РАМКОВО РЕШЕНИЕ 2005/222/ ПВР НА СЪВЕТА

от 24 февруари 2005 година

относно атаките срещу информационните системи

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално членове 29, 30, параграф 1, буква а), 31, параграф 1, буква е), и 34, параграф 2, буква б) от него,

като взе предвид инициативата на Комисията,

като взе предвид мнението на Европейския парламент[1],

като има предвид, че:

(1) Целта на това рамково решение е да подобри сътрудничеството между съдебната и другите компетентни власти, в това число полицията и други специализирани правоприлагащи служби на държавите-членки, чрез сближаване на правилата в наказателното право в сферата на атаките срещу информационните системи.

(2) Има доказателства за атаки срещу информационните сфери като резултат от заплахата на организираната престъпност и засилване на загрижеността от потенциалната възможност от терористични атаки срещу информационните системи, които формират част от най-важната инфраструктура на държавите-членки. Всичко това представлява заплаха за постигането на едно по-безопасно информационно общество и на зона на свобода, сигурност и справедливост и следователно се изисква ответна реакция на ниво Европейски съюз.

(3) Една ефективна ответна реакция на тези заплахи изисква всестранен подход към мрежовата и информационна сигурност, както се подчертава в Плана за действие електронна Европа в съобщение на Комисията „ Мрежова и информационна сигурност: предложение за общ европейски подход”, а също и в резолюцията на Съвета от 28 януари 2002 година относно общия подход и конкретните действия в сферата на мрежовата и информационна сигурност[2].

(4) Необходимостта от по-добро разбиране на проблемите, свързани с информационната сигурност и от оказване на практическа помощ в тази насока се подчертава и в резолюцията на Европейския парламент от 5 септември 2001 г.

(5) Значителните пропуски и различия в законите на държавите-членки в тази област могат да препятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят ефективното сътрудничество между полицията и съда в областта на атаките срещу информационните системи. Транснационалния и безграничен характер на съвременните информационни системи означава, че атаките срещу тези системи често са трансгранични по характер, което идва да подчертае още веднъж спешната

[1] ОВ С 300 Е, 11.12.2003 г., стр. 26
[2] ОВ С 43, 16.2.2002 г., стр. 2

необходимост от осъществяване на действия за сближаване на наказателното право в тази сфера.

(6) Планът за действие на Съвета и Комисията относно най-добрия начин за прилагане на разпоредбите на Договора от Амстердам в една област на свобода, сигурност и справедливост[3], Европейският съвет в Тампере на 15 и 16 октомври 1999 г., Европейският съвет в Santa Maria da Feira от 19 и 20 февруари 2000 г., Комисията в Таблицата за оценка и Европейския парламент в своята резолюция от 19 май 2000 година, посочват или призовават към законодателни действия, насочени срещу престъпността в сферата на високите технологии, в това число изработване на общоприети дефиниции, инкриминиране и санкциониране.

(7) Необходимо е да се допълва работата, извършвана от различни международни организации, по-специално работата, извършвана от Съвета на Европа по сближаване на националните закони в сферата на наказателното право, а също така и дейността на Г8 относно международно сътрудничество в борбата срещу престъпността в сферата на високите технологии, като приложи общ подход в Европейския съюз в тази област. Този призив беше разработен по-подробно в Съобщение от Комисията до Съвета, Европейския парламент, Икономическия и социален комитет и Комитета на регионите относно „ създаване на по-сигурно информационно общество чрез повишаване сигурността на информационните инфраструктури и борбата срещу компютърните престъпления”.

(8) Наказателното право в областта на атаките срещу информационните системи трябва да стане обект на сближаване в националните законодателства, за да осигури възможно най-широка база за сътрудничество между полицията и съдебните власти в сферата на престъпленията, свързани с атаки срещу информационните системи, а също така да даде своя принос в борбата срещу организираната престъпност и тероризма.

(9) Всички държави-членки са ратифицирали Конвенцията на Съвета на Европа от 28 януари 1981 г. относно защитата на личността във връзка с автоматичното обработване на лични данни. Обработваните лични данни, в контекста на прилагането на настоящото рамково решение следва да бъдат защитени в съответствие с принципите на упоменатата по-горе конвенция.

