EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2010/0273(COD)

3.6.2013

AMENDMENT 129

Draft report
Monika Hohlmeier
(PE476.089v01-00)

on the 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

Proposal for a directive
(COM(2010)0517) – C7-0293/2010 – 2010/0273(COD))

AM_Com_LegConsolidated

Amendment 129
Monika Hohlmeier

Proposal for a directive
–

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on attacks against information systems and *replacing* 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[1],
After transmission of the draft legislative act to the national Parliaments,
Having regard to the opinion of the European Economic and Social Committee[2],
Having regard to the opinion of the Committee of the Regions,
Acting in accordance with the ordinary legislative procedure,

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol ▌.
1 OJ C […], […], p. […].
2 ***OJ C […], […], p. […].***

Whereas:

(1) The objective of this Directive is to approximate ***the criminal legislation*** in the Member States in the area of attacks against information systems, ***by establishing minimum rules concerning the definition of criminal offences and the sanctions in this area, and to*** improve cooperation between ▌ competent authorities, including the police and other specialised law enforcement services of the Member States***, as well as the competent specialised agencies of the Union, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).***

(1a) Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of these systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring appropriate levels of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(2) Attacks against information systems, in particular ***attacks linked to*** organised crime, are a growing menace ***both in the EU and globally***, 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 ***and improved cooperation and coordination at international level***.

(2a) 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 the Union that the measures against cyber attacks should be complemented by serious criminal penalties reflecting the gravity of such attacks. Critical infrastructure may be understood as 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, such as power plants, transport networks or government networks 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 ***often can be*** critical to states or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated ***methods, such as the creation and use of the so called "botnets", which involves subsequent stages of the criminal act, where each stage alone could pose serious danger to public interests. In this respect, the Directive aims, inter alia, to introduce criminal sanctions for the stage where the "botnet" is created, namely, where remote control over a significant number of computers is established by infecting them with malicious software, through targeted cyber attacks. At a later stage, the infected network of computers, constituting the "botnet", could be activated without the computer users' knowledge in order to launch a large scale cyber attack, which usually would have the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, which may include disrupted system services of significant public importance, or major financial cost or loss of personal data or sensitive information.***

(3a) Large scale attacks can cause substantial economic damage both through interruption of information systems and communications and through loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative SMEs of related threats and vulnerabilities, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

(4) Common definitions in this area 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.

(5a) Interception includes, but is not necessarily limited to the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

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

(6a) The directive provides for criminal sanctions at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. The case may be considered minor, for example, when the damage caused by the offence and/or the risk it carries to public or private interests, such as to the integrity of a computer system or computer data, or to a person's integrity, rights and other interests, is insignificant or is of such nature, that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

(6b) The identification and reporting of threats and risks posed by cyber attacks, as well as related vulnerabilities of information systems is a pertinent element of an effective prevention and response to cyber attacks and of improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities, so as to allow the legal detection and reporting of security gaps.

(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[1] ***or*** when the attack is conducted on a large scale, ***thus affecting a significant number of information systems or causing serious damage, including when the attack is intended to create a "botnet" or is carried out through a "botnet", thus resulting in serious damage***. It is also appropriate to provide for more severe penalties where such an attack ***is conducted against a critical infrastructure.***

(7a) Setting up effective measures against identity theft and other identity related offences constitutes another important element of an integrated approach against Cybercrime. Any need for EU action regarding this type of criminal behaviour could be also considered in the context of evaluating the necessity for a comprehensive horizontal EU instrument.

(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. ***Completing the process of ratification of the Convention by all Member States as soon as possible should thus be considered a priority.***

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

(9) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive ***refers*** to 'tools' that can be used in order to commit the crimes listed in this Directive. Tools refer to, for example, malicious software, including ***those able to create*** botnets, used to commit cyber attacks. ***Even if a tool is suitable or even especially suitable for carrying out the mentioned offences the tool might be produced for legitimate purposes. Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as testing the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be used for the purposes of committing any of the offences referred to in the Directive must be also fulfilled.***

▌

(10a) This Directive does not intend to impose criminal liability where the objective criteria of the crimes listed in this directive are met, but the acts are committed without criminal intent, for instance when the person did not know that the access was unauthorised or in the case of mandated testing or protection of information systems, e.g. when a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict the access to information systems by way of user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of the employer for private purposes, should not incur criminal liability, where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceeding. This Directive is without prejudice to the legally guaranteed right of access to information as laid down in national and EU legislation, while at the same time it may not serve as an exemption to justify unlawful and arbitrary access to information.

(10b) The commission of cyber attacks could be facilitated by various circumstances, such as when the perpetrator within the scope of his employment has access to the security systems inherent in the affected information systems. In the context of national law such circumstances should be appropriately taken into account in the course of criminal proceedings.

(10c) Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders. It remains within the discretion of the judge to assess these circumstances together with the other factual elements of the particular case.

(10d) This Directive does not govern the conditions that should be met in order to exercise jurisdiction over any of the offences referred to in Art. 3 to 8, such as a report made by the victim in the place where the offence was commited, or a denunciation from the State of the place where the offence was commited, or the fact that the offender has not been prosecuted in the place where the offence was committed.

(10e) In the context of this Directive, States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations.

(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***. Such points of contact should be able to deliver effective assitance thus facilitating for example the exchange of available relevant information or provision of technical advice or legal information*** for the purpose of investigations or proceedings concerning criminal offences ***relating*** to information systems and ***associated data involving the requesting Member State. In order to ensure the smooth operation of the networks each contact point should have the capacity to carry out communications with the point of contact of another Member State on an expedited basis supported inter alia by trained and equipped personnel***. Given the speed with which large-scale ***cyber*** 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 information is accompanied by telephone contact, in order to ensure that the request is processed swiftly by the requested Member State and that feedback will be provided within 8 hours.***

(11a) Cooperation between the public authorities and the private sector and civil society is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. The cooperation may include, for example, support by service providers in helping to preserve potential evidence, in providing elements helping to identify perpetrators and, as a last resort, shutting down, completely or partially, in accordance with national law, including national legislation and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive.

