COUNCIL OF THE EUROPEAN UNION

Brussels, 23 March 2011

7837/11

Interinstitutional File: 2010/0273 (COD)

LIMITE

DROIPEN 21
TELECOM 28
CODEC 431

NOTE

from:	Presidency
to:	Working party on Substantive Criminal Law
No. prev. doc.:	6776/11 DROIPEN 12 TELECOM 14 CODEC 263
Subject:	Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, (…) replacing[1] Council Framework Decision 2005/222/JHA

I. GENERAL INFORMATION

At its meeting on 2-3 March 2011, DROIPEN concluded a second reading of the proposal, and examined a number of drafting suggestions, submitted either by the Presidency or by the delegations[2].

The discussions of DROIPEN highlighted a number of outstanding issues. The Presidency subsequently submitted four questions to CATS for further guidance with a view to examining the possibilities to finalize the draft in the Working Party at this stage of the negotiations[3].
The objective of the Presidency during the DROIPEN on 29 of March is to conclude a third reading of the articles of the proposal, while identifying those provisions that may gather sufficient support in order to bring them to the attention of the Justice and Home Affairs Council for at least a partial general approach.

1 Brought in line with the wording of Art. 15. See item 3 of the Cover note.
2 6776/11, 6841/11, 7111/11, DS 1153/11, DS 1154/11, DS 1157/11, DS 1158/11.
3 See doc. 7517/11.

The Working Party on 29 March will briefly examine the amendments and reservations brought to the main text starting by Article 1; however, the provisions indicated under “Specific issues” will be dealt with separately and in a detailed manner. Delegations are invited to consider withdrawing reservations wherever possible. To facilitate the discussions, the suggestions for recitals, as long as they concern clarification of the main provisions, will be examined together with the main text and are therefore included in footnotes. The respective provisions are equally inserted in the preamble in order to indicate their place in the text.
After the discussion in the DROIPEN, the amended draft will be presented to COREPER on 7 April in order to prepare the Council meeting.

II. SPECIFIC ISSUES

1. Article 9 - Penalties

1. 1. The compromise proposal

Following the guidance of CATS on the issues presented in 7517/11, the Presidency suggests a compromise consisting of the following elements:

- The reference to "minor cases" shall be extended to all offences referred to in the Directive (Article 3 to Article 7). Therefore the minor cases are entirely excluded from the scope of the Directive.
- The scope of Article 3 "Illegal access to information systems" is limited to cases in which the infringement of a security measure is a constituent element of the offence.
- The Commission's proposal related to the level of penalties of the basic offences - maximum of at least two years of imprisonment is maintained.

Delegations are invited to confirm the Presidency proposal.

1.2. General structure and level of penalties

In its proposal, the Presidency draws on the suggested structure and the catalogue of various levels of penalties put forward in DS 1157/11, which gained a substantial support at the last meeting of the Working Party. The document also reflects the positions expressed by delegations on the material aspects of Article 9.

1.3. Misuse of identity data of another person - Article 9 (5)

The Presidency has taken note of the consistently expressed views of a number of delegations that the aggravating circumstance relating to the misuse of identification data of another person shall not form part of this directive. The Presidency equally noted the support of another group of delegations arguing in favour of retaining the concept of an identity related aggravating circumstance in committing cyber attacks.

Taking into account the serious threat which this type of cyber-attack poses for the general public, business and public entities, the Presidency would like to explore further with delegations the possibility to keep this element of the Commission proposal, while rewording the text in order to respond to the call of delegations for a precise and clearly defined scope of the provision. The suggested wording to that end (currently found in Article 9 (5)), builds upon the written submissions of delegations, while aiming to define the constituent elements of the offence in an as comprehensive manner as possible.

The Presidency would like to invite delegations to consider accepting Article 9 (5).

2. Exchange of information - Article 14.

Most delegations insisted on the fact that Article 14 should be further clarified. Some argued that it should be clearly indicated that this provision regulates swift reaction in the framework of police cooperation as opposed to judicial cooperation. A further clarification on the nature of the obligation of the competent authorities imminently responding to such requests was also examined. Delegations are invited to consider that a similar position – without the latter addition – appeared in the framework decision.

Insofar as the definition of the competences of the 24/7 contact points are not subject of this Directive, the Presidency is of the opinion that it is not necessary to predefine the type of cooperation and the exchange channels that may be used. According to Article 14, the obligation of the Member States is to ensure that the contact points are operational and adequately equipped to respond to urgent requests. As long as these objectives are fulfilled, the Member States should be free to decide the procedures and the specific functions of the 24/7 contact points in accordance with their national law. Therefore only an indication of the type of competences of the contact points could be provided in the recitals to the Directive, as indeed contained in the initial proposal (see recital 11). In addition, the Presidency suggests a further clarification of the issue, as indicated in the footnotes to the note.

