COMPUTER-RELATED CRIMES IN GREECE

SUBSTANTIVE LAW ASPECTS*

Christos MYLONOPOULOS**

The problems arising from computer-related criminal conduct, due to the creation of unknown to date legal interests and to the intangible nature of information, have caused the appearance of new challenges and needs in the field of criminal policy and have revealed the inadequacy of traditional criminal law, suggesting the necessity of promulgating new criminal law provisions. The response of the Greek legislator to the aforesaid questions of criminal policy are contained in Law 1805/1988 and constitute the main object of this work. It is obvious, however, that the understanding of the new regulations presupposes the examination of the possibilities and insufficiencies of the old ones.

I. COMPUTER-RELATED CRIMINAL CONDUCT UNDER THE TRADITIONAL LEGISLATION

1.1. Traditional criminal law provisions are either totally incapable of confronting unbearable forms of computer abuse or they can do it in a very limited extent. Thus, in the case of programme piracy and unauthorized copying of data, the provisions concerning theft (Art. 372 P.C.) or embezzlement (Art. 375 P.C.) do not apply (because information is neither a «corporeal object» nor energy) even if we follow the so-called value theory about the nature of appropriation, since in case of unauthorized acquisition of the information, the usefulness of the original data carrier is not affected[1]. *Time-theft* cannot be subsumed either under Art. 374a P.C. (*furtum usus*), which applies only in the case of motor vehicles or under Art. 372 para. 2

---

* National Report at the XIIIth International Congress of Comparative Law (Montreal, Canada 19-24 August 1990).

** Associate Professor in Criminal Law, Athens University.

1. Mylonopoulos, *Poin. Chron.* 38, 1988, p. 7/8, cf. Sieber, *The International Handbook on Computer Crime,* 1986, p. 53.

P.C. (theft of electrical energy) because the offender does not act «in order to» appropriate the energy consumed during the use of the computer[2]. Total or partial erasure or alteration of data can be qualified as damage to property (Art. 381 P.C.), insofar as they constitute an intervention to the usefulness of the material carrier of the data[3]. However, this provision does not apply if the act takes place during the transmission of data or, according to an opinion, in case of hindering the access to the programme[4].

1.2. As far as the problem is concerned, whether illegal copying or alteration of programmes or data can be qualified as forgery under traditional provisions, the prevailing opinion would rather give a posivite answer: in fact, since 1983 the Supreme Court of Greece[5], supported by some writers[6], considers magnetic tapes as documents, in an effort to punish their illegal reproduction and commercial exploitation as forgery at felony degree, with regard to the fact that the lenient penalties of the Greek Copyright Law (Law 2387/1920 as subsequently amended) was incapable of effectively deterring copyright infringements. The main (but not incontestable) argument was based on Art. 444 para. 3 of the Code of Civil Procedure which considers as private documents every mechanical representation such as photos, films or magnetic tapes. This provision has also been deemed enforceable in the field of criminal law, according to the principle of the unity of the legal order[7]. On the basis of this point of view, it was hence plausible that data carriers could also be protected as documents by the provisions concerning forgery[8]. This opinion was not, however, incontestable[9] and leads to questionable consequences. If we accept this, for example, we would also have to accept that unauthorized access to data and illegal copying of information could also be subsumed under Art. 370 P.C. (breach of privacy of the mails) which reprimands, *inter alia*, anyone who «violates another's privacy by reading, rewriting or otherwise copying a letter or other document»[10]. Even this wide interpretation, however, could not justify the applicability of the provision if the act takes place during the data transfer.

---

2. Mylonopoulos (N. 1), p. 9.
3. Cf. Sieber, *Int. Handbook*, p. 78.
4. Büchler, *MDR* 87, p. 455, BT – Drs. 10/5058, p. 35.
5. Supr. Court 462/83 NoV 31, 1983, p. 571 (Attorney General C. Stamatis).
6. Manoledakis-Margaritis, *Poin. Chron.* 35, 1985, p. 753.
7. Supr. Court, *NoV* 31 (1983), p. 571, 462/83.
8. Stamoulis, *NoV* 35, 1987, p. 1013.
9. Cf. with regard to magnetic tapes: Constantinidis, *in: Collected Essays to the Memory of Chorafas – Gafos – Gardikas*, vol. A 1986, p. 269 and *Poin. Chron.* 37, 1987, p. 934. Theodorakis, *Poin. Chron.* 35, 1985, p. 287.
10. This point of view would render unjustified the provisions contained in Art. 370 C para. 2 P.C. (cf. *infra* 6.3.1. et seq).

1.3. Furthermore, software is also protected to some extent by the penal provisions of the Greek Copyright Law (Art. 16 of Law 2387/1920 as amended by Art. 3 of Law 4301/1929). Greek theory and jurisprudence have already affirmed the copyrightability of computer programmes and accepted that they are protected if they constitute works of intellect having creative character[11]. The criminal protection assured by the aforesaid Law is, however, totally insufficient. Public representations, translations or adaptations of computer programmes are not reprimandable[12], while, on the other hand, the penalties provided for are so lenient (imprisonment for up to three months and pecuniary penalty up to ten thousand drs.) that they are incapable of preventing organized copyright infringments.

