COUNCIL OF THE EUROPEAN UNION

Brussels, 24 February 2011

6776/11

Interinstitutional File: 2010/0273 (COD)

LIMITE

DROIPEN 12
TELECOM 14
CODEC 263

NOTE

from:	Presidency
to:	Working party on Substantive Criminal Law
No. prev. doc.:	5528/11 DROIPEN 6 TELECOM 9 CODEC 79 6004/11 DROIPEN 8 TELECOM 11 CODEC 147
Subject:	Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, repealing Council Framework Decision 2005/222/JHA

I. GENERAL INFORMATION

A general exchange of views and a first detailed examination of the proposal for the Directive on attacks against information systems was concluded by the Working Party on Substantive Criminal Law (hereinafter DROIPEN) at its meetings on 13-14 and on 28 January 2011. On 28 January 2011 DROIPEN addressed some policy issues[1] in order to enable the Presidency to work on the drafting of the instrument. At that meeting, delegations expressed their views on a number of options which had appeared from the discussions so far, related in particular to the application of the directive to minor cases, the level of penalties, the scope of Article 7 "Tools used for committing offences", the structure and content of Article.10 "Aggravating circumstances" and the rules of jurisdiction set out in Article 13.

[1] Set out in doc. 5528/11 DROIPEN 6 TELECOM 9 CODEC 79.

On two occasions, the Commission proposal was referred to CATS for guidance on specific issues. First on some general issues[2] prior to the technical discussions in the Working Party on 13 December 2010, secondly on 11 February in relation to Article10 (3)[3]. CATS was also informed about the state of the discussions conducted so far.

Delegations were invited to submit their drafting proposals by 15 February 2011, while taking into account the outcome of the debate so far. The written contributions submitted by delegations to that end have been given a thorough consideration, and the Presidency sought to reflect as many of them as possible in the revised version of the proposal found in the Annex to this note with a view to providing a coherent basis for bringing the discussions forward. The positions of delegations are available in doc. 6841/11.

UK and IE participate in the adoption of the Directive. DK does not take part in the adoption of this instrument. UK has a Parliamentary scrutiny reservation. DE, SI, LT, FR and SE entered a general scrutiny reservation on the proposal.

The DROIPEN meeting of 2-3 March will be used for drafting on the basis of the text found in the annex, starting by Article 1. The outstanding issues set out below will be discussed together with the Article to which they are relevant. The recitals will be discussed only in so far as they are relevant from the point of view of a specific drafting problem raised during the meeting. The section below is provided as a preliminary indication as to how the Presidency sees the evolution of the debate.

[2] 17500/10 DROIPEN 146 TELECOM 147 CODEC 1464.
[3] 6004/11 DROIPEN 8 TELECOM 11 CODEC 147.

II. SPECIFIC ISSUES

1. Minor cases and scope of criminalization

Following a detailed examination of this issue, it appeared that an emerging majority of delegations were of the opinion that the reference to "at least for cases which are not minor" in Articles 3-5 of the proposal should be maintained. Therefore the directive will maintain the discretion of Member States to criminalise, or not, these cases in accordance with their national legal systems. This option leaves certain margin of manoeuvre for not imposing a criminal penalty in a particular case or imposing a sanction below the minimum threshold. The assessment whether the case is minor shall be made by taking into account the particular circumstances of the case.

It also emerged from the discussions that the definition of a notion of a "minor case" should not be included in the main text. In order to avoid uncertainty in that matter, some Member States suggested that this notion should be clarified at least in a recital and the majority of delegations indicated their flexibility in this regard.

Subject to further comments, the Presidency has submitted the following proposal for a recital:

"The case may be considered minor when, notwithstanding the fact that the behaviour fulfils the constituent elements of the offence, the damage and/or the risk it carries to public or private interests, such as the integrity of a computer system or computer data, or a person's integrity, rights and other interests, is so insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold is not necessary."

Delegations are invited to indicate their own ideas as to the acceptable drafting of such recital when discussing Article 3.