Another issue which is subject of a debate concerns the deadline in which Member States have to react at least by indicating whether they will be able to respond to the request.

Delegations are invited to accept the deadline of 8 hours, taking into account the additional elements included in the current version of the text aiming to clarify further the type of answer that is requested under Article 14.

3. Ensuring consistency in EU substantive criminal law instruments

In conformity with the guidance given by CATS (doc. 18057/10) a number of provisions in this proposal has been brought into a standard wording, in line with the respective provisions of the Directive on Trafficking in Human Beings (hereinafter THB Directive), following the lawyer-linguists check (PE-CONS 69/10).

In this respect, Article 16 refers currently to the replacement of Framework Decision 2005/222/JHA and the wording was modelled after Article 21 of the THB Directive. This amendment implies further changes in the heading of the draft proposal (see footnote 1) and the insertion of the following recital in line with recital 30 of the THB Directive:

This Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA. Since the amendments to be made are of substantial number and nature, the Framework Decision should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive.

Delegations are invited to agree on this wording, without prejudice to the discussions in relation to other instruments under consideration in the Council preparatory bodies.

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 **(…)** 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. […].

(2a) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. It emerges from the need to increase the critical infrastructure protection capability in Europe that the fight against the attacks against information systems should be complemented by serious criminal sanctions reflecting the gravity of such attacks. For the purposes of this directive, critical infrastructure means an asset, system or part thereof located in Member States which is essential for instance for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(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.

(6a) The directive provides for criminal sanctions at least for cases which are not minor. Member States shall determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, 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.

(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.

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

(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.

(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, including with a view to collecting evidence in electronic form (…).(…) Such assistance may include, for instance, 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, (…) the locating of suspects. 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. In such cases, it may be expedient that the request for assistance is accompanied by a telephone contact , in order to ensure that it will be processed swiftly by the requested state within the limit of 8 hours.

(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].

(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 (…)

(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.

(19) This Directive aims to amend and expand the provisions of Framework Decision 2005/222/JHA. Since the amendments to be made are of substantial number and nature, the Framework Decision should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive.

[6] OJ L 350, 30.12.2008, p.60.
[7] OJ L 8, 12.1.2001, p. 1.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter

This Directive establishes minimum rules concerning the definition of criminal offences (…) and the sanctions in the area of attacks against information systems. (…) It also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities [8].

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" 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;

[8] An amendment introduced upon the request of some delegations for greater coherence with the objectives of the Directive. Keeping in mind Article 14, delegations are invited to consider the flexibility in this new drafting as opposed to the original wording: “aims to introduce common provisions to (...) improve European criminal justice cooperation in this field” The current wording takes into account recital 1 of Framework Decision 2005/222/JHA. ES maintained its scrutiny reservation.

(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 access, interference or interception [9] not authorised by the owner, other right holder of the system or of part of it, or not permitted under national legislation.

Article 3

Illegal access to information systems[10][11]

Member States shall take the necessary measures to ensure that when committed intentionally[12] (…), the access without right to the whole or any part of an information system is punishable as a criminal offence, at least when the offence is committed by infringing a security measure [13] and for cases which are not minor

---

[9] FR has requested to introduce the expression "performing an act" in order to ensure consistency of the definition with the wording of Article 6 and 7. This amendment, however, created difficulties to some delegations. In this regard, the Presidency suggests a slight modification on the initial Commission proposal. As an alternative, "access, interference" may be left out.

[10] AT, UK entered a scrutiny reservation.

[11] The majority of delegations in CATS agreed that the notion of minor cases should be clarified in a recital. The following wording was suggested:
The directive provides for criminal sanctions at least for cases which are not minor. Member States shall determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, 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.

[12] Amendment intended to take into account the UK's concerns, as regards the element of "knowledge"/ mens rea. The wording is in line with the Convention on Cybercrime.

[13] Amendment confirmed by CATS at its meeting on 22 March 2011. The insertion of an accompanying recital was not supported by delegations. (see doc. 7517/11)

Article 4

Illegal system interference

Member States shall take the necessary measures to ensure that 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 is punishable as a criminal offence when committed intentionally[14] and without right, at least for cases which are not minor.

Article 5

Illegal data interference[15]

Member States shall take the necessary measures to ensure that the (…) deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed intentionally[16] and without right, at least for cases which are not minor.

---

[14] See the explanation found in the footnote regarding the same amendment in Art. 3.

[15] 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."* However, this proposal was not supported by the other delegations.

