за контакт следва да разполага с капацитет за бързо свързване със звено за контакт на друга държава членка с помощта на, *inter alia*, обучен и оборудван персонал. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни кибератаки, държавите членки следва да са в състояние да реагират незабавно на спешни искания, отправени по тази мрежа от звена за контакт. В подобни случаи може да бъде наложително искането за информация да се придружава от телефон за връзка, за да се гарантира, че замолената държава членка ще обработи своевременно искането и обратната информация ще бъде предоставена в рамките на осем часа.

(23) Сътрудничеството между публичните органи, от една страна, и частния сектор и гражданското общество, от друга, е от голямо значение за превенцията и борбата с атаките срещу информационните системи. Необходимо е да се насърчава и подобрява сътрудничеството между доставчиците на услуги, производителите, правоприлагащите и съдебните органи при пълно зачитане на принципите на правовата държава. Сътрудничеството би могло да включва съдействие от доставчиците на услуги за оказване на помощ за съхраняване на евентуални доказателства, за предоставяне на елементи, които да спомогнат за идентифицирането на извършителите, и като крайна мярка, частичното или пълното спиране в съответствие с националното право и практика на информационните системи или функции, които са били засегнати или използвани за незаконни цели. Държавите членки следва да обмислят също създаването на мрежи за сътрудничество и партньорство с доставчиците на услуги и производителите за обмен на информация във връзка с престъпленията, които попадат в обхвата на настоящата директива.

(24) Необходимо е да се събират съпоставими данни за престъпленията, посочени в настоящата директива. Съответните данни следва да се предоставят на компетентните специализирани агенции и органи на Съюза, като Европол и ENISA, в съответствие със задачите и информационните им потребности, за да се добие по-цялостна представа за проблема с киберпрестъпността и мрежовата и информационна сигурност на равнището на Съюза и по този начин се допринесе за изготвянето на по-ефективна реакция. Държавите членки следва да предоставят на Европол и Европейския център по киберпрестъпност към него информация за начина на действие на извършителите, за да се извършат оценка на заплахите и стратегически анализи на киберпрестъпността в съответствие с Решение 2009/371/ПВР на Съвета от 6 април 2009 г. за създаване на Европейска полицейска служба (Европол) ([1]). Предоставянето на информация може да улесни по-доброто разбиране на настоящите и бъдещите заплахи, като допринесе за по-подходящо и целенасочено вземане на решения относно борбата с атаките срещу информационните системи и тяхното предотвратяване.

(25) Комисията следва да представи доклад за прилагането на настоящата директива и ако е необходимо, да направи законодателни предложения, които може да доведат до разширяване на нейния обхват, отчитайки промените в областта на киберпрестъпността. Тези промени могат да включват технологично развитие, като например такова, което позволява по-ефективно правоприлагане в областта на атаките срещу информационните системи или улеснява предотвратяването на подобни атаки или смекчаването на последиците от тях. За тази цел Комисията следва да вземе под внимание наличните анализи и доклади, изготвени от съответните заинтересовани страни, и по-специално от Европол и ENISA.

(26) С цел ефективна борба с престъпленията в киберне-тичното пространство е необходимо също така да се повиши устойчивостта на информационните системи с предприемането на подходящи мерки за по-ефективната им защита от кибератаки. Държавите членки следва да предприемат необходимите мерки за защита от кибератаки на информационните системи, които представляват част от тяхната критична инфраструктура, и следва да обмислят защитата на информационните системи и свързаните данни като част от тази защита. Осигуряването на подходящо равнище на защита и сигурност на информационните системи от юридически лица, например във

([1]) ОВ L 121, 15.5.2009 г., стр. 37.