2. Penalties

Some delegations confirmed their opposition to the suggested levels of penalties in the draft Directive. At the same time, the Presidency noted an open attitude to examining the solution suggested by the general approach of the Council on the Draft Directive on combating the sexual abuse, sexual exploitation of children and child pornography (doc.17583/10), namely to provide for a list of sanctions for the different offences, taking into account the seriousness and pertinent characteristics of the criminal act.

It should also be noted that in the course of the discussions on aggravating circumstances, a number of delegations indicated that the structure of the provision should provide for enough flexibility in order for the proposed aggravating elements to be dealt with either by providing for a higher level of penalty or by indicating that they should be resulting in a penalty towards the maximum level envisaged for the general offence under their respective national law.

In the light of these conclusions, the Presidency suggests that those two aspects of the issue be addressed together. Instrumental in this regard would be the model of Article 4 of the THB Directive, which provides for a comprehensive structure of the provision on penalties, including both the general levels of penalties and the aggravated special circumstances linked to the general offence resulting in higher penalties (see Article 4 (3)), as well as indication of those elements that should be considered as aggravating in the determination of the actual punishment by the courts without envisaging a specific threshold of penalties in the directive.

The aim of this suggestion is to offer a structure which will provide a common framework for the penalties envisaged for a variety of offences contained in the directive. For the purposes of testing this approach, Articles 9 and 10 of the initial COM proposal have been merged but the general wording and the levels of sanctions have been retained provisionally. This question will be addressed as part of the debate on Article 9.

3. Aggravating circumstances in the former Article 10 (3)

At its meeting on 11 February, CATS was called to confirm that the use of identification data without right while causing prejudice to the legitimate interests of the rightful owner is directly linked to various forms of cyber attacks covered by the scope of the draft directive and therefore should be addressed as an aggravating element. A number of delegations indicated that this element should be distinguished from an identity theft, which is a complex phenomenon of a partially different nature. At the same time, as far as cyber attacks were concerned, this modus operandi was perceived as a pertinent issue by most delegations. Some other delegations still expressed their concerns on disconnecting the criminal behaviour referred to in Article 10 (3) from identity theft. The COM reiterated its position and indicated that Article 10 (3) had not been aimed at legislating on the phenomenon of identity theft, but had been introduced because of its direct implication in increasing the gravity of the relevant cyber attacks. In the Commission's view it is necessary to respond to the increasing threat posed in practice by the misuse of identification data. CATS concluded that the discussions on the issue should continue in the working party, where it should be examined in detail with a view a further clarification and possible adaptation of the wording to be sought.

The Presidency would like to bring to the attention of delegations once again the nature of the problem and the modi operandi of this type of cyber attacks, as contained in document no. 6004/11. The suggested wording of this provision as contained in the Annex (new Article. 9 (4)b)), seeks to bring clarity on this issue, while taking into account the written contributions received by delegations.

4. Jurisdiction (Article 13)

A clear majority of delegations were in favour of applying the rules of jurisdiction as laid down in the THB directive. The Presidency has also taken note of the positions of some delegations that this solution should be adapted to the specific subject of this Directive. The latter is the rationale for the proposed wording to that end found in the annex.

5. Ensuring consistency in EU substantive criminal law instruments

In conformity with the guidance from CATS (doc. 18057/10) and following the meeting of the jurist linguists on the Directive on Trafficking in Human Beings held on 18 February 2011, the Presidency has brought some of the provisions in this proposal into a standard wording, in line with the respective provisions of the Directive on Trafficking in Human Beings. A clear indication of those changes is found in the footnotes in the Annex.

_____

2010/0273 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and repealing Council Framework Decision 2005/222/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular

Article 83(1) thereof,

Having regard to the proposal from the European Commission[4],

After transmission of the draft legislative act to the national Parliaments,

Having regard to the opinion of the European Economic and Social Committee,

Having regard to the opinion of the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The objective of this Directive is to approximate rules on criminal law in the Member States in the area of attacks against information systems, and improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States.

