PREPARATORY COLLOQUIUM SECTION I
GREEK NATIONAL REPORT*

M. KAIAFA-GBANDI, K. CHATZIIOANNOU*

I. Electronic Crime and legal interests that are worthy of protection in Greek Criminal Law-A basic systematization

In the Greek criminal law literature, it has been argued that the protected legal interest should serve as a criterion for the classification of all types of electronic crimes. Specifically, according to this opinion, the term of electronic crime includes the following categories[1]:

(i) Crimes that have as *an object* of assault *the information systems and electronic data themselves* and are therefore defined as *genuine electronic crimes*.

(ii) Crimes that are committed *via* information systems primarily violating or aiming at the violation of other legal interests, thus determined as *non-genuine electronic crimes.* This latter field is the most heterogeneous one, and could be divided in the following subcategories of criminal offences:

a) Acts committed via computers, which violate traditional legal interests, but *differ from an existent similar offence* in such a way that their punishment would not be possible without a distinct provision, since the opposite would conflict with the prohibition of applying criminal law rules by analogy. Computer fraud, for example, belongs to this category. Both in Greece and in other countries, it has been necessary to criminalize this conduct separately (in Greek Criminal law Article 386 A grCC), since here the property damage is not a result of a deception of another person, but the result of an intervention on a program or other computer data.

b) Criminal acts that violate other legal interests and may take place via an information system or a network of information systems, but the violation per se derives from the *content* of data (*content related crimes*). To this subcategory belong not only modern crimes, such as child pornography (Article 348 A grCC), but also acts of racism (Article 1 and 2 of Law 927/1979) via the internet. Such crimes are not solely committed via information systems. Furthermore, to this subcategory also belong traditional criminal offences, such as insult and defamation via the internet[2].

c) Last but not least, there is a number of several traditional criminal offences, the commitment of which, is facilitated especially by the use of information systems, but at the same time these offences entail *a parallel assault on electronic data which either leads to a special legal interest, regarding exclusively electronic data, or is inextricably connected to another legal interest*. This last subcategory lies *between genuine and non-genuine electronic crimes*, since the offences that are embraced here are committed via information systems, but they necessarily violate also

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* M. Kaiafa-Gbandi, Professor of Criminal Law, International and European Criminal Law at the Law Faculty of Aristotle University Thessaloniki, Fulbright Grantee, Harvard Law School Visiting Scholar

K. Chatziioannou, LLM (Heidelberg), PhD candidate (Aristotle University of Thessaloniki), Faculty of Law, Department of Criminal Law and Criminology), Scholar of the Programme IRAKLITOS II.

1 See *Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Armenopoulos, 1062 ff.

2 See Decision of Areopag 1105/2005, Poiniki Dikaiosyni 2005, and 1385 ff.

the electronic data that are either incorporated into a special legal interest (for example, writings), or are connected inextricably to it (for example, intellectual property relating to computer programs).

The above categorization will be used in the following in order to present the legal interests that are worthy of protection, according to the Greek legal order in the framework of electronic crime.

II.1. Genuine electronic crimes-Article 370 C grCC as a means of protecting confidentiality of electronic data and the deficiencies in protecting integrity and availability of information systems and electronic data

Among the main legal interests that are deemed in need of protection by criminal law nowadays are confidentiality, integrity and availability of information systems and electronic data. Computer systems and electronic data have become essential for carrying out state and individual activities, as due to the evolution of their processing power they have permeated almost every aspect of life[3].

1. In Greek Criminal law the main Article that seems to protect the *confidentiality of electronic data* is Article 370 C grCC. This Article is considered to protect the right of disposal of the legal holder of data[4]. It is also argued that the protected legal interest of Article 370 C par. 2 grCC is a kind of formal secrecy, i.e. the right of the legal holder of data to ban the access to them, without any prerequisite of a substantial secrecy[5]. This view underestimates secrecy[6] and it would be more prudent to claim that the protected legal interest of Article 370 C par. 2 grCC is the confidentiality of electronic data.

The importance of information as a legal interest has already been emphasized in Greek criminal law theory[7]. Generally, it has been argued that information is an intangible legal interest with peculiarities when compared to substance and energy[8]. Due to the technological evolution, information has obtained a great importance and this development has rendered it worthy of protection. However, one could even consider data, themselves, as a legal interest worthy of protection, because electronic data constitute the representation of information and have the required manifestation in the empirical world that a legal interest should have in order to be protected by criminal law means. Electronic data constitute, on the other hand, the means for participation in the information society. According to international legal documents, the term "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 making an information system perform a function[9]. Consequently, a piece of information must take the form of electronic data in order to be processed by information systems and for this reason, the proper function of an information system

[3] See *Kaiafa-Gbandi* (2012), Criminalizing Attacks against Information Systems in the EU, European Journal of Crime, Criminal Law and Criminal Justice, 67.
[4] Cf. regarding the equivalent Article 202 a of the German Criminal Code *Schünemann* σε LK, 11. Auflage, StGB, § 202 a, margin no. 2) or the right of disposal of information (See *Vassilaki* (1993), Combating computer crime [in Greek], 83.
[5] See *Mylonopoulos* (1991), Computers and criminal law [in Greek], 92, cf. *Farantouris,* Modern criminal actions on the internet [in Greek], Poiniki Dikaiosyni 2003, 193
[6] Cf. *Bühler,* Ein Versuch, Computerkriminellen das Handwerk zu legen, MDR 1987, 452.
[7] See *Mylonopoulos* (1991), ibid, 11 ff., *Nouskalis* (2003), Criminal protection of the computer program [in Greek], 58 ff.
[8] See *Mylonopoulos*, Computer Crimes, in Greek Association of Criminal law (1991), The financial Crimes [in Greek], 83 ff.
[9] See Art. 1 b of the Proposal for a Directive on attacks against information systems, COM (2010) 517 final, 30.9.2010.

depends on the proper function of electronic data. Thus, the confidentiality, availability and integrity of the latter and of the information systems as well, are considered legal interests worthy of protection.

Article 370 C para 2 grCC protects *the confidentiality of computer data*. This provision covers the access to data (of a data bank or a personal computer) without right, i.e. hacking, the surpassing of codes and other security measures, the access to the electronic mail of a third person, the eavesdropping of electronic communications etc.[10] The wording of the provision refers to data that have been "introduced to a computer or a peripheral store of a computer or are transmitted via telecommunication systems". Consequently, it is out of dispute that computer data are also protected when they are in a state of transmission. However, in contrast to the provision of the international legal texts for the interception of data[11], the attack against computer data that are transmitted within a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (e.g. through the keyboard) is not regulated by Article 370 C para 2 grCC.

Another problem is that Article 370 C para 2 grCC *does not protect, according to its wording, the confidentiality of the information systems, themselves*. The perpetrator that gains access to an information system usually gains access to the computer data as well. This is not always the case, though[12]. It must be also emphasized that the confidentiality of an information system cannot be sufficiently protected by criminalizing only the obtaining of access to computer data, given the fact that the holder of the right to access an information system could differ from the holder of the right to access certain computer data, themselves.

Article 292 A grCC, which criminalizes –inter alia- the unauthorized access to a connection or network for the provision of telecommunication services or to a system of hardware or software, that is used for the provision of such services, in a way that endangers the security of telecommunications, does not provide an adequate protection of confidentiality to information systems and electronic data, since it aims at the protection of the security of telecommunications, as it is made clear by its wording. Therefore the protection, according to this provision, is limited to specific computer software and hardware and the criminalization requires a further specific intent. Information systems and electronic data may be protected under specific circumstances in the framework of the provision, but, in any way, they constitute the object of the assault and not the main protected legal interest.

The same is also true for Article 370 a grCC, which –inter alia- criminalizes whosoever, without authorization, intercepts or otherwise intervenes in a device, connection or network for provision of telecommunication services or in a system of software or hardware, which is used for the provision of such services. Secrecy of telecommunication is the main protected legal interest in the framework of this provision and the confidentiality of electronic data and information systems are protected only as objects of the assault, when they contribute to the provision of telecommunication services.

---

[10] See *Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Armenopoulos, 1065.

[11] Article 3 of Convention on Cybercrime, Article 6 of the Proposal of a Directive on attacks against information systems.

[12] Cf. *Sieber*, in *Sieber/Brüner/Satzger/von Heintschel-Heinegg* (2011), Europäisches Strafrecht, §24, Computerkriminalität, p. 419, margin no. 88.

On the other hand, Article 370 B CC, proscribing interception of computer data, is narrowly interpreted so as to only address classified data (such as State, scientific or professional data)[13], thus covering cases such as industrial espionage (punishable with imprisonment of up to three months). In reality this provision does not protect the confidentiality of electronic data themselves, but several forms of secrecy that merely have the form of electronic data. As it is stated in the Explanatory Report of Law 1805/1988 that introduced this provision into the Greek legal order, the safeguard and protection of state, scientific and professional secrets that have the form of data or computer programs was here the main goal.

2. Referring now to *the integrity and availability of information systems and electronic data* it should be emphasized that in the Greek legal order there is no relevant special criminal provision. These legal interests are protected only to the extent that they are related to a violation of property. Property as a legal interest refers to ownership of an item in the sense of having the power of disposition for it[14].

As it is said, data alteration constitutes the "virtual damaging of another person's property"[15]. It would be more prudent to consider that protection of the integrity of electronic data provides a shield against the damaging of "virtual property". However, the concept of an item, as an object of assault in crimes against property, is determined in the Greek legal order by civil law[16]. Contrary to information systems and means of data storage, electronic data could not be subject to the concept of an item, since they do not constitute corporal items, determined in space[17]. Electronic data are not even subject to ownership[18] and do not constitute an item, neither from the view of the information that they include, nor when they are stored in an information system[19].

On the other hand, electronic data do not constitute a form of energy, since they do not merely consist in the magnetic recording of arranged bipolar elements as a means of data storage, but they base upon their reasonable configuration[20]. To hold otherwise, would equate information with energy by giving to the former properties of the

---

[13] See *Kaiafa-Gbandi* (2007), ibid., at 1068, *id.* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice, 74, *Kioupis* (1999), *ibid*., at 132, *Mylonopoulos* (1991), *ibid*., at 83–84. In terms of case-law see indicatively S.Ct. 121/2003, Poinika Chronika 2003, 910 ff., (comment by *Konstantinides*), also published in Poiniki Dikaiosyni 2003, 619 (comment by *Nouskalis*), Athens Ct. App. 217/1997, Yperaspisi 1997, 846 ff. (comment by *Kaiafa-Gbandi*).

[14] See *Manoledakis/Bitzilekis* (2007), Crimes against property [in Greek], 3. See also *Manoledakis* (1998), The legal interest [in Greek], p. 333, margin no. 538. See also *Manoledakis/Bitzilekis*, ibid, 4, Cf. *Mylonopoulos* (2006), ibid., p. 2, margin no. 3, *Pavlou* (2006), Crimes against property [in Greek], p. 4 , margin no. 2, *Spinellis* (2012), Crimes against property and financial legal interests [in Greek], 3.

[15] See *Ernst* in *Ernst* (2004), Hacker, Cracker und Computerviren, 95 margin no. 268, regarding the German provision for data alteration and computer sabotage (Articles 303a και 303b of German Criminal Code (StGB).

[16] See *Manoledakis/Bitzilekis,* ibid, 4.

[17] Cf. regarding software *Manoledakis/Bitzilekis* (2007), Ibid, 24, *Mylonopoulos* (1988), Criminal protection of software, Poinika Chronika, 7, *Fasoulas* (1991), Criminal law, Special part, 48.

[18] See *Wessels/Hillenkamp*, Strafrecht Besonderer Teil 2, Straftaten gegen Vermögenswerte, 28. Auflage, 26, margin no. 49.

[19] See *Wolff* in LK, § 303, margin no. 6.

[20] See *Mylonopoulos* (2006), p. 11, margin no, 23, *Mylonopoulos* (1991), ibid, 23.

latter[21]. Consequently, electronic data are not items and therefore they cannot be adequately protected via the protection of the legal interest of property[22].

More particularly, it should be noted that the alteration or deletion of data could not be considered as damaging other means of storage according to Article 381 grCC, since for such an interpretation there should be a damage or destruction of the means of storage themselves[23], since the deletion of the magnetic recording constitutes, at the same time, a change in the bipolar elements that are arranged in the surface of the hard disk[24]. However, this opinion has been formulated 30 years ago and refers to magnetic recordings and particularly to the deletion of data and not to any type of interference with them[25]. Furthermore, it is not sure whether the mere reorientation of magnetic fields could be subject to the concept of damage[26]. However, even the authors who accept that the deletion of tapes constitutes damaging another person's property, they accept that it is disputable whether electronic data are items or not and therefore that it is prudent to introduce a special provision for data deletion and computer sabotage[27].

It has been argued that there is damage even without alteration of the corporal means of storage of electronic data, i.e. without any effect on the material status of the item, since there is a –non minor- reduction of the usefulness of the items[28]. According to this opinion, there is damage, when there is a reduction of the usefulness of the means of storage, i.e. when the data are deleted or altered[29]. Referring to computer viruses, it has been deemed that they constitute damage to the computer, in the form of the reduction of the usefulness of the means of storage, according to their determination, even when they merely delete or alter electronic data of a file[30]. Although this opinion is not indisputable[31], it could be taken into consideration as an option. It is not, however, certain whether we could accept a damage of modern means of data storage, in view of the unpredictable changes that will take place in the field of modern technologies[32]. It is not certain that the provisions against the damaging of another person's property will always protect the integrity and availability of electronic data. The only clear cases, where the provisions regarding

---

[21] See *Mylonopoulos* (1988), Ibid, 9.
[22] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1076.
[23] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1075). It has been argued that alteration of data constitutes, in any case, damaging of property (of their means of storage.
[24] See *Mylonopoulos* (1991), ibid, 25 ff.
[25] See indicatively *Sieber* (1977), Computerkriminalität und Strafrecht, 192.
[26] See *Frey* (1987), Ibid, 127, regarding destruction and not damage.
[27] See *Arzt/Weber* (1986), Strafrecht Besonderer Teil, Vermögensdelikte, 9.
[28] See *Mylonopoulos* (2006), ibid, p. 346, margin no, 777.
[29] See *Mylonopoulos* (2006), ibid, p. 34, margin no. 382.
[30] See *Mylonopoulos* (2006), ibid, 782.
[31] See indicatively *Wessels/Hillenkamp*, Strafrecht Besonderer Teil/2, Straftaten gegen Vermögenswerte, 28. Auflage, margin no. 49, with citations to the opposite opinion.
[32] Cf. *Leckner/Winkelbauer (*1986*),* Computerkriminalität und das 2. WiKG (III), CR, 828, Möhrenschlager *(*1986*),* Das neue Computerstrafrecht, wistra, 141.

the damaging of another person's property can be applied, are the cases where the hard disk of the information system gets full due to the computer viruses or is completely out of use[33].

In any case the damage of immaterial electronic data per se could not be covered by the provisions for the damage of property. The holder of the right to access electronic data, i.e. the holder of the legal interest of their integrity and availability, could differ from the owner of the means of data storage and data processing systems in general. If we provide protection only to the property, the rightholder of integrity and availability of electronic data cannot be protected against the attacks that are launched by the owner.

Furthermore, the provisions against damaging another person's property cannot correspond to the harm that is caused in the sense of the informational damage, since the judgment for the aggravated case of damage will be based upon the value of corporal means of data storage, and not upon the value of the data themselves (Article 382 par. 2 b grCC)[34]. However, electronic data have an important economic value, since they play an important role in every aspect of social life. Their value is, indeed, several times higher than the value of information systems that process them[35].

Besides, completely minor assaults do not constitute damage[36] and damages that do not require special effort, time or cost for their restoration are not criminalized[37]. It is possible that in a certain case there is a completely minor assault on the corporal means of data storage, but a severe assault on the integrity of electronic data per se. The former might exclude the application of the provision for damaging another person's property, while the latter could not be taken into account since it refers to electronic data. Consequently, also in these cases provisions protecting property cannot offer an adequate protection of electronic data.

Regarding the integrity and availability of electronic data, it should be noted that there are also modern forms of intervention in electronic data, such as the damage of data that are in the phase of transmitting[38]. Such forms could in no case be subject to the concept of damaging another person's property[39].

Moreover, the attacks against integrity and availability of electronic data and information systems could not be covered adequately by the provisions concerning forgery and destruction of writings (Articles 216 and 222 of CC in combination with 13 c grCC)[40]. As it will be analyzed further on, these offenses prerequisite specific characteristics of electronic data[41] and thus they do not protect the emerging legal interest of integrity and availability of electronic data

---

[33] See *Kaiafa-Gbandi* (2007), Ibid, 1076.
[34] See *Kioupis* (1999), ibid, 140.
[35] Cf. for the importance of information in the decade of 80ties BT-Drs. 10/5058, 34 of 2. WiKG, where there is a mention to the economic value of information and to the great dependence of economy and administration on them.
[36] See *Gafos* (1967), Criminal law, Special part, 6th Volume, 100, *Bouropoulos* (1964), Interpretation of Criminal Code, Special part, Third volume, Art. 381, p. 52, margin no. 7.
[37] See *Stree/Hecker* in, *Schönke/Schröder* StGB, § 303, margin no. 9.
[38] See *Mylonopoulos* (1991), ibid, 26, *Haft (*1987*),* Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, Teil 2, NStZ, 10, *Möhrenschlager (*1986*),* Das neue Computerstrafrecht, wistra, 141.
[39] Cf. *Tolksdorf* in MK, § 303 a, margin no. 1.
[40] See page 22 of the present report, *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1075.
[41] See page 22 of the present report.

and information systems, adequately. Any alterations of data that constitute a computer program may also be covered by the Law for Intellectual Property, if they constitute an unlawful arrangement or adaptation of a computer program which is criminalized by Art. 66 para 1 of Law 2121/1993[42]. However, this law also aims at the protection of the intellectual property and not to that of the electronic data per se and prerequisites the existence of a "work"[43]. If electronic data and information systems contain personal data, then the Laws for the Protection of personal data could be applied. The latter aim to the protection of a special category of personal data and not to all types of them. Besides, they protect the person to whom the data refer (data subject) and not the person who has the right to access electronic data which may differ from the data subject[44].

For these reasons, regarding illegal data interference, namely the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data, the Greek legal order needs a separate provision[45], which would protect the legal interest of integrity and availability of electronic data. Indeed, such conducts, as the above mentioned, are currently addressed only to the extent electronic writings are protected under the Greek Criminal Code (Article 13(c) grCC). Pertinent offences would be forgery (Article 216 grCC), spoliation (Article 222 grCC), or even breaches of personal data or intellectual property rights (Article 22 para 4 of Statute no. 2472/1997, Article 15, para 1 of Statute no. 3471/2006, and Article 66, para 1 of Statute no. 2121/1993, respectively), while possible material damage might call for the application of Article 381 grCC proscribing damage to property as a criminal offence. As it has already been mentioned, these provisions do not adequately address the full extent of data interference[46].

