CONTENTS

Chimec S.p.A.

Organisation, Management and Control Model pursuant to Legislative Decree 231/2001

SPECIAL SECTION "E"

CYBERCRIME OFFENCES

Approved by the Board of Directors of CHIMEC S.p.A. on October 25th 2016
Update of November 12th 2020

1. – Cybercrime offences: general characteristics

This Special Section covers the offences that aim to safeguard our so-called "computer domicile", i.e. the space where our personal details are stored and which must be kept safe from undue encroachment by anyone.

A computer domicile can be defined as an ideal expansion of a person's environment (the legislators have recognised the same *ius excludendi* – right of exclusion – that applies to one's physical home), a space in which a person may freely exercise any legal activity.

Therefore, taking into account this legal interest, cybercrime offences are generally included in the category of offences against the person or property, except in the case of the offence referred to in article 491-*bis* of the Criminal Code, which aims to project (besides the set of data related to a certain computer domicile) the authenticity of the evidential value of the documents and data contained in the said system.

These are all offences committed with criminal intent, which means that the perpetrator: (i) is aware of the fact that he or she is committing an offence, and (ii) is intent on committing the offence (meaning that he or she intentionally wishes to introduce himself or herself into a system that he or she is not otherwise allowed to enter, for the purpose of unlawfully altering, destroying or disseminating the content thereof).

2. – Offences referred to in article 24-*bis* of Legislative Decree 231/2001

2.1. – Electronic documents (article 491-*bis* of the Criminal Code)

This provision – set out in Book II, Title VII, Chapter III of the Criminal Code – contemplates the offences against "public faith" and refers to the so-called forgery offences, which include either "*falsità materiale*"[1] (i.e. the forging or counterfeiting of documents) or "*falsità ideologica*"[2] (i.e. misrepresentation) (articles 476 et seq. of the Criminal Code) – and states that "*if the forgery referred to herein regards a public electronic document that can be used as evidence in court, the provisions applying to all public documents and records shall apply*".

Legislators have introduced this offence to safeguard the evidential value of certain documents subject to so-called "privileged faith", as referred to in articles 2699 et seq. of the Civil Code, as well as any document deemed worthy of protection by the legal system, because of its evidential value.

Therefore, the offence referred to in article 491-*bis* of the Criminal Code also applies to the forgery – whether in the form of material counterfeiting or misrepresentation – of public or private electronic documents.

2.2. – Illegally gaining access to a computer system (article 615-*ter* of the Criminal Code) 130

This offence sanctions "*whoever illegally gains access to a computer or online system protected by security measures or remains there against the will, whether expressed or tacit, of the person(s) entitled to exclude him*".

Legislators aim to protect the integrity of the system and of the data and software included therein, as well as –most importantly – the confidentiality of the data and software stored therein.

The penalty is a prison sentence from 1 to 5 years:

1) if the offence is committed by a public official or a public service officer, by abusing his or her powers and authority or breaching the duties inherent in the function or service provided, or by any person illegally practising the profession of private investigator, or by abusing the qualification of system officer;

2) if the perpetrator uses violence against property or persons to commit the offence, or is clearly armed;

[1] Forgery as "*falsità materiale*" (articles 476 and 482 of the Criminal Code) entails intentionally tampering with a document after it has been drafted (e.g., by making alterations or additions to the document, or when there appear to be differences between the apparent and real authors of the document).

[2] Misrepresentation as "*falsità ideologica*" (articles 479 and 483 of the Criminal Code) means providing incorrect or misleading information in a document, without otherwise tampering with it.

3) if the commission of the offence destroys or damages the system, or leads to the full or partial interruption of its operation or the destroys or damages the data, information or software contained therein.

If the above mentioned offences are committed with regard to a computer or online system of military interest or relating to public order or law enforcement or healthcare or civil protection or of public interest in general, the penalty shall be a prison sentence of between 1 and 5 years and 3 and 8 years, respectively.

