# Judicial cooperation in criminal matters: combating attacks against information systems

2010/0273(COD) - 12/08/2013 - Final act

PURPOSE: to approximate Member States' criminal law in the area of attacks against information systems.

LEGISLATIVE ACT: Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

CONTENT: the Directive establishes **minimum rules concerning the definition of criminal offences and 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**.

**Offences:** for **cases which are not minor, and are committed intentionally and without right,** the following actions must be punishable as criminal offences:

- **illegal access to information systems**: illegal access to the whole or to any part of an information system where committed by infringing a security measure;
- **illegal system interference**: seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;
- **illegal data interference**: deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible;
- **illegal interception**: intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data;
- **tools used for committing offences**: the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to above: (i) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to above; ii) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

**Incitement, aiding and abetting and attempt**: the Directive provides that:

- the incitement, or aiding and abetting, to commit any of the five offences referred to above must be punishable as a criminal offence;
- the **attempt to commit illegal system interference and illegal data interference** must be 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 offences relating to illegal system interference and illegal data interference 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 relating to illegal system interference and illegal data interference are: (i) committed within the framework of a criminal organisation, or (ii) causing serious damage, or (iii) committed against a critical infrastructure information system.

When offences relating to illegal system interference and illegal data interference are committed by **misusing the personal data of another person, with the aim of gaining the trust of a third party**, thereby causing prejudice to the rightful identity owner, this may be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

A recital in the Directive states that 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 Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.

**Legal persons**: the Directive makes provision for ensuring that legal persons may be held liable and sanctioned.

**Jurisdiction:** the Directive sets out rules on the establishment of jurisdiction with regard to the offences described above. A recital notes that 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 law in this area.

**National contact point**: Member States must 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 must 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**: a recital in the text states that there is a need to collect comparable data on the offences laid down in this Directive. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, 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 to contribute to formulating a more effective response. Member States should submit information on the modus operandi of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA.

**Replacement of Framework Decision 2005/222/JHA**: 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.

**Report:** by 4 September 2017, the Commission must submit a report assessing the extent to which the Member States have taken the necessary measures in order to comply with the Directive. It will, also take

into account the technical and legal developments in the field of cybercrime, particularly with regard to the scope of the Directive.

ENTRY INTO FORCE: 3 September 2013.

TRANSPOSITION: by 4 September 2015.