Furthermore, the integrity and availability of information systems is not adequately protected in Greek Criminal law, since the interference in data processing is not fully covered by the damaging of the material part of the information system, as the latter cannot express the gravity of the violation to the data processing[47]. Illegal system interference, i.e. the intentional serious hindering or interruption of the functioning of an information system, e.g. by inputting or rendering inaccessible computer data[48], should be included in a separate provision, because its key element lies not in the potential damage to the system, but rather to the data itself[49]. The distinct criminalization is also essential due to the fact that, here, the holder of the legal interest of integrity and availability of information systems may differ from

---

[42] See *Kaiafa-Gbandi* (2007), Armenopoulos, 1075.
[43] See page 23 ff. of the present report.
[44] Cf. *Leckner/Eisele* in *Schönke/Schröder,* StGB, § 202a, margin no. 11, *Hilgendorf* in LK, 12. Auflage, § 202a, margin no. 26, *Maurach/Schröder,* p. 344, § 29 VII, margin no. 104, contra *Schlüchter* (1987), Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 63.
[45] See *Kioupis* (2000), Yperaspisi 966, *Id.,* Provisions of criminal code for internet crime, in e-themis (2012), Law in Digital era, Protection of personality, Modern forms of criminality, Electronic commerce, 159; also see *Kaiafa-Gbandi* (2007), Armenopoulos, 2007, 1076, 1084.
[46] See also *Kaiafa-Gbandi* (2007), Armenopoulos, 1076, *Kioupis* (1999), Ibid, 140–141, *id.* (2000), Yperaspisi, 965 ff.; *cf. Farantouris* (2003), Contemporary trends in Internet criminality: Defining and addressing hacking and virus attacks [in Greek], Poiniki Dikaiosyni, 194 ff.
[47] See *Kaiafa-Gbandi* (2007), Armenopoulos, 1075.
[48] Article 4 of the proposed EU Directive on attacks against information systems, COM (2010) 517 final, 30.9.2010.
[49] See *Kaiafa-Gbandi* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice, 75 ff.

the legal holder of property. The informational damage is reflected in the intervention in electronic data that in turn affects the function of the information system. The provision of damaging another person's property may be applied only in cases where the acts of computer sabotage attack things and not electronic data per se[50]. The protection of other legal interests, such as writings, intellectual property and informational self-determination, offers a limited and indirect protection to information systems, only to the extent that they contain electronic writings, works and personal data. The importance of the integrity and availability of the information systems that play a major role in modern digital societies justify, without any doubt, the need for a distinct treatment.

II.2. Criminal offences committed via computers, assaulting traditional legal interests and requiring a distinct regulation- The criminalization of computer fraud (Article 386 A grCC) and the protection deficit of electronic assaults of property

The offence of computer fraud (386 A of the Greek Criminal Code) was introduced by Article 5 of Law 1805/88 and the basic reason for this amendment of the Criminal Code was –according to the relative Explanatory Report- the fact that common fraud is limited to cases of causing an error to a person and not to a machine, i.e. a computer[51]. The protected legal interest of the above provision is the property[52], and this is made clear by the systematic integration of this provision into the offences against property as well as by the wording of the provision itself ("damages the property of another"). Other legal interests, such as the security of transactions or the security of the computer as a means of transfer and safeguarding of property[53], although proposed, have not been accepted. The main reason is that, even if another protected legal interest exists in the cases of computer fraud, property remains the main protected legal interest and the provision of Article 386 A grCC focuses on it[54]. Additionally, if one accepts that the basic protected legal interest is the electronic program, this would create problems with the joinder of offences that are articulated by Articles 370 B and 370 C para 2 grCC[55]. Besides, the fact that Article 386 A grCC provides the same penalty with Article 386 grCC (common fraud) does not allow arguing for a co-protected legal interest under the same provision, because in such a case the penalty would have to be more severe.

It has been argued that the provision of computer fraud is characterized by legal integrity[56]. However, this opinion is not widely accepted. The main problem of Article 386 A grCC is the actus reus element described as "influencing the computer data *otherwise*". This description tries to regulate the cases where the perpetrator uses, unlawfully correct, data of another person. Whereas, in German Criminal Code (§ 263a StGB), from which the Greek legislator was influenced, the unauthorized use of data ("unbefugte Verwendung von Daten"), is expressly criminalized, this is not the case in Greek criminal law. In Germany, this amendment also took place just before the vote of the relative law

---

[50] See *Bär,* Computerkriminalität, in *Wabnitz/Janowsky* (2007), Handbuch des Wirtschafs- und Steuerstrafrecht, 768, margin no. 70.

[51] See Explanatory Report of Law 1805/1988, *Kontaksis* (2000), Criminal Code, Volume 2, Art. 386 A, 3561, cf. indicatively referring to computer fraud in German Criminal law *Fisher,* StGB, § 263 a, margin no. 2.

[52] See *Vassilaki* (1993), ibid,, 185 ff.

[53] See *Nouskalis*, The criminal law protection of digital information [in Greek], in *Maniotis/Marinos/Anthimos/Igglezakis/Nouskalis/Foudedakis, ENOVE* (2004), Digital Technology and the Law, 132 ff.

[54] See *Namias* (2003), Modern forms of (electronic) fraud in bank transactions, PoinChr, 493.

[55] See *Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Armenopoulos, 1082, footnote 98.

[56] See *Mylonopoulos* (2006), ibid, 56.

in Parliament[57], whereas in the initial governmental proposal the relevant provision did not exist. An explicit regulation of committing the crime in the above way, was, however, preferred, because during the law-drafting process it was made clear by legal experts that cases in which an unauthorized person, via the use of another person's card, would withdraw an amount of money from an automated teller machine (ATM), could not be regulated by any other way of committing the crime of computer fraud (mainly via the use of incorrect or incomplete data)[58]. In any case, the new forms of criminality that are related to illegal transactions of assets related to cashless payments (for example Home banking) should not be excluded from the application field of traditional offences against property, such as theft and embezzlement[59]. Unfortunately, Greek criminal law concerning computer fraud is not characterized by such legal certainty, and the fact that the above way of committing the crime is not expressly regulated creates problems in practice.

It has been argued that in cases of unauthorized use of correct data, the prerequisite of "influencing the computer data otherwise" is fulfilled, because the perpetrator proceeds to statement by implying that he/she is the legal holder of the account[60]. The main argument upon which this opinion is based is that due to the structural similarity between computer fraud and common fraud, conduct "equivalent to the act of deception" should be subjected to the meaning of influencing the computer data[61]. This opinion seems to be justified, given the fact that, if a perpetrator would present to a bank employee a deposit book acquired via theft, the employee would take for granted that he/she is the legal holder and the offence of common fraud would be committed via a statement made by implication[62].

However, it is pointed out that the "influencing of computer data otherwise" must be of the same significance with the rest of the ways of committing the crime described in Article 386A grCC[63]. When an unauthorized use of correct data takes place, nothing changes in the automatic function of the machine and the computer data are not influenced. The perpetrator simply exploits the (uninfluenced) automatic mechanical function of the computer[64]. In this case the computer data function as they function in cases of their legal use and it cannot be accepted that they are influenced[65]. The argument that data are influenced in one way or another, given the fact that the result of the data process declines from what would be achieved via the normal and legal application of the program[66], tends to be petitio principi[67], and has systematic inconsistencies[68].

---

[57] Second Law combating financial crime-Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität

[58] See *Scheffler,* Strafrecht, σε Computerrechts-Handbuch, margin no. 63, *Cramer/Perron* σε *Schönke/Schröder*, StGB, 27.Auflage, § 263 a, margin no. 7 , *Wohlers*, in MK StGB, § 263a, margin no 34.

[59] Cf. *Leckner/Winkelbauer* (1986), Computerkriminalität-Möglichkeiten und Grenzen des 2. WiKG (II), CR, 657, *Möhrenschlager* (1986), Das neue Computerstrafrecht, wistra, 133, contra *Haft* (1987), Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, NStZ, 8.

[60] See *Mylonopoulos,* Ibid, 66 ff., Cf. *Kioupis* (1999), Criminal law and internet, 116.

[61] See *Mylonopoulos* (2006)*,* Criminal law, Special part, margin no. 1258 ff.

[62] See indicatively *Spinellis* (2011)*,* Criminal law, Crimes against property and financial legal interests, p. 360, margin no. 18.

[63] See *Papadamakis* (2000), Financial crimes [in Greek], 189.

[64] See *Papadamakis*, Financial crimes [in Greek], 190. Cf. for a broader concept of influencing *Samios* (2010), 272 ff.

[65] See *Kaiafa-Gbandi* (2007), Ibid, Armenopoulos, 1080.

[66] See *Mylonopoulos* (2006), Ibid margin no. 1255.

[67] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1080

Additionally, it is worthwhile to mention that the argument about "equivalent acts to deception", which should be subject to the "influencing of data" is not indisputable[69]. This theory, that is referred as "betrugsnahe or betrugsähnliche Auslegung", has been developed in Germany and is primarily related to the term "unauthorized" use of (correct) data in Article 263a of the German Criminal Code ("unbefugte Verwendung von Daten")[70] and not to the other ways of committing the crime of computer fraud. Consequently, it could not be applied in order to interpret the Greek provision, given also the fact that the latter differs from the relative German one, as it refers to influencing data and not to influencing the result of a data processing operation[71]. Besides, the application of the provision for computer fraud in such cases would mean in practice an unlawful imposition of sanctions by analogy, since it would equate the influencing of computer data with the exploitation of their automated function[72].

With regard to such cases in practice there is a tendency to consider scriptural money as an item, and thus, as an object of a property. It has been argued that considering scriptural money as an object contributes to the application of the provision for embezzlement to the modern transactions, releases concepts of criminal law, such as "an object", from their civil law interpretation, and constitutes an expanding interpretation that is compatible with Article 7 of the Greek Constitution. More particularly, scriptural money is, nowadays, deemed to be subject to the meaning of the term "item"[73], because this responds to the linguistic sense, given the fact that the majority of people say that they have money in a bank and mean that they have a bank account, from which it is possible to take the money, whenever they want[74]. Furthermore, it has been argued that, monetary units do not lack material status from the moment that they are incorporated to the computer of the bank[75].

On the other hand, there is a justified criticism of the above opinions, because scriptural money cannot in principle be considered an object, given the fact that it constitutes an immaterial claim[76]. For those who claim that the bank has the ownership and possession over the money[77], it would be more appropriate to apply common fraud, when the perpetrator presents his/her deposit book to the bank, where the scriptural money has been transferred, and withdraws money[78]. If he/she withdraws money from an ATM, then the provision of embezzlement should be applied[79]. For those who claim that the depositor has the ownership and possession over the money in the bank

---

[68] See *Namias* (2003), ibid, Poinika Chronika, 491 ff.
[69] See *Mylonopoulos* (2006), Ibid, margin no. 1257.
[70] See *Cramer/Perron,* in *Schönke/Schröder,* StGB, § 263 a StGB, 27. Auflage, margin no. 9 ff. and margin no. 21, *Samios* (2010), ATM cards and criminal law, 253 ff., *Wohlers* in MK,§ 263a StGB, margin no. 36 ff.
[71] See *Namias* (2003), Ibid, Poinika Chronika, 492. Contra *Samios* (2010), ATM cards and criminal law, 249 ff.
[72] See *Kaiafa-Gbandi* (2007), Ibid, Armenopoulos, 1081.
[73] See *Spinellis* (1996), Private Consultation, PoinChr, 432 ff.
[74] See *Androulakis* (1995), Criminal Varia, Poinika Chronika, 687.
[75] See *Symeonidou-Kastanidou* (1998), Embezzlement and scriptural money, Yperaspisi, 942.
[76] See *Mylonopoulos* (2006), ibid, margin no. 418 ff.
[77] See *Mylonopoulos* (2006), ibid, 181 ff. Cf. *Fasoulas* (1995), Private Consultation, Poinika Chronika, 1304.
[78] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1081.
[79] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1081.

account[80] it is more appropriate to accept that an embezzlement is committed only when the perpetrator receives interests, withdraws money or proceeds to payments[81].

Consequently, the legal interest of another person's property is not adequately protected, given the fact that, according to the above opinion, in these cases of transfer of scriptural money, computer fraud is not always committed, while embezzlement cannot cover the loopholes. Thus, Article 386 A grCC should be revised, in order to cover the cases of use of correct data without right, explicitly.

II.3. Content related crimes-The criminalization of child pornography and the controversy over the protected legal interest

The Greek Criminal Code has a special provision for child pornography when committed by means of a computer system or through the internet (Article 348A para 2), providing for a higher penalty. However, the main problems related to this provision do not refer to the special means of committing the crime, but to the determination of the protected legal interest, which has been a controversial issue[82].

Minority as a legal interest is related to the evolution of man from his birth until his physical, mental and sentimental integration[83]. It is deemed as a highly important legal interest (given the fact that the society's maintenance and promotion are based on it) and a distinct one from other personal legal interests (such as physical integrity or personal freedom), thus calling for distinct protection.

If somebody takes into account the influence of computer systems and internet, as means of knowledge, communication entertainment etc.[84], on the development of minors, then the possible interconnection between attacks against minority and information systems or the internet becomes easily understandable.

The offences of the Greek Criminal Code against minority that refer expressly to the use of computer systems or the internet are Articles 348 para 3, 348A para 2, 348B and 337 paras 3 and 4 grCC. They refer respectively to: facilitation of fornication with juveniles on commercial scale, child pornography, attracting children for sexual reasons and insult to sexual dignity of juveniles. This does not mean, however, that other offences against minority, such as the advertising of sexotourism against juveniles (Article 323 B grCC) cannot be committed via the use of information systems or the internet. It is reasonable to ask why then only the above mentioned specific internet-cyber attacks against minority have been regulated and not others, whereas the above criminal offences –except for one (348 B grCC) - can be committed according to law also without the use of information systems or the internet. The answer to this question is related on one hand, to the expansion of the specific forms of criminality via the internet[85], and to the other, to the relative international and European legislation that is binding for Greece in respect of criminalizing

---

[80] See *Androulakis* (1994), Criminal Varia, Poinika Chronika 673 ff., *Simeonidou-Kastanidou* (1998), ibid, Yperaspisi, 943.
[81] See *Kaiafa-Gbandi* (2007), ibid, Armenopoulos, 1081.
[82] See for the following considerations *Kaiafa-Gbandi* (2012), Internet assaults on infancy, Poinika Chronika, 162 ff.
[83] See *Manoledakis* (1998), The legal interest as a fundamental concept of Criminal law, 281 ff.· cf. for a critical view for the specific legal interest *Paraskevopoulos,* Sexual self-determination a common legal interest of the nineteenth capital of Criminal Code, in Honorary Volume for St. Alexiadis (2010), 810-811.
[84] See indicatively *Ahmed*, Who does what to children, where, why and how?, in D. Spinellis (ed.) (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, 195-201.
[85] See indicatively *Ahmed* (2004), ibid, 195-201.

specific behaviors. Of particular importance are the relevant Conventions of the Council of Europe for: [86]a) Cybercrime, b) the protection of children against sexual exploitation and sexual abuse[87] , as well as c) the relevant legal instruments of the E.U[88].

As already mentioned the main issue with Article 348 A grCC is the legal interest that the provision aspires to protect[89]. In other words, the classification of child pornography to the violations against minority is not indisputable.

The problem arises not only out of the fact that the legislator criminalizes the various acts that are depicted in Article 348 A grCC even if the pornographic material that is produced, sold etc., is totally virtual (: concerning non-existent minors), but also out of the fact that the relative acts are criminalized even if this material concerns minors over the age limit for sexual consent (15 years). Thus, the challenging question is: why the lascivious act with a minor over 15 years old is not punishable, whereas the representation with his/her consent of the sexual activity that has taken place should be punishable?

In the least problematic cases, i.e. in those that refer to pornographic material which is produced with real minors, and particularly under the age of 15 years, we can claim that the protected legal interest is minority, as determined above, i.e. the undisturbed development in the sector of sexual life of minors that are used in the specific case for the production of the pornographic material. It plays no role, if the minors provide their consent for these acts, nor if the acts take place on their own initiative, as is the case also in the offence of seduction.

However, regarding the acts of distribution, obtaining or possession of this material by persons that have not produced it, a violation of minority regarding the minors that have been used for the production cannot be claimed, as this is already completed and minority cannot be further influenced by the acts of the persons that take place after it[90]. In these cases one could, however, recognize a violation of the sexual dignity and of the sensitive personal data of the specific minors depicted, given the fact that the pornographic material produced is destined not to be subject to their own power of disposal but to be distributed to other persons, perpetuating, in this way, the humiliating treatment

---

[86] Convention on Cybercrime, ETS 185, 23.XI.2001

[87] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.X.2007, and for its ratification see Law 3727/2008.

[88] See Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA**, t**his Directive was remunerated from 92 to 93 via the Corrigendum to Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011.

[89] See the different opinions in *Kaiafa-Gbandi* (2012)*,* Ibid, Poinika Chronika, 163 ff., *Karanikolas* (2005), Child pornography on the internet: Concerns about the new regulation of Article 348 A of the Greek Criminal Code, Poiniki Dikaiosyni, p. 973 ff., *Kioupis* (2008), Child Pornography- Interpretative approaches to article 348A PC, Poinikos Logos, 6-8, 12, 19, *Kostaras* (2007), Criminal law, Compendium of Special Part, third edition, p. 905, *Nouskalis* (2006)*,* Child Pornography: The crucial issues of article 348A of the Greek Criminal Code, Poiniki Dikaiosyni, 910, *Simeonidou-Kastanidou* (2006), Crimes against personal legal interests, 247-248, cf. *Perron / Eisele*, in: *Schönke/Schröder*, StGB, 184b, margin no. 1.

[90] See *Neumann, U*., The criminal liability of the participant in the purchase, in *Kaiafa-Gbandi/Prittwitz*, Surveillance and criminal suppression (in Greek), 2011, 203-204.

of minors as objects of sexual exploitation. This latter element is also traced in the criminalization of child pornography, when it concerns a real child that is over the age of sexual consent.

It is self-evident that different acts referring to the pornographic material can also constitute a violation against other minors, since viewing such material is possible to have negative effects on the undisturbed sexual development of young individuals who have not been used for its production, at least whilst they are under the age-limit of sexual consent. This point of view is now favored by the punishability that is founded upon Article 339 para 4 of grCC, which criminalizes the forcing or inducement of a minor (under 15 years old) to be simply present during a lascivious act between other persons, although this form of violation of the legal interest of minority does not claim to have the same intensity.

Defining the legal interests aspired to be protected in the forms of committing the crime by means of virtual child pornographic material is far more difficult. This holds true, even under the necessary prerequisite that virtual representation is at least realistic (See so the Article 2 c (iv) of the Directive 2011/93/EU), so that the image can affect its viewers in the way that the real representation, for example of lascivious acts with minors, does.

Regarding this category of conduct, it has been argued that the criminalization of acts related to virtual pornography protects the public order, in the sense –and under the condition- that via such acts, an undercover provocation to committing crimes of sexual exploitation of minors takes place[91]. However, such a violation of public order would require committing the act *in public*. Besides, it has not been empirically proven that the view of children pornographic material (virtual or real), even by pedophiles, functions provocatively in the committing of similar acts[92] .