1.4. Also the wider penal protection provided for by Art. 16-18 of Law 146/1914 on Unfair Competition is not less obsolete and ineffective. According to Art. 16, communication by an employee of software constituting a trade secret is reprimandable if the offender obtained knowledge of it during the term of his employment and acted with intent of competition or with the purpose to damage the proprietor (para. 1). Unauthorized use of or communication to a third party of trade secrets (and consequently of software) for purposes of competition is further punishable, if the offender has acquired knowledge of it through an act designated in the preceding paragraph or through violation of the law or of the moral principles (para. 2). According to Art. 17, anyone who makes unauthorized use or communicates to third parties «technical standards» or «models» (such as software)[13] that have been confided to him in the course of business is also reprimandable. The above offences are sanctioned by imprisonment of up to six months and a pecuniary penalty not exceeding 3.000 drs. These punishments, reduced by half, apply to anyone who, for purposes of competition, attempts to induce someone to commit one of the above mentioned offences (Art. 18 para. 2).

Ineffectiveness of the aforesaid penalties is not the sole deficiency of the Unfair Competition Law. Moreover, its provisions do not cover several cases of computer abuse such as hacking and copying of secret software if it has not been communicated or if the act has been committed by a third party. Similarly, reproduction of a software copy is not reprimandable if it

---

11. Koumantos, *Copyright Law,* p. 54, Liakopoulos, *Questions of Commercial Law,* Vol. I, 1985, p. 137, Marinos, *Commercial Law Review* 86, p. 572, Misdemeanour Court of Athens 52873/87, Stamoulis, *NoV* 35, 1987, p. 1010, Civil Court of First Instance 13760/88, *Elliniki Dikaiosyni* 30, 1989, p. 371 (373).

12. Mylonopoulos (N. 1), p. 20.

13. Cf. Sieber, *Computerkriminalität und Strafrecht.* 2/84, Braun, *BB* 71, p. 1345.

is made without intent of use or communication. The third party who acquires knowledge of secret programmes or uses or exploits them commercially remains unpunishable, unless Art. 394 P.C. (receiving stolen goods) is applicable. Finally, the provisions do not cover employees acting without purpose of competition, even if their motives are blameworthy, or employees acting after the end of the terms of employment[14].

1.5. Computer manipulations causing damage to another's property do not constitute fraud (Art. 386 P.C.), unless a person checking the data has been deceived. The formulation of the traditional disposition, which requires that the offender, by false representations or by illegal concealment or suppression of true facts, persuades another, leaves no doubt that the deception of a natural person (who subsequently proceeds to the disposition of an asset) is an indispensable element of the offence. Art. 386 P.C. presupposes, therefore, that the offender influences the mind of another but it does not apply if the damage to property is due directly to the computer manipulation and not to the dissuasion of a person[15].

II. LAW 1805/1988: GENERAL ASPECTS

2.1. The Greek legislation has tried to fill the aforementioned gaps in four intercalary sections contained in Law 1805/1988, without however asking, during the elaboration of the draft, for the views of interested groups such as the Technical Chamber of Greece, criminal law and computer experts, users, etc.[16]. The provisions are widely formulated and technology neutral. Thus the danger that they are soon rendered obsolete is minimalized[17]. On the other hand some contradictions have not been avoided, (cf. *infra* paras. 3.5.2., 3.5.3.) and many of the new legal interests created by the expansion of computerization, such as reliability of the function of a computer system, availability of the data and exclusivity of the programme[18] are only partially protected by amended provisions which focus, however, on traditional legal interests (*infra* para. 3.5.1.). It is also worth noting that the

14. Mylonopoulos (N. 1), p. 26.

15. Haft NStZ 87,7, StR BT 191/2. Further cf. Supr. Court 2107/85 *Poin. Chron.* 36, 1986, p. 389, 40/87 *Poin. Chron.* 37, 1987, p. 382.

16. This has been underlined also during the discussions in the Parliament by Deputies Korakas and Bouloucos (Sess. 21 (26.7.88) p. 525 and 531 respectively) as well as by Marinos, *Software Protection and Software Contracts,* 1989, p. 85.

17. Cf. the suggestions of Sieber, European Committee on Crime Problems, Final Activity Report on Computer-related crime, 1989, p. 26 (hereinafter: F.A.R.).

18. Cf. Sieber, F.A.R., p. 16.

provisions concerning intellectual property and unfair competition have not been modified at all.

The new law has been considerably influenced by the second German Economic Offences Act of 1986 (2 WiKG). This fact, however, has not only enabled dogmatical correctness, but it has also caused that provisions connected to the amended ones but unknown to the German law, have not been respectively modified (cf. *infra* 4.5.2.).

Further it cannot be denied that Law 1805/1988 conforms, to a certain extent, to international trends and suggestions of International Organizations, e.g. in case of computer fraud, computer forgery and unauthorized interception of communications from a computer system. In other cases criminalization is insufficient with regard to the minimum list of the recommendations contained in the F.A.R. of the Council of Europe (cf. N. 17) There is no specific provision, for example, punishing unauthorized reproduction of a topography and it is not quite clear whether distribution or communication of an unlawfully reproduced programme can be subsumed under «use» of Art. 370 C para. 1 P.C.

