

# EUROPEAN PARLIAMENT

1999



2004

---

*Committee on Industry, External Trade, Research and Energy*

PROVISIONAL  
2002/0086(CNS)

2 August 2002

## **DRAFT OPINION**

for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

on the proposal for a Council Framework Decision on attacks against  
information systems

(COM(2002) 173 – C5-0271/2002 – 2002/0086(CNS))

Draftsman: Marco Cappato



## PROCEDURE

The Committee on Industry, External Trade, Research and Energy appointed Marco Cappato draftsman at its meeting of 4 June 2002.

It considered the draft opinion at its meeting(s) of ....

At the latter/last meeting it adopted the following amendments by ... votes to ..., with ... abstention(s)/unanimously.

The following were present for the vote: ... chairman/acting chairman; ... vice-chairman; ..., vice-chairman; ... draftsman; ..., ... (for ...), ... (for ... pursuant to Rule 153(2)), ... and ... .

## SHORT JUSTIFICATION

The proposal for a framework decision on attacks against information systems seeks to ensure that such attacks are punishable by penalties including a custodial sentence with a maximum term of imprisonment of no less than one year, so as to bring into play the instruments of European police and judicial cooperation and various forms of extraterritorial jurisdiction.

In the case of such specific measures as these, however, it is necessary to ensure that the approximation of laws does not violate basic legal principles or criminalise individuals' conduct solely by virtue of the use of new technologies. The principle of technological neutrality, which already exists in EU law, should not be interpreted solely as requiring non-discrimination as regards the use of one type of technology as opposed to another, but also as preventing a given activity from being criminalised merely because it involves the use of technology. Care should be taken, therefore, to ensure that the legislation targets the offence (be this a terrorist attack, theft, violation of privacy, vandalism, or some other offence) rather than the means whereby it is committed.

That approach would also make it possible to establish a clear distinction between, on the one hand, forms of 'on-line' political activity, civil disobedience, demonstrations and activities of little or no consequence (some of which might be covered by the term 'hacking') and, on the other hand, 'cracking', violent action directed not only against property, but also against physical persons. To ensure that the legislation can make such distinctions without having to keep up with every technological advance, it must be confined to a few precise rules based as closely as possible on general legal principles and the rules governing 'off-line' activities.

It is not acceptable to oblige Member States to impose criminal penalties on activities which are already adequately regulated (such as violation of privacy) or which are permissible and tolerated in any democratic country, or indeed which deserved to be recognised as contributing to the public good, even if they involve actions which might be covered by the term 'attacks against information systems'. For example, action to combat censorship and disinformation which involves interference in, or sabotage of, the means used to repress individuals or whole nations.

If Member States are to be required to treat attacks against information systems as criminal offences, it is not appropriate to rely on the powers of individual judges to assess the facts, and the specific circumstances, of each case. It is essential to include in the proposed framework decision explicit references to fundamental rights and freedoms, and to reaffirm, in line with the subsidiarity principle, that Member States may include in their own legislation exemption clauses which may be applied without thereby infringing the law of the European Union.

The draftsman considers that, unless the proposed amendments – particularly those to Articles 1, 3 and 4 – are adopted, the proposed framework decision could not be regarded as a positive step in terms of extending into the realm of cyberspace the 'area of freedom, security and justice' which is the objective of the European Union's cooperation in the field of justice and home affairs.

## AMENDMENTS

The Committee on Industry, External Trade, Research and Energy calls on the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Text proposed by the Commission<sup>1</sup>

Amendments by Parliament

Amendment 1  
Recital 13 a (new)

*(13a) 1. The protection of information systems is a key element in the creation of an area of freedom, security and justice, but it must be remembered that such systems can also be used – particularly by the machinery of dictatorial, authoritarian or totalitarian governments – as a means of repressing fundamental freedoms and imposing censorship; it is necessary, therefore, in line with the subsidiarity principle, to exclude from the scope of this directive, and leave within the purview of national legislation, attacks against, or illegal interference in, information systems in the event of such systems being used for purposes which are inimical to fundamental rights and freedoms, and hence to protect interests that are not legitimate;*

*2. Also, activities which, under national law, are regarded as being of little or no consequence or are not regarded as punishable offences, or to which the excuse of justification applies, should be exempted explicitly from obligatory criminal penalties, and hence should be excluded from the scope of this framework decision;*

---

<sup>1</sup> OJ C.

*Justification*

*See Articles 3 and 4*

Amendment 2  
Recital 13b (new)

***(13b) It is necessary to uphold the principle of the technological neutrality of the law in relation to personal conduct, and to that end it is of crucial importance to ensure that no forms of behaviour that are not regarded as offences in the real world – such as non-violent demonstrations carried out in accordance with common law – may be regarded as offences solely because they involve the use of digital technology;***

*Justification*

*The principle of technological neutrality is often referred to as a fundamental principle of EU legislation on the new technologies in order to avoid discriminating against the use of any specific technology; this principle should also be extended to cover the relationship between ‘on-line’ and ‘off-line’ technologies. A particularly important example is provided by the freedom to demonstrate, in view of the risk that a demonstration held in cyberspace – which, like a demonstration ‘in the real world’ may also generate a certain amount of ‘acceptable’ inconvenience – could be criminalised solely on the grounds that information systems are involved.*