If someone attempts to trace back a violation of existent legal interests through the production and distribution of virtual (but realistic) child pornography, then one has to require the existence of a realistic possibility that viewers of this material could be minors, since this is apt to damage their undisturbed sexual development[93]. According to this concept, the act that refers to the virtual child pornographic material, especially in the case that has to do with forms of the offence referring to an early stage, such as production of the material, should –also- be meant to address minor viewers, in order to bear substantial punishability. Of course, this element does not, always, derive, easily, from objective data. Given the fact, however, that nowadays in most cases, and especially in the framework of child pornography that is distributed via the internet, the possibility of access of minor viewers to the (virtual) child pornographic material cannot be excluded, the punishability of such acts could also be based upon the violation of an existent legal interest, in the form of an establishment of a source of danger for the minority by the act of production of child pornographic material. It is necessary, however, that this possibility is not excluded in the concrete case under scrutiny. In other words, such conditions that, objectively, establish the possibility of risk for the distribution of

---

[91] See *Simeonidou-Kastanidou* (2006), Crimes against personal legal interests, 247-248.

[92] See *Paraskevopoulos-Fitrakis,* Punishable sexual acts, Articles 336-353 of the Greek Criminal Law, 282-283). On the contrary, it is argued that viewing such material can even restrain from similar behavior (*Seto / Cantor / Blanchard* (2006), Child Pornography Offenses Are a Valid Diagnostic Indicator of Pedophilia, Journal of Abnormal Psychology Copyright, 614, *Williams* (2004), Child pornography Law: Does it protect children?, Journal of Social Welfare and Family Law, 251.

[93] *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 164. Cf. the Explanatory Report of Cybercrime Convention, margin no, 45· see also *Carr/Williams* 2002, Computer Law and Security Report, 84.

the material –also- to minors and a further intent for addressing them should exist. Such an opinion does not imply, of course, that the legislator should overlook the ultima ratio principle with regard to acts that are related to virtual child pornographic material, especially given the fact that this is distributed primarily via the internet and in this framework there are other, milder, possibilities to address the problem, e.g. controlling websites with illegal content [94].

It is, of course, questionable, whether such an interpretation could be applied even after the obligatory implementation of Directive 2011/93/EU of the European Parliament and the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA in the Greek law[95].

This Directive includes in the definition of child pornography the virtual pornographic material as well, and more particularly, it refers both to pornographic material of realistic images of a child and to pornographic material of images of a person appearing to be a child (Article 2 c (iii) and (iv)). However, Article 5 para 7 provides that it shall be within the discretion of the Member States to decide over the criminalization of any of the behaviors that are referred to in the provision as offences of child pornography, where the person appearing to be a child was in fact 18 years or older at the time of depiction[96]. Thus, virtual pornography to this extent can –and should- remain out of the scope of criminal law. This choice is based not only on the difficulties of establishing a substantial punishability in such cases, but also on the need of using criminal law as ultima ratio. On the other hand, for the cases that refer to realistic images of children with pornographic content, Article 5 para 8 of the new Directive provides the possibility to the Member States not to criminalize acts of production and possession of such virtual pornographic material, where it is established that it is produced and possessed by the producer solely for his or her private use, in so far as no pornographic material of real people (even adults appearing as juveniles) has been used for the purpose of its production, and provided that the act involves no risk of dissemination of the material. This choice of limiting punishability is also positive, since it contributes substantially to a limitation of the relevant problems. Consequently, both pornographic material that concerns adult persons appearing to be children, and also the production and possession of virtual pornographic material with realistic images of minors, solely for the use of the producer, could be excluded from punishability. Still, the production, acquisition or possession of virtual pornographic material with the characteristics of Article 8 para 5 of the Directive for the distribution to a third person, even an adult, for the personal use of the latter, remains punishable according to the Directive. The European legislator obviously considers that as long as the producer or the possessor of virtual pornographic material provides it to a third person, he/she cannot control the risk of further distribution of it to others, among which there could also be minors, even if the receiver claims that he/she will use it solely for his/her own personal use. This seems to be the underlying reason for criminalizing the relevant conduct.

According to a restrictive interpretation of the Directive, and particularly of Article 5 para 7 and 8[97] Member states should criminalize all acts concerning virtual pornographic material with realistic images of minors, provided that they constitute a form of distribution-dissemination of the material. If they are prior to distribution (production, acquisition,

---

[94] See *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 165.
[95] See for the following *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 165 ff.
[96] See also Article 3 para 2 a of the Framework Decision 2004/68/JHA.
[97] See *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 166.

possession) criminalization is deemed acceptable only when such conduct takes place with a further intent of distribution or of possession not for personal use, and therefore, it objectively constitutes a risk of dissemination of the material. In such cases one can still establish punishability in a form of violation (even at an early stage) of an existent legal interest that concerns the possibility of minors to gain access to and view this material. Of course, this latter element is not expressly written in the Directive, but it can be concluded by its whole text, which concerns the protection of minors in the field of sexual life.

The extent of punishability could also be controlled by the Greek legislator in a much better way via the use of the possibility of limitation, recognized by the Directive in Article 8 para 3[98]. According to this provision, Member States are offered the chance not to punish the production, acquisition or possession of material involving children who have reached the age of sexual consent, when that material is produced and possessed with their consent and only for the private use of the individuals involved. A violation of a legal interest cannot be traced in such a case, as well, since the depicted person is over the age of sexual consent and the production or possession of the pornographic material is undertaken solely for personal use and with his/her consent[99].

II.4. Traditional criminal offences particularly facilitated by the use of information systems

In Greek Criminal Law the term "writing" covers, after a relative alteration of Article 13 grCC (by Article 2 of Law 1805/1988), every means that is used by a computer or a peripheral computer memory, electronically, magnetically or otherwise, for the registration, storage, production or reproduction of data or other materials in which any information, image, symbol or sound is registered, separately or in combination with another, provided that these means and materials are intended or are adequate to prove facts that have legal significance. Although this Article may seem to require only the evidentiary function for the notion of a "writing", it is argued that the writing must also be incorporated constantly on a material substance (perpetuate function of the writing), whereas the author of the writing must also be deductable (guarantee function of the writing)[100].

In particular, the guarantee function -a prerequisite for the notion - of a writing could create many problems, given the fact that computer data which are electronically stored in a computer system, do not usually bear the name of their author[101] . However, this argument could be dispelled, as according to the intellectual theory for the detection of the author, it is vital to know the person who takes the responsibility that derives from a writing[102]. Consequently, it is not necessary to know the person who may type a text, but the person who is responsible for the input of data[103]. However, there are many problems, when trying to detect the author of an electronic document, as computer data may be stored to a hard disk to which many individuals may have access[104].

---

[98] See *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 166.
[99] Cf. *Kioupis* (2008), Ibid, Poinikos Logos, 18, who criticizes the Greek legal order for the inconsistencies that are created by the lack of exemption of punishability.
[100] See *Mylonopoulos* (1991), ibid, 46 and 42.
[101] See *Sieber* (1980), Computerkriminalität und Strafrecht, 2. Auflage, 357, footnote 56.
[102] See indicatively *Mylonopoulos* (2005), Criminal law, Crimes referring to writings [in Greek], 44 ff.
[103] See *Leckner/Winkelbauer* (1986), Computerkriminalität-Möglichkeiten und Grenzen des 2. WiKG (III), CR, 825.
[104] See *Kioupis* (1999), Criminal law and internet [in Greek], 150 ff.

Elements that could lead to the detection of the author are the restrictions of access to data, but also the fact that only specific individuals may know a password[105]. The existence of a person who is responsible to set in motion the electronic data process and approve of this process may also be helpful[106] .

Due to the difficulties referring to the detection of the author of a writing, but also due to the lack of the evidentiary function of many computer data, or of the perpetuate function, Article 13 c grCC offers a limited protection. Besides, data that are transmitted via telecommunication systems are not protected[107]. The problem in such cases lies in the risk of protecting data through provisions referring to other legal interests, such as the notion of a writing, as this could lead to misunderstandings or even to an excessive expansion of the application filed of the relevant provisions[108].

II.5. Provisions referring to intellectual property

Various opinions have been expressed with regard to the protected legal interest of the criminal provisions of Law 2121/1993 (Art. 66, 66 A and 66 B). It has been argued that the protected legal interest here is the information, and more particularly, its utilitarian and exchange property[109]. This opinion could hold true as far as Articles 66 A and Article 66 B of Law 2121/1993 are concerned. These provisions criminalize the bypassing of technical measures and the alteration of data for the status of rights without the rightholder's license. This may also be true for offences against intellectual property concerning digital work, such as work that is created, exclusively, via the use of a computer system or one that is resolutely influenced from its use[110]. However, according to the Greek legal theory, intellectual property law does not protect information per se and pieces of work are not information[111]. Thus, it is argued that the form or expression is the real object of protection, and not the idea itself[112].

It is also claimed that the protected legal interest is the economic right deriving from a piece of work, as well as the right of protection of the personal nexus of the author with his/her work (moral right). More particularly, it is argued that the forms of committing the offence described in Article 66 para 1 of Law 2121/1993 are connected to the work's economic exploitation without the consent of the author, and thus, violate the property of the author[113]. Besides, these forms of violation are completely in line with the economic powers of the author[114].

On the other hand, referring to the ways of committing the relevant offence that violates the moral right of the author, i.e. the power to have a say on the ways of communicating his/her work to the public, as well as to present it without additions or distortions, following arguments have been expressed: Article 66 para 1 of Law 2221/1993 criminalizes only the violation of the moral right, concerning the power of publication and safeguarding of the work, since it is

[105] See *Mylonopoulos* (2005), ibid, 47.
[106] See *Cramer/Heine* in *Schönke/Schröder*, StGB, § 269, margin no. 12.
[107] See *Mylonopoulos* (1991), ibid, 52.
[108] See *Mylonopoulos* (1991), ibid, 50.
[109] *Nouskalis,* Criminal protection of computer program in Law 2121/1993, 63 επ.
[110] See for digital works *Marino*s, Intellectual Property, 2nd edition, 122 ff.
[111] See indicatively *Kallinikou* (2005), Intellectual property, Second Edition, 39.
[112] See *Marinos* (2004), Intellectual Property, Second Edition, p. 71, margin no. 139.
[113] See *Ouroubeis* (2000), Criminal protection of intellectual property, 85.
[114] Cf. *Kotsiris* (2005), Intellectual Property Law, Forth Edition, p. 259, margin no. 420.

easier to trace the violation in comparison to other moral rights[115]. The violation of these two moral rights results to a violation of the legal interest of the author as a particular aspect of one's individual freedom, which is regulated principally in Article 330 grCC[116].

II.6. The protection of personal data

In many occasions the protection of personal data and the criminal suppression seem to be in conflict, since personal data protection addresses the minimization of their collection, storage and transmission, whereas penal repression demands as much information as possible, in order to ensure an effective criminal prosecution[117]. The Law for the Protection of the Individual with regard to processing of personal data (Law 2472/1997) protects private life or informational self-determination[118]. Informational self-determination constitutes an aspect of the protection of the right to personal life[119]. In this context, it would be more prudent to argue that the informational self-determination is the protected legal interest in the frame of Law 2472/1997. This includes the right of an individual to determine the disclosure and use of information that concern him/her.

The evolution of information systems has offered uncountable possibilities of storage and interconnection of information for all aspects of an individual's private and public life. Such possibilities are combined with serious interventions to his/her personality[120]. For this reason, informational self-determination is a legal interest worthy of protection in a modern digital world entailing numerous and serious risks for one's personal life.

III. Typical examples of Greek criminal laws concerning electronic crimes

a) Criminal law provisions concerning attacks against IT systems

The attacks of the confidentiality of IT Systems are criminalized in Article 370 C paras 2-4 grCC. According to this provision: "Whosoever obtains access to data that have been entered into a computer or a peripheral computer memory or are transmitted via telecommunication systems, provided that these acts were unauthorized, especially by infringing prohibitions or security measures that have been taken by the legal holder, shall be punished with imprisonment of not more than three months or a fine of at least ten thousand drachmas [29,00 Euros]. If the act refers to international relationships of the security of the state, shall be punished according to Article 148.

3. If the perpetrator is at the service of the legal holder, the act of the former paragraph shall be punished only if it is expressly forbidden by an internal regulation or by a written decision of the legal holder or his/her competent employee.

---

115 See *Kallinikou* (2005), Ibid, 308.

116 See *Simeonidou-Kastanidou* (1991), Commentary on decision 77/1991 of the *Pre-trial Chamber of the Court of Appeals,* Yperaspisi, 870.

117 See *Bär,* Straftaten und Ordnungswidrigkeiten gegen den Datenschutz, in *Roßnagel,* Handbuch Datenschutzrecht, 913, margin no. 1, see also *Nouskalis* (2007), Criminal protection of personal data, 80 ff. for the use of evidence, that derives from acts that infringe the Law for the Protection of Personal Data, in criminal proceedings.

118 See *Paraskevopoulos,* The distinction between risk and damage in modern Criminal Law, in *Courakis* (Ed.) (2001), Criminal Sciences in the 21st century, Honorary Volume for Spinellis, 806.

119 See *Igglezakis* (2003), Sensitive personal data, 55. Cf. *Tinnefeld/Ehmann*, Einführung in das Datenschutzecht, 84, *Nouskalis* (2007), Criminal protection of personal data, 13.

120 See *Augoustianakis*, Protection of individual referring to processing of personal data, Rights of Individual 2001, 679

4. The acts or paragraphs 1 to 3 are prosecuted only upon a complaint".

The attacks of integrity and availability of IT Systems are criminalized by Article 381 of the grCC. If IT Systems contain an electronic storage device that satisfies the prerequisites for the application of Article 13 (c) of the grCC (which refers to the notion of "writing") then Article 222 of grCC is applicable.

Article 381 grCC (Damaging another person's property) prescribes that: "Whosoever intentionally damages or destroys an object, wholly or partially, not belonging to him/her or otherwise renders its use impossible shall be punished with imprisonment of not more than two years".

b) Criminal law provisions concerning IT privacy

IT privacy is protected by Article 370 B grCC, Article 370 A grCC (referring to a system of software or hardware for the provision of telecommunication services) and the laws regarding the protection of personal data, i.e. Law 2472/1997 and Law 3471/2006.

Article 370 B grCC reads as follows:

"1.Whosoever unlawfully copies, imprints, uses, discloses to a third party or in any way infringes data or computer programs, that constitute state, scientific or professional secrets or secrets of a company of the public or private sector, shall be punished with imprisonment of at least three months. As secrets are also considered data that are treated as such by the legal holder of a justified interest, especially when he/she has taken measures in order to prevent third parties from being aware of them.

2. If the perpetrator is at the service of the legal holder of the data, or if the secrecy has great economic value, the act shall be punished with imprisonment of at least one year.

3. In case of military or diplomatic secrets, or secrets that refer to state security the act of paragraph 1 shall be punished according to articles 146 and 147.

4. The acts that are prescribed by paragraphs 1 and 2 are prosecuted only upon a complaint".

Article 370 A para 1 grCC (Violation of secrecy of telecommunication and oral conversation) provides that: "Whosoever, without authorization, intercepts or intervenes otherwise to a device, connection or network that is used for the provision of telecommunication services or to a system of software or hardware, which is used for the provision of such services, so that he/she or a third person obtains information or records to a means of storage the content of a telephone conversation between a third party or the location or traffic data of such a communication, shall be punished with imprisonment of up to ten years. The act of the former subparagraph shall be punished also with the same sentence, when the perpetrator records to a means of storage the content of his/her telecommunication with another person without his/her consent".

Article 22 para 4 of Law 2472/1997 provides that: "Whosoever unlawfully interferes in any way in a personal data file or takes knowledge of such data or deprives, alters, destroys, damages, processes, transmits, discloses, makes these data available to unauthorized individuals, or allows these individuals to take knowledge of these data or exploits them in any way, shall be punished with imprisonment and a fine, and in case of sensitive data with imprisonment of at least one (1) year and a fine amounting one (1.000.000) to ten million (10.000.000) drachmas, unless the offence is subject to a more severe penalty under other provisions".

Article 15 of Law 3471/2006 provides that: "Whosoever, by infringing the present law, uses, collects, stores, takes knowledge, deprives, alters, destructs, transmits, discloses, publicizes personal data of subscribers or users, or makes the above data available to unauthorized individuals or allows these individuals to take knowledge of them or exploits them in any way, shall be punished by imprisonment of at least one (1) year and a fine amounting ten thousand to one hundred thousand Euros (10.000-100.000), unless the offence is subject to a more severe penalty under other provisions".

c) Criminal law provisions concerning forgery and manipulation of digitally stored data

Forgery and manipulation of digitally stored data are punished by Article 216 and 222 grCC, which criminalize forgery and misappropriation of writings. In the Greek criminal code the meaning of a writing can include digital data storage media under specific conditions. In particular, Article 13 c grCC provides that: "Writing shall mean every written material that is intended or adequate to prove a fact with legal significance as well as every sign that is intended to prove such a fact. Writing is also every means that is used by a computer or a peripheral computer memory, electronically, magnetically or otherwise, for the registration, storage, production or reproduction of data or other material in which any information, image, symbol or sound is registered, separately or in combination with others, provided that these means and material are intended or are adequate to prove facts that have legal significance".

Article 216 grCC (Forgery) provides that : "1. Whosoever produces a forged writing or alters a writing with intent to use it in order to defraud a third person concerning a fact which may have legal significance, shall be punished with imprisonment of not less than three months. The use of the writing by him/her shall be deemed as an aggravating circumstance.

2. Whosoever uses knowingly a forged or altered writing for the above purpose shall be subject to the same punishment."

Article 222 grCC (spoliation) reads as follows: "Whosoever with intent to cause damage to a third person conceals, damages or destroys a document of which he/she is not the owner, or the exclusive owner, or of which a third person has the right under civil law provision to demand the delivery or presentation shall be punished with imprisonment of not more than two years."

Article 386 A grCC (computer fraud) provides that: "Whosoever with intent of obtaining for himself or for a third party an unlawful material benefit, damages the property of another, influencing the computer data either via incorrect configuration of a program or via intervention in its application or by using incorrect or incomplete data or otherwise, shall be punishable with the penalties of the former Article {Article 386-fraud}. Property damage exists even if the victims are unknown. For the estimation of damage the number of victims is irrelevant".

d) Criminal law provisions regarding the distribution of computer viruses

Distribution of computer viruses is not regulated per se in the Greek criminal law[121].

e) Criminal law provisions regarding virtual identities of users

Crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities, are only criminalized when the prerequisites of Article 13 c grCC are fulfilled[122].