2.2. The main characteristic of the new provisions, however, is an unbearable overcriminalization. They reprimand, for example, every illegal reproduction or use of computer programmes, without limiting punishability only to those protected, and every case of computer espionage without any restriction, in violation of the subsidiarity principle[19], although the latter has been taken into consideration insofar as in some cases the procedural prerequisite of a complaint is required. Finally, it must be mentioned that the aforesaid provisions are encumbered by a terminological pluralism which can influence the uniformity of interpretation and application[20].

III. THE IMPACT OF THE ENLARGED CONCEPT OF «DOCUMENT» (ART. 13c P.C.) ON COMPUTER-RELATED FORGERY AND OTHER OFFENCES

3.1.1. Article 2 of Law 1805/1988 has enlarged the concept of «document» by adding the following passage to its original legal definition contained in

19. Cf. Sieber, F.A.R., p. 22.

20. Examples: «unlawfully» (Art. 370 B para. 1) – «without right» (Art. 370 C paras. 1 and 2). «In the service of the data holder» (Art. 370 B para. 2) – «of the legitimate data holder» (Art. 370 C para. 3). «Measures hindering third parties...» (Art. 370 B para. 1b) – «Security measures» (Art. 370 C para. 2). «Violates» (Art. 370 B para. 1) – «Obtains access» (Art. 370 C para. 1).

with regard to magnetic tapes of records, to data files of data banks, to computerized files of the criminal record or of private archives and in any case where data are electromagnetically or optically stored (e.g. COM or CIM)[28]. Furthermore, photos, films and music or video tapes are considered as documents too.

3.3.1. This broad formulation seeks not only adaptation to technical and socioeconomical evolution, but also harmonization of the concept of document with the permanent precedents of the Supreme Court (cf. *supra* para. 1.2.). As it has already been underlined however, with regard to forgery[29], the extension of protection is only necessary if the traditional provisions require direct perceptibility of the data and maker, which is not the case in Greek Law, at least as far as the content of the document is concerned. The supplement of Art. 13c P.C. by Art. 2 of Law 1805/1988 seems thus to be unjustified. Moreover, it does not clarify whether the maker must be perceptible or not. The above provision, however, must not be conceived as a mere approvement of the prevailing aspect: it extinguishes every doubt about the document quality of data carriers and thus terminates the uncertainty due to the dissenting opinions which existed with regard to this subtle problem (cf. *supra* 1.2.). The legislator's intervention was therefore necessary.

3.3.2. In fact, at least some of the data and software carriers could not be subsumed under the traditional concept of document: magnetic fields and electrical charges which are embodied in diskettes or electrostatic memories (ROM, EPROM, Bubble) have no «rules of use» connecting people as members of a language community. Consequently, they do not prove through their meaning. Electrical impulses do not have communicative meaning and hence no intensio (as coded texts or microfilms do for example), since they can be understood only by the machine. So far the new regulation of Art. 2 of Law 1805/1988 has modified the intensio of the concept of document in a twofold way. It has declared:

1. That data carriers (as well as music, video tapes etc.) are documents, although the electrical charges embodied in them have no meaning (intensio) per se.

2. That they are documents even if the data they contain are the product of a machine, provided that the programming can be attributed to a person[30].

---

28. Cf. Tiedemann, 32, 86, 870, Sieber, *Computerkriminalität* 2/41, Schlüchter, *Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität,* Heidelberg, 1978, p. 97, Hass, «Der strafrechtliche Schutz von Computerprogrammen», in: *Rechtsschutz und Verwertung von Computerprogrammen,* Köln 1987, RdN 43, 45.

29. Sieber, F.A.R., p. 30.

30. Cf. Sieber, *Computerkriminalität,* p. 288, 290.

3.3.3. The modification of the concept was possible too. «Document» is a so-called «porous» concept open to the future. Consequently, its meaning changes with the social evolution and the enrichment of empirical reality[31].

3.3.4. Despite the fact that the aforementioned enlargement creates the impression that under «document» the RAM or the screen can also be subsumed (although data are not firmly embodied in them), or firmware or the bootstrap programme carrier (although their maker is not perceptible), Law 1805/1988 has not rendered unnecessary the indispensable elements of the concept of document, such as guaranteeing and perpetuating functions. Otherwise the concept would be functionless within the Greek penal system and would lead to unacceptable consequences: e.g. we would have to consider the whole computer as a document. A restrictive interpretation is therefore indicated: the modification of the concept concerns only the above mentioned aspects, according to the suggestions of the technical evolution.

3.5. Consequently, a mere recording in the RAM or in the stratch pad memory is not sufficient[32]. It is on the contrary necessary that data be stored in a non-volatile memory and that they are firmly embodied in their carriers[33]. The data carrier must further indicate a maker to whom the intellectual content of the data can be imputed (cf. note 32). It is hereby enough that the maker can be identified by the circumstances, e.g. the logo of the printer paper, access restrictions contained in the programme, the fact that only certain persons had knowledge of a password etc.[34].

3.3.6. In case of stored computer data, however, the maker is not always perceptible, even with the aid of a technical device, so that it is very doubtful whether such data carriers can be qualified as documents. The same problem arises when the content of the data «is essentially determined by the manipulated data processing computer»([35]) and particularly when a programme has been totally elaborated by another programme[36]. Here the aforesaid modification of the concept applies, according to which it is enough that the programming can be imputed to a natural person (cf. note 32).