(2) Attacks against information systems, in particular as a result of the threat from organised crime, are a growing menace, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. This constitutes a threat to the achievement of a safer information society and an area of freedom, security and justice, and therefore requires a response at the level of the European Union.

[4] OJ C […], […], p. […].

(3) There is evidence of a tendency towards increasingly dangerous and recurrent large scale attacks conducted against information systems which are critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated tools that can be used by criminals to launch cyber-attacks of various types.

(4) Common definitions in this area, particularly of information systems and computer data, are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(5) There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

(6) Member States should provide for penalties in respect of attacks against information systems. The penalties provided for should be effective, proportionate and dissuasive.

(7) It is appropriate to provide for more severe penalties when an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime[5], when the attack is conducted on a large scale, or when an offence is committed by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner. It is also appropriate to provide for more severe penalties where such an attack has caused serious damage or has affected essential interests.

(8) The Council Conclusions of 27-28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention.

(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive shall refer to 'tools' that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including botnets, used to commit cyber attacks.

(10) This Directive does not intend to impose criminal liability where the offences are committed without criminal intent, such as for authorised testing or protection of information systems.

[5] OJ L 300, 11.11.2008, p. 42.

(11) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis to exchange information in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to information systems and data, or for the collection of evidence in electronic form of a criminal offence. Given the speed with which large-scale attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. Such assistance should include facilitating, or directly carrying out, measures such as: the provision of technical advice, the preservation of data, the collection of evidence, the provision of legal information, and the locating of suspects.

(12) There is a need to collect data on offences under this Directive, in order to gain a more complete picture of the problem at Union level and thereby contribute to formulating more effective responses. The data will moreover help specialised agencies such as Europol and the European Network and Information Security Agency to better assess the extent of cybercrime and the state of network and information security in Europe.

(13) Significant gaps and differences in Member States' laws in the area of attacks against information systems area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a trans-border dimension, thus underlining the urgent need for further action to approximate criminal legislation in this area. Besides that, the coordination of prosecution of cases of attacks against information systems should be facilitated by the adoption of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings.

(14) Since the objectives of this Directive, i.e. ensuring that attacks against information systems are punished in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, as rules have to be common and compatible, and can therefore be better achieved at the level of the Union, the Union may adopt measures in accordance with the principle of subsidarity as set out in Article 5 of the Treaty on European Union. This Directive does not go beyond what is necessary in order to achieve those objectives.

(15) Any personal data processed in the context of the implementation of this Directive should be protected in accordance with the rules laid down in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[6] with regard to those processing activities which fall within its scope and Regulation (EC) No. 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[7].

---

[6] OJ L 350, 30.12.2008, p.60.

[7] OJ L 8, 12.1.2001, p. 1.

(16) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, including the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for these rights and principles and must be implemented accordingly.

(17) [In accordance with Articles 1, 2, 3 and 4 of the Protocol on the position of United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on the Functioning of the European Union, the United Kingdom and Ireland have notified their wish to participate in the adoption and application of this Directive] OR [Without prejudice to Article 4 of Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, the United Kingdom and Ireland will not participate in the adoption of this Directive and will not be bound by or be subject to its application].

(18) In accordance with Articles 1 and 2 of Protocol on the position of Denmark annexed to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is therefore not bound by it or subject to its application.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive defines criminal offences in the area of attacks against information systems and establishes minimum rules concerning penalties for such offences. It also aims to introduce common provisions to prevent such attacks and improve European criminal justice cooperation in this field.[8]

8 ES entered a scrutiny reservation.

Article 2

Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) "information system" means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance;

(b) "computer data"[9] means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

(c) "legal person" means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations;

(d) "without right" means performing an act[10] not authorised by the owner, other right holder of the system or of part of it[11], or not permitted under national legislation.

---

9 IE suggested to delete "computer" from the definition of "computer data" in order to take into account the new technological developments, pointing out that there are already in existence many so-called smart devices which would fall within the definition of an information system but which would not normally be described as computers.