The conduct prosecuted here consists in unlawfully entering and remaining – against the will of the owner of the computer domicile or other person with the authority to exclude any undesired entrance therein – in a computer or online system protected by a password or other qualifications allowing access only to the authorised users or the holders of specific credentials.

Therefore, it must be specified that the offence in question shall be deemed to have been committed also when the persons holding credentials enter or remain inside the system in breach of the requirements and limits imposed by the owner of the relevant computer domicile.

2.3. – Holding and illegally disseminating the access codes of computer or online systems (article 615-*quater* of the Criminal Code) 131

This provision sanctions the illegal acquisition and dissemination, in any way, of the means or codes enabling unauthorised persons to enter into a computer or online system belonging to others and protected by security measures, by "*whosoever, for the purpose of securing a profit for himself or others, or causing damage to others, illegally procures, disseminates, communicates or delivers codes, keywords or other means for entering a computer or online system protected by security measures, or otherwise provides indications or instructions suited to this purpose*".

The conduct of the perpetrator consists in procuring or reproducing a password or access credentials in an illegal manner or without the owner's consent – the owner being the only person entitled to exclude anyone from using the said system – of the hacked computer system and must be motivated by the specific purpose of either (i) securing a profit, or (ii) causing damage.

2.4. – Circulating computer equipment, devices or software for damaging or interrupting the operation of a computer or online system (article 615-*quinquies* of the Criminal Code)

This provision provides that "*whosoever, for the purpose of illegally damaging a computer or online system, and the information, data and software contained therein or related thereto, or fosters the total or partial interruption or*

alteration of the operation thereof, procures, produces, reproduces, imports, circulates, communicates, delivers or otherwise makes available to others the necessary computer equipment, devices or software".

For the purpose of establishing this offence, it shall be necessary that the perpetrator of the above mentioned actions (committed using computer equipment, devices or software) to pursue the specific purpose of damaging or otherwise illegally tampering with the computer or online system.

2.5. – Intercepting, impeding or otherwise unlawfully interrupting computer or online communications (article 617-*quater* of the Criminal Code)

This provision sanctions "*whosoever fraudulently intercepts communications relating to a computer or online system or between two or more systems, or otherwise prevents or interrupts the said communications*", and, unless the fact constitutes a more serious offence, the penalty shall also apply to "*whosoever discloses to the public, by any means, in whole or in part, the content of the said communications*" referred to in the preceding paragraphs.

The provision extends the protection of secrecy, freedom and confidentiality of telephone or telegraph communications covered by article 617 to include communications using computer or online systems or between systems.

This is a so-called "free form offence", established each time the perpetrator carries out a fraudulent action or intentionally intercepts – during transmission – any communications taking place between computer or online systems.

The other two sanctionable behaviours consist in preventing and interrupting communications relating to a computer or online system or between various systems, in such a manner as to prevent it from starting or causing it to stop if it is already under way.

Paragraph two sanctions another type of conduct consisting in the illegal disclosure to the public of data or facts contained in the communications, without necessarily having intercepted the communications in question beforehand, it being sufficient for the perpetrator to disclose confidential information by any means.

2.6. – Installing equipment suited to intercepting, preventing or interrupting computer or online communications (article 617-*quinquies* of the Criminal Code)

This provision sanctions "*whosoever, excepts in the cases allowed by law, installs equipment suited to intercepting, preventing or interrupting communications relating to a computer or online system or between such systems*".

This provision faithfully reproduces the approach already adopted by the offence of danger referred to in article 617-*bis*, providing the early protection of a good – the secrecy and freedom of computer or online communications – the violation of which is sanctioned by the preceding article.

The conduct sanctioned here – featuring a generic malicious intent – is preliminary to intercepting, preventing or interrupting communications, as entailed, for example, by setting up specific unauthorised equipment and devices for the purpose of interception, or preventing or interrupting exchanges of information between computer systems.

The offence represents a concrete danger (and requires an assessment, by the court, of the effective harmful potential of the equipment installed) and is committed in advance, being finalised once the illegal equipment is attached to or installed on the system targeted by the perpetrator.