3.3.7. Finally, data or programmes without any evidentiary function,

---

31. Hassemer, *Einführung in die Grundlagen des Strafrechts,* 1981, p. 168. Koch-Rüssmann, *Juristische Begründungslehre,* 1982, p. 150.

32. Cf. Möhrenschlager, wistra 86, 135. Samson SK art. 269, Rdn 18, Sieber, *Computerkriminalität,* p. 283/84.

33. Cf. Hass (N. 28), Rdn 45 et seq., Samson SK art. 269, Rdn 31.

34. Möhrenschlager, wistra 86, 135, Hass (N. 28), Rdn 44.

35. Sieber, F.A.R., p. 29.

36. Commission of the European Communities, Green Paper on Copyright and the Challenge of Technology, 1988, nr. 5.6.25.

such as intermediate results, are not protected as documents. Consequently, forgery is committed only with regard to data having an evidentiary value, e.g. illegal entries into the magnetic part of cash-dispenser cards[37]. This conceptual element, however, is interpreted by jurisprudence in an extremely wide sense: the plenary session of the Supreme Court has recently accepted, with respect to magnetic tapes, that legal evidentiary significance exists if «it is willfully declared by the tape itself [sic] that the sound recorded on its surface has been produced according to the law by an authorized person and directly from the original matrix»[38]. If this point of view was correct, it could be transferred to analogous cases of programme piracy. It is however unacceptable, since it leads to the abandonment of the guaranteeing function of documents. Moreover, evidentiary aptness cannot be easily affirmed in case of scientific or technical data which are not immediately connected to a legal fact[39].

3.4.1. The main practical importance of the enlargement of the concept consists in the fact that a series of computer-related economic crimes such as programme piracy, erasure and alteration of data (i.e. damage to computer data and computer programmes), computer sabotage, hindering the use of computer software and data, are collectively (but incompletely) confronted by the provisions pertaining to documents which have been respectively modified. Thus Art. 216 P.C. (forgery), 217 P.C. (forgery of certificates), 220 P.C. (swearing a false certificate), 222 P.C. (suppression of documents), 242 P.C. (false certification, alteration of public documents etc. committed by an official) now also apply with regard to data carriers, while Law 1608/1950 (as subsequently amended by Law 1738/1987), according to which imprisonment for up to twenty years or imprisonment for life is imposed if certain offenses have caused prejudice to the State, applies also in case of computer forgery[40]. More precisely:

3.4.2. *Unauthorized copying* of data or software constitutes forgery if the author acts with intent to use the copy to defraud another concerning a fact which may have legal significance and is punished by imprisonment for up to five years. The use of the document by the offender is an aggravating circumstance (Art. 216 para. 1 P.C.) but it constitutes an independent offence if committed by another. If the offender intended to enrich himself or another by causing damage or harm to another party, imprisonment for up

37. Cf. Möhrenschlager, wistra 86, 135, *Sieber,* F.A.R., p. 29.
38. Supr. Court (Plenary Session) 203/89.
39. Cf. Sieber, *Computerkriminalität,* p. 289.
40. Some dispositions, however, such as Art. 179 and 370 P.C. contain a broader concept of document: Gafos, *Criminal Law,* Special Part, vol. 5, p. 191, N. 2.

to ten years is provided for by Art. 216 para. 3 P.C.). Further: *alteration* of data can also be subsumed under forgery in the form of falsification, under condition that the aforementioned criminal intent is given. The act can in addition consist of transformation or partial erasure of data, influencing their evidentiary value. In case, however, of *total erasure*, the misdemeanor of Art. 222 P.C. is committed (i.e. suppression of documents)[41], and, under other conditions, that of Art. 381 P.C. (damaging another's property). The above provisions also apply when the offender merely hinders the access of the use of the data, e.g. when he causes the data to disappear without being erased by giving corresponding instructions (e.g. new addressing of the data or input of a new password). The application of Art. 222 P.C. presupposes, however, that the disturbance concerns the evidentiary function of the document. *Damage to computer data and computer programmes* can therefore be punished as forgery or suppression of documents, only insofar as the data carrier is a document having an evidentiary value which is influenced. Similarly *computer sabotage* as conceived by the F.A.R. of the Council of Europe (i.e. input, alteration, erasure etc. of data with the intent to hinder the functioning of a computer)[42] is punishable only under the aforesaid conditions, unless it also constitutes damage to property (Art. 381, 382, 382α para. 2a P.C.) which is, nevertheless, not always the case (cf. *infra* para. 1.1).

3.5.1. The above amendments introduced by Art. 2 of Law 1805/1988 create, however, certain problems: they alter the meaning of the provisions concerning documents, since they try to protect new or unrelated legal interests (such as financial interests constituting «a state similar to property»[43], intellectual property, integrity and proper functioning or use of data and programmes)[44], with the aid of legal instruments oriented to the protection of the security and reliability of written evidence[45]. It is hence very doubtful whether protecting data through the aforesaid provisions is a dogmatically correct choice[46]. The fact that indispensable conceptual ele-

---

41. According to Art. 222 P.C. «Every one who, with intent to cause damage to another conceals, damages or destroys a document of which he is not the owner, or the exclusive subject or of which another has the right of delivery or presentment under civil law provisions shall be punished by imprisonment for not more than two years». Cf. also Schlüchter (N. 28), p. 98, SK-Samson StGB art. 269, N. 31.