[121] See page 22 of the present report.

f) Criminal law provisions regarding the creation and possession of certain virtual images

The criminalization of the creation and possession of certain virtual images is provided by Article 348 A grCC (child pornography). This article reads as follows:

"1. Whosoever intentionally produces, distributes, publicly displays, presents, imports or exports from the territory, transports, offers, sells or supplies otherwise, purchases, acquires, obtains, or possesses child pornography material or diffuses or transmits information about the perpetration of the above acts, shall be punished with imprisonment of at least one year and a fine amounting ten thousand to one hundred thousand euro.

2. Whosoever intentionally produces, offers, sales or makes available otherwise, distributes, forwards, purchases, acquires, or possesses child pornography material or transmits information about the perpetration of the above acts via a computer system or using the internet, shall be punished with imprisonment of at least two years and a fine amounting fifty thousand to three hundred thousand euro.

3. Child pornography material in the frame of the above paragraphs shall mean the representation or the real or virtual recording in a electronic or other storage media of a child´s body or part of his/her body, in such a way that manifestly causes sexual arousal, as well as the real or virtual lascivious act that is performed by or with a child.

4. The acts of the first and second paragraphs shall be punished with imprisonment not exceeding ten years and a fine amounting fifty thousand to one hundred thousand euros:

a. if they were committed on a commercial basis or habitually,

b. if the production of the child pornography material is connected to the exploitation of the need, the psychological or mental disease of a child, the physical malfunction due an organic disease, or the use or threat of use of violence against a child, or the use of a child that is below fifteen years old.

If the act of subsection b1 resulted to grievous bodily harm, the act shall be punished with an imprisonment of at least ten years and a fine amounting one hundred to five hundred euro, and if it has resulted to death, it shall be punished with life imprisonment".

g) Criminal law provisions referring to the violation of copyright in the virtual sphere

The violation of copyright in the virtual sphere is criminalized by Article 66 of Law 2121/1993 (Criminal sanctions). This article prescribes that: "Whosoever unlawfully and in breach of the provisions of the present law or the provisions of the multilateral conventions for the Protection of Intellectual Property that are ratified by law, records works or copies or reproduces them directly or indirectly, temporarily or permanently, in any form, in part or in whole, translates, arranges, adapts or alters them, proceeds to distributing them to the public by sale or otherwise, or possesses with intent to distribute, rents, performs publicly, broadcasts by any means, communicates to the public, by any means, works or copies, imports copies of the work that were produced unlawfully abroad without the consent of the rightholder and generally exploits works, copies, or transcripts that are subject to intellectual property, or violates the moral right of the rightholder to decide for the communication of his/her work, as well as to present it without additions or distortions, shall be punished with imprisonment of at least one year and a fine amounting 2.900 to 15.000 euro (Article 8 par. 1 of Directive 2001/29)."

---

[122] See pages 22 ff. of the present report.

IV. The typical description of criminal conduct (actus reus) of electronic crimes and the definition of the object

The criminal conduct (actus reus) of electronic crimes is typically defined in Greek law by a detailed description. This appears to be reasonable, since such criminal conduct, related to new forms of criminality, could not be precisely delimited by describing only a kind of result. The need for specificity (n.c.n.p.s.l principle) leads to the need of defining the relative offences with clarity. For example, one could not prescribe computer fraud (386 A grCC) just by providing that such an offence commits "Whosoever with intent of obtaining for himself or a third party an unlawful material benefit damages the property of another, by influencing the computer data ….", because in such a case the notion of "influencing the computer data" would be unclear.

The term "data", which is the object of the offence in Articles 370 B (infringement of secrecy), 370 C (access to data), 386 A (computer fraud) grCC, is not further defined in the Greek Criminal Code and therefore there is a problem of vagueness in these provisions. The term of "writings", as it was analyzed above[123] was extended in order to cover electronic means of storage under specific conditions[124]. The notion of "Writing" is defined as we have already seen in Article 13 (c) grCC. This definition, although aiming at clarity, is still problematic, because it does not clarify whether the new storage devices are supposed to provide all three functions that the other writings ought to have[125]. Furthermore, instead of providing special protection to data providing proof (as it is the case in Article 269 of the German Criminal Code), Article 13 c grCC extends the criminal protection to electronic storage means. Consequently, the protection is oriented to tangible objects and not to data, whereas the latter may demand a special protection due to their autonomy from their means of storage.

V. Criminal liability for certain electronic crimes - Particular groups of perpetrators and/or victims

1. Perpetrators and victims

In the majority of electronic crimes **the perpetrator** can be anyone ("whosoever"), and the criminal liability is not limited to a particular group of individuals. In this sense, electronic crimes are "common" and not special crimes, i.e. they could be committed by anyone.

In some cases, if a member of a particular group of perpetrators commits an electronic crime, a higher penalty may be provided, because the perpetrator's capacities or status reveal a more severe violation of the protected legal interest. For example, the perpetrator of the crime plays a role in article 370 A para 4 which provides that: "If the perpetrator of the acts of paragraphs 1, 2 and 3 of the present Article is a provider of telecommunication services or his legal representative or a member of the administration or a responsible for the safeguarding of the secrecy or an employee or a collaborator of the provider or a person who performs private investigations or performs these acts on a commercial basis or habitually or someone who intended to receive payment, shall be punished with imprisonment of up to ten years and a fine amounting from fifty five thousand (55.000) to two hundred thousand (200.000) Euros". Article 370 B para 2 of the Greek Criminal Code stipulates also that: "2. If the perpetrator is at the service of the legal holder of data, or if the secrecy has great economic value, the act shall be punished with imprisonment of at least

[123] See page 22 of the present report.
[124] See page 22 of the present report.
[125] See page 22 of the present report.

one year." A distinct treatment is also provided for a particular group of perpetrators in Article 370 C par. 3 grCC. According to this provision: "3. If the perpetrator is at the service of the legal holder, the act of the later paragraph shall be punished only if it is expressly forbidden by an internal regulation or by a written decision of the legal holder or his/her competent employee."

Another, general, category of electronic crimes, where the perpetrator's capacities or status could play a role is the category of offences committed via omission. In Article 292 par. 3 grCC an offence by omission is laid down and more particularly it is prescribed that: "A provider of telecommunication services or his legal representative or the responsible for the safeguarding of the secrecy of communications according to Article 3 of the present law, who omits to take the necessary measures for the prevention of an act of paragraph 1, shall be punished with imprisonment of at least two years and a fine amounting from fifty thousand (50.000) to two hundred thousand (200.000) euro, provided that the act was committed or an attack to commit it took place, irrespective of whether the perpetrator will be punished or not".

On the other hand, the only electronic crimes that are limited to a certain group of **victims** are the offences of Articles 348 A (child pornography) and 348 B (attracting of children for sexual reasons) grCC, that protect the legal interest of minority in the modern digital world. Minors are nowadays viewed as victims at the centre of the modern evolution of electronic criminality. They are the main users of information systems and the internet and thus, the need for penal repression of electronic attacks against minors is evident[126]. Article 348 B grCC provides relevantly that: "Whosoever, via the information and communication technology, intentionally proposes to an adult to meet a juvenile, that has not completed the fifteenth year of his/her age, with an intent of committing the offences of paragraphs 1 and 2 of the Articles 339 and 348 A grCC against him/her, when such a proposal is followed by further acts that lead to committing of the offences, shall be punished with an imprisonment of at least two years and a fine amounting from fifty thousand to two hundred thousand euro".

2. Mens rea of electronic crimes

Criminal liability in the area of ICT and the internet is limited to acts that are committed intentionally, since it is not especially prescribed by law, as Article 26 para 1 grCC requires, that they could be committed also with negligence[127]. Only in Laws concerning personal data, one can find offences that are punished in case of negligent conduct.

More particularly, Article 22 par. 8 of Law 2472/1997, referring to the protection of individuals with regard to the processing of personal data**,** stipulates that: "If the acts of paras 1 to 5 of the present article are committed by negligence, the perpetrator shall be punished with imprisonment of up to three (3) years and a fine". On the other hand, Article 15 para 4 of Law 3471/2006 regulating the protection of personal data and private life in the field of electronic communications, provides that: "If the acts of paragraphs 1 and 2 of the present Article are committed by negligence, the perpetrator shall be punished with imprisonment of up to eighteen (18) months and a fine of up to ten thousand euro (10.000)". A negligent offence is to be found also in Article 11 para 4 of Law 4070/2012 regulating –

[126] See *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 161 ff.

[127] According to Article 26 para 1 grCC "Felonies and misdemeanors are punished only when they are committed with intent. Exceptionally, in cases where it is prescribed by law, misdemeanors shall be punished also when they are committed by negligence".

inter alia- electronic communications, which provides that: "If the acts of paragraphs 1 and 2 have been committed by negligence, the perpetrator shall be punished with imprisonment of at least two years." The same is true for Article 292 para 1 grCC, which foresees that: "Whosoever intentionally hinders the operation of a public facility that serves transport and particularly a train, airplane, bus, post or telegraph that is destined for common use, shall be punished with imprisonment of at least three months", and for Article 292 para 2 grCC, which provides that: "If the act was committed by negligence, the perpetrator shall be punished with imprisonment of up to six months".

VI) Differences between the definition of electronic crimes and "traditional" crimes

By defining electronic crimes there is a legislative tendency of referring to as many ways of committing the crime as possible. This fact becomes also clear if one takes a look at the provisions of international and European legal instruments that foresee the criminalization of electronic crimes and compares them with the relative offences of the Greek Criminal Code, particularly in the field of offences against the confidentiality, integrity and availability of information systems and electronic data. For example, under illegal data interference, the international legal instruments foresee the criminalization of the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data of an information system[128]. This could lead to inconsistencies, where some ways of committing the crime coincide. For instance, the terms suppression or rendering inaccessible of computer data of an information system seem to be pretty close and it is not clear where the dividing line between them should be drawn.

Referring to the technological terms that are used in electronic crimes, it should be emphasized that, in the Greek Criminal Code, there is no definition of the terms "information systems" and "electronic data". This can create serious problems based upon the vagueness of the relevant provisions using these terms. Thus it would be prudent, by incorporating the international legal instruments into the Greek legal order, to include a clear-cut definition of the terms "information system" and "computer data" under Article 13 grCC, based on the definitions contained in the relevant proposal for an EU Directive and the Council of Europe Convention[129], an 'information system' is defined as "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". On the other hand, Article 2(b) of the proposed directive defines 'computer data' as "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".

With regard to the term of "writings" it has already been noted that, in the Greek Criminal Code, this term has been explicitly broadened, in order to cover "every means that is used by a computer or a peripheral computer memory,

[128] Article 5 of the Proposal for a Directive on attacks against information systems and in Article 4 of the Framework Decision on attacks against information systems; cf. Article 4 of Convention on Cybercrime, which does not prescribe the rendering inaccessible of computer data on an information system.

[129] See *Kaiafa-Gbandi* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice 2012, 77). According to Article 2(a) of the Proposal for a Directive on attacks against information systems (COM (2010) 517 final, 30.9.2010, 15.

electronically, magnetically or otherwise, for the registration, storage, production or reproduction of data or other materials in which any information, image, symbol or sound is registered,……."[130].

VII) Problems with respect to the principle of legality

In the Greek Criminal Law, problems regarding the principle of legality arise also in the frame of electronic crimes. These are connected to the vagueness of Articles 370 C para 2, 370 A, 386 A and 348 A grCC. The main of these problems are analyzed in the following paragraphs, with the exception of the one raised by the term "without right", which is analyzed in a distinct section[131].

a) The vagueness, due to the lack of a definition for data and security measures, in Article 370 C para 2 grCC

Article 370 C para 2 grCC which criminalizes the unauthorized access to data, causes problems of vagueness, given the fact that is does not provide any definition for the concept of "data".

Furthermore, it should be pointed out that the above provision is general, demanding the mere access to computer data without requiring an infringement of security measures[132]. The lack of a right to access data is merely implied by prohibitions and security measures that are indicatively mentioned in Article 370 C para 2 grCC, whereas in any case it is sufficient that the counter will of the legal holder has been expressed in any other way[133].

Although this formulation of Article 370 C para 2 grCC offers a broad coverage of cases, it leads to ambiguity. Besides, security measures should be expressly determined by using neutral terms that will also cover future developments. On the other hand, it is not clear whether some ways of protection fall within the scope of security measures. For example, according to an opinion, the concealment of data, i.e. the storage of data to another directory via the alteration of their names, constitutes a security measure[134], while others contest such an opinion[135]. Those who claim that concealment, as described above, constitutes a security measure, note that in this way the will of the legal rightholder to maintain his/her data secret is expressed[136]. In any case, for clarity purposes, it should be defined if for a security measure's notion it is enough that the illegal access is objectively restrained, even if an experienced user could easily overcome such obstacles. In a digital world the clear delimitation of term "security measures" is highly important.

---

[130] See page 22 of the present report.
[131] See p. 41 ff. of the present report.
[132] Cf. *Mylonopoulos* (1991), Ibid, 93 and 97 et seq.
[133] See *Mylonopoulos* (1991), Ibid, 97 et seq.
[134] See Schünemann, σε LK, 11. Auflage, § 202a, margin no. 16.
[135] *Bosch* in *Satzger/Schmitt/Widmaier,* StGB, § 202a, margin no. 5, *Lenckner/Eisele* in *Schönke/Schröder,* StGB, § 202a, margin no. 8, *Grühl,* Datenverarbeitung, in *Müller-Gugenberger/Bender*, Handbuch des Wirtschaftsstraf- und –ordnungswidrigkeitenrechts, § 42, margin no. 88.
[136] Cf. *Hilgendorf* (1996), Grundfälle zum Computerstrafrecht, JuS, 703, who mentions that the way of hiding should not be obvious.

b) The vagueness of Article 370 B grCC referring to the infringement of secrets "in any way"

Article 370 B grCC criminalizes –inter alia- whosoever unlawfully infringes data or computer programs "in any way". This general formulation is considered to create a risk of excessive punishability[137]. For this reason it is suggested to interpret the term "in any way" narrowly and to demand that this way of committing the crime is as important and serious, as the other ways described (copying, imprinting, using, disclosing to a third party). Therefore, according to the above-mentioned interpretation, Article 370 B grCC should not be applied for the cases of mere illegal access to computer data[138].

In the modern digital world the need for a specific formulation is even greater, taking into account the rapid technological revolution that renders many people unable to keep up with these developments. On the other hand, the legislator should adapt to these developments by using neutral terms that will cover such cases, without sacrificing, however, the n.c.n.p.s.l. certa principle.

c) The vagueness of the term "interception" in Article 370 A grCC

As already noted[139] Article 370 A grCC criminalizes –inter alia- the unauthorized interception or intervention in any other way to a system of software or hardware, which is used for the provision of telecommunication services. The term "interception", referring to software or hardware, is obviously vague, because the concept or interception or intervention in any other way is not easily conceivable in the modern digital world. The same problem can be allocated also in instruments of international law for criminalizing attacks against the confidentiality, integrity and availability of information systems and electronic data. The proposed directive on attacks against information systems (Article 6 for the illegal interception of non-public transmissions of computer data by technical means*)* does not even attempt to delimit the notion of 'interception'. Likewise, the Council of Europe Convention contains no definition of 'interception' either. However, a mere look at the explanatory report to the Convention on Cybercrime suffices to demonstrate the need for a comprehensive definition, as the Council of Europe interprets it so as to include, among other things, the monitoring or surveillance of *the content* of communications[140]. According to the Explanatory Report of the Convention on Cybercrime, "Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications They may include the use of software, passwords and codes"[141].

---

[137] *Karakostas* (2009)*,* Law and Internet, 162.
[138] *Karakostas* (2009), Ibid, Contra *Kioupis* (1999), Ibid, 129 ff.
[139] See p. 27 of the present report.
[140] See *Kaiafa Gbandi* (2012)*,* Ibid, European Journal of Crime, Criminal Law and Criminal Justice*,* 67, *Id.,* Evaluation of the proposal for a Directive on attacks against information systems (COM 2010, 517 final) on the basis of the Manifesto for a European Criminal Policy, 11.
[141] See the Explanatory Report by the Council of Europe, para. 53.

d) The vagueness of "influencing computer data in any way" in the criminal offence of computer fraud - Article 386 A grCC

Furthermore, doubts have been expressed concerning the constitutionality of committing the crime of computer fraud by "influencing computer data in any way", since this is an excessively broad and vague formulation, not fully compatible with the n.c.n.p.s.l. certa principle[142]. Even if one would not accept this opinion, it must be emphasized that Article 386 A grCC, in its current form, offers a basis for supporting an extremely broad interpretation, which also includes the unauthorized use of correct data to the actus reus of the criminal offence[143].

e) The vagueness of the definition of child pornography material in Article 348 A para 3 grCC

The definition of child pornography material could also be deemed, to a certain extent, vague[144]. Let us recall that according to Article 348 A para 3 grCC "Child pornography material in the frame of the above paragraphs shall mean the representation or the real or virtual recording in a electronic or other storage media of a child´s body or part of his/her body, in such a way that manifestly causes sexual arousal, as well as the real and virtual lascivious act that is performed by or with a child". Since this definition involves ambiguous concepts like "in a way that manifestly causes sexual arousal", it has been argued that one should interpret the terms restrictively, so as to safeguard the n.c.n.p.s.l. certa principle. One should also take into account the definition of child pornography material provided in the Directive 2011/93/UE that introduces a significant relevant improvement, since it limits the representation of a child's body exclusively to its genitals.

However, in the new Directive's definition it is also referred that the relevant depiction should take place for primarily sexual purposes, whereas there is no correlation with a representation that manifestly causes sexual arousal, as this is the case in the Greek Criminal Code. Nonetheless, on the basis of the definition of the new Directive, the act of depicting the genitals of a child should determine and manifest the aim of serving a sexual purpose, as primary, indeed. This element is connected –also- to sexual arousal, since it belongs to the content of sexual purposes.

On the other hand, by referring to the act of depicting that takes place primarily for sexual purposes, the Directive indicates that the act should express, per se and with clarity, the sexual purposes, whereas if the child pornography material does not concern the perpetration of an act of sexually explicit conduct with a child, it is limited to the depiction of his/her genitals. In this context, criminalizing pornographic material in any mere depiction of any other erogenous zones of a child's body is excluded.

As long as the new Directive is not implemented in the Greek legal order, it is highly important to interpret Article 348 A para 3 grCC in this direction. Such an interpretation is not only desirable, but also absolutely practicable. It is desirable, because in the definition of Article 348 A grCC vague concepts are used, and therefore a restrictive

---

[142] See *Courakis*, Fraud via computer system ("electronic fraud"), Poinikos Logos 2001, 2594, *Margaritis M*., Criminal Code, Article 386 A, margin no. 7, *Samios* (2010), Ibid, 308. Cf. the equivalent concern for the regulation of computer fraud in German law *Cramer/Perron*, in *Schönke/Schröder*, StGB, § 263 a, margin no. 16 referring to "the influencing the result of a data processing operation" other unauthorized influence on the course of the processing".

[143] See for more details p. 12 ff.