10 Amendment introduced upon the request of FR to ensure consistency of the definition with the wording of Art. 6 and 7.

11 FR suggests deletion of the expression " not authorised by the owner, other right holder of the system or of part of it".

Article 3

Illegal access to information systems[12]

Member States shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor[13][14][15].

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor[16][17].

---

12 AT entered a scrutiny reservation.

13 See Item 1 of the Cover note as regards the "cases which are not minor". ES would change this by “at least for serious cases”.

14 DE, AT, FR, CZ, LV, ES, LT requested the possibility under Art. 2 (2) of the FD 2005/222/JHA allowing Member States to require in addition the offence to be committed by infringing a security measure to be retained.
The following wording is suggested in this regard:
Member States shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least <u>if the offence is committed by infringing security measures and</u> for cases which are not minor.

15 UK suggests to add the following: <u>"and where at the time of the action the perpetrator knows that the action is unauthorised."</u>

16 See Item 1 of the Cover note as regards the "cases which are not minor".

17 See footnote 17.

Article 5

Illegal data interference[18]

Member States shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor[19][20].

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that the intentional interception by technical means, of non-public transmissions of computer data to, from or within[21] a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed without right[22].

---

18 RO raised the question whether the "unauthorised transfer of data" is covered by Art. 5, and considered it necessary to introduce a new paragraph: *"The unauthorized transfer of data from an information system or from an information data storing device is punishable as a criminal offence when committed without right."*

19 See Item 1 of the Cover note as regards the "cases which are not minor".

20 See footnote 17.

21 UK suggests the expression "or within" to be removed.

22 ES suggested to include additional qualifiers, such as "dishonest intent".

Article 7

Tools used for committing offences[23][24]

(1) Member States shall take the necessary measures to ensure that the production, sale, procurement for use[25], import, […], distribution or otherwise making available of the following[26] is punishable as a criminal offence when committed intentionally and without right:

(a) device, including a[27] computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6.[28]

---

23 SK and UK entered scrutiny reservations.

24 DROIPEN confirmed the interpretation of the scope of this provision suggested in item 3 of the cover note of doc. 5528/11 and called for more synergies with the structure and approach of the respective provision of the CoE Convention on Cybercrime. The Presidency has therefore amended the provision accordingly.

25 RO have a scrutiny reservation on the expression "procurement for use".

26 UK suggests the following wording:
"Member States shall take the necessary measure to ensure that the production, sale, procurement for (…) supply, import for supply, possession with a view to supply, distribution or otherwise making available of the …"

27 DE suggest deletion of the following: "device, including a".

28 PL suggested this addition in its written comments.

(2) Member States shall take the necessary measures to ensure that the possession[29] of any item referred to in paragraph 1, with the intent that it be used to commit any of the offences referred to in Articles 3 to 6 is punishable as a criminal offence when committed intentionally and without right.[30]

Article 8

Inciting , aiding, abetting and attempting[31]

1. Member States shall ensure that the inciting, aiding and abetting to commit (…)an offence referred to in Articles 3 to 7[32] is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit (…) an offence referred to in Articles 3 to 6 is punishable as a criminal offence[33].

Article 9

Penalties[34]

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

---

29 DE and AT entered a reservation on the absence of possibility the Member States to reserve the right not to apply Art. 7 under certain conditions, as provided in Art. 6(3) of the Budapest Convention. In this regard DE suggests to move out the provision as relates to "possession".

30 LT suggested that similarly to Art. 6 (1)(b), last sentence of the Budapest convention a the criminalisation of possession to be linked to a minimum number of items referred to in this article.

31 The provision has been brought in line with the wording of the THB Directive

32 FR entered a scrutiny reservation as regards the scope of the provision.

33 DE and SI entered reservation on the mandatory incrimination of attempt resulting from the suppression of the possibility for reservations in this respect provided for in the FD 2005/222/JHA.