42. Sieber, F.A.R., p. 35.

43. «Eigentümerähnliche Interessenlage».

44. Sieber, F.A.R., p. 32.

45. This is deemed to be the legal interest protected by Art. 216 et seq. P.C.: Stamatis, *General Principles of Apparent Concurrence*, p. 54, Gafos (N. 23), p. 69, c.f. Sieber, F.A.R., p. 30.

46. In this sense cf. Schönke-Schröder-Cramer art. 209 Nr. 1.

ments, such as the maker's identity and the firm fixation, are not –beyond any doubt– required henceforth explicitely (cf. *supra* para. 3.3.5), indicates that the concepts of document and forgery are in danger of being distorted. As the Attorney General of the Supreme Court has emphasized[47], the subsumtion of the reproduction of a magnetic tape under forgery, even if the maker is not perceptible, constitutes «an effort to protect the interests of phonographic companies» although such an act is merely a violation of copyright law and can be effectively confronted only by a specific regulation.

3.5.2. Despite the wide formulation of the amended Art. 13c P.C., many cases of computer abuse remain uncovered: if, for example, erasure or alteration of data occurs during their transmission, no material carrier exists, so that the offender does not influence any document or corporeal object. In this case the provisions about forgery or property damage do not apply. The new regulations do not cover further alterations of data where the maker is not identifiable or which are not firmly embodied on the carrier. There is also a very important deficiency in that the provisions pertaining to documents do not apply if a programme has been reproduced after decompiling and therefore contains only cosmetic changes, although this modus of programme copying constitutes an extremely blameworthy and dangerous infringement of intellectual property (cf. *infra* para. 6).

3.5.3. The modification of Art. 216 P.C. leads further, in case of unauthorized copying of data, to the absurd consequence that, if the offender does not act with intent to defraud (e.g. if he merely accepts such a detrandation or he does not intend to conceal the fact of the illegal reproduction from the purchaser)[48], only Art. 370 C para. 1 P.C. can be applied (imprisonment for up to six months and pecuniary sentence). With regard, however, to the particularities of programme piracy (the producer's loss and the necessity of protection are in both cases identical) we can conclude that the aforementioned serious difference in the treatment of the offender is not sufficiently justified. Finally, the regulation of Art. 13c P.C. also contains the danger that copying out of common programmes can mean punishment for forgery as well, although these are not considered worth being protected as intellectual property.

---

47. Proposition to Supr. Court (Pl. Sess.) 203/89, pp. 2b and 5b.

48. It occurs very often that offenders do not act with this intent while purchasers as a rule know that the cheap programme without covering the buy (or acquired free with the hardware) is an illegal one.

IV. COMPUTER FRAUD (ART. 386 A P.C.)

4.1. As it has been mentioned above (1.5.), before Law 1805/1988 punishability of causing damage to another's property through computer manipulation depended on whether a natural person had been deceived or not[49]. Art. 5 of Law 1805/1988 seeks to cover the deficiency by adding to the P.C. Art. 386 A («Computer Fraud») according to which:

«Everyone who, with intent to enrich himself or another with an unlawful gain, influences computer data by improper programming or by an intervention during the application of the programme or by the use of incorrect or incomplete data or in any other way and thus causes damage to the property of another, shall be punished by the penalties of the preceding Article.[50]. Damage to property exists even if the harmed persons are not identifiable. For the estimation of the extent of the damage it is irrelevant whether victims are more than one person».

4.2. Art. 386 A P.C. has been influenced by Art. 263a of the German P.C. and is attached to the structure of the provision concerning common fraud (Art. 386 P.C.). In fact, instead of false representations to another person, the law requires manipulations aiming at the influencing of computer data. Instead of dissuasion and property disposition the «influencing» itself (i.e.: incorrect data processing) is presupposed. The formulation of the provision as well as its classification among offences pertaining to property, shows that protected legal interest is property[51]. The orientation of the provision to traditional fraud is also valuable with respect to its interpretation. The influencing of computer data, which can take place in any phase of the processing (that is with input, programme, consol, or output manipulations or even with hardware manipulations[52] thus causing alteration of data) is relevant only when a situation analogous to fraud exists, i.e. when the result of the data processing is different from the expected one[53] and this divergence can be imputed to the offender.

---

49. Cf. Tiedemann, JZ 86, p. 868, with regard to German law.

50. According to Art. 386 P.C., in case of fraud, imprisonment for not less than three months is inflicted and if the resulting damage is great, imprisonment for not less than two years. The act, however, is a felony (penalty: imprisonment from five to ten years) if the offender perpetrates frauds by profession or habitually or if the circumstances of the offense prove that the offender is dangerous.

51. Cf. Schlüchter (N. 28) p. 85, Hass (N. 28) Nr. 301, Sieber, F.A.R., p. 28, supports that «also trust in the security and reliability of transfer of funds, by the means of data processing» can subsidiarily be considered as an interest protected.