(10) Приемането на общи дефиниции в тази област, по-конкретно на информационни системи и компютърни данни, са изключително важни за осигуряването на един систематичен подход в държавите-членки при практическото осъществяване на настоящото рамково решение.

(11) Необходимо е постигането на общ подход към състава на престъпленията при общи престъпления на неправомерен достъп до информационни системи, неправомерна интерференция в такива системи и неправомерна интерференция в данните им.

(12) В интерес на борбата с компютърните престъпления, всяка държава-членка трябва да осигури ефективно сътрудничество по отношение на престъпления, базирано на видовете престъпно поведение, упоменати в членове 2,3,4 и 5.

[3] ОВ С 19, 23.01.1990 г., стр. 1

(13) Необходимо е да се избягва свръхкриминализацията, най-вече на леки престъпления, а също и да се избягва криминализацията при субекти на такива права и упълномощени лица.

(14) Необходимо е за държавите-членки да въведат разпоредби относно наказания при атаки срещу информационни системи. Така разпоредените наказания следва да бъдат ефективни, съразмерни и разубеждаващи.

(15) Подходящо е да се въведат разпоредби за по-сериозни наказания в случаите, когато атаката срещу информационната система е извършена в рамките на престъпна организация, както е разпоредено в Съвместно действие 98/733 ПВР от 21 декември 1998 г. прието от Съвета на основание на член К.3 от Договора за Европейски съюз относно инкриминирането в държавите-членки на Европейския съюз на участието в престъпна организация [(4)]. Подходящо е също така да се въведат по-сериозни наказания в случаите, когато такава атака е причинила сериозни щети или е засегнала съществени интереси.

(16) Следва да се предвидят мерки за целите на сътрудничеството между държавите-членки с цел осигуряването на по-голяма ефективност на противодействието спрямо атаки срещу информационни системи. Държавите-членки следва да се възползват от съществуващата система от оперативни точки за контакт, упоменати в препоръката на Съвета от 25 юни 2001 година относно точките за контакт, предоставящи 24-часови услуги за обмен на информация в борбата срещу престъпленията в сферата на високите технологии[(5)].

(17) Тъй като целите на настоящото рамково решение, гарантиращи че санкционирането на атаките срещу информационните системи във всички държави-членки води до ефективни, съразмерни и разубеждаващи наказания, стимулиращи сътрудничеството между съдебните системи, чрез премахването на потенциалните усложнения, не могат да бъдат напълно от държавите-членки, тъй като правилата трябва да бъдат еднакви и съвместими и следователно по-лесно достижими на Съюзно ниво, Съюзът би могъл да приеме мерки в съответствие с принципа на субсидиарността, както е посочено в член 5 от Договора за ЕС. В съответствие с принципа на пропорционалността, както се посочва в същия член, настоящото рамково решение не излиза извън границите на необходимото за постигане на тези цели.

(18) Настоящото рамково решение съблюдава основните права и принципите, признати от член 6 от Договора за Европейския съюз и отразени в Хартата на основните права в Европейския съюз и по-точно Глави II и VI от нея,

ПРИЕ НАСТОЯЩОТО РАМКОВО РЕШЕНИЕ:

Член 1

Дефиниции

За целите на настоящото рамково решение се прилагат следните дефиниции:

[(4)] ОВ L 351, 29.12.1998 г., стр. 1
[(5)] ОВ C 187, 2.7.2001 г., стр. 5

а) „информационна система” означава всяко устройство или група от свързани или подобни устройства, едно или повече от които, съобразно дадена програма, извършват автоматична обработка на компютърни данни, както и компютърни данни, съхранявани, обработвани, извличани или пренасяни от тях с цел тяхното опериране, използване, защита или поддръжка;

б) „компютърни данни” означава всяко представяне на факти, информация или понятия във форма, годна за обработка в информационна система, включително програми, способни да дават указания на информационни системи за изпълнение на функции;

в) „юридическо лице” означава всеки субект, притежаващ такъв статут в съответния закон, с изключение на държави или други публични органи, при упражняване на държавна власт, както и на публични международни организации;

г) „неправомерен” означава всеки достъп или интерференция, неоторизирани от собственика, от друг субект на правото до системата или до части от нея, или непозволени по силата на националното законодателство.