Amendment 3  
Article 1

The objective of this Framework Decision is to ***improve co-operation between judicial and other competent authorities, including the police and other specialised***

The objective of this Framework Decision is to ***approximate the*** rules on criminal law in the Member States in the area of attacks against information systems. ***This***

*law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.*

*Framework Decision respects the fundamental rights and freedoms and upholds the principles recognised, in particular, by the European Convention on Fundamental Human Rights and Freedoms and the case law of the European Court of Human Rights, the Charter of Fundamental Rights of the European Union and national and international law on human rights and fundamental freedoms.*

#### *Justification*

*The specific objective of this Framework Decision, like other similar initiatives, is to approximate laws while at the same time guaranteeing minimum standards with regard to respect for fundamental rights and freedoms, with particular reference to the potential impact of the Framework Decision on freedom of opinion, expression, demonstration and association. It is therefore necessary to refer explicitly not only to the European Convention on Human Rights, but also to the case law of the Strasbourg Court of Human Rights. Improved cooperation between the competent authorities is only one of the effects the Framework Decision would have.*

#### *Amendment 4*

#### *Article 2, letters (f) and (g)*

*(f) ‘Authorised person’ means any natural or legal person who has the right, by contract or by law, or the lawful permission, to use, manage, control, test, conduct legitimate scientific research or otherwise operate an information system and who is acting in accordance with that right or permission.*

*Deleted*

*(g) ‘Without right’ means that conduct by authorised persons or other conduct recognised as lawful under domestic law is excluded.*

*Deleted*

### *Justification*

*The definitions of 'authorised person' and 'without right' are not included in the Council of Europe's Convention on Cybercrime. In particular, the definition of 'authorised person' implies that it is necessary to obtain specific authorisation to access information systems on every occasion, in defiance of the liberal principle that everything that is not prohibited is permitted. It would be much better to use the term 'unlawful conduct', which is generally used to define conduct that infringes national or international law.*

### Amendment 5 Article 3

Member States shall ensure that the intentional access, ***without right***, to the whole or any part of an information system is punishable as a criminal offence where it is committed:

- (i) against any part of an information system which is subject to specific protection measures; or
- (ii) with the intent to cause damage to a natural or legal person; or
- (iii) with the intent to result in an economic benefit.

Member States shall ensure that intentional ***illegal*** access to the whole or any part of an information system is punishable as a criminal offence where it is committed:

- (i) against any part of an information system which is subject to ***appropriate*** specific protection measures ***based on the protection of legitimate rights and interests***; or
- (ii) with the intent to cause damage to ***the legitimate rights and interests of*** a natural or legal person; or
- (iii) with the intent to result in an economic benefit ***by fraudulent means***.

### *Justification*

*The obligation to regard as a criminal offence access 'without right' to information systems should not be extended to activities of little or no consequence (which would not be punished if they were carried out 'off line', i.e without using new technologies) or to activities that could be regarded as a form of self-defence or civil disobedience directed against systems being used to the detriment of fundamental freedoms and rights. The subsidiarity principle demands that we avoid imposing binding, criminalising measures at European level.*

### Amendment 6

Article 3, paragraph 1a (new)

***1a. The following do not fall within the scope of the Framework Decision, and so remain within the purview of the Member States' domestic law:***

***-minor or trivial conduct;***

***-activities which are not regarded as punishable offences or to which the excuse of justification applies under national law;***

***-access to information systems used in breach of fundamental freedoms and rights.***

*Justification*

*See justification to Amendment 5*

Amendment 7  
Article 4

Member States shall ensure that the following intentional conduct, ***without right***, is punishable as a criminal offence:

- (a) the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;
- (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

Member States shall ensure that the following intentional ***unlawful*** conduct is punishable as a criminal offence:

- (a) the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;
- (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

*Justification*

*See justification to Amendment 5*

Amendment 8  
Article 4, paragraph 1a (new)

***1a. The following do not fall within the scope of the Framework Decision, and so remain within the purview of the Member States' domestic law:***  
***-minor or trivial conduct;***  
***-activities which are not regarded as punishable offences or to which the excuse of justification applies under national law;***  
***-access to information systems used in breach of fundamental freedoms and rights.***

*Justification*

*See justification to amendment 5*

Amendment 9  
Article 7, paragraph 1, letters (b) and (c)

(b) the offence caused, or resulted in, ***substantial direct or indirect economic loss***, physical harm to a natural person or substantial damage to part of the critical infrastructure of the Member State;  
(c) ***the offence resulted in substantial proceeds; or***

(b) the offence caused, or resulted in, physical harm to a natural person or substantial damage to part of the critical infrastructure of the Member State;

***Deleted***

*Justification*

*The principle that an offence that gives rise to substantial economic loss or substantial proceeds should be regarded as a separate offence (and attract penalties up to four times*

*greater) would be a completely new development in criminal law. Such a novel concept would be as dangerous as it was discriminatory in terms of the economic circumstances of those committing an offence and those against whom it was committed. The question of compensation, which is obviously linked to any economic damage sustained or profit obtained, is a different matter altogether.*

Amendment 10  
Article 10, paragraph 1, letter (a)

***(a) exclusion from entitlement to public benefits or aid;***                      ***Deleted***

*Justification*

*Criminal judges cannot usually impose this kind of sanction, which are the exclusive prerogative of the administrative courts.*