52. Cf. Schönke-Schröder-Cramer art. 263a Nr. 4.

53. Lenckner-Winkelbauer, CuR 86, p. 659.

4.3. As far as the modes of perpetration are concerned, their enumeration has indicative character, since computer data can be influenced «also in any other way». That means, consequently, that the legislator has taken into consideration the necessity of a wide formulation, so that the effectiveness of the provision is not influenced by technical evolution. More precisely:

4.3.1. *Improper programming* (incorrect formation of the programme) constitutes in reality a particular case of the third alternative (use of incorrect or incomplete data)[54]. It can consist not only of elaboration of a new programme but also of addition, alteration, suppression or erasure of logical steps. «Erasure» is considered to be «the removal of data from a data medium», while the «suppression» has been defined as «the holding back and the concealment of data which may have the result that such data are not fed into the data processing as required for its correct application»[55]. Every transformation of the programme can also be subsumed under improper programming if it creates the possibility that programmed controls are circumvented or the processing of certain data does not take place in the anticipated way[56].

4.3.2. As far as the meaning of «improper programming» is concerned, the dispute expressed in Germany about it constitutes a problem also existing as far as Greek law is concerned. Thus the so-called subjective opinion, according to which a programme is not correct if it does not correspond to the will and the intentions of the right holder, is the prevailing[57] and the most plausible one. Against this, however, remarkable objections can be proposed. Thus, the exact will of the right holder is not always easy to be discovered. Further, it is highly dubious whether relatively unimportant changes to a programme can be considered as acts worth repremanding. This subjective opinion finally afflicts the legal nature of computer fraud inasmuch as it transforms it into a crime pertaining to the authenticity of the programme instead of to property[58]. The adherents of this point of view have been obviously influenced by cases of computer abuse where the divergence from the objectified will of the right holder could be ascertained beyond any doubt. However, in cases of improper programmes elaborated

---

54. Möhrenschlager, wistra 86, 132.

55. Sieber, F.A.R., p. 28.

56. Möhrenschlager, wistra 86, 132, Schönke-Schröder-Cramer, art. 263a Nr. 6, Schlüchter (N. 28), p. 87.

57. Lenckner-Winkelbauer, CuR 87, p. 654, 656, Dreher-Tröndle, StGB art. 263a Nr. 6, Schönke-Schröder-Cramer art. 263 a Nr. 6, Möhrenschlager, wistra 86, 132.

58. Cf. Haft, NSt Z 87, p. 7, Hass (N. 28), Rdn 12, Schlüchter (N. 28), p. 87.

by the programmer himself, with the intent to damage property of other people (e.g.: a banker elaborates a suitable programme in order to obtain higher interests[59]) the subjective interpretation cannot give any satisfactory solution.

4.3.1.3. On the other hand the objective opinion needs a more precise justification: if we accept that a programme is correct when it accomplishes its purpose[60], then the banker of the above mentioned example should not be punished. A solution oriented at the concordance of the achieved with the original purpose of the programme is, therefore, uncertain: since, if a programme is made with the intent to cause damage to another's property, its programming in this direction is (according to this interpretation) always «correct».

A solution could perhaps be found if we proceed as in the case of negligent crimes, where the diligence, which has to be observed, can be derived from the legal interest protected by the particular disposition (if no specific rule of objective due diligence is available). Similarly we could say that a programme is incorrect, with regard to the legal interest protected by Art. 386 P.C., if it is apt (either from the beginning of or after a subsequent intervention) to cause or to increase damage to another's property or, in other words, when the intentional behaviour of the offender increases the danger of damage to property caused by the application of the programme. Consequently, the question of whether a programme is correct or not must be answered not only with regard to its aptness to accomplish its purpose but also on the basis of the question of whether it becomes fit to cause harm to another's property (Risikoerhöhungsprinzip)[61].

4.3.2. The general element of «interference with the course of data processing» has been considered to include also every intervention with the mechanical parts of the computer (hardware) influencing the processing as well as every consol – or output manipulation[62].

4.3.3. As far as the «*use of incorrect or incomplete data*» is concerned, it can be said that, since this modus operandi constitutes the equivalent to the respective conduct of the traditional fraud[63], we can conclude that also according to Greek law data can be qualified «incorrect» when they do not

---

59. Haft, NStZ 87, p. 7.

60. Schlüchter (N. 28), p. 87.

61. Cf. with regard to this principle: Roxin, ZStW 74 (1962), p. 411 et seq., ZStW 78 (1966), p. 217 et seq., Honig-Festschrift p. 133 et seq.

62. Cf Bühler MDR 87, p. 450. Schönke-Schröder-Cramer, art. 263a Nr. 12, Hass (N. 28), Rdn 16, Lackner StGB art. 263a, Rdn 4d, but also the contrary opinion of (Dreher-) Tröndle StGB art. 263a Nr. 5 concerning output manipulations.

63. Haft, NStZ 87, p. 8, Möhrenschlager, wistra, 86, 132.

correspond to reality and «incomplete» if they express only a part of the reality to which they refer[64].

Such deficient data must however be used. The offense is therefore not realized if the use has not at least begun. The mere elaboration, for example, of an incorrect list, constitutes a mere preparatory act which cannot be punished since data are not yet recorded. On the other hand, anyone who records and therefore uses incorrect or incomplete data through another person acting in good faith, is punishable as indirect principal[65], because the intermediate person acts *inter alia* without the further intent to enrich himself or another with an unlawful interest.