връзка с предоставянето на общественодостъпни електронни съобщителни услуги в съответствие с действащото законодателство на Съюза относно неприкосновеността на личния живот, електронните съобщения и защитата на данните, представлява съществена част от цялостния подход за ефективна борба срещу киберпрестъпността. Следва да се осигуряват подходящи равнища на защита срещу заплахи и уязвимости, които могат да бъдат разумно идентифицирани, в съответствие със съвременните постижения в конкретните сектори и предвид конкретните ситуации, свързани с обработването на данни. Разходите и тежестта по осигуряване на такава защита следва да бъдат пропорционални на вероятните вреди, които евентуална кибератака може да причини на засегнатите лица. Държавите членки се насърчават да предвидят в националното си право подходящи мерки, водещи до отговорност, за случаите, когато юридическо лице явно не е осигурило подходящо равнище на защита срещу кибератаки.

(27) Значителните пропуски и различия в законите и наказателните производства на държавите членки в областта на атаките срещу информационните системи могат да възпрепятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят ефективното полицейско и съдебно сътрудничество в тази област. Транснационалният характер на съвременните информационни системи, които функционират отвъд националните граници, предполага, че атаките срещу тези системи имат трансгранично измерение, което показва още веднъж спешната необходимост от осъществяване на допълнителни действия за сближаване на наказателното право в тази област. Освен това координирането на наказателното преследване по дела за атаки срещу информационни системи следва да бъде улеснено с подходящото изпълнение и прилагане на Рамково решение 2009/948/ПВР на Съвета от 30 ноември 2009 г. относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства ([1]). В сътрудничество със Съюза държавите членки следва също да се стремят към подобряване на международното сътрудничество, свързано със сигурността на информационните системи, компютърните мрежи и данни. При всяко международно споразумение, включващо обмен на данни, следва надлежно да се разгледа сигурността на прехвърлянето и съхраняването на данните.

(28) По-доброто сътрудничество между компетентните правоприлагащи и съдебни органи в Съюза е изключително важно за ефективната борба срещу престъпленията в кибернетичното пространство. Във връзка с това следва да се насърчава активизирането на усилията за осигуряване на подходящо обучение за съответните органи, за да се подобри разбирането за киберпрестъпността и нейните последици, и за стимулиране на сътрудничеството и обмена на най-добри практики, например чрез компетентните специализирани агенции и органи на Съюза. Целта на подобно обучение, *inter alia*, следва да бъде повишаването на осведомеността за различните национални правни системи, евентуалните правни и технически предизвикателства при наказателни разследвания и разпределението на области на компетентност между съответните национални органи.

(29) В настоящата директива следва да се зачитат правата на човека и основните свободи и да се съблюдават принципите, признати по-специално в Хартата на основните права на Европейския съюз и Европейската конвенция за защита на правата на човека и основните свободи, включително защитата на личните данни, правото на личен живот, свободата на изразяване и на информация, правото на справедлив съдебен процес, презумпцията за невиновност и правото на защита, както и принципите на законност и пропорционалност между престъплението и наказанието. По-специално настоящата директива има за цел да осигури пълното спазване на тези права и принципи и трябва да бъде прилагана в съответствие с това.

(30) Защитата на личните данни е основно право в съответствие с член 16, параграф 1 от ДФЕС и член 8 от Хартата на основните права на Европейския съюз. Ето защо всяко обработване на лични данни при изпълнението на настоящата директива следва изцяло да зачита съответното законодателство на Съюза относно защитата на данните, прието въз основа на Договорите.

(31) В съответствие с член 3 от Протокола относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, приложен към Договора за Европейския съюз и Договора за функционирането на Европейския съюз, посочените държави членки са уведомили за желанието си да вземат участие в приемането и прилагането на настоящата директива.

(32) 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, Дания не участва в приемането на настоящата директива и следователно не е обвързана от нея, нито от нейното прилагане.

(33) Доколкото целите на настоящата директива, а именно да обвърже атаките срещу информационните системи във всички държави членки с ефективни, пропорционални и възпиращи наказания, както и да подобри и насърчи сътрудничеството между съдебните и други компетентни органи, не могат да бъдат постигнати в достатъчна степен от държавите членки и затова поради техния обхват и последици могат да бъдат по-добре постигнати на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящата директива не надхвърля необходимото за постигането на тези цели.