[144] See *Kaiafa-Gbandi* (2012), Internet assaults on minority, Poinika Chronika, 166 ff.

interpretation, that safeguards the n.c.n.p.s.l. certa principle, is essential[145]. Causing of sexual arousal from any depiction of a child´s body or part of his/her body depends largely on its viewers, who could have diverse reactions even to the same spectacle[146]. Besides, it is possible to support that a depiction of a child's body part in a way that manifestly causes sexual arousal cannot exist without involvement of the child's genitals as such, and particularly in a way that the depiction per se serves the primarily sexual purpose with clarity. The latter has to be expressed objectively on the basis of the depiction's features.

f) The vagueness of the concept of scriptural money when conceived as an object

The opinion that scriptural money constitutes an object[147] could lead to the view that also modern electronic data, which lack any material status, such as items in virtual worlds[148], constitute objects as well and are therefore subject to theft or damaging of another person's property. However, such an opinion would lead to an excessive expansion of punishability, given the fact that, due to the vagueness of the concept of an object, everything could be subject to it. In the context of electronic crime, this would mean that any electronic data, which could be incorporated in an information system at any time, could be subsumed under the notion of an object.

VIII) Ways of avoiding undue chilling effects on legitimate use of ICT or of the internet

Criminal legislation could avoid undue chilling effects on legitimate use of ICT or of the internet by providing that the prescribed acts must take place "without right"[149].

Despite the clear tendency to limit excessive criminalization, it should be noted that the term "without right" is vague and could create problems, even in the process of harmonizing criminal law provisions in the frame of the EU. For example, it is not clarified if the mere surpassing of the terms of use that are set by the legal holder of an information system could constitute a criminal infraction. From a purely rule-of-law standpoint, such definition appears problematic, as it effectively allows the owner – especially in the case of a contract – to even unduly restrict the free flow of information[150], which is absolutely essential in a democratic society[151].

Hackers that gain access to computer data seem to act basically without right. However, it is unclear whether this is actually the case with an insider, who has right of access to parts of a network on the basis of a working contract or any other form of relationship and who gains access to other parts of the network by exceeding his/her right[152]. Given the fact that attacks launched by trusted employees with increased powers, represent a greater risk for

---

[145] See for this type of interpretation of vague concepts that create constitutional problems *Papakiriakou* (2002), Das Europäische Unternehmensstrafrecht in Kartellsachen, 23 ff.
[146] See *Paraskevopoulos-Fitrakis* (2011), Ibid, 291-292.
[147] See p. 14 of the present report.
[148] See for example Second life - http://secondlife.com-, which is the most famous virtual world.
[149] See Explanatory Report of Convention on Cybercrime, margin no 38, and Article 2 d of the Proposal for a Directive on attacks against information systems, Article 1 d of the Framework Decision on attacks against information systems, and element 13 of the Preamble of the Framework Decision on attacks against information systems, element 10 of the Proposal for a Directive on attacks against information systems.
[150] See *Kaiafa-Gbandi (*2007), Ibid, Armenopoulos, 1084.
[151] See *Kaiafa-Gbandi* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice 2012, 69.
[152] See *Downing,* Shoring up the weakest link, 43 Colum. J. Transnat'l L. 2005, 721.

companies regarding the possible damages and cost that could be caused in such cases, this issue is deemed essential[153]. In the digital world, all information that companies possess is normally stored in a central information system[154].

In the Greek criminal law it is provided that the relative offences should take place "unlawfully"[155]. This element is held to be either an actus reus element, since there is no violation of the legal interest if the holder of the right consents to a third person's access to them, and this is considered as a consent that precludes the fulfillment of the actus reus of the crime[156] or a "special element of the wrongful character of the act", since -according to this opinion- there is an initial violation of the protected legal interest, which cannot be justified when the act is undertaken without right[157].

In order to avoid the vagueness that is caused by the general reference to the lack of a right Article 370 C para 3 grCC provides that: "If the perpetrator is at the service of the legal holder, the act of the later paragraph shall be punished only if it is expressly forbidden by an internal regulation or by a written decision of the legal holder or his/her competent employee". This shows the importance of appropriate corporate security policies that would define which data, when and for what reason, the employee has access to[158].

Many times it is difficult to determine, according to the circumstances, for which acts an employee has a right and which are not allowed. It is therefore prudent that the Greek law entail a specific provision that criminalizes the above conduct, only if it is expressly forbidden by an internal regulation or by a written decision of the legal holder or his/her competent employee.

It should be, however, emphasized that the modern form of electronic criminality may demand an even more concrete delimitation of punishability. For example, the Convention on Cybercrime prescribes in Article 6 para 2 (regarding the misuse of devices) that this article shall not be interpreted as imposing criminal liability in cases where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence, established in accordance with Articles 2 through 5 of this Convention, such as for authorized testing or protection of a computer system. One might contend that such an exception is superfluous, as the requisite intent of the offence could *per se* preclude conduct carried out for an authorized testing or protection of a computer system. However, given the fact that the proscribed conduct lies distant from any actual harm to computer systems or data, the above clarification can only be regarded as a positive addition[159] . In general, whenever the offence could interfere with a legitimate use of ICT or of the internet, the legislator should expressly limit criminalization by describing –at least indicatively- cases which are not criminalized. This is the case with the criminalization of preparatory acts that could be mixed with the legitimate use of new

---

[153] See *Mattsson* (2007), Data security for PCI and beyond, 3
[154] See *Goodman* (1997), Why the police don't care about computer crime, 10 Harv. J. L. & Tech., 171
[155] See Articles 370 A par. 1, 370 B par. 1 grCC) or "without right" (Article 370 C par. 2 grCC and 22 par. 4 of Law 2472/1997.
[156] Cf. *Kontaksis* (2000), Criminal Code, 3517 and more generally *Paraskevopoulos,* Ibid, 134.
[157] See *Kaiafa-Gbandi* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Criminal Law *General* Part *Compendium*, margin no. 110 and 1030 et seq.
[158] See indicatively *Souris/Patsos/Gregoriadis* (2004), Information Security, 53.
[159] See *Kaiafa-Gbandi* (2007), European Journal of Crime, Criminal Law and Criminal Justice, 67.

technologies, but also with other electronic crimes, such as illegal access to information systems or computer data, where the term "without right" may not be as concise as necessary.

IX) Ways through which legislation avoids becoming obsolete in light of rapid technological innovation

Criminal legislation avoids becoming obsolete in light of rapid technological innovation by choosing neutral terms. The Greek Criminal law does not expressly refer, for example, to social networks. However, there are references to the use of the internet and computer data. More particularly, Article 370 C para 2 grCC (illegal access to data) protects –inter alia- data that are transmitted via telecommunication systems. Article 370 A para 1 grCC protects, among others, systems of software or hardware, which are used for the provision of telecommunication services. Article 348 A para 2 grCC provides an aggravated circumstance of child pornography for the cases of committing the crime via a computer system or using the internet.

X) The extent of criminalization-Considerations over the criminalization of mere preparatory acts that carry a risk of furthering abuse

In the Greek criminal law, mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", or computer fraud, are not criminalized. There has been a controversy about introducing such criminalization. The main problem is that the proposed directive (just like the Council of Europe Convention) also proscribes tools that are not, by their very nature, designed for the sole purpose of attacking information systems. Coupled with the distance between acts like the production or possession of such tools and the actual attack, it becomes evident that criminalization of such conduct is not associated with a tangible threat to information systems, thus risking punishment over one's mere intent[160].

It is argued that for effectively addressing the dangers related to hacking tools (i.e. the creation of a black market for their production and distribution), the criminal law should prohibit specific, potentially dangerous, acts at their source, preceding the committing of offences against the confidentiality, integrity and availability of information systems and electronic data[161]. Thus, it is argued that the criminalization of the above preparatory acts protects the confidentiality, integrity and availability of information systems and electronic data at an earlier stage, before the actual infringement. The main issue is whether it is reasonable to protect the specific legal interest at such an early stage.

In the Explanatory Report of the Convention on Cybercrime it is mentioned that a similar approach has also been taken in the 1929 Geneva Convention on currency counterfeiting[162]. However, it should be emphasized that Article 3 para 5 of the specific Convention provides that: "The following should be punishable as ordinary crimes: ….(5) The fraudulent making, receiving or obtaining of instruments or other articles peculiarly adapted for the counterfeiting or altering of currency". The main difference lies in the fact that these tools must be particularly adapted for counterfeiting or altering currency. Thus, here a form of distant endangerment of a protected legal interest could be

[160] See *Kaiafa-Gbandi* (2012), Criminalizing Attacks against Information Systems in the EU, European Journal of Crime, Criminal Law and Criminal Justice, 73. Cf. for the emerging problems of criminalizing such preparatory acts, *Chatziioannou* (2011), The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data (under publication in Proceedings of the 4th International Conference on Information Law, Values and Freedoms in Modern Information Law and Ethics, 20th & 21st May 2011, Thessaloniki, Greece.

[161] See Explanatory Report of the Convention on Cybercrime, margin no 71.

[162] Explanatory Report of the Convention on Cybercrime, margin no 71.

accepted. However, with regard to hacking tools that are designed or adapted primarily for committing crimes against the confidentiality, integrity and availability of information systems, it is not easy to find out, through their features, if they contain a risk asset for the protected legal interest[163].

Besides, with regard to computer programs that are used for committing crimes against currency, one could refer to Article 149 of the German Criminal Code that penalizes "whosoever prepares to counterfeit money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another 1... computer programs or similar equipment which by their nature are suitable for the commission of the offence". The criminalization of acts that are related to computer programs was introduced by a law that –inter alia- transposed the Framework Decision on increasing protection by criminal penalties and other sanctions against counterfeiting in connection with the introduction of the euro to the German legal order[164]. Article 3 para 1(d) of this document prescribes the obligation for criminalizing the fraudulent making, receiving, obtaining or possession of instruments, articles, computer programs and any other means, particularly adapted for the counterfeiting or altering of currency. It must be emphasized that also article 4 of Framework Decision on combating fraud and counterfeiting of non cash means of payment provides that each Member State shall take the necessary measures to ensure that the following conduct is established as a criminal offence, when committed intentionally: the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of: (….) instruments, articles, computer programs and any other means peculiarly adapted for the commission of any of the offences described under Article 2(b), i.e. for counterfeiting or falsification of a payment instrument in order for it to be used fraudulently.

While Article 149 of the German Criminal Code refers to programs which by their nature are suitable for committing the above crimes, in German theory it is widely accepted that the suitability of the programs must be of a specific nature and only programs that are exclusively suitable for counterfeiting are penalized[165]. In the relative Explanatory Report it is mentioned that in the devices that are criminalized, a special applicability for the execution of counterfeiting should be inherent by their nature[166]. In such a case the above programs are per se dangerous for the protected legal interest of the currency and no specific problems of delimitation of the programs that are used for criminal purposes, arise.

Moreover, one should emphasize that the need of delimitation of hacking tools in comparison with the rest of the programs is even greater, compared to the programs that are used to counterfeit currency. Programs that are suitable for the counterfeiting of currency are not at all useful for its protection. The authenticity of currency could, for example, be checked via special mechanisms. On the contrary, tools that are designed or adapted primarily for committing crimes against the confidentiality, integrity and availability of information systems and electronic data constitute per se essential means for the control of their security. More particularly, these tools are usually used for

---

[163] Cf. *Kaiafa-Gbandi* (2007), Ibid, 1086.

[164] Law (2002): Law for the Implementation of the Second Protocol of the 19th of June 1997 for the Convention on the protection of the European Communities' financial interests, the Joint Action on combating corruption on the private sector of the 22th of December 1998, and the Framework Decision of the 29th of May 2000 on increasing protection by criminal penalties and other sanctions against counterfeiting in connection with the introduction of the euro of 22.8.2002[in German], BGBl I 2002, 3387.

[165] See *Erb*, (2005), in MK, § 149, margin no. 3, *Ruß*, (2009) in LK, § 149. margin no. 3.

[166] See *Stree/Sternberg-Lieben* in *Schönke/Schröder*, Strafgesetzbuch-Kommentar, § 149, margin no 3.

the monitoring of security gaps and the development of security strategies[167]. Consequently, an attempt to criminalize, even the mere possession of such tools, could expose innocent people to the danger of prosecution, while the proof of a further intent of committing a criminal offence against the confidentiality, integrity and availability of information systems and electronic data is very difficult to prove, especially in a digital environment.

The delimitation of the tools which are designed or adapted primarily for committing the above crimes is especially difficult. Programs are multidimensional and the ones used by hackers are also used by companies, in order to examine the passwords that are used by their employees[168]. Consequently, many hacking tools cannot be delimited from applications that are necessary for the security of information systems[169].

On the other hand, banning such tools would also create adversities to those who want to function legally and trace security gaps in information systems, despite the reservation that is laid down in the Convention[170]. Art. 6 para 2 expressly provides that this article should not be interpreted as imposing criminal liability where the acts referred to in paragraph 1 are not for the purpose of committing an offence, such as for the authorized testing or protection of a computer system. However, this provision has a declarative character and it would, obviously, be difficult to determine exactly, when these acts take place.

Regarding the allegation that criminalization is significantly restricted by requiring a further intent of committing a crime against the confidentiality, integrity and availability of information systems and data, it should be mentioned that, generally, when referring to preparatory acts, it is often difficult to determine the intent with clarity[171]. Even more difficult is the attempt to delimit the intent of committing a crime against the confidentiality, integrity and availability of information systems and electronic data in a digital environment.

Therefore, it has been argued in the Greek legal theory that the adoption of criminalization of the programs that are exclusively adapted to the committing of crimes against the confidentiality, integrity and availability of information systems and electronic data would be more appropriate and fair. However, it should be mentioned that the letter of Article 6 of the Convention on Cybercrime, contrary to Art. 4 para 2 (b) of the above Framework Decision, does not put limits to a wide interpretation of the scope of such programs. Furthermore, the Explanatory Report of the Convention shows that the drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow and leading to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances[172].

One way to achieve the delimitation of excessive criminalization is thought to be the introduction of an additional element, namely that the production, sale, etc., of software primarily designed to attack information systems (as described in Article 7 of the proposed directive) only be carried out upon obtaining formal permit. Aside from

---

[167] See *Stuckenberg* (2010), "Viel Lärm um nichts?, *wistra,* 43 ff.
[168] See *Borges* (2007), Stellungnahme zum Gesetzentwurf der Bundesregierung –Entwurf eines Stafänderungsgesetzes zur Bekämpfung der Computerkriminalität (StrÄndG) für die öffentliche Anhörung am 21. Mai 2007, 8.
[169] See *Sommer* (2006), Criminalizing hacking tools, Digital investigation, and 68.
[170] See *Furnell* (2006), Cybercrime, Destroying the Information Society [in Greek], 290.
[171] *Jescheck/Weigend* (1996), Lehrbuch des Strafrechts: Allgemeiner Teil, Fünfte Auflage, 523.
[172] See Explanatory Report of the Convention on Cybercrime, margin no 73.

contributing to setting up a list of software applications that pose a genuine threat to information systems (which would enable the outlawing of some of them), such an addition is held helpful for keeping tabs on those producing or selling these applications, thus rendering the lack of a permit as a formal element of the proscribed conduct. Accordingly, any person producing or selling them with permission would not incur criminal liability, at least not until attempting to launch an attempt against an actual information system. On the other hand, the lack of a permit would not necessarily justify the conclusion that the person is acting without a right; indeed, such right might derive from other exceptional circumstances precluding wrongfulness, such as a state of necessity or even self-defense[173]. In addition, domestic law should follow –according to this opinion- the example of Article 6 para 2 of the Council of Europe Convention and explicitly state that every act proscribed in Article 7 of the proposed directive is justified (even in the case of an absence of permit), if carried out for the purpose of authorized testing or protection of a computer system. Such a clause is thought to be compatible with the proposed directive, as the latter, indeed, requires a special intent to commit crimes which is all but absent in the situations described above[174]. In point of fact, it has been proposed to consolidate the two limitations into a clause exempting the procurement and possession for personal use of the applications in question by the authority issuing permits, providing that such procurement shall take place for the purpose of authorized testing or protection of a computer system in the context of personal or professional use[175].

A Committee for the Reform of the Greek Criminal Code, which has been authorized with this task by the Minister of Justice in 2010[176], has introduced its draft to the public in December 2012 and has made efforts to avoid over criminalization by the implementation of the international provisions that prescribe the criminalization of preparatory acts. In Article 272 para 1 of the Proposal for a Criminal Code it is provided that: "1. Whoever without a license produces, imports, proceeds to procurement for use, distributes or makes available otherwise, the tools of paragraph

[173] See *Kaiafa-Gbandi* (2012), Ibid, 78.
[174] See *Kaiafa-Gbandi M.* (2012), Ibid, 77 ff.
[175] See *Kaiafa-Gbandi* (2012), ibid, 78.
[176] The legislative Committee for the Reform of the provisions of the Greek Criminal Code was established with the Decision of the Minister for Justice, Transparency and Human Right with number 27789 / 17-3-2010 (Government Gazzette Vol. YODD 96 /17−3−2010), as this Decision was amended by the Decisions with numbers 123825 / 22-12-2010 (Government Gazzette Vol. YODD, 424 / 31-12-2010 and Government Gazzette Vol. YODD 56 / 9-3-2011, where a correction of error was published), 7954/15-2-2011 (Government Gazzette Vol. YODD 33 / 16-2-2011) and 66403 / 29-7-2011 (Government Gazzette Vol. YODD264 / 12-8-2011). The following persons were initially appointed as members of the Committee: I. Manoledakis, emeritus Professor of Criminal law at AUTH (President of the Committee) , I. Anagnostopoulos, Associate Professor of Criminal law at UoA, M. Kaiafa-Gbandi, Professor of Criminal law at AUTH, N. Livos, Assistant Professor of Criminal law at UoA, N. Bitziliekis, Professor of Criminal law at AUTH, Ch. Mylonopoulos, Professor of Criminal law at Uoa, D. Papageorgiou, Prosecutor at the Court of Appeals, S. Pavlou, Professor of Criminal law at DUTH, E. Symeonidou-Kastanidou, Professor of Criminal law at AUTH, A. Charalabakis, Professor of Criminal law at DUTH, V. Cheirdaris, lawyer. On February 2011 after the resignation of the Member of the legislative Committee I. Anagnostopoulos, G. Dimitrainas, Assistant Professor at DUTH, substituted him. On August 2011, after the sudden death of the President of the Committee, I. Manoledakis, the Presidency of the Committee was appointed to E. Symeonidou-Kastanidou. On 2 November of 2011 the member of the legislative Committee Ch. Mylonopoulos was resigned and was not substituted, since the Committee had already completed its work.

2 with intent to commit any of the offence that are prescribed in Article 268 until 271, shall be punished, in "cases which are not minor", with imprisonment of up to one year.

2. Tools that are used according to the previous paragraph are:

a) computer programs, designed or adapted primarily for the purpose of committing of these offences

(b) computer passwords, access codes, or similar data by which the whole or any part of an information system is capable of being accessed

3. The acts of paragraph 1 shall not be punished, if they were committed for the testing or protection of an information system.