34 See item 2 of the Cover note. The positions of delegations on the level of penalties and the exact scope of the provision will be considered depending on the outcome of the discussions on the suggested structure of the provision.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum penalty of at least two years of imprisonment[35].

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum penalty of at least five years of imprisonment[36] when committed within the framework of a criminal organization as defined in Framework Decision 2008/841/JHA.

4. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by a maximum penalty of at least five years of imprisonment[37] when committed in any of the following circumstances:

(a) through the use of a tool designed to launch attacks affecting a significant number of information systems, or attacks causing considerable damage, such as disrupted system services, financial cost or loss of personal data[38].

---

35 Brought in line with THB Directive.

36 Brought in line with THB Directive.

37 Brought in line with THB Directive.

38 A number of delegations called for rewording of this provision in order to use technologically neutral language. Some raised doubts as for the expression "*through the use of a tool designed to"* would limit the scope of criminalisation beyond reason.
UK suggests the following wording instead: *when a tool is used in order to intentionally.*
FR suggested a similar wording to be included in the original Article 10 para (3) but referred to "third parties".
Alternately the following wording could be considered aiming at providing a technologically neutral provision, which would allow to prosecute large scale attacks regardless of the means used:
(4) Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6 are punishable by criminal penalties of a maximum term of imprisonment of at least five years when committed in any of the following circumstances:
(a) when affecting a significant number of information systems or causing considerable damage, such as disrupted system services, financial cost or loss of personal data.

(b) by using the identity of another person or of any individual which enables that person to be identified, whereby concealing the real identity of the perpetrator [and resulting in considerable damage or affecting essential interests][39]

5. In so far as the following circumstances do not already form part of the constituent elements of the offences referred to in Art. 3 to 7[40], Member States shall take the necessary measures to ensure that the fact that an offence referred to in this Directive has caused considerable damage or has affected essential interests is regarded as an aggravating circumstance.

(…)

Article 11

Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8[41], committed for their benefit by any person, acting either individually or as part of an organ of the legal person, and having a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

---

39 See Item 3 of the Cover Note. CZ, DE, DK, ES, IE, UK entered scrutiny reservation in written comments.

40 DE and UK would like to limit the application of the former version of clause to Articles 4-5.

41 SI expressed misgivings as regards the extension of the liability of legal persons to Art. 8 in relation to the lack of possibility for reservations on criminalising the attempt.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators of, inciters[42], or accessories to, any of the offences referred to in Articles 3 to 8.

Article 12

Penalties on legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 11(1) is punishable by effective, proportionate and dissuasive penalties, which shall include criminal or non-criminal fines and may include other sanctions, for example:
   (a) exclusion from entitlement to public benefits or aid;
   (b) temporary or permanent disqualification from the practice of commercial activities;
   (c) placing under judicial supervision;
   (d) judicial winding-up;
   (e) temporary or permanent closure of establishments which have been used for committing the offence.
2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 11(2) is punishable by effective, proportionate and dissuasive penalties or measures.

[42] Brought in line with THB Directive.

Article 13
Jurisdiction

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

(a) in whole or in part within the territory of the Member State concerned; or

(b) by one of their nationals[43] (…)

(…)

2. When establishing jurisdiction in accordance with paragraph 1(a), Member States shall ensure that the jurisdiction includes cases where:

(a) the offender commits the offence when physically present on the territory of the Member State concerned, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on the territory of the Member State concerned, whether or not the offender commits the offence when physically present on its territory.

3. Member States shall inform the Commission where they decide to establish further jurisdiction over an offence referred to in Articles 3 to 7 committed outside of their territory e.g. where:

a) the offender has his or her habitual residence in the territory of that Member State; or

b) the offence is committed for the benefit of a legal person established in the territory of that Member State.

[43] FR would like the extension of the national jurisdiction to nationals to be put on the condition that the offence is punishable under the criminal law of the country, where it was committed. The Presidency is of the opinion that such an option may be considered only if the offence has been committed in a third country, outside the territory of the EU, and on condition there have not been consequences for any EU MS. ES and UK suggests deleting the jurisdiction based on nationality, while PL would make it conditional upon double criminality.