(34) Настоящата директива има за цел да измени и разшири обхвата на разпоредбите на Рамково решение 2005/222/ПВР на Съвета от 24 февруари 2005 г. относно атаките срещу информационните системи ([2]). Тъй като измененията, които трябва да се направят, са значителни по брой и естество, за по-голяма яснота Рамково решение 2005/222/ПВР следва да бъде изцяло заменено по отношение на държавите членки, участващи в приемането на настоящата директива,

([1]) ОВ L 328, 15.12.2009 г., стр. 42.

([2]) ОВ L 69, 16.3.2005 г., стр. 67.

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

Член 1

Предмет

Настоящата директива установява минимални правила за определянето на престъпленията и наказанията в областта на атаките срещу информационните системи. Тя има за цел също да способства за предотвратяването на тези престъпления и да подобри сътрудничеството между съдебните и други компетентни органи.

Член 2

Определения

За целите на настоящата директива се прилагат следните определения:

а) „информационна система“ означава устройство или група от взаимосвързани или сходни устройства, едно или повече от които, съобразно дадена програма, извършват автоматизирана обработка на компютърни данни, както и компютърните данни, съхранявани, обработвани, извличани или предавани от такова устройство или група от устройства с цел оперирането с тези данни и използването, защитата и поддръжката им;

б) „компютърни данни“ означава представяне на факти, информация или понятия във форма, поддаваща се на обработка в информационни системи, включително и програма, която е в състояние да направи така, че дадена информационна система да изпълни определена функция;

в) „юридическо лице“ означава всяко образувание, притежаващо статут на юридическо лице съгласно приложимото право, с изключение на държави членки, трети държави или други публични органи при упражняване на държавна власт, както и на публични международни организации;

г) „неправомерно“ означава поведение, което не е разрешено от собственика или от друг притежатели на права върху системата или част от нея, или не е позволено по силата на националното право.

Член 3

Незаконен достъп до информационни системи

Държавите членки предприемат необходимите мерки, за да гарантират, че когато е извършен умишлено, неправомерният достъп до цялата информационна система или до части от нея е наказуем като престъпление, когато е извършен чрез нарушаване на мярка за сигурност, поне в случаите, които не се считат за маловажни.

Член 4

Незаконна намеса в система

Държавите членки предприемат необходимите мерки, за да гарантират, че сериозното възпрепятстване или спиране на функционирането на информационна система чрез въвеждане на компютърни данни, пренасяне, увреждане, изтриване, влошаване, променяне или скриване на такива данни или спиране на достъпа до компютърни данни, когато е извършено умишлено и неправомерно, е наказуемо като престъпление, поне в случаите, които не се считат за маловажни.

Член 5

Незаконна намеса в данни

Държавите членки предприемат необходимите мерки, за да гарантират, че изтриването, увреждането, влошаването, променянето, скриването на компютърни данни в дадена информационна система или спирането на достъпа до такива данни, когато е извършено умишлено и неправомерно, е наказуемо като престъпление, поне в случаите, които не се считат за маловажни.

Член 6

Незаконно прихващане

Държавите членки предприемат необходимите мерки, за да гарантират, че извършеното с технически средства прихващане на непублични компютърни данни, изпращани до дадена информационна система, от нея или в нейните рамки, включително електромагнитните емисии от информационна система, пренасящи такива компютърни данни, когато е извършено умишлено и неправомерно, е наказуемо като престъпление, поне в случаите, които не се считат за маловажни.

Член 7

Инструменти, използвани за извършване на престъпления

Държавите членки предприемат необходимите мерки, за да гарантират, че умишленото производство, продажба, набавяне за употреба, внос, разпространяване или друга форма на предоставяне на някой от следните инструменти, когато е извършено неправомерно и с намерение да се използва за извършването на което и да било от престъпленията, посочени в членове 3—6, е наказуемо като престъпление, поне в случаите, които не се считат за маловажни:

а) компютърна програма, проектирана или адаптирана главно с цел извършване на което и да било от престъпленията, посочени в членове 3—6;

б) компютърна парола, код за достъп или други подобни данни, с чиято помощ може да се получи достъп до цялата информационна система или до част от нея.