2.7. – Procuring damage to computer information, data and software (article 635-*bis* of the Criminal Code)

Unless the fact constitutes a more serious offence, this provision sanctions – subject to the lodging of a complaint by the injured party – "*whosoever destroys, deteriorates, erases, alters or supresses other people's computer information, data or software.*"

If the commission of the offence involves the use of violence or threats, or by abusing the qualification of system operator, a prison sentence of between 1 and 4 years shall apply.

The legal interest protected by this provision is the inviolability of the ownership and availability and the integrity of the computer content and software.

This too is a "free form offence", in that it includes any conduct that involves tampering with and altering a computer system, to the point that it is rendered unserviceable, regardless of whether or not the damage can be reversed and the system restored.

2.8. – Damaging computer information, data or software used by the State or other public entities or otherwise of public usefulness (article 635-*ter* of the Criminal Code)

Unless the fact constitutes a more serious offence, this provision sanctions "*whosoever commits actions aimed at effectively destroying, deteriorating, erasing, altering or suppressing computer information, data or software used by the State or other public entities, or otherwise of public usefulness*".

If the commission of the offence involves the destruction, deterioration, erasing, alteration or suppression of the computer information, data or software, a prison sentence of between 3 and 8 years shall apply.

If the commission of the offence involves the use of violence or threats, or by abusing the qualification of system operator, the penalty shall be increased.

The structure of this offence differs from that in article 635-*bis* of the Criminal Code exclusively in that the computer or online systems targeted by the perpetrator, and involved in the commission of the offence, are used by or belong to the State or other public Entity or are otherwise of public usefulness.

2.9. – Damaging computer systems (article 635-*quater* of the Criminal Code)

This provision sanctions, unless the fact constitutes a more serious offence, "*whosoever, by adopting the conduct referred to in article 635-bis, or through the introduction or transmission of data, information or software, destroys, damages or renders fully or partially unserviceable the information or online systems owned by others or seriously impairs their operation*".

If the commission of the offence involves the use of violence or threats, or by abusing the qualification of system operator, the penalty shall be increased.

The offence is deemed to be a so-called "restricted form offence", centred on the determination, by the perpetrator, to render the system unserviceable or to otherwise seriously impair its operation.

The offence in question may be committed through various types of conduct, as stated in article 635-*bis*, or through the introduction or transmission of data, information or software by means of computer viruses or malware introduced into the system and capable of fully or partially impairing the operation of the computer and online systems.

Regarding the establishment of this offence, the total destruction of all the data shall not be required, it being sufficient that the ordinary operation of the system is irreversibly damaged and that the perpetrator's conduct renders the operation of the system, and of the relevant services, irregular and fragmentary.

2.10. – Damaging public information or online systems (article 635-*quinquies* of the Criminal Code)

This offence, which is related to the offence described in the preceding paragraph, features an increased penalty if the conduct is "*aimed at destroying, damaging and rendering fully or partially unserviceable any public computer or online systems or seriously hindering their operations."*

If the offence entails the destruction or damaging of the public computer or online system, of if this is rendered fully or partially unserviceable in any way, a prison sentence of between 1 and 8 years shall apply.

If the commission of the offence involves the use of violence or threats, or by abusing the qualification of system operator, the penalty shall be increased.

The legislators have aimed to put into place stronger safeguards for public data and systems against damage, compared to private data and systems.

2.11. - Art. 640-*quinquies* of the Criminal Code (computer fraud by the party providing electronic signature certification services)

This offence is established when a party providing electronic signature certification services breaches the applicable regulations in order to secure an unjust profit, for himself or others, or otherwise damages others.

This is obviously a so-called "proper" offence, in that it can only be committed by a party possessing the qualifications provided in the provision.

2.12. – Penalties applicable to the offences referred to in article 24-*bis* of the Decree

Regarding the offences referred to in articles 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* and 635-*quinquies* of the Criminal Code a penalty of between 100 and 500 quotas shall apply.

