Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 04/07/2013 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 541 votes to 91, with 9 abstentions, a legislative resolution 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.

Parliament adopted its position at first reading under the ordinary legislative procedure. The amendments adopted in plenary are the result of a compromise reached between the European parliament and the Council. They amend the Commissions proposal as follows:

Objective of the Directive: the objective of the Directive is to establish 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.

Definitions: a definition of without right was added: "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.

It should also be noted that, in the recitals, a definition of interception has been introduced: 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.

Illegal system interference: Member States shall take the necessary measures to ensure that, when committed intentionally and without right, at least for cases which are not minor, 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. The same follows in respect to the illegal access to illegal data interference or in the case of illegal interception within the meaning of the Directive.

Incitement, aiding and abetting and attempt: provision should also be made for measures to ensure that the incitement, aiding and abetting to commit an offence within the meaning of the Directive is punishable as a criminal offence. Member States are called upon to ensure that the attempt to commit an offence is punishable as a criminal offence.

Penalties: offences that fall within the scope of the Directive should be subject to the following penalties:

- a maximum penalty of at least two years of imprisonment, in cases which are not minor;
- a maximum penalty of at least three years of imprisonment when certain offences covered by the Directive are committed intentionally, and when a significant number of information systems have been affected through the use of a tool designed or adapted primarily for this purpose;
- a maximum penalty of at least five years of imprisonment when offences covered by the Directive are:

  - committed within the framework of a criminal organisation, or

  - causing serious damage, or

  - committed against a critical infrastructure information system.

In a recital, it is stipulated that criminal sanctions should be envisaged 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.

Furthermore, if certain when certain offences 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 be regarded as aggravating circumstances. A recital stipulates that identity theft and other identity-related offences of the same type could require action at EU level in the form of a comprehensive horizontal EU instrument.

Jurisdiction: a Member State shall inform the Commission where it decides to establish further jurisdiction over an offence covered by the Directive committed outside their territory, e.g. where:

- the offender has his or her habitual residence in the territory of that Member State ; or
- the offence is committed for the benefit of a legal person established in the territory of that Member State.

National contact point: Member States should 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. They should 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.

Data collection: it is stipulated that 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. The objective is 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.

Replacement of the Framework Decision 2005/222/JHA: it is clearly stipulated that the Directive aims to amend and expand the provisions of

Framework Decision 2005/222/JHA concerning attacks against information systems.

Reports: lastly, the Commission should submit, within four years of the adoption of this Directive, 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.