Член 8

Подбудителство, помагачество и опит за извършване на престъпление

1. Държавите членки гарантират, че подбудителството или помагачеството за извършване на някое от престъпленията, посочени в членове 3—7, е наказуемо като престъпление.

2. Държавите членки гарантират, че опитът за извършване на престъпление, посочено в членове 4 и 5, е наказуем като престъпление.

Член 9

Наказания

1. Държавите членки предприемат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—8, са наказуеми с ефективни, пропорционални и възпиращи наказания.

2. Държавите членки предприемат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—7, се наказват с лишаване от свобода с максимален срок не по-малко от две години, поне в случаите, които не се считат за маловажни.

3. Държавите членки предприемат необходимите мерки, за да гарантират, че когато са извършени умишлено и когато значителен брой информационни системи са били засегнати

посредством използването на инструмент, посочен в член 7, проектиран или адаптиран главно за тази цел, посочените в членове 4 и 5 престъпления се наказват с лишаване от свобода с максимален срок не по-малко от три години.

4. Държавите членки предприемат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 4 и 5, се наказват с лишаване от свобода с максимален срок не по-малко от пет години, когато:

а) те са извършени в рамките на престъпна организация съгласно определението в Рамково решение 2008/841/ПВР, независимо от размера на наказанието, предвидено в него; или

б) те са причинили сериозни вреди; или

в) те са извършени срещу информационна система, която е част от критична инфраструктура.

5. Държавите членки предприемат необходимите мерки, за 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 съгласно националното право като квалифициращо обстоятелство, освен ако тези обстоятелства не са вече част от друго престъпление, което е наказуемо съгласно националното право.

Член 10

Отговорност на юридическите лица

1. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическите лица могат да бъдат подведени под отговорност за престъпленията, посочени в членове 3—8, извършени в тяхна полза от лице, което действа самостоятелно или като част от орган на юридическото лице и което заема ръководна длъжност в това юридическо лице, въз основа на едно от следните:

а) пълномощие да представлява юридическото лице;

б) правомощие да взема решения от името на юридическото лице;

в) правомощие да упражнява контрол в рамките на юридическото лице.

2. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическите лица могат да бъдат подведени под отговорност, когато липсата на надзор или контрол от страна на лице, посочено в параграф 1, е направила възможно извършването от негово подчинено лице на някое от престъпленията, посочени в членове 3—8, в полза на това юридическо лице.

3. Отговорността на юридическите лица съгласно параграфи 1 и 2 не изключва образуването на наказателни производства срещу физически лица, които са извършители, подбудители или съучастници в престъпленията, посочени в членове 3—8.

Член 11

Санкции спрямо юридически лица

1. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическо лице, подведено под отговорност съгласно член 10, параграф 1, подлежи на санкции, които са ефективни, пропорционални и възпиращи, включват глоби по наказателното право или друг вид глоби и може да включват други санкции, като например:

а) лишаване от правото да се ползва от публични облаги или помощи;

б) временно или постоянно лишаване от правото да упражнява търговска дейност;

в) поставяне под съдебен надзор;

г) съдебна ликвидация;

д) временно или постоянно затваряне на структури, използвани за извършване на престъплението.

2. Държавите членки предприемат необходимите мерки, за да гарантират, че юридическо лице, подведено под отговорност съгласно член 10, параграф 2, подлежи на ефективни, пропорционални и възпиращи санкции или други мерки.

Член 12

Компетентност

1. Държавите членки установяват компетентността си по отношение на престъпленията, посочени в членове 3—8, когато престъплението е извършено:

а) изцяло или отчасти на тяхната територия; или

б) от един от техните граждани, поне в случаите, когато деянието се явява престъпление на мястото, където е извършено.