4.4. Despite the wide formulation of Art. 386 A P.C., it is not clear whether the provision also covers unauthorized inputs of correct data, such as misuse of a credit card in a bank automat by violation of the credit limits or the use of a stolen credit card. It has been argued that such unauthorized use of correct data does not constitute influence on the programme or on the data[66]. The dangers of overcriminalization have been mentioned too, with regard to cases which are not equivalent to common fraud, as e.g. cases of mere violation of contractual duties[67]. As far as the Greek provision is concerned, the aforementioned reservations do not create, however, an impasse: since computer data lead, after their processing, to a result different from that expected, it can be said that they are influenced, and since this influence can be caused by any means (Art. 386 A subs. a: «or in any other way»), the provision covers, in accordance with the recommendations of the Council of Europe[68], cases of unauthorized use too. Even if we require, therefore, as many writers do,[69] a symmetry to common fraud, i.e. that a natural person would have also been deceived by a respective act, the aforementioned modes of perpetration can be subsumed under computer fraud: the only use of another's credit card which has been unlawfully acquired or an input made in violation of the credit limits have a function, which in the case of common fraud would be a false «implied statement»: the offender, namely, «informs» impliedly the computer that he has a right either on the credit card or on the sum, i.e. that he has the right to input such data and

64. Leckner-Winkelbauer, CuR 86, p. 654-656, Hass (N. 28), p. 88.

65. Cf. Supr. Court 555/86 *Poin. Chron.* 36, 1986, 686, concerning perpetration of common fraud through an intermediate person who transmitted the false representations.

66. Schönke-Schröder-Cramer, art. 263a Nr. 8.

67. Schönke-Schröder-Cramer, art. 263a Nr. 2, 9, 11.

68. Sieber, F.A.R., p. 28.

69. Schlüchter (N. 28), p. 91. Lackner, StGB art. 263a Nr. 4C, Schönke-Schröder-Cramer, art. 263a Nr. 2, 11.

to cause such processing with the consent of the person entitled[70]. Since, however, the violation of the credit limit has already been qualified as theft[71], the question arises of whether a conceptual relationship between these offenses is possible or not[72].

4.5.1. Art. 386 A P.C. has rendered wider, by analogy *in bonam partem*, the field of application of Art. 387 (fraud resulting to slight damage) and 393 P.C. (prosecution of fraud upon complaint and atonement). Thus, if the damage caused by the computer fraud is small, the act is prosecuted only upon complaint and the sentence is much more lenient (imprisonment for not more than six months or pecuniary penalty). If, however, the victims are more than one, the extent of the damage is estimated on the basis of the total loss caused by the offender (Art. 386 A para. 3 P.C.) even if the particular losses are unimportant.

Furthermore, if the act has been committed against persons very close to the offender (relatives in a direct line, guardians and trustees etc.), the act is prosecuted only upon complaint (but is not punished more leniently) according to Art. 393 and 378 P.C. Finally, punishability of computer fraud is eliminated, according to Art. 393 P.C. (under the conditions provided in Art. 379 P.C.) in case of atonement, i.e. when the offender voluntarily returns the unlawfully taken property of a third party without unlawful injury and prior to any interrogation of him, or when he wholly satisfies the victim.

4.5.2. If, on the contrary, the offender damages another's property by improper programming but without any special intent required by Art. 386 A P.C. («intent of procuring an unlawful gain»), the above provision does not apply. Nevertheless, the application of Art. 389 P.C. («damage to property by fraud») would constitute prohibited analogy *in malam partem* and is consequently not possible. The legislator has omitted to modify respectively the latter provision and has thus created a considerable deficiency. Consequently, an employee seriously disturbing the data processing of a computer in order to cause loss to the proprietor of the enterprise cannot be punished according to these provisions.

4.5.3. The legislator has further omitted to modify Law 1608/1950 (as amended by Law 1738/1987) concerning increase of penalties in case of offenses against the State. Thus, although forgery (Art. 216 P.C. as amended by Art. 2 Law 1805/1988) and fraud (Art. 386 P.C.) are extremely repriman-

---

70. Cf. Hass (N. 28), Rdn 14.

71. Military Court of Thessaloniki 401/86 *Poin. Chron.* 36/774.

72. Cf. Schönke-Schröder-Cramer, art. 263 Nr. 67, 263a Nr. 18 (subsidiarity), Krey, *Strafrecht*, BJ vol. II, p. 129.

dable in this case, the penalties of computer fraud have not been respectively increased.

4.5.4. Finally, the provision concerning computer fraud does not apply in the case of time theft because the latter consists in mere (unauthorized) use of data which are, nevertheless, either altered or influenced[73].

V. COMPUTER – RELATED BREACH OF SECRECY (ART. 370 B P.C.)

5.1. The provisions of Art. 370 B P.C., introduced by Art. 3 of Law 1805/1988, are characterized by the fact that they do not only protect trade and industrial secrets but also state ones, scientific (sic) and professional. If there is a similarity to the Unfair Competition Act (Law 146/1914), it consists only in the fact that the above provisions protect software in a wider way than Greek Copyright Law, since they do not require the programme to be a personal work of creative character, or that the misappropriated programme has been considerably altered[74]. According to Art. 370 B P.C.:

«1. Everyone who unlawfully copies, imprints, uses, discloses to a third party or by any means violates data or computer programmes constituting state, scientific or professional, secrets, or secrets of an enterprise of the public or private sector, shall be punished by imprisonment for not less than three months. Secrets are also considered to be those, whose legitimate holder maintains secret, because he has a justified interest in it, especially when he has taken measures hindering third parties to acquire knowledge of them.