[16] See the explanation found in the footnote regarding the same amendment in Art. 3.

Article 6

Illegal interception

Member States shall take the necessary measures to ensure that the (…) interception by technical means, of non-public transmissions of computer data to, from or within[17] a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed intentionally[18] and without right[19], at least for cases which are not minor[20].

Article 7

Tools used for committing offences[21]

(1) Member States shall take the necessary measures to ensure that the production, sale, procurement for use[22], import, (…), distribution or otherwise making available of the following[23] is punishable as a criminal offence when committed intentionally and without right, with the intent that it be used for the purpose of committing any of the offences referred to in Articles 3 to 6[24] at least for cases which are not minor[25]:

---

17 UK suggests the expression "or within" to be removed. This suggestion did not gain support from the other delegations.

18 See the explanation found in the footnote regarding the same amendment in Art. 3.

19 ES suggested to include additional qualifiers, such as "dishonest intent". It was not supported by the other delegations.

20 Insertion agreed by CATS

21 SK and UK entered scrutiny reservations.

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

23 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 …" This proposal was not supported by other delegations.

24 FR and LT asked to move the last part of the sentence to the chapeau.

25 Insertion agreed by CATS

(a) device, including [26] a 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,

(2) Member States shall take the necessary measures to ensure that the possession[27] 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, at least for cases which are not minor[28].

Article 8

Incitement , aiding and abetting and attempt[29]

1. Member States shall ensure that the incitement, aiding and abetting to commit an offence referred to in Articles 3 to 7[30] 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[31].

---

26 DE suggests deletion of the following: "device, including a". SK expressed doubts on this suggestion.

27 DE and AT entered a reservation on the absence of possibility the Member States to reserve the right not to apply Article 7 under certain conditions. Such possibility is envisaged in Art. 6(3) of the Budapest Convention. In this regard DE suggests to delete the provision regarding "possession".

28 Insertion agreed by CATS.

29 The provision has been brought in line with the wording of the THB Directive (PE-CONS 69/10)

30 FR proposed to limit the scope of this provision to Article 3 to 6, in order to avoid a second degree of criminalisation of preparatory acts, which would be the case for example in relation to procurement for use of an access code under Article 7 (1) (b).

31 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. **As a compromise proposal DE suggested to limit the scope of the provision to Articles 4 and 5.**

Article 9

Penalties

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.

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[32].

3. [33] Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 6[34] are punishable by a maximum penalty of at least three years of imprisonment when a tool is intentionally used (…) in order[35] to launch attacks affecting a significant number of information systems, or causing (…) serious[36] damage, such as disrupted system services, financial cost or loss of personal data[37]

---

[32] The approach in relation to the level of penalties of the basic offences was thoroughly discussed by CATS. One group of delegations supported the suggestion to maintain the approach of Framework decision 2005/222/JHA, which provides for maximum penalties of at least between one and three years of imprisonment. Another group argued in favour of increasing in a definitive manner the level of penalties to at least 2 years of a maximum term of imprisonment, like indeed envisaged in the Commission proposal. Neither of those positions received a qualified majority support.

[33] FR suggest the introduction of a new aggravating circumstance when the offences referred to in Art. 3 to 6 are committed *"through the use of a network of computers that have been compromised or infected by malicious software".*

[34] DE and UK supported by CZ would like to limit the application of this provision to Articles 4-5.

[35] Amendment initially put forward by UK, to clarify the meaning of this provision.

[36] Change requested by LT. It should be noted that the amendment is coherent with the respective wording of Art. 7 of FD 2005/222/JHA.

[37] A number of delegations called for rewording of this provision in order to use technologically neutral language. An alternative wording in this regard was considered by DROIPEN at its meeting on 2-3 March. On the other hand, the COM together with some delegations pointed out that both the tools and the damage caused should be taken into account in the provision. The Presidency is of the opinion, that the concerns about ensuring technologically neutral provision should be satisfied by the wording of Art. 9 (4) (b). At the same time, the provision in relation to "botnets", as put forward in the COM proposal, should be maintained in order to respond to a continuously growing specific threat.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 3 to 6[38] when

(a) committed within the framework of a criminal organisation, as defined in Framework Decision 2008/814/JHA[39] or

(b) causing serious damage or

(c) committed against a critical infrastructure information system[40].

are punishable by a maximum penalty of at least five years of imprisonment.

---

[38] DE and UK supported by CZ would like to limit the application of this provision to Articles 4-5.