2. При установяването на компетентност в съответствие с параграф 1, буква а) дадената държава членка гарантира, че тя има компетентност, когато:

а) извършителят извършва престъплението, когато се намира физически на нейната територия, независимо дали престъплението е насочено срещу информационна система, намираща се на нейна територия; или

б) престъплението е насочено срещу информационна система, намираща се на нейната територия, независимо дали извършителят се намира физически на нейна територия, когато го извършва.

3. Дадена държава членка уведомява Комисията, когато реши да установи компетентност по отношение на престъпления, посочени в членове 3—8, извършени извън нейната територия, включително когато:

а) извършителят има обичайно местопребиваване на нейната територия; или

б) престъплението е извършено в полза на юридическо лице, установено на нейната територия.

Член 13

Обмен на информация

1. За целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8, държавите членки осигуряват наличието на оперативно национално звено за контакт и използват съществуващата мрежа от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. Държавите членки гарантират също, че разполагат с процедури, чрез които в случай на спешно искане за съдействие компетентният орган в рамките най-много на 8 часа от получаването посочва поне дали на искането за помощ ще бъде отговорено, както и формата и приблизителното време за отговор.

2. Държавите членки информират Комисията за определеното от тях звено за контакт, посочено в параграф 1. Комисията съобщава тази информация на останалите държави членки и на компетентните специализирани агенции и органи на Съюза.

3. Държавите членки предприемат необходимите мерки, за да гарантират наличието на подходящи канали за докладване с цел да се улесни докладването без необосновано забавяне на компетентните национални органи за престъпления, посочени в членове 3—6.

Член 14

Контрол и статистика

1. Държавите членки гарантират наличието на система за записване, производство и предоставяне на статистически данни за престъпленията, посочени в членове 3—7.

2. Статистическите данни, посочени в параграф 1, като минимум включват съществуващите данни относно броя на посочените в членове 3—7 престъпления, които са регистрирани от държавите членки, както и броя на лицата, срещу които е възбудено наказателно преследване и които са осъдени за престъпления, посочени в членове 3—7.

3. Държавите членки предават на Комисията събраните по настоящия член данни. Комисията прави необходимото консолидираният преглед на тези статистически отчети да бъде публикуван и представен на компетентните специализирани агенции и органи на Съюза.

Член 15

Замяна на Рамково решение 2005/222/ПВР

Рамково решение 2005/222/ПВР се заменя по отношение на държавите членки, които участват в приемането на настоящата директива, без да се засягат задълженията на тези държави членки във връзка със сроковете за транспониране на Рамковото решение в националното право.

По отношение на държавите членки, които участват в приемането на настоящата директива, позоваванията на Рамково решение 2005/222/ПВР се считат за позовавания на настоящата директива.

Член 16

Транспониране

1. Държавите членки въвеждат в сила законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата директива, до 4 септември 2015 г.

2. Държавите членки съобщават на Комисията текста на мерките, с които се транспонират в националното им право задълженията, наложени им с настоящата директива.

3. Когато държавите членки приемат тези мерки, в тях се съдържа позоваване на настоящата директива или то се придружава от подобно позоваване при официалното им публикуване. Условията и редът на позоваване се определят от държавите членки.

Член 17

Докладване

До 4 септември 2017 г. Комисията представя на Европейския парламент и на Съвета доклад за оценка на степента, в която държавите членки са предприели необходимите мерки, за да се съобразят с настоящата директива, придружен при необходимост от законодателни предложения. Комисията отчита също техническото и правното развитие в областта на киберпрестъпността, по-специално по отношение на обхвата на настоящата директива.

Член 18

Влизане в сила

Настоящата директива влиза в сила на двадесетия ден след публикуването ѝ в *Официален вестник на Европейския съюз*.

Член 19

Адресати

Адресати на настоящата директива са държавите членки в съответствие с Договорите.

Съставено в Брюксел на 12 август 2013 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
M. SCHULZ	L. LINKEVIČIUS