32005F0222

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 член 29, член 30, параграф 1, буква а), член 31, параграф 1, буква д), и член 34, параграф 2, буква б) от него,

като взе предвид предложението на Комисията,

като взе предвид становището на Европейския парламент ([1]),

като има предвид, че:

(1) Целта на настоящото рамково решение е да подобри сътрудничеството между съдебните 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 системи 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 правосъдие и следователно изисква ответна реакция на равнище Европейски съюз.

(3) Ефективната ответна реакция на тези заплахи изисква всестранен подход към мрежовата и информационната сигурност, както се подчертава в плана за действие „еЕвропа“, в съобщението на Комисията „Мрежова и информационна сигурност: предложение за общ европейски подход“ и в Резолюцията на Съвета от 28 януари 2002 г. относно общия подход и специфичните действия в сферата на мрежовата и информационната 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. Транснационалният и безграничен характер на съвременните информационни системи предполага, че атаките срещу тези системи често са трансгранични по характер, което показва още веднъж спешната необходимост от осъществяване на действия за сближаване на наказателното право в тази област.

(6) Планът за действие на Съвета и Комисията относно най-добрия начин за прилагане на разпоредбите на Договора от Амстердам в едно пространство на свобода, сигурност и правосъдие ([3]), Европейският съвет в Тампере на 15 и 16 октомври 1999 г., Европейският съвет в Санта Мария да Фейра от 19 и 20 февруари 2000 г., Комисията в „Таблицата за оценка“ и Европейският парламент в своята Резолюция от 19 май 2000 г., посочват или призовават към законодателни действия, насочени срещу престъпността в сферата на високите технологии, в това число изработване на общоприети дефиниции, инкриминации и санкции.

(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 международното сътрудничество в борбата срещу престъпността в сферата на високите технологии, като се приложи общ подход в Европейския съюз в тази област. Този призив беше разработен по-подробно в съобщението от Комисията до Съвета, Европейския парламент, Икономическия и социален комитет и Комитета на регионите относно „Създаване на по-сигурно информационно общество чрез повишаване на сигурността на информационните инфраструктури и борба 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.

([1]) ОВ C 300 E, 11.12.2003 г., стр. 26.
([2]) ОВ C 43, 16.2.2002 г., стр. 2.
([3]) ОВ C 19, 23.1.1999 г., стр. 1.

(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 горепосочената конвенция.

(10) Приемането на общи дефиниции в тази област, по-конкретно за информационни системи и компютърни данни, е изключително важно за осигуряването на систематичен подход в държавите-членки при прилагането на настоящото рамково решение.

(11) Необходимо е да бъде постигнат общ подход към елементите, съставляващи наказателни престъпления, като неправомерният достъп до информационни системи, неправомерната намеса в такива системи и неправомерната намеса в данните им се включат като общи престъпления.

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

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

(14) Държавите-членки следва да предвидят санкции при атаки срещу информационни системи. Предвидените санкции следва да бъдат ефективни, съразмерни и възпиращи.

(15) Подходящо е да се предвидят по-сериозни наказания в случаите, когато атаката срещу информационната система е извършена в рамките на престъпна организация, както е определено в Съвместно действие 98/733/ПВР от 21 декември 1998 г. относно инкриминирането в държавите-членки на Европейския съюз на участието в престъпна организация ([1]). Подходящо е също така да се предвидят 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, посочени в Препоръката на Съвета от 25 юни 2001 г. относно точките за контакт, предоставящи 24-часови услуги за обмен на информация в борбата срещу престъпленията в сферата на високите технологии ([2]).

(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 възпиращи наказания, стимулиращи сътрудничеството между съдебните системи чрез премахването на потенциалните усложнения, не могат да бъдат постигнати в достатъчна степен от държавите-членки, тъй като правилата трябва да бъдат еднакви и съвместими, и следователно могат да бъдат по-добре постигнати на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарността, посочен в член 5 от Договора за ЕС. В съответствие с принципа на пропорционалността, посочен в същия член, настоящото рамково решение не надхвърля необходимото за постигането на тези цели.

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

ПРИЕ НАСТОЯЩОТО РАМКОВО РЕШЕНИЕ:

Член 1

Определения

За целите на настоящото рамково решение се прилагат следните определения:

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 компютърните данни, съхранявани, обработвани, извличани или пренасяни от тези устройства с цел опериране с, използване, защита или поддръжка на тези данни;

б) „компютърни данни“ означава представянето на факти, информация или понятия във форма, удобна за обработка в информационни системи, включително и програмите, задаващи указания на информационни системи за изпълнение на определени функции;

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

([1]) ОВ L 351, 29.12.1998 г., стр. 1.