[39] SE expressed concerns as regards the practical application of this provision taken in conjunction with the definition of an organised criminal group in Framework Decision 2008/814/JHA. The Presidency would like to recall that in conformity with Art. 83, TFEU, the Directive establishes only minimum rules concerning the definition of criminal offences and the respective levels of sanctions. Therefore the Member States may have criminalised the offences referred to in this Directive beyond the threshold of maximum penalty of at least 4 years, envisaged in Art. 1 (1) of the Framework Decision 2008/814/JHA. According to the circumstances of every particular case, the organised criminal activities may vary significantly thus covering a broad range of offences, including such for which the sanctions may exceed 4 years. Taking this into account, the Presidency is of the opinion that the current provision shall be maintained the way it stands now in order to provide for an abstract rule and thus not excluding various possibilities which may arise in practice. This approach is in conformity with the approach already taken by the Framework Decision by which the Member States are bound. In this respect the alternative proposal to tackle the crimes committed within a criminal organisation as an aggravating circumstance without envisaging a specific sanction shall be regarded as deviating from the standards already set at EU level and therefore not an appropriate solution for the Council following the entry into force of the Lisbon treaty.

[40] The Presidency suggests the following recital to clarify the meaning of critical infrastructure: "There are a certain number of critical infrastructures in the Union, the disruption or destruction of which would have significant cross-border impacts. It emerges from the need to increase the critical infrastructure protection capability in Europe that the fight against the attacks against information systems should be complemented by serious criminal sanctions reflecting the gravity of such attacks. For the purposes of this directive, critical infrastructure means an asset, system or part thereof located in Member States which is essential for instance for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 3 to 6 is committed by using personal data that identifies or may identify another person, without the consent of the owner, thereby concealing the real identity of the perpetrator and thus gaining trust of a third party, it is regarded as an aggravating circumstance provided that the act results in serious[41] damage or affects essential interests[42].

(…)

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, 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.

---

41 See the footnotes as regards Art. 9(3)

42 FR, LU, PT, MT, BG, IT and EL expressly requested this element of the COM proposal to be retained in the directive, while the Working Party shall continue examining the most appropriate way to do this.

3. Liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators of, inciters[43], 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.

Article 13

Jurisdiction[44]

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:

[44] UK and ES maintain a scrutiny reservation on this article.

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

(b) by one of their nationals, at least in cases when the act is a criminal offence at the place where it was performed[45]

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.

[45] Amendment inserted following the discussion in CATS.

Article 14

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8[46], (…)[47], 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 in urgent requests they can indicate (…) within a maximum of 8 hours[48] (…) at least whether the request for help will be answered, as well as the form and the estimated time of this answer.[49] (…)

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.

---

[46] A clarification of the type of cooperation referred to in this provision was required in the course of the discussions. **The Presidency suggests that this should be clarified further in recital 11, where the following wording may be considered:**
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, including with a view to collecting evidence in electronic form (…).(…) Such assistance may include, for instance, 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, (…)the locating of suspects. 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.
BE pointed out that in order to ensure that the urgent request will be promptly dealt with by the competent authority it may be instrumental to confirm the request by phone. **In this respect the Presidency suggests that recital 11 reads further, as follows:**
In such cases, it may be expedient that the request for assistance is accompanied by a telephone contact , in order to ensure that it will be processed swiftly by the requested state within the limit of 8 hours.

[47] DE entered scrutiny reservation on the deletion of the expression "in accordance with data protection rules". It should be noted that the issue is already covered by recital 15 and the Data protection FD(2008/977/JHA).

[48] A number of delegations expressed reservations as regards the specific time limit for responding to urgent requests. DE suggests to set up the time limit at 24 hours.

[49] The suggested amendment, aims to clarify the nature of the obligation of the requested state. Namely, that in the specified time limit the competent authority shall respond at least as to whether it would be in a position to provide assistance, and if so to indicate further some of the provisional modalities of the expected answer, such as the form or estimated time.

Article 15

Monitoring and statistics[50]

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[51].

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(…) investigated, (…) prosecuted and (…) 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.

Article 16

Replacement of Framework Decision 2005/222/JHA[52]

Framework Decision 2005/222/JHA is hereby replaced in relation to Member States participating in the adoption of this Directive,without prejudice to the obligations of the Member States relating to the time-limit 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.

---

50 The amended text seeks to reflect, as much as possible the alternative wording, suggested by DE, which received a positive feedback at the last DROIPEN meeting, while not limiting excessively the categories of data which should be provided by Member States. ES lodged a scrutiny reservation.

51 COM maintained their proposal on the scope of the provision, which should cover Art. 3 to 8.

52 The text of the provision has been further aligned with the final wording of the respective article in the THB Directive.

Article 17

Transposition

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[53] 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.

Article 18

Reporting

1. By [FOUR YEARS FROM ADOPTION], 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.

[53] 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 19

Entry into force

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*