4. The criminal culpability of the offences of paragraph 1 is deleted, if the perpetrator destroys, at his own will, the items that are referred in it, before he uses them for the committing the offences of Articles 268 until 271".

In the Proposal for the new Greek Criminal Code it is stated that it has been chosen to make clear that the mentioned offences shall not be punished when they are committed for the testing or protection of an information system, in order to control the excessive criminalization, particularly, if somebody takes into account the fact that the tools referred in the provision are used, beyond illegal purposes, also for the safety and protection of information systems. Besides, the introduction of the lack of a license for the production, import etc. of the above tools as a prerequisite of the criminalization constitutes an effort to control over-criminalization, also. "Minor cases" are excluded from criminalization as well, while, finally, extinction of culpability is prescribed for the cases where the tools are destroyed by the perpetrator before their use for committing the offences of the chapter[177].

XI) The possession of data as a criminal offense-The emerging criminalization of the mere viewing of data

The possession of computer data is criminalized in the Greek legal order when the latter depict child pornographic material.[178] The main problem that concerns child pornography committed via the use of a computer system or internet, is related to the notion of "possession", which in an electronic environment acquires a special meaning.[179]

The problem does not concern cases in which pornographic material has been recorded in a means of storage that is possessed by the perpetrator, in the sense of a physical power of disposition.[180] Problematic are: (a) the cases in which a third person (and not the one that collected and stored the electronic data) has the real power of disposition over their material means of storage (e.g. hard disc, DVD etc.), (b) the cases of recording of pornographic material in the cache memory of a computer, and last but not least, (c) the cases of viewing pornographic material, for which a dividing line to possession has to be drawn.

Regarding the first category of possession cases, modern developments show that one can talk about possession of a specific electronic material not only when one has the power of disposition over the means of storage on which the

[177] See Explanatory Report of the Proposal for Greek Criminal Code, p. 208.
[178] See for the following considerations *Kaiafa-Gbandi* (2012), Ibid, Poinika Chronika, 167 ff..
[179] See *Kioupis* (2008), Child Pornography- Interpretative approaches to article 348A PC, Poinikos Logos, 15-17, *Bourmas* (2009), Attempts of conceptual determination of possession of electronic data with a pornographic character, Poiniki Dikaiosyni, 322 ff., *Paraskevopoulos-Fitrakis* (2011), Ibid, 302-303.
[180] See *Kioupis* (2008), Ibid, 16.

electronic data are recorded, but also when the person that recorded them on this means has the real possibility of undisturbed access to and interaction with them, without being necessary that he/she has the power of disposition over the means of storage itself.[181] For example, we could accept material possession, if a factory employee "loads" pornographic material on the hard disc of a factory computer, on which he has access without any restrictions, and every time when he/she finds the opportunity, due to the absence of other individuals in the specific area, "enjoys" viewing this material or updates it, keeping it stored to a specific hidden file of another person's computer. We could also accept possession in cases where the person who stored the pornographic material in another person's computer could gain access to it via the use of a program (Trojan horse), that secretly stores the material on a computer and simply allows viewing by the person that controls the foreign computer via the use of the specific program (Trojan horse). Thus, it would be more prudent to accept a broad concept of electronic possession, which does not necessarily depend on the power of disposition over the material means of data storage, but refers to the real possibility of disposition over the pornographic material itself, to which the alleged possessor should have formerly gained access and processed it in any way.

In theory it is argued that a permanent storage of the pornographic material on means of data storage is necessary in order to accept possession, and therefore temporary storage in RAM is not sufficient.[182] On the other hand, it is questionable whether the notion of pornographic material possession could be accepted in cases where electronic data are stored or –better formulated- are contained in the cache memory or temporary internet files of the computer system, after for example viewing a website for which the viewer realized that it contains child pornography and abandoned it immediately.[183] The peculiarity lies here in the fact that this content is not absolutely temporary, since if the data are not deleted by the user or the system, they could remain accessible for some time. However, what is contained is not the complete file/material, but only some data that assist a possible access to the material via the internet in the future.[184] In these cases it would be more prudent to deny the concept of possession. The reason is that the data that are contained in the system –even if they are not sufficient in the specific case to constitute pornographic material- are destined to be deleted automatically by the system. Possession of child pornography could be accepted in such cases, only if the subject, being aware of the storage of specific data in his/her computer's cache memory, proceeds to additional acts showing that their automatic deletion is not sure, e.g. installs a reminder of the electronic system before their deletion, so that he/she has the opportunity to decide whether to delete them or not etc.

Finally, cases of mere viewing of pornographic material, e.g. in a computer screen or mobile phone's screen, as long as neither real power of disposition over the means of data storage, nor over electronic data themselves in the above mentioned way, can be established, are not deemed possession of pornographic material[185]. This is also true for the

---

[181] See *Bourmas* (2009), Poiniki Dikaiosyni 2009, 326. Cf *Paraskevopoulos-Fitrakis* (2011), Ibid, 303, Chamber of Supreme Court 810/2007, Poiniki Dikaiosyni 2007, 813, Chamber of Supreme Court 628/2006, Poiniki Dikaiosyni 2006, 1249.

[182] See *Hilgendorf / Frank / Valerius* (2005), Computer- und Internetstrafrecht, p. 114, margin no. 418, *Perron/Eisele* in *Schönke/Schröder*, StGB, § 184b, margin no. 15. Contra *Wilhelm-Laufhütte-Roggenbuck,* in LK, margin no. 8, *Loewenheim/ Koch/ Hage*, Praxis des Online-Rechts.

[183] See *Paraskevopoulos-Fitrakis* (2011), Ibid, 303.

[184] See *Paraskevopoulos-Fitrakis* (2011), Ibid, 303.

[185] See *Kioupis* (2008), Poinikos Logos 2008, 16, *Paraskevopoulos-Fitrakis* (2011), Ibid, 302-303.

opening of an electronic message or a file that has not been requested and (covertly) contains pornographic material[186], since, even if the opening of the message or file would be deemed an act of disposition over it, is not covered by the necessary intent. The same is also true for the mere existence of a message with pornographic content in the "inbox" of the computer correspondence. Besides, the viewing of websites with child pornographic material does not constitute a possession of pornographic material,[187] unless acts of storage of the material, that surpass the automatic storage-containing of relative data in the computer's cache memory, are undertaken.

However, the new Directive for combating child pornography in the E.U. obliges Member States to criminalize -with the same penalty that is provided for the acquisition and possession of child pornographic material- the " Knowingly obtaining access, by means of information and communication technology to it" (Article 5 par. 3). Thus, whereas the coincidental viewing of child pornographic material or the viewing with eventual intent (dolus eventualis) will continue to be out of the scope of criminalization, this is not the case according to the E.U. choices for the viewing of pornographic material, when it is committed with direct intent. The new provision refers to "knowingly obtaining access" to child pornography by means of information or communication technology.[188] It uses a term that is basically broader, since viewing constitutes obtaining access, but also requires something more, i.e. actually watching the material. Therefore, the term used by the Directive could refer, for example, to the act of entering a website which contains exclusively pornographic material via the use of a special code allowing the entrance, without yet having seen the material itself. This choice constitutes an exceptional expansion of criminalization, which -despite the option of limitations that the E.U. has given to its Member States- remains problematic. A prudent approach of the Directive should, therefore, lead to the adoption of the specific limitation, i.e. to the connection of obtaining access at least to the viewing of pornographic material, since otherwise no relevance of the specific material to the alleged violation of minority or of a number of other legal interests, is practically established. Besides, the delimitation of criminalization is also ne cessary in cases where minors are the "perpetrators" of obtaining access, since the criminalization of distributing pornographic material aims –also- at the protection of the minority of possible viewers of such material.

XII) The criminal liability of ISPs

Given the fact that the possession of or the granting of access to certain data could be defined as a criminal act, a question of possible criminal liability of ISPs, who offer the means for internet use, arises. The liability of service providers, in general, is regulated in the Greek legal order by the Presidential Decree 131/2003, which incorporated the Directive 2000/31/EC into Greek law. This Decree refers to every type of liability, thus, including criminal liability as well.[189] This is also deemed to be the case with the EU directive.[190] The aim of the European legislator was to

[186] See *Paraskevopoulos-Fitrakis* (2011), Ibid, 302-303.

[187] *Paraskevopoulos-Fitrakis* (2011), Ibid, 302-303.

[188] See para 18 of Directive's Preamble 2011/93/EE, which stipulates that: «Knowingly obtaining access, by means of information and communication technology, to child pornography should be criminalized. To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to individuals inadvertently accessing sites containing child pornography. The intentional nature of the offence may notably be deduced from the fact that it is recurrent or that the offence was committed via a service in return for payment».

[189] See *Igglezakis* (2003), The legal framework of electronic commerce, 167, *Alexandridou* (2010), Law of electronic commerce, Greek and European, Second Edition, p. 131, margin no.2, cf. *Diamanti* (2004), Liability of internet service providers according to

limit any kind of legal consequences against internet service providers and to limit them reasonably, without being concerned whether, according to national law, the aforementioned consequences have the form of civil, administrative or criminal sanctions. Given the fact that the Greek legislator explicitly provides for a limitation, e.g. referring to a civil compensation (Art. 13 a f) a and b subparagraph), whenever he/she wants to limit the field of application, the above conclusion is widely accepted.[191]

The criminal liability of Internet Service Providers was a matter of theoretical dispute based upon general principles of criminal law until 2003, until the afore-mentioned Presidential Decree incorporated Directive 2000/31.[192] Nowadays the dogmatic classification of the above provisions raises even more problems. It has been argued that the above provisions alter the general principles of criminal law, as they are stipulated in the Greek Criminal Code, especially for the cases of criminal liability of an internet service provider, as it is defined by Presidential Decree 2000/31. They tacitly alter the prerequisites of punishability of Article 14 grCC, especially for the criminal acts that are related to the activities of ISPs in the framework of the information society.[193]

According to a certain view, the criminal liability of ISPs should be judged upon their omission to prevent the criminal result.[194] In fact, the above mentioned Presidential Decree does not preclude the application of the general principles of criminal law. In the framework of the omission's doctrine it constitutes the necessary "special legal obligation" for a criminal liability of ISPs. For criminal liability based on omissions, the Greek Criminal law focuses on the so called "special legal obligations". Therefore, the above Presidential Decree could not ignore the basic doctrine of criminal liability for omissions in Greek law. Neither could one refer here to a "Vorfilter-Theorie" or to other theoretical constructions that have been proposed in the German Criminal law, since the "special legal obligation" is fundamental for the establishment of criminal liability in the Greek Criminal law. This "special legal obligation" is provided under certain conditions and according to several types of ISPs as foreseen by the above Presidential Decree[195].

Presidential Decree 131/2003, Incorporation of Directive 2000/31/EC for electronic commerce into national law, Dikaio Epixeirisewn kai Etairiwn, 986.

[190] See *Morozinis* (2005), Criminal Liability of Internet Service Providers, Archeio Nomologias, 309.

[191] See *Morozinis* (2005), Ibid.

[192] See *Kioupis,* Cybercrime Legislation in Greece, Revenue hellenique de droit international, 522.

[193] See *Morozinis* (2005), Ibid, 314.

[194] See *Panagiotopoulos*, Criminal liability of internet service providers, in *e-Themis* (2011), Confronting modern technological developments, Personal Data-Electronic Crime-Electronic Commerce, 48, *Kritharas* (2009), Criminal law and Internet, 72.

[195] The provisions of Presidential Decree 131/2003 that provide the relevant legal obligations for each category of ISPs read as follows:

"Article 11

Mere conduct

1.Where an information society service is provided consisting of the transmission in a communication network of information provided by a recipient of the service, or of the provision of access to a communication network, the service provider is not liable for the information transmitted, on condition that the provider:

a) does not initiate the transmission of information

b) does not select the receiver of the transmission, and

c) does not select or modify the information contained in the transmission

The relevant provisions of the Presidential Decree concern the objective determination of specific obligations of the ISPs, which dogmatically belong to the actus reus of offences committed via omission.

In the majority of cases no liability of ISPs based on an action could exist, since the procedure of storage and transmission of data to receivers, technically, takes place in an automated way and the provider does not control, ab initio, the content of data.[196] The omission could be connected to the fact that the service providers do not do something that is socially anticipated,[197] although they have the possibility to act.[198] The main issue here is whether

---

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
3. This Article shall not affect the possibility for a court or administrative authority of requiring the service provider to terminate or prevent an infringement.
Article 12
Cashing
1. Where an information society service is provided consisting of the transmission in a communication network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that the service provider:
a) does not modify the information
b)complies with conditions on access to the information
c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry
d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and
e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.
Art. 13 reads as follows:
"(Hosting)
1. Where an information society service is provided consisting of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
a) the service provider does not have actual knowledge of an illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
b) the service provider, upon obtaining such awareness, acts expeditiously to remove or to disable access to the information.
2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the service provider.
3. This Article shall not affect the possibility for a court or administrative authority of requiring the service provider to terminate or prevent an infringement".

[196] See *Kritharas* (2009), Ibid, 72.

[197] See *Symeonidou-Kastanidou* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Criminal Law *General* Part *Compendium*, p. 187, margin no. 291, *Androulakis* (2006), Criminal law, General part, I, 159 ff., *Kotsalis* (2005), Criminal law, General part, I, 222 ff.

ISPs have the possibility to control the illegal content or not. Indicators that help determine this possibility, e.g. the size, the name of data etc, should be used. Such possibility could be judged only in concreto. Furthermore, the foundations of a "special legal obligation", upon which the liability is based, according to Greek law are: the law itself, contractual obligations and the offender's prior dangerous and unlawful behavior. In the case of the service providers, usually, there are neither contractual obligations (e.g. between the service provider and the users) nor a prior dangerous and unlawful behavior of them. Obligations of this nature could be prescribed by the contract,[199] but normally this is also not the case, because the contract, in the majority of cases, does not expressly refer to such issues. It has also been argued that a prior dangerous behavior could be assumed,[200] if one considers that the Internet is a continuous foundation of risks, in the sense that a minor user could, coincidentally, become the receiver of pornographic material at any time. However, according to Greek Criminal law theory, the term of a prior dangerous act is associated with an act, whose wrongful character is based upon the infringement of a provision that protects the exact interest, whose violation was not prevented,[201] and the provision of internet services does not constitute, in any way, such an act. Furthermore, the mere provision of internet services could not constitute a prior dangerous act, since it is lawful and it provides access to new technologies to people, which is, indeed, constitutionally protected (Article 5A of the Greek Constitution).

Referring to a form of participation via omission, it has been argued that the omission of the provider to proceed to the necessary legal action constitutes an action of "negative" assistance to the principal actor of the criminal activity and therefore it renders him an accessory to the commitment of the offence.[202] In order to have a principal that acts via omission, the content of his/her special legal obligation should be exactly to prevent the result and to have the self-sustained possibility to, self-sustainably, deter the act that is committed by another person as long as this act lasts.[203] Given the fact that the role of ISPs is not to control the content of information and that they could not, self-sustainably, prevent the result, one could here refer only to an accession via omission. A direct accession via omission is given when the omission does not have the above characteristics, which equate it to the principal act, but there is a legal obligation to act and the omission constitutes an exposure of the legal interest to the violation that takes place by the principal actor.[204] If this is not the case, a simple accession should be accepted, when the omission assists the main act in any way, as long as the accessory has a relevant legal obligation that is not fulfilled.[205]

It has been argued that the reason precluding criminal responsibility may refer to any type of liability for a behavior that is subject to any prohibitive provision of law, no matter if it is subject to civil, criminal, competition, intellectual

---

[198] See *Androulakis* (2006), Ibid, 161, *Symeonidou-Kastanidou* (2005), Ibid, p. 187, margin no. 289) and having perception of the circumstances that call for action (See *Androulakis* (2006), Ibid, 162.
[199] See *Morozinis* (2005), Ibid, 314.
[200] See *Morozinis* (2005), Ibid, 314.
[201] See *Androulakis* (2006), Ibid, p. 232 ff.
[202] See *Kritharas* (2009), Ibid, 72, cf. *Panagiotopoulos* (2009), 46.
[203] See *Kaiafa-Gbandi* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Ibid, p. 506 ff., margin no. 857 and p. 553, margin no. 934.
[204] See *Kaiafa-Gbandi* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), p. 558 ff., margin no. 940.
[205] See *Kaiafa-Gbandi* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Ibid, p. 571, margin no. 963.

property or industrial property law.[206] The counter opinion argues that this view ignores both the Presidential Decree 131/2001 and the Directive referring exclusively to electronic commerce and not concerning in any way the criminal liability of internet service providers, that has to be judged according to Article 45 ff. grCC.[207] However, it should be emphasized that Article 14 of the Presidential Decree 2000/31 does not exclude the criminal liability of ISPs, but it stipulates the role of lack of a general legal obligation to monitor the information.[208] This means that from the viewpoint of criminal law criminal liability of ISPs could not be founded on their omission to monitor information. This is reasonable, as many times it is not technically possible to control all the information that is transmitted and therefore, the role of ISPs is not to be the internet enforcement agencies that monitor the communications of the users.

XIII) Constitutional limits to criminalizing conducts referring to ICT and internet crime

Criminalizing conducts with respect to ICT and internet crime is in the Greek legal order subject to several constitutional limits.

The main limitation emanates from Article 7 of the Constitution which provides the safeguards of the n.c.n.p.s.l. principle[209]. The main considerations are related here to the vagueness that characterizes some provisions criminalizing electronic crime, i.e. Articles 370 C par. 2, 370 A, 386 A and 348 A grCC[210], the lack of a definition for electronic data[211] and the non-specification of the term "without right"[212]. Furthermore, as it has already been analyzed above[213], according to the n.c.n.p.s.l. principle causing property damage by influencing computer data could not be subject to the crime of fraud (Article 386 grCC), because the latter demands a deception of a natural person, and therefore, the introduction of computer fraud, as a separate offence of the Greek Criminal Code (Article 386A grCC), became necessary.

Article 2 para 1 (referring to human dignity) in combination with Article 5 para 1 (referring to free development of personality) of the Greek Constitution is deemed to prohibit the criminalization of acts of self-harm[214]. However, one has to consider in this respect that some conducts, although initially giving an impression of causing self-harm (e.g.

---

[206] *Bourmas* (2009), The role of the Internet service providers in relation to the application of Intellectual Property law, Dikaio Meson Enhmerwsis kai Epikoinwnias, 492, *Igglezakis* (2003), The *legal* framework of electronic commerce, 167 ff.

[207] See *Panagiotopoulos*, Criminal liability of internet service providers, in *e-Themis* (2011), Confronting modern technological developments, Personal Data-Electronic Crime-Electronic Commerce, 46.

[208] See *Alexandridou* (2010), Ibid, 137, margin no. 16.

[209] See indicatively *Chrysogonos* (2006), Personal and social rights, 235 ff., *Dagtoglou* (2010), Personal rights, p. 319 ff., margin no. 417 ff, *Manesis* (1982), Constitutional rights, 191 ff., *Manoledakis,* in *Kassimatis/Mavrias* (1999), Commentary of Constitution, Art. 7, 1 ff., *Paraskevopoulos* (2008), Ibid, 29 ff., *Symeonidou-Kastanidou,* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Criminal Law General *Part* Compendium, p. 21 ff., margin no. 34 ff.