Article 14

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, and in accordance with data protection rules[44], Member States shall make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that they can [respond within a maximum of eight hours to urgent requests.[45] Such response shall at least indicate whether and in what form the request for help will be answered and when.

2. Member States shall inform the Commission of their appointed point of contact for the purpose of exchanging information on the offences referred to in Articles 3 to 8. The Commission shall forward that information to the other Member States.

---

[44] UK suggests to delete the expression " in accordance with data protection rules", since it has been already covered by recital 15 of the Data protection FD(2008/977/JHA).

[45] The majority of delegations expressed reservations as regards the specific time limit for responding to urgent requests. BE, FR, NL, UK, RO indicated a positive attitude, whereas a clarification of the type of cooperation referred to in this provision was required. COM clarified that the period of eight hours refers to the obligation of the requested state to at least respond as to whether it would be in a position to provide assistance.
DE suggests the following wording:
Member States shall also ensure that they have procedures in place so that they can ***indicate*** within a maximum of ***24*** hours ***in*** urgent requests ***(…)*** at least ***(…)*** whether and in what form the request for help will be answered and when.

Article 15

Monitoring and statistics[46]

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to 8.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover the number of offences referred to in Articles 3 to 8 reported to the Member States and the follow-up given to these reports[47], and shall indicate on an annual basis the number of reported cases investigated, the number of persons prosecuted, and the number of persons convicted for the offences referred to in Articles 3 to 8.

3. Member States shall transmit the data collected according to this Article to the Commission. They shall also ensure that a consolidated review of these statistical reports[48] is published.

---

46 AT, IT, ES, PT and PL entered scrutiny reservations. A number of general issues were raised by delegations, among which the categories of data, subject to reporting obligation, the comparability of data, the role of Europol in collecting statistical data. The following alternative wording suggested by DE could be considered:

Article 15
Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to ***7***.

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover the number of offences referred to in Articles 3 to **7** ***registered by*** the Member States ***(…)*** and the number of persons convicted for the offences referred to in Articles 3 to ***7***.

3. Member States shall transmit the data collected according to this Article to the Commission. ***The Commission*** shall ***(…)*** ensure that a consolidated review of these statistical reports is published.

47 EE and RO raised a question as regards the meaning of "follow-up".

48 FR asked for clarification of the obligation to provide a consolidated review of the statistical reports.

Article 16

Replacement of Framework Decision 2005/222/JHA[49]

Framework Decision 2005/222/JHA is hereby replaced, without prejudice to the obligations of the Member States relating to the time limits for transposition of the Framework Decision into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision 2005/222/JHA shall be construed as references to this Directive.

Article 17

Implementation [50]

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by [two years from adoption] at the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table[51] between those provisions and this Directive. When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

---

49 Brought in line with the respective provision of the Directive on Trafficking in Human Beings.

50 The title has been brought in line with the respective provision of the Directive on Trafficking in Human Beings.

51 This is a horizontal issue which will be addressed by the Presidency in accordance with and subject to a decision of COREPER in this respect.

Article 18

Reporting[52]

1. By [FOUR YEARS FROM ADOPTION] (…)[53], the Commission shall submit a report to the European Parliament and the Council on the application of this Directive in the Member States including any necessary proposal.

2. Member States shall send to the Commission all the information that is appropriate for drawing up the report referred to in paragraph 1. The information shall include a detailed description of legislative and non-legislative measures adopted in implementing this Directive.

Article 19

Entry into force[54]

This Directive shall enter into force on the (…)day (…) of its publication in the *Official Journal of the European Union*.

Article 20

Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

_____

[52] DE proposed the deletion of this article.
[53] Brought in line with THB upon request of FR, DE, NL, ES, UK.
[54] This provision was brought in line with the respective provision of the Directive on Trafficking in Human Beings.