▌

(12a) There is a need to collect comparable data on offences referred to in this Directive. Relevant data should be made available to the competent specialised agencies, such as Europol and the European Network and Information Security Agency in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby contribute to formulating more effective responses. Member States should submit information on the modus operandi used by the perpetrators to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with the Council Decision 2009/371/JHA. Providing information can facilitate a better understanding of present and future threats and thus contribute to a more appropriate and targeted decision-making on combating and preventing attacks against information systems.

(12b) In accordance with this Directive the Commission has to submit a report on the application of the Directive and to make any necessary legislative proposals possibly leading to broadening of the scope of this Directive taking into account developments in the field of Cybercrime. Such developments could include any technological developments enabling for example more effective enforcement in the area of attacks against information systems or which facilitate prevention or minimise the impact of such attacks. For this purpose the Commission should take into account the available analysis and reports produced by relevant actors and in particular Europol and ENISA.

(12c) In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against Cyber attacks. Member States should take necessary measures to protect critical infrastructures from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in line with existing EU legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(13) Significant gaps and differences in Member States' laws ***and criminal procedures*** in the area of attacks against information systems ▌ 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 ***cross-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 ***adequate implementation and application*** of Council Framework Decision 2009/948/JHA on prevention and settlement of conflict of jurisdiction in criminal proceedings. ***Member States in cooperation with the European Union should also seek to improve international cooperation related to security of information systems, computer networks and computer data. Proper consideration to the security of data transfer and storage should be given in any international agreement involving data exchange.***

(13a) Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective fight against cybercrime. In this context stepping up the efforts to provide adequate training to the relevant authorities in order to raise the understanding of cybercrime and its impact, and to foster cooperation and exchange of best practices, for example via the competent specialised EU agencies should be encouraged. Such training should aim inter alia at raising awareness about the different national legal systems, the possible legal and technical challenges faced in criminal investigations, or the distribution of competences between the relevant national authorities.

(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.

I

(15a) The protection of personal data is a fundamental right in accordance with Article 16 (1) TFEU and Article 8 of the Charter on Fundamental rights. Therefore, any processing of personal data in the context of the implementation of this Directive should fully comply with the relevant EU legislation on data protection adopted on the basis of the Treaties.

(16) This Directive respects the fundamental ***freedoms and*** rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union ***and the European Convention for the Protection of Human Rights and Fundamental Freedoms***, including the protection of personal data***, the right to privacy***, 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 Article 3*** 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.

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.

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;

(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, interception, or any other conduct referred to in this Directive,*** 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

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

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 and*** without right, at least for cases which are not minor.

Article 5

Illegal data interference

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 and*** without right, at least for cases which are not minor.

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 a information system, including electromagnetic emissions from an information system carrying such computer data, is punishable as a criminal offence when committed ***intentionally and without right, at least for cases which are not minor***.

Article 7

Tools used for committing offences

1. Member States shall take the necessary ***measures*** to ensure that the production, sale, procurement for use, import, ▌ distribution or otherwise making available of the following 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, at least for cases which are not minor***:

(a) ▌ 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.

Article 8

***Incitement**, aiding **and** abetting and attempt*

1. Member States shall ensure that the ***incitement***, aiding and abetting ***to commit*** an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit ***an offence*** referred to in ***Articles 4 to 5*** is punishable as a criminal offence.

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, at least in cases which are not minor***.

3. Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 to 5, when committed intentionally, are punishable by a maximum penalty of at least three years of imprisonment when a significant number of information systems have been affected through the use of a tool, referred to in Article 7 (1), designed or adapted primarily for this purpose.

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 to 5 are punishable by a maximum penalty of at least five years of imprisonment when

(a) committed within the framework of a criminal organisation, as defined in Framework Decision 2008/814/JHA irrespective of the penalty level referred to therein, or

(b) causing serious damage, or

(c) committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing personal data of another person, with the aim of gaining trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with relevant provisions of national law, be regarded as aggravating circumstances, unless these circumstances are already covered by another offence, punishable under the national legislation.

▌

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.

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

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

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

I

2. When establishing jurisdiction in accordance with paragraph 1(a), ***a Member State*** 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. A Member State shall inform the Commission where it decides to establish further jurisdiction over an offence referred to in Articles 3 to 8 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.

Article 14

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3 to 8, ***Member States shall ensure that they have an operational national point of contact and*** 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 at least whether the request for help will be answered, as well as the form and the estimated time of this answer***.

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 ***and competent specialised EU agencies and bodies***.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate reporting without undue delay of the offences referred to in Article 3 to 6 to the competent national authorities.

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 ***existing data on*** the number of offences referred to in Articles 3 to *7* ***registered by*** the Member States***,*** and ▌ the number of persons***, 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 ***and submitted to the competent specialised EU agencies and bodies***.

Article 16

Replacement *of Framework Decision 2005/222/JHA*

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.

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] ▌.

▌

3. Member States shall transmit to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Directive.

4. When Member States adopt these measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

Article 18

Reporting

▌

The Commission shall by [FOUR YEARS FROM ADOPTION], submit a report to the European Parliament and the Council, assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. In this respect, the Commission shall also take into account the technical and legal developments in the field of cyber crime, particularly with regard to the scope of this Directive.

▌

Article 19

Entry into force

This Directive shall enter into force on the twentieth day following 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.

Or. en