[210] See p. 36 ff. of the present report.

[211] See page 31 of the present report.

[212] See page 41 of the present report.

[213] See page 11 of the present report.

[214] See indicatively *Margaritis* (2000), Bodily injuries, 81 ff., *Paraskevopoulos* (1991), Criminal liability by self-destructive acts, Ellhnikh Epethrida Egklhmatologias, 58 ff.

the destruction of one's own information system), may actually entail a violation of another person's legal interests (e.g. when the latter has stored his /her data in the information system of the former).

The principle of proportionality also plays a major role and sets limits to criminalization[215]. The proportionality refers here to the wrongfulness and guilt expressed by an offence, on the one hand, and to the legislative authorized sanction, on the other hand[216]. The aggravating circumstances of Article 348 A par. 4 grCC, regarding the possession etc. of pornographic material that takes place habitually, combined with the tendency of the Greek criminal courts for often applying the repetitious commission of the crimes as an aggravating circumstance, may easily lead to an imposition of a felony sanction, even where only two viewings of pornographic material –which could be virtual as well- might have been proven. Such an application of Art.348A para 4 grCC contravenes the principle of proportionality.[217] The same is true for the penalty provided by Article 370A grCC (up to ten years imprisonment). A mere comparison with other provisions, that protect personal legal interests (e.g. severe bodily injury with intent - Art. 310 par. 3 grCC, human trafficking-Art. 323A para 1 grCC) and authorize for the same penalty level, can clearly demonstrate the problem.[218]

With regard to the criminalization of attacks against the confidentiality, integrity and availability of information systems and electronic data in the E.U. framework it has already been emphasized that the principle of proportionality plays a major role.[219] However, Articles 7 and 9 para 2 of the Proposed Directive (COM (2010) 517 final, of 30.9.2010) referring to the sanctions, aside from undermining the principle of proportionality, lead the E.U. towards inflexible sentences, as they distance themselves from the framework decision providing for maximum terms of imprisonment in a more flexible fashion (e.g. a maximum term of at least one to three years under Article 6, para 2 of the framework decision). The above E.U. choice, if realized in the legal act to be enacted, is going to influence, of course, the Member States as well. Unfortunately, similar flaws are also detectable with regard to the ultima ratio principle.

As regards the criminalization of "genuine electronic crimes", an additional problem could emerge out of the incorporation of the criminalization of hacking tools in the Greek legal order, if the proposed Directive retains its actual form[220]. Article 16 para 1 of the Greek Constitution protects –inter alia- the freedom of research.[221] By criminalizing mere preparatory acts referring to hacking tools, without requiring that they should be used exclusively for criminal purposes, no effective research in the field of data security can be developed. Moreover, the criminalization of dual use programs is expected to deter even individuals -and not only information security experts-

---

[215] See indicatively *Chrysogonos* (2006), Ibid, 90 ff., *Dagtoglou* (2010), Personal rights, p. 216 ff., margin no. 308 ff., *Orfanoudakis* (2003), The principle of proportionality, passim, *Paraskevopoulos* (2008), Ibid, 33. Compare also Supreme Court 1469/2010, Poinika Chronika 2011, 522.

[216] *Paraskevopoulos* (2008), Ibid, 33.

[217] See *Courakis,* Child pornography and internet, p. 15, margin no. 18, accessible in www.theartfcrime.gr.

[218] See *Symeonidou-Kastanidou,* The amendment of Article 370A with Law 3674/2008, in Etaireia Nomikon Voreiou Ellados (2009), Infringement of privacy, 13 ff.

[219] See *Kaiafa-Gbandi* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice, 69.

[220] See p. 44 ff. of the present report.

[221] See indicatively *Chrysogonos* (2006), Ibid, 326 ff., *Dagtoglou* (2010), 765 ff., margin no. 931 ff.

to experiment with different programs aiming to deepen their knowledge in security issues and contribute to security development in the field.

As to "genuine electronic crimes", apart from the above mentioned problems, it is worthwhile mentioning that criminal prosecution itself may often lead to a breach of fundamental rights, such as the confidentiality of communication (Article 19 of the Constitution), the informational self-determination (Article 5A of the Constitution and private life (Article 9), or the domestic sanctuary (Article 9 of the Constitution). It may also infringe the constitutional right to the protection of confidentiality and integrity of information systems (Article 5 para 1 in combination with Articles 2 para 1 and 5 A). However, the above constitutional rights are not absolute, as they are subject to specific limitations. Characteristic in this respect is a ruling of the European Court of Human Rights[222] according to which: "Although the freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislature to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not however in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media came too late for the applicant".

With regard to criminalizing child pornography, the constitutional problem arising refers to the compatibility of certain criminalization forms with the freedom of expression and the freedom of art. It has been argued that such freedoms should not be sacrificed in the name of a puritan moralistic perception of law or under the pressure of an "ethical panic". [223] A weighing between freedom of art (Article 16) and protection of childhood (Article 21) is here necessary. [224] Given the fact that the Constitution does not provide expressly for any solution concerning a possible conflict of the above constitutional provisions[225] a weighing that takes into account the principle of proportionality is the only way out. The Three Member Court for Misdemeanors of Athens (case 75582/2008, Poinlog 2009, 171) ruled that when a book constitutes a work of art according to Article 16 para 1 of the Constitution and an endangerment or violation of minority does not derive from its production and distribution, then Article 20 grCC is applicable and the wrongful character of the act is justified.[226] The European Court of Human Rights, on its part, referring to the case of an exhibition of a Finnish artist that contained over 100 pornographic images of minors that were made in this way accessible to a wider public, has acknowledged that the conceptions of sexual morality which support the criminalization of possession and distribution of child pornographic material have changed in recent years. However, according to the Court, the domestic courts balanced at length the relationship between the freedom of expression,

[222] ECHR case of 2/12/2008 K.U. v. FINLAND (Application no. 2872/02), margin no. 49, accessible in HUDOC database.
[223] See *Courakis* (2012), Ibid, 9, margin no. 9.
[224] See *Courakis* (2012), Ibid, p. 11, margin no. 10, footnote 28.
[225] See *Dagtoglou* (2010), Ibid, p. 757, margin no. 925.
[226] Contra Supreme Court 254/1980, Poinika Chronika 1980, 537: see for these references *Courakis,* Ibid, p. 11, margin no. 10, footnote 28.

on the one hand and morals, reputation and rights of others, on the other hand and found that the applicant's freedom of expression did not justify the possession and public display of child pornography.[227] With regard to the claim of the applicant, that she had included the pictures in her work in an attempt to encourage discussion and raise awareness of how wide-spread and easily accessible child pornography was, the Court noted that the domestic courts acknowledged the applicant's good intentions and therefore did not impose any sanctions on her. However, possessing and distributing sexually obscene pictures depicting children was still an act subject to criminal liability. Thus, it ruled, it does not follow from the applicant's contentions that her conviction did not, in all the circumstances of the case, respond to a genuine social need.[228]

It is worth mentioning at this point that according to the Greek constitutional theory an artwork includes any human creation, that depicts external characteristics corresponding to the definition of each art, and its potential provocative or appalling character does not play a role.[229] Denial of the classification "a work of art", just because a piece of work belongs to a rejected "school", style or mentality, contravenes the constitutionally protected freedom of art.[230]

With regard to the criminalization of "cybercrimes stricto sensu", i.e. traditional crimes in the frame of which the internet is used simply as a means of committing them, issues associated also with the freedom of speech, arise. A typical example of content related crimes are the ones described in Articles 1 and 2 of Law 927/1979, which criminalize aspects of racism.[231] For the specific offences related to racism, there is an Additional Protocol to the Convention on Cybercrime of the Council of Europe, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. The Protocol demonstrates the importance of criminalizing the specific conducts at an international level. However, the issues of racism and xenophobia have not been regulated by the main Convention on Cybercrime. The reason was that states such as the USA have a broad and constitutionally enshrined protection of the freedom of expression, so that regulations restricting this freedom could not be accepted during the drafting of the Convention.[232] According to Areopag (in Plenum) a restrictive and strict interpretation of the provisions of Law 927/1979 is necessary, in view of the Constitution (Article 14 para 1 and 16 para 1) and the European Convention on Human Rights (Article 10 para 1), i.e. in the view of the freedoms of expression, arts, education, research and teaching, as guaranteed by law. From the above rights derives the possibility of a scientist to record and interpret according to his/her judgment the historical facts, on one hand, and the freedom of every citizen to take knowledge of the specific facts and the writer's approach, on the other hand. The scientific assessment could extend to the point of sharp criticism and negative labeling of specific individuals and their acts, respecting, however, the constitutionally enshrined human dignity, an aspect of which is also the racial and ethnic origin of an individual[233].

---

[227] ECHR KARTTUNEN v. FINLAND of 10.05.2011 (Application no. 1685/10), margin no.23, accessible in HUDOC.
[228] ECHR case of of 10.05.2011 KARTTUNEN v. FINLAND (Application no. 1685/10), margin no. 24, accessible in HUDOC database.
[229] See *Chrysogonos* (2006), Ibid, 329). Thus, even pornographic material could be embraced in the notion of a piece of art (See *Chrysogonos* (2006), Ibid, 329.
[230] See *Dagtoglou* (2010), Ibid, p.748, margin no. 915.
[231] See *Kaiafa-Gbandi* (2007), Ibid, Arm, 1063.
[232] See *Gercke* (2004), Die Cybercrime Konvention des Europarates, CR 2004, 783.
[233] See Supreme Court (in Plenum) 3/2010, PoinChr 2010, 456.

The issue of freedom of speech and possible insults or defamation that occur in the frame of expressing views in blogs, the social media or internet fora has also been discussed in the Greek theory and practice. In all these new forms of communication the individual expresses freely his/her view and it is possible that through such actions the honor of other individuals is violated. The freedom of expression in the frame of the internet is protected as well, and therefore, it would be unconstitutional to create "opinion crimes" with regard to the Internet, or to make the access to it dependent upon the expression of a specific opinion.[234] The expression, which is constitutionally protected, could be oral, written, via the press, or via image (electronic image, graphics etc.)[235]. It is argued that the criminalization of conduct against the legal interest of an individual's honor, even if they are committed in the frame of the internet, constitutes a licit limitation of the freedom of expression, to which the freedom to insult is not included[236]. In general, it is deemed that the criminalization of the introduction of pornographic material or material of violent images, the criminalization of access to files with confidential information for the national defense, misleading and unfair advertising, offences against dignity and telecommunication security constitute legitimate limitations of the freedom of information in the frame of the internet.[237] The provision referring to the protection of honor constitutes a constitutional limit of the freedom of expression.[238] However, insults against the honor of a person may also be justified by the freedom of art, and thus a weighing between the constitutional rights to honor and to the freedom of art should be undertaken.[239]

The constitutional protection of the freedom of press (Article 14 para 2 of the Constitution) also covers the internet, since Websites, address catalogues, messages in internet fora usually contain texts that are produced with a combination of a mechanical, physico-chemical and electronic procedure and are destined to be distributed via the internet. Every recall of the specific material constitutes, on the other hand, a "copy". Thus, an important part of the above material is subject to the term of "press" as provided in Article 14 para 2 subparagraph 1 of the Constitution. [240] Consequently, when internet crimes referring to violations against the honor of a person are being committed, the right to the freedom of press may also be applicable. Weighing the diverse interests in such cases should take into account: a) the constitutional recognition of the freedom of expression and the special aspects of the freedom of press, and b) the international legal instruments referring to the role of press.[241] In any way, a proportion between the measure and the goal should be ensured, i.e. the publication should not surpass the objectively necessary measure and the goal should not be achievable via another milder means.[242] The Areopag has ruled that the freedom of press

[234] *Karakostas* (2009), ibid, 42.
[235] See *Karakostas* (2009), Ibid, 42.
[236] See *Karakostas* (2009), Ibid, 45.
[237] See *Mantzoufas,* Freedom of expression and internet, p. 5, accessible in www.constitutionalism.gr.
[238] See *Kioupis* (2009), Violations of honor, 76.
[239] See for example cases where the honor of a person is insulted so much that the freedom of art fades away, *Kioupis* (2009), Ibid, 205 ff.
[240] See *Karakostas* (2009), Ibid, 47 ff.
[241] See *Spinellis* (2010), Criminal Law, Special Part, Crimes against honour, 109, margin no. 13.
[242] See *Spinellis* (2010), Ibid, p. 111, margin no. 15.

could not extend to the violation of private life, especially when the conduct of a person is not related to his/her public position and the power that he/she exerts.[243]

Criminalization of different conduct in the Greek legal order does not follow the "Harm principle". It is based on the existence of a fundamental interest to be protected against the criminalized conduct (legal interest). Thus, the existence of such an interest also functions, to a certain extent, as a constitutional limit to criminalization of conducts with respect to ICT violations. In the civil law jurisdiction the protection of a legal interest is widely accepted as a necessary prerequisite of criminalization.[244] With regard to offences against the confidentiality, integrity and availability of information systems and electronic data, attention has been drawn to the issue of a reasonable protection of such interests, and particularly to a reasonable protection against their potential endangerment by preparatory acts (i.e. by acts aiming at illegal access, illegal interception, data interference and system interference).[245] Furthermore the protected legal interest plays a major role in the interpretation of child pornography.[246]

XIV) Lack of criminal sanctions specifically targeting cyber criminals

The Greek Criminal law does not provide any criminal sanctions particularly targeting cybercriminals, e.g. a temporary ban from using the internet. The confiscation of the perpetrator's information system may apply, but this sanction is not limited to cyber criminals.

XV) Alternatives to criminalization

According to the ultima ratio principle criminalizing, in the area of ICT as well, conduct that can be addressed through milder means is not justified. Civil sanctions are provided in the Greek legal order, for example, for violations of the right to personality,[247] infringements against domain names, [248] or infringements against intellectual property.[249] Administrative sanctions are also provided by Laws for the protection of personal data[250]. In such cases, priority

[243] See Areopag 1567/2010, Poiniki Dikaiosyni 2011, 1086.
[244] See indicatively *Hassemer* (1973), Theorie und Soziologie des Verbrechens- Ansätze zu einer praxisorientierten Rechtsgutslehre, 100 ff., *Id.,* in *Neumann/Puppe/Schild* (ed.) Nomos Kommentar zum Strafgesetzbuch, Band 1, Vor § 1, *Hefendehl/ A. von Hirsch/ Wohlers* (ed.) (2003), Die Rechtsguttheorie- Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?, 119-196, *Kaiafa-Gbandi* (2000), Ein Blick auf Brennpunkte der Entwicklung der deutschen Strafrechtsdogmatik vor der Jahrtausendwende aus der Sicht eines Mitglieds der griechischen Strafrechtswissenschaft, in *Eser/ Hassemer/ Burckhardt* (ed.), Die deutsche Strafrechtswissenschaft vor der Jahrtausendwende. Rückbesinnung und Ausblick, 263 ff., *Manoledakis* (1998), The function of the concept of "legal interest", passim, *Margaritis* (1981), The legal interest as a basis for the solution of interpretative problems of Article 224 of the Greek Criminal Code, 41 ff., *Paraskevopoulos* (2008), Ibid, 94 ff., *Roxin* (2006), , Strafrecht Allgemeiner Teil, Band I, Grundlagen- Der Aufbau der Verbrechenslehre, 8 ff./*Simeonidou-Kastanidou* (2001), Crimes against life, 25 ff., *Spyrakos* (1996), The analytic function of the concept of 'fundamental interest', passim.
[245] See p. 44 ff. of the present report.
[246] See *Kaiafa-Gbandi* (2012), Internet assaults on infancy, Poinika Chronika, 162 ff. and pages 15 ff. of the present report.
[247] See *Karakostas* (2009), Ibid, 56 ff.
[248] See *Karakostas* (2009), 36 ff.
[249] See indicatively *Sidiropoulos* (2008), Law of Internet, 307.
[250] See Article 21 of Law 2472/1997.

should be given to civil and administrative sanctions in order to preserve the ultima ratio function of criminal law. This is, however, not always the case with the relevant Greek criminal law provisions.

XVI) Non-criminal means of combating offensive websites

Article 64A of Law 2121/1993 (Security measures) is a special relevant provision of non-criminal means combating offensive websites. It refers to the protection of the rightholder in the frame of intellectual property and provides that: "The rightholder may demand security measures against intermediaries, whose services are used by a third person to infringe a copyright or a related right. The same applies for the right of special nature of the database creator (Article 8 para. 3 Directive 2001/29)."

According to the combination of Articles 64, 64 A of Law 2121/ 1993 and Article 17 of Presidential Decree 131/2003, security measures against intermediaries include –inter alia- the temporary blocking of access to the illegal content, the interruption of connection of the suspected users, as well as the temporary input of filters by the intermediaries, so that access to the specific content or service is not possible.[251] The Decision no. 4658/2012 of the One Member District Court of Athens[252] has accepted the claim of the Collective Administration Organizations for Musical and Audiovisual Works to oblige Greek ISPs to take technological measures, so that the access of their subscribers to websites, where illegal presentation and transaction of works takes place, can be blocked.

General technological interventions, such as the interruption of access to services and content, are deemed to be incompatible with Greek law, because they contradict Article 5 A para 2 of the Greek Constitution, which stipulates the right of participation to the information society, in combination with Articles 5 para 1, 5 a para 1, 14 para 1 and 16 para 1 of the Greek Constitution[253]. However, it is argued that the blocking of access to specific websites with specific illegal content based on a relevant court's decision is compatible with the Constitution[254], when the judicial decision takes into account the principle of proportionality in the weighing between the imposed limitations of the above freedoms and the protection of intellectual property, and thus does not interrupt access arbitrarily.

XVII) The self-protection of users in the field of electronic crime-Measures of encouragement

ICT users are expected to protect themselves against electronic crime by different means, such as encryption of messages, use of passwords, as well as use of protective software, because in the field of electronic crime the best measure of protection is actually their own self-protection. No matter how effective the criminal measures against electronic crimes may be, they are not surely sufficient to protect a negligent user of new technologies. According to the Explanatory Report of the Convention on Cybercrime "the most effective means of preventing unauthorized access, is, of course, the introduction and development of effective security measures. However, a comprehensive response [to electronic crime] has to also include the threat and use of criminal law measures. A criminal prohibition of unauthorized access is able to give additional protection to the system and the data as such and at an early stage …."[255]

---

[251] See *Vagena* in *Kotsiris/Stamatoudi* (2009), Law for intellectual property, p. 1073, margin no. 16.
[252] See Nomiko Vima 2012, 1204 ff.
[253] See *Bourmas* (2009), Ibid, Dikaio Meswn Enhmerwshs kai Epikoinwnias, 495.
[254] See *Bourmas* (2009), Ibid, 496.
[255] See the Council of Europe Explanatory Report, para. 53.