([2]) ОВ C 187, 3.7.2001 г., стр. 5.

г) „неправомерен“ означава достъп или намеса, който/която не е оторизиран/а от собственика или от други субекти на правото на собственост върху системата или части от нея, или е забранен/а по силата на националното законодателство.

Член 2

Неправомерен достъп до информационни системи

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

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

Член 3

Неправомерна намеса в система

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

Член 4

Неправомерна намеса в данни

Всяка държава-членка следва да предприеме необходимите мерки за постигане на разумна степен на сигурност, 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 в 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 гарантира, че подбудителството, подпомагането и съдействието за извършване на престъпленията, посочени в членове 2, 3 и 4, са наказуеми като криминални престъпления.

2. Всяка държава-членка следва да гарантира, че опитът за извършване на престъпленията, посочени в членове 2, 3 и 4, е наказуем като криминално престъпление.

3. Всяка държава-членка може да реши да не прилага параграф 2 по отношение на престъпленията, посочени в член 2.

Член 6

Наказания

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

2. Всяка държава-членка следва да предприеме необходимите мерки за постигане на разумна степен на сигурност, че престъпните деяния, посочени в членове 3 и 4, са наказуеми с максимална присъда от една до три години лишаване от свобода.

Член 7

Утежняващи вината обстоятелства

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

2. Всяка държава-членка може да предприеме мерките, посочени 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 предприеме необходимите мерки за постигане на разумна степен на сигурност, че юридическите лица ще бъдат държани отговорни за престъпните деяния, посочени 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, предвидени в параграф 1, държавите-членки следва да гарантират, че юридическите лица ще бъдат държани отговорни в случаите, когато недостатъчният надзор или контрол от лицата, упоменати в параграф 1, е създал възможност за извършване на престъпните деяния, посочени 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 престъпните деяния, посочени в членове 2, 3, 4 и 5.

Член 9

Наказания спрямо юридически лица

1. Всяка държава-членка следва да предприеме необходимите мерки за постигане на разумна степен на сигурност, че юридическите лица, подведени под отговорност съгласно член 8, параграф 1, ще бъдат наказани с ефективни, съразмерни и разубеждаващи мерки, включващи наказателни и ненаказателни глоби и други санкции като:

а) отнемане на правото за получаване на държавни помощи и субсидии;

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

в) поставяне под съдебен надзор; или

г) издаване на съдебна заповед за ликвидация.

2. Всяка държава-членка следва да предприеме необходимите мерки за постигане на разумна степен на сигурност, че юридическите лица, подведени под отговорност съгласно член 8, параграф 2, ще бъдат наказани с ефективни, съразмерни и разубеждаващи наказания или мерки.

Член 10

Юрисдикция

1. Всяка държава-членка създава своя юрисдикция спрямо престъпните деяния, посочени 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 главно управление е разположено на територията на държавата-членка.

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

а) правонарушителят извърши престъпление, физически присъствайки на нейна територия, независимо дали престъплението е насочено или не 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 съгласно своето законодателство 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 престъпните деяния, упоменати в членове 2, 3, 4 и 5, в случаите, когато са извършени от неин гражданин извън територията ѝ.

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 по 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 чиято територия са извършени престъпленията в съответствие с параграф 1, буква а) и параграф 2,

— държавата-членка да бъде тази, чийто гражданин е правонарушителят,

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

5. Държавата-членка би могла да реши да не прилага или да прилага само в конкретни случаи или при конкретни обстоятелства правилата за юрисдикцията, определени в параграф 1, букви б) и в).

6. Държавите-членки информират генералния секретариат на Съвета и Комисията, когато решат да прилагат 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 гарантират, че ще използват съществуващата мрежа от оперативни точки за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата.

2. 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 предприемат необходимите мерки, за да се съобразят с разпоредбите на настоящото рамково решение до 16 март 2007 г.

2. До 16 март 2007 г. държавите-членки предоставят на генералния секретариат на Съвета и на Комисията текстовете на разпоредбите от тяхното национално законодателство, които транспонират задълженията, произтичащи от настоящото рамково решение. Въз основа на тази информация и писмения доклад, изготвен от Комисията, Съветът проверява до 16 септември 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 в деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 24 февруари 2005 година.

За Съвета

Председател

N. SCHMIT