Regarding the offences referred to in articles 615-*quater* and 615-*quinquies* of the Criminal Code, a maximum penalty of 300 quotas shall apply.

Regarding the offences referred to in articles 491-*bis* and 640-*quinquies* of the Criminal Code, subject to article 24 of the Decree in the case of computer fraud to the detriment of the State or other public entity, a maximum penalty of 400 quotas shall apply.

Finally, if the entity is found guilty for any of the offences indicated in paragraph 1, the disqualification penalty pursuant to article 9, paragraph 2, letters a), b) and e) of the Decree shall apply. If the entity is found guilty for any of the offences indicated in paragraph 2, the disqualification penalty pursuant to article 9, paragraph 2, letters b) and e) of the Decree shall apply. If the entity is found guilty for any of the offences indicated in paragraph 3, the disqualification penalty pursuant to article 9, paragraph 2, letters c), d) and e) of the Decree shall apply.

3. – Risk areas

Taking into account Chimec's operations, the following risk areas have been identified:

- the activities carried out by the Recipients using computer systems, emails and Internet access;
- the monitoring and action procedures for maintaining and operating the Chimec IT systems;
- the control and security activities relating to the Company's IT systems;
- the use of software and databases by all the Recipients;
- the organisation and management of internal and/or external information and computer flows.

The areas specified above are relevant also if the relevant activities are carried out, in whole or in part, by individuals or corporations in the name and on behalf of Chimec, also based on proxies or powers or attorney or under contracts and other arrangements, of which the SB must be promptly informed.

4. – General rules of conduct and implementation.

The purpose of this Special Section is to provide a set of rules of conduct aimed at preventing the commission of cybercrime offences, giving rise to the penalty system set out in the Decree in the event the entity is found liable.

The rules of conduct apply to all the Recipients[3] of the Model and, in particular to all those who operate in the risk areas defined above, including any persons who are not part of the Company.

The Board of Directors of Chimec, together with the SB, shall be responsible for the circulation and implementation of the said systems.

The Recipients are expected to know and abide by the rules set out herein, as well as the:

- Code of Conduct;
- disciplinary system;
- the procedures adopted by Chimec relating to the management software used to ensure the proper operation of the corporate IT systems;
- the protocols for ensuring the secure flow of communications between the internal and external corporate systems;
- the provisions relating to the use of software and databases;
- the internal procedures for ensuring the safety of the computer and/or online systems.

The Recipients and all external collaborators – duly informed by means of dedicated contractual clauses – are prohibited from adopting any kind of conduct capable of fostering the commission of cybercrime offences.

It is also forbidden to:

- disclose the passwords or other access credentials relating to the Chimec computer systems to any person – whether inside of outside the Company – who has not been authorised to use the said systems;
- possess or use any software and/or hardware capable of damaging or jeopardising the security of the systems and the data contained therein;
- access and/or remain within the system for purposes other than work and/or in breach of the requirements imposed by the owner of the computer system;
- tamper with the software and/or hardware of the workstations in violation of the Company rules or without the Company's authorisation;

[3] For the definition of Recipients, reference should be made to the General Section of the Model, Glossary.

- exploit the password and/or access credentials to tamper with the security measures of the system, in order to obtain confidential data or information;
- modify the data posted in the Chimec website;
- send falsified or otherwise altered data or information from one's computer system;
- perform spamming or spamming response activities;
- disclose any information or data the disclosure of which is forbidden, as a result of unauthorised access to the Company's computer system.

Chimec undertakes to provide for periodical training and updating courses for Recipients and to disseminate the protocols adopted by the Company for the management and operation of its computer systems.

Chimec also undertakes to put into place an internal control system for monitoring the security of the system to protect against unauthorised interference and counter any tampering of the system and data.

Finally, the Board of Directors may provide for other measures aimed at protecting the identified risk areas, in addition to the obligations and requirements mentioned above.