In Greek Criminal law, as it has already been analyzed above, Article 370 C para 2 grCC, which criminalizes unauthorized access, is formulated in a general way, without requiring the infringement of security measures for the access to computer data. Lack of the right to access data is merely implied by prohibitions and security measures that are indicatively mentioned in this provision. According to Article 370 C para 2 grCC it is sufficient that the counter will of the legal holder for another person's access to his/her data has been expressed in any other way. Thus, the lack of a reasonable self-protection could provide a defense for those accused of illegally entering or abusing another person's computer system or abusing their data. Defendants could argue, in such cases, that they did not know the above mentioned counter will of the rightholder, i.e. they could claim that they ignored the fact that their acts have been committed without right. Such a mistake is deemed a mistake of fact (Article 30 grCC), by those who claim that this is an actus reus element[256], whereas by those who claim that it is "a special element of the wrongful character of the act", it is deemed to be a mistake of law (Article 31 grCC).[257]

However, it has been argued that, when illegal access concerns data that are transmitted via telecommunication systems, and especially via the internet, security measures should necessarily have been taken, since only such measures efficiently prevent the access via the internet[258].With regard to the internet, it seems that it is in fact not easily possible to express the counter will of the legal rightholder of access to electronic data without such measures, when the violation is undertaken by perpetrators that have no connection with the victim.

In order to encourage computer users to install security measures to their information systems and electronic data, Article 370 C para 2 grCC should be amended. However, this is not an obligation emerging from international legal instruments, since they also give to the states the mere option to criminalize unauthorized access dependent on the requirement of infringing a security measure. All the same, taking advantage of this option would encourage users to protect their own systems and this would actually be the best computer safety practice.

As far as the international legal instruments are concerned, let us recall here first of all Article 2 subparagraph b of the Convention on Cybercrime, which provides –inter alia- the possibility of parties to require that the offence of illegal access is committed by infringing security measures. On the other hand, Article 2 para 2 of the Framework Decision on attacks against information systems, relevantly, foresees that each Member State may decide to incriminate the illegal access to information systems, only where the offence is committed by infringing a security measure. Whereas the initial Commission's Proposal for a new Directive on attacks against information systems did not prescribe a relevant delimitation of criminalization, Article 3 of the Proposal, as it stands at this phase of the legislative procedure, provides the obligation of the Member States to criminalize illegal access to information systems, at least -inter alia- when the offence is committed by infringing a security measure. This version of the Proposal for a Directive on attacks against information systems is also in line with the requirement that criminal law be used as a last resort (ultima ratio principle), because it allows Member States to introduce certain limitations,[259]

---

[256] See p. 42 of the present report.

[257] See *Symeonidou-Kastanidou* in *Manoledakis/Kaiafa-Gbandi/Symeonidou-Kastanidou* (2005), Criminal Law *General* Part Compendium, p. 605, margin no. 1030, contra *Paraskevopoulos* (2008), Ibid, 134 who includes the above element to the actus reus.

[258] See *Kioupis* (1999), Ibid, 126

[259] On the application of this principle in European Criminal Law see *ECPI* (2010), at 707.

particularly in view of the fact that efficient security measures could protect information systems much more efficiently than unrestrained criminalization[260]. In that sense, one can only applaud the now pending proposal, which reintroduces the infringement of security measures as a requirement for the affirmation of illegal access to information systems[261].

In any case, demanding the infringement of security measures for criminalizing the illegal access to information systems or electronic data, finds the silver line, since it prevents over-criminalization of minor cases. Whereas minor cases are inherently ambiguous, the provision for the infringement of security measures constitutes an accurate delimitation of criminalization via technological measures that are at the disposal of the information system rightholder. Besides, security measures make clear the intrusion into the electronic "domicile" of the rightholder to access the data and the limits that he/she has set. Such clarity is highly important in the fluid digital world of information systems. Moreover, it is important that the parties concerned express their interest in the maintenance of the confidentiality of information systems and electronic data.[262]

Under no circumstances can users be sanctioned in the Greek legal order for not protecting their own information systems and electronic data to a reasonable extent. This would not be compatible with Article 2 of the Greek Constitution, from which –inter alia- emerges the prohibition of criminalization for causing self-harm. Given the fact that the latter is not permitted, the omission to take measures against the violation of confidentiality of one's own information systems and electronic data could not be sanctioned as well.

XVIII) Limiting anonymity

XVIII.1. Storage of user's personal data by ISPs

Law 3917/2011 incorporated the Data Retention Directive ("Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC") into the Greek legal order.

Article 3, which also transposed Articles 3 and 5 para 2 of the Directive to the Greek Law, obliges internet service providers to store users' personal data[263], while the categories of data, which should be retained are determined in Article 5[264] of the same law.

---

[260] Cf. the Explanatory Report by the Council of Europe, para. 45; also see *Carr*, and *Williams* (2002), Computer Law and Security Report, 84.

[261] See the Presidency's proposal to the Council, 8795/11, DROIPEN 27-TELECOM 43-CODEC 609, 8.4.2011, 7, 26 and *Kaiafa-Gbandi* (2012), Ibid, European Journal of Crime, Criminal Law and Criminal Justice, 66.

[262] Cf. *Hilgendorf/Frank/Valerius* (2005), Ibid, p. 176, margin no. 660.

[263] Article 3 reads as follows: "Obligation of providers to retain data

1.By way of derogation from the relevant provisions of Law 3471/ 2006, providers of publicly available electronic communications services or of a public communications network are obliged to retain the data specified in Article 5, to the extent that those data are generated or processed by them in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated, processed, stored, or logged by the providers.

With regard to the obligation of providers to make personal data available to law enforcement agencies article 1 of Law 3917/2011 provides that: "The providers of, publicly available, electronic communications services or public communications networks are obliged to retain data of Article 5 which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation of particularly serious crimes, as defined by Article 4 of Law 2225/1994" Furthermore, Article 4 of the same law ensures that the retained data are provided "only to the competent national authorities according to the process, the prerequisites and the conditions of access that are set in Law 2225/1994".

Law 2225/1994, on the other hand, regulates the declassification of telecommunication secrecy for the investigation of specific felonies that are included in a provided list (Article 4 para 1). However, the same provision foresees that: "Moreover, the declassification of secrecy is permitted for the investigation of preparatory acts of the crime of money

---

3. No data revealing the content of the communication may be retained".

[264] Regarding the internet services article 5 of law 3917/2011 provides that:

"The following categories of data are retained:

1) data necessary to trace and identify the source of a communication:

…

b) concerning Internet access, internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an IP (Internet Protocol) address was allocated at the time of the communication, a user ID or a telephone number

2) data necessary to identify the destination of a communication:

…

b) concerning Internet e-mail and Internet telephony:

(i) the name and address of the subscriber or registered user and user ID of the intended recipient of the communication

(ii) the user ID or telephone number of the intended recipient of an Internet telephony call;

3) data necessary to identify the date, time and duration of a communication:

…

b) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

4) data necessary to identify the type of communication:

…

b) concerning Internet e-mail and Internet telephony: the Internet service used;

5) data necessary to identify users' communication equipment or what purports to be their equipment:

….

c) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication.".

counterfeit according to 211 grCC, as well as for the crimes of Article 342 para. 3 and 4 grCC [insult of the modesty of a juvenile and contact with a juvenile under 16 years old via the internet and insult of his/her modesty] and 348A paras 1 and 2 grCC [child pornography] ". The latter crimes were added to the list via Law 3666/2008, and can also be misdemeanors, while Article 3 para 8 of Law 3727/2008 repealed Article 342 para. 4, but did not amend Law 2225/1994. The relevant procedure is regulated by Articles 4 and 5 of Law 2225/1994 and requires, in general terms, a well-founded decision of a reasoned judicial decree justifying that the detection of the accused's residence is impossible or essentially difficult without it (Article 4 para 2). The decision has to refer to a certain person or individuals that are related to the case under investigation (Article 4 para 3). The request for a decision is submitted to the Chamber of the Court of Appeals of Misdemeanors by the competent Prosecutor and the Chamber decides over the issue within 24 hours (Article 4 para 5). In extremely urgent cases, the Prosecutor can order the declassification himself/herself, but he/she has to introduce the issue to the Chamber within three days (Article 4 para 6).

The preventive retention of data, practically, refers not only to data related to particularly serious crimes that have already been committed. Thus, all the users are rendered "potential suspects"[265]. The provisions' scope is made clear by the purpose of the Law and the relative Directive, the risk being the establishment of a huge "tank" of citizens' telecommunication data, which could be used by national security, police and law enforcement agencies with all the negative consequences for the protection of the relevant individual rights[266]. With regard to the above procedure of secrecy declassification, it should also be noted that although data retention expands access to a huge amount of data, Law 3917/2011 maintained the same procedure, prerequisites and conditions for the stored telecommunication data that are provided for all types of secrecy of telecommunications by Law 2225/1994, and did not proceed to any necessary amendments,[267] as for example for the declassification of secrecy in extremely urgent cases, for which a decision of a Judicial Chamber in service for urgent cases or an assessment of the President of the Court of Appeals could be introduced.[268] On the other hand, for the above critical procedure, as far as individual rights of users are concerned, specialized judges and prosecutors in the field of electronic crime, who would be able to monitor the whole procedure and to cooperate efficiently with the specialized law enforcement agency for the combating of electronic crime, are also deemed essential.

XVIII.2. Laws obliging an internet service provider to register users prior to providing services

Elements for registration of users prior to providing services are not expressly included in Article 5 of Law 3917/2011. However, it might be argued that registration of all users is a kind of logical prerequisite for providing services. Article 3 of Law 3783/2009 provides expressly for the identification of the users only of card-mobile-telephones, the holders of which have no contract for services with a service provider.

---

[265] See *Tsolias* (2006), The retaining and processing of data in the sector of electronic communications according to the Directive 2006/24/EC, Dikaio Meswn Enhmerwshs kai Epikoinwnias, 351 ff.
[266] See *Kaiafa-Gbandi* (2010), Models of surveillance in security state and fair criminal trial, 41.
[267] See *Kaiafa-Gbandi* (2010), Ibid, 45.
[268] See *Kaiafa-Gbandi* (2010), Ibid, 45.

XVIII.3. The lack of provisions limiting the encryption of files and messages on the internet and imposing obligations to suspects to disclose the passwords they use

Article 19 paras 3 and 4 of the Convention on Cybercrime provide that:

"3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system."

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2."

In the Greek legal order, no provisions limiting the encryption of files and messages on the internet or setting an obligation of suspects to disclose passwords they use are available. The first would run contrary to the fact that security measures of the user's self-protection constitute the best way to protect their legal interests against digital attacks, and the second, particularly with reference to a suspect in order to reveal the password of his/her information system or electronic data, would also be highly disputable, because of the nemo tenetur se ipsum accusare principle.

XIX) Internationalization of law regarding electronic crime

XIX.1. Place of commission of internet crimes

According to Article 5 grCC the Greek Criminal law is applicable to all acts committed within the Greek territory, even if committed by aliens. On the other hand, as place of commission of the crime is deemed, according to Article 16 grCC, the place where the perpetrator committed in whole or in part the punishable act or omission and the place where the punishable result occurred, or in case of an attempt, should have occurred according to the perpetrator's intent.

Thus, according to Greek criminal law, places of the commission of a crime are deemed to be not only the place of the final result of an act, but also the ones of intermediate results which are also elements of the actus reus.[269] Notwithstanding the peculiarities of the internet, the basic provisions referring to the place of commission of crimes are also applicable for internet crimes. For example, Greece is the place of the commission of a fraud (Article 386 grCC), even if only the deception of a person or the financial transaction took place in Greece,[270] whereas, the fact that the perpetrator intended to achieve the financial benefit in Greece is not sufficient in order to consider Greece as

[269] See *Mylonopoulos* (2006), Ibid, p. 554, margin no. 1168, *Id,* International Criminal law, 166 ff.
[270] See *Mylonopoulos* (2006), Ibid, p. 555., margin no. 1169.

the place of commission, since achieving a financial benefit through fraud is not an element of the fraud's actus reus.[271]

With regard to crimes, which have a result, no special problems arise.[272] The main problems are related to the determination of the place of a crime's commission with regard to crimes of endangerment.[273] The German Supreme Court has ruled that from keeping [illegal] electronic data in a foreign server emanates a possibility for the violation of the social surrounding's peace,[274] and thus in cases of abstact-concrete crimes of endangerment, every place where the concrete act could develop its dangerousness, with regard to the protected legal interest, could be accepted as a place of commission.[275] This extensive interpretation of the place of a crime's commission is based upon the view, that the place of result is wherever the abstract risk could be realized.[276] This opinion has also been criticized in the Greek legal theory, since it leads to an unacceptable broad interpretation of the term of result, -and thus the term of place of commission- to the disfavour of the accused and to the favor of an excessive expansion of the limits of each national legal order when referring to internet acts, approaching the absurd view that every internet act is committed -and consequently criminalized- everywhere[277]. The web-site creator cannot limit locally the access and he/she is not obliged to adapt its content to the imperatives of all legal systems of the places where its users may be.[278] Furthermore, in such a case, the internet user would have to take into account the legal orders of all national states, with the result that the strictest criminal law system would set the standards.[279]

In order to delimit the term of place of commission in the frame of internet crimes, different criteria have been proposed. On one hand, in order to sustain a teleological interpretation, attention has been drawn to a special relationship to a certain state, such as the language in which the text of the internet publication is written, the issues and the individuals that are referred in it, and generally a special nexus to the specific legal order.[280] On the other hand, as far as the perpetrator is concerned, criteria like permanent residence or the intent to act in a specific territory are also discussed, and as far as the victim is concerned, his/her residence as well.[281] Another criterion that has been proposed is also the way of accessing the data, i.e. whether the data are pushed to a legal order, or in other words transmitted actively in a legal order from another or if they are pulled (retrieved) to a legal order by the users.[282]

---

[271] Cf. *Mylonopoulos* (2006), Ibid, 555 ff., margin no. 1170, *Id* (1993), Ibid, p. 169.
[272] See *Hilgendorf/Frank/Valerius* (2005), Computer- und Internetstrafrecht, p. 65 ff, margin no. 230, *Kritharas* (2009), Ibid, 42 ff.
[273] See *Gercke,* in *Gercke/Brunst* (2009), Ibid, p. 60 ff., margin no. 81.
[274] See BGHSt46, 212 ff.
[275] See *Gercke,* in *Gercke/Brunst* (2009), Ibid, p. 60 ff., margin no. 81.
[276] See *Satzger* (2010), Internationales und Europäisches Strafrecht, p. 64, margin no. 47.
[277] See *Kioupis* (2001)*,* Publication of web-sites with illegal; content, Poinikos Logos, 402
[278] See *Kioupis* (2001)*,* Ibid, 403.
[279] See *Satzger* (2010), Ibid, p. 64, margin no 47.
[280] See *Hilgendorf* (1997), Überlegungen zur strafrechtlichen Interpretation des Übiquitätsprinzips im Zeitalter des Internet, NJW, 1876 ff.
[281] See *Hilfendorf* (2001), Die Neuen Medien und das Strafrecht, ZStW, 670.
[282] See *Sieber* (1999), NJW, 2071.

In crimes of expression it is argued that data are globally accessible, but the place where somebody takes knowledge of the content is the place of the perpetrator's conduct, i.e. the place of his/her physical existence and the place where he/she stores the data.[283]

Last but not least, referring to child pornography (Article 348 A grCC) Article 8 grCC provides that the Greek Criminal law is applicable to national citizens and aliens for acts committed abroad, regardless of the law of the place of commission, where the conduct might even be a non-punishable one.

In any case, given the peculiarities of the internet, a particular provision for the place of commission in the case of all internet crimes is essential in order to ensure the necessary legal certainty. Article 5 para 3 of the Proposal of the Committee for the Reform of the Greek Criminal Law, relevantly, provides that: «When the act is committed via the internet or other means of communication, Greece is also deemed to be the place of commission, provided that an access to the specific means is provided in its territory". In the relative Explanatory Report it is mentioned that this amendment was necessary in order to combat the new forms of criminality via the internet.

XIX.2. International legal instruments that have influenced criminal law in the area of ICT

Law 1805/1988, which introduced the main electronic crimes to the Greek Criminal Code, was influenced by the Recommendation 89 (9) of the Council of Europe which was accompanied by a minimum list of crimes.[284] The provisions of the Convention on Cybercrime of the Council of Europe and of the E.U. Framework Decision 2005/222 have not been incorporated yet into the Greek legal order. With regard to special issues there has been an incorporation of relevant E.U. legal instruments, as it has already been mentioned, for example in the field of personal data, the criminalization of violations of intellectual property, the criminal liability of ISPs, the retention of data and the criminalization of child pornography.

XIX.3. Participation of Greece in discussions about the harmonization of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)

(No information available, a request for information has been addressed to the ministry of Justice)

XX) Future developments- Current trends of legislation and legal debate in Greece concerning ICT and internet crime

The main trends of legislation concerning electronic crime are focused on the implementation of the provisions of the E.U. Framework Decision 2005/222 on attacks against information systems, of the relevant Proposal for a Directive and of the Cybercrime Convention of the Council of Europe. The Committee for the Reform of the Greek Criminal Code[285] has already proposed the introduction of a new chapter, concerning the violations against information systems and electronic data, into the Greek Criminal Code. As it is mentioned in the relative Explanatory Report of its Proposal, in the chapter that is dedicated to violations against information systems, all basic acts referring to such violations foreseen in the relevant international instruments are criminalized. In particular, the crimes of this chapter are: illegal access to information system or data, illegal system interference, the so-called damage of electronic data, as well as the interception of electronic data by technical means in the frame of non public transmissions. At the

[283] See *Kioupis* (2001), Ibid, Poinikos Logos, 407.
[284] See *Mylonopoulos* (1991), Ibid, 15 ff.
[285] See for this Committee p. 49 of the present report.

same time, there is also an attempt to keep criminalization at a reasonable and controllable level, both via the express exclusion of punishability for particularly minor cases, but also via the fact that, at least, the basic offences of the chapter are prosecuted only upon complaint. Besides, the preparatory acts of the above offences -to the extent that the relative E.U. provisions imposes their criminalization- are also criminalized with important limitations, and particularly only when they concern either tools that are designed or adapted primarily for the purpose of committing these offences or relative computer passwords and access codes, provided that the specific acts were not committed for the purpose of testing or protecting an information system. The chapter also contains special definitions about: i) the concepts of information systems and electronic data, contributing in this way to legal certainty, ii) the particularly minor cases, which are excluded from criminal repression for all the chapter's acts, aiming also at a clear delimitation of punishability, and iii) the concept of critical infrastructure information systems, whose violation leads to aggravating forms of the relevant offences, so that the objects of attack, that can lead to higher penalties, are clearly defined as well. On the basis of the above, the new Chapter of the Proposal aims to serve in a balanced way, both the modern needs for protection of information systems and electronic data and the principles of the Rule-of-Law by the criminalization of conducts that violate them.[286]

[286] See Explanatory Report of the draft, which was presented in December 2011 by the Committee for the Reform of the Greek Criminal Code.