Член 2

Неправомерен достъп до информационни системи

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че всеки умишлен неправомерен достъп до цялата или до части от информационни системи е наказуем като престъпно деяние поне за случаите, в които престъплението не се счита за леко.

2. Всяка държава-членка би могла да реши, че деянието, упоменато в параграф 1, се инкриминира само в случаите, когато то се извършва в нарушение на мярка за сигурност.

Член 3

Неправомерна интерференция в системите

Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че всяко умишлено спиране или възпрепятстване на функционирането на една информационна система чрез неправомерно вкарване, пренасяне, увреждане, изтриване, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни е наказуемо като престъпно деяние поне за случаите, в които престъплението не се счита за леко.

Член 4

Неправомерна интерференция в данни

Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че всяко умишлено изтриване, увреждане, влошаване, променяне, скриване или предоставяне на забранени за достъп компютърни данни в

дадена информационна система е наказуемо като престъпно деяние поне за случаите, в които престъплението не се счита за леко.

Член 5

Подбудителство, подпомагане, съдействие и опит за извършване на престъпление

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че подбудителството, подпомагането и съдействието за извършване на престъпления, упоменати в членове 2,3,4 и 5, следва да са наказуеми с ефективни, съразмерни и разубеждаващи наказания в максимален размер от една до три години лишаване от свобода.

Член 6

Наказания

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че престъпните деяния, упоменати в членове 2,3,4 и 5, следва да са наказуеми с ефективни, съразмерни и възпиращи наказания.

2. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че престъпните деяния, упоменати в членове 4 и 5 са наказуеми с наказания в максимален размер от една до три години лишаване от свобода.

Член 7

Отегчаващи вината обстоятелства

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че престъпното деяние, упоменато в член 2, параграф 2, както и това, упоменато в членове 3 и 4 са наказуеми с наказания в максимален размер от две до пет години лишаване от свобода, когато са извършени в рамките на престъпна организация в съответствие с определението в Съвместно действие 98/733/ПВР отделно от нивото на наказание, упоменато в него.

2. Всяка държава-членка може да предприеме мерките, упоменати в параграф 1 в случаите, когато престъпното деяние е предизвикало сериозни вреди или е засегнало съществени интереси.

Член 8

Отговорност на юридически лица

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че юридическите лица да бъдат държани отговорни във връзка със престъпните деяния, упоменати в членове 2,3,4, и 5, извършени в тяхна полза от лице, действащо самостоятелно или като част от структурата на юридическо лице, което заема водеща позиция в юридическото лице на базата на:

а) пълномощия за представителство на юридическото лице, или

б) правото за вземане на решения от името на юридическото лице, или

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

2. Освен в случаите, уредени в параграф 1, държавите-членки следва да вземат необходимите мерки за постигане на разумна степен на сигурност, така че юридическите лица да могат да бъдат държани отговорни в случаите, когато недостатъчният надзор или контрол от лица, упоменати в параграф 1 е създал възможността за извършване на престъпните деяния, упоменати в членове 2,3,4 и 5, в полза на юридическо лице от лице под негово ръководство.

3. Отговорността на юридическото лице в съответствие с параграфи 1 и 2 не изключва наказателно преследване спрямо физически лица, въвлечени като извършители,подбудители или съучастници в извършването на престъпни деяния, упоменати в членове 2, 3, 4, и 5.

Член 9

Наказания спрямо юридически лица

1. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че юридическите лица, държани отговорни съгласно член 8, параграф 1, да могат да бъдат наказани с ефективни, съразмерни и разубеждаващи мерки, включващи наказателни и ненаказателни глоби и други санкции като:

а) отнемане на правото за получаване на социални и парични помощи;

б) временно или постоянно лишаване от правото на извършване на търговска дейност;

в) поставяне под съдебен надзор; или

г) издаване на съдебна заповед за ликвидация.

2. Всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че юридическите лица, държани отговорни съгласно член 8 , параграф 2, да могат да бъдат наказани с ефективни, съразмерни и разубеждаващи мерки.

Член 10

Юрисдикция

1. Всяка държава-членка създава своя собствена юрисдикция спрямо престъпните деяния, упоменати в членове 2,3,4 и 5, когато престъпното деяние е извършено:

а) изцяло или частично на нейна територия; или

б) от неин гражданин; или

в) в полза на юридическо лице, чието седалище е разположено на територията на държавата-членка.

2. При създаване на своя собствена юрисдикция в съответствие с параграф 1 (а), всяка държава-членка следва да вземе необходимите мерки за постигане на разумна степен на сигурност, така че тя да включва случаи, когато:

а) правонарушителят извърши престъпление, физически присъствайки на нейна територия, независимо дали престъплението е насочено или не е срещу информационна система на нейна територия; или

б) престъплението е срещу информационна система на нейна територия независимо дали нарушителят го извършва, присъствайки физически на нейна територия.

3. Държава-членка, която, по силата на собствените си закони, не екстрадира или не предава свои граждани, следва да вземе необходимите мерки за действие на своята юрисдикция и да заведе съдебно дело, когато е подходящо, във връзка с престъпни деяния, упоменати в членове 2,3,4 и 5, в случаите, когато са извършени от неин гражданин извън територията й.

4. В случаите, когато престъпното деяние попада под юрисдикцията на повече от една държава-членка и когато всяка от засегнатите държави-членки може действително да заведе съдебно дело, обосновано на същите факти, засегнатите държави-членки следва да си сътрудничат, за да решат коя от тях ще подведе закононарушителите под съдебна отговорност с цел, при възможност, да се централизират всички действия в една единствена държава-членка. За постигане на тази цел, държавите-членки могат да се обърнат за помощ към всеки орган или механизъм, създаден в рамките на Европейския съюз за подпомагане на сътрудничеството между техните съдебни власти и за координиране на техните действия. Могат да бъдат последователно взети предвид следните фактори:

- държавата-членка да бъде тази на територията, на която са извършени престъпленията в съответствие с параграф 1 , буква а) и параграф 2

- държавата-членка да бъде тази, чиито гражданин е правонарушителя,

- държавата-членка да бъде тази, в която е намерен правонарушителя.

5. Държавата-членка би могла да реши да не прилага или да прилага само в конкретни случаи или при конкретни обстоятелства правните норми, определени в параграф 1, буква б) и параграф 1, буква в).

6. Държавите-членки информират Генералния секретариат на Съвета и Комисията относно решението си за прилагане на параграф 5, когато е подходящо с посочване на конкретните случаи или условия, в които решението е приложимо.

Член 11

Обмен на информация

1. За целите на обмена на информация, свързана с престъпленията, упоменати в членове 2,3,4 и 5, и в изпълнение на изискванията относно защитата на данни, държавите-членки следва да вземат необходимите мерки за постигане на разумна степен на сигурност, така че да се възползват от съществуващата мрежа от оперативни точки за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. Всяка държава-членка информира Генералния секретариат на Съвета и Комисията за определената от нея точка за контакт относно обмена на информация по престъпления, свързани с атаки срещу информационни системи. Генералният секретариат изпраща информацията до останалите държави-членки.

Член 12

Изпълнение

1. Държавите-членки приемат необходимите мерки за изпълнението на разпоредбите на настоящото рамково решение преди 16 март 2007 г..

2. До 16 март 2007 г. държавите-членки предоставят на Генералния секретариат на Съвета и на Комисията текста на разпоредбите от тяхното национално законодателство, които транспонират задълженията, произтичащи от настоящото рамково решение. Въз основа на доклада с тези сведения, изготвен от Комисията, Съветът проверява преди 16 март 2007 г. степента на съответствие с разпоредбите на настоящото рамково решение в отделните държави-членки.

Член 13

Влизане в сила

Настоящото рамково решение влиза в сила на датата на неговото публикуване в *Официалния вестник на Европейския съюз.*

Съставено в Брюксел на 24 февруари 2005 година.

За Съвета:
Председател
N. SCHMIT