2. If the perpetrator is in the service of the data holder or if the secret is of particularly high financial importance, imprisonment for not less than one year shall be imposed.

3. In case of a military or diplomatic secret or of a secret concerning the security of the State, the offense, provided for by para. 1, shall be prosecuted only upon complaint».

5.2.1. The definition of the concept of trade and industrial secret is not particularly difficult since the so-called mixed theory is almost unanimous-

---

73. Cf. Schönke-Schröder-Cramer, art. 263a, Rdn 11, Schlüchter (N. 28), p. 93, Lenckner-Winkelbauer, CuR 86, p. 658/9, Dreher-Tröndle, art. 263a, Rdn 8, Hass (N. 28), Rdn 17.

74. Mylonopoulos, *Poin. Chron.* 38, 1988, p. 22, cf. Sieber, Int HB, p. 59, Massé, *Informatique,* p. 32, Goutal, «La protection pénale des logiciels», in: *Le droit criminel face aux technologies nouvelles de la communication,* 1986, p. 252.

ly supported[75]. According to this conception, computer data are qualified as secret when they are:

(1) accessible to a restricted circle of persons and not commonly known,

(2) connected to an enterprise and

(3) maintained secret according to the declared will of their holder, who has a justified interest in this. The latter is deemed to exist if the disclosure of the secret is apt to shake the competitiveness of the business.

Consequently, a programme can be considered secret even if it has not been elaborated by an employee of the enterprise but has been purchased by a third party.

5.2.2. It is incontestable that the Greek legislator has taken account of the aforementioned mixed theory, since Art. 370 B para. 1b P.C. qualifies also as secrets data or programmes whose holder has actually expressed («treats») his intention to maintain the secrecy. Nevertheless, the formulation of the provision at this point («secrets are also considered to be those ones...») does not exclude the protection of data or programmes, even if such intention has not been expressed or the interest is not justified. Since such secrets are irrelevant to the competitiveness of the enterprise, the protection assured in those cases is not legitimate, because it enables abuse and arbitrary exploitation of data in the field of the employer-employee relationship (e.g. a businessman could qualify as secrets the personal data of his employees he has collected).

This problem is due to the fact that the Greek legislator has preferred to protect *inter alia* competitiveness of enterprises by a provision mainly focusing on a totally different legal interest, i.e. state secrets, professional, scientific etc.

It would therefore be more preferable, if the provision were exclusively oriented to the mixed theory and narrowly interpreted so that only the objective secret is protected.

5.3.1. Inasmuch as the offence is realized by anyone who «by any means violates» secret data, the provision penalizes, at least prima facie, every violation indiscriminately. Some modes of perpetation are however mentioned. Thus: «*copying*» (reproduction) is «the fixation of the programme

---

75. Rokas, *Unfair Competition,* p. 127. Kotsiris, *Law of Competition,* 2ed., p. 178, *Vassilaki,* NoV 36, 1988, p. 1340. Cf. Schafheutle, *Wirtschaftsspionage und Wirtschaftsvertat im Deutschen und Schweizerischen Strafrecht,* 1972, p. 86. Baubach-Hefermehl, *Wettbewerbsrecht,* 12 ed., 1978, par. 17 Nr. 3-7 BGH GRUR 61, 43 Arians, «Der strafrechtliche Schutz des Geschäft - und Betriebsgeheimnisses in der Bundesrepublik Deutschland», in: *Kölner Studien zur Rechtsvergleichung,* vol. 2, 1978, p. 326.

on a data carrier. Even the loading of the programme from an external carrier into the internal memory can be considered as copying».[76]. Any reproduction, therefore, can be conceived of as «copy», even if made without technical means. An «*imprint*» is the reproduction of a corporeal copy of a programme or of data, even if the perpetrator has not acquired knowledge of them. The «*disclosure*» of the secret can consist in its (total or partial) communication to a third party, provided that its use remains possible,[77] while the «*use*» of a secret can also consist in its advantageous commercial exploitation[78].

5.3.2. The offence is further commited by anyone who delivers or makes such secrets available to the possession or knowledge of a third party (e.g. delivering of the carrier of the data), even if the offender has not himself any knowledge of them[79]. A violation of secrets in the above mentioned forms can finally be committed too by a person who is authorized to know and use the data of software but not to produce copies of them or to disclose them[80].

5.3.3. The wide formulation of the provision creates the danger of overcriminalization. With regard, however, to the modes of perpetration for by the provision, it is reasonable to be said that a «violation by any other means» is only given if the offender obtains access to the secret data by an act of analogous seriousness to copying, disclosing etc. This is the case, e.g., when the offender steals the carrier of the secret data without intending to deliver it to a third party[81]. It is, therefore, questionable whether the provision should also apply in cases of mere acquisition of the knowledge of data without further blameworthy intent.

5.3.4. The disclosure of the secret data can finally be committed by *omission*[82] if there exists a result (e.g. acquisition of knowledge[83] or possession of a carrier of secret software) and the person who omitted to prevent it was under a special legal obligation according to Art. 15 P.C.

5.4. Just as in other offences pertaining to privacy, Art. 370 B P.C. applies only when the violation of the secret data or software has been committed *unlawfully*. Although during the discussion of the Bill in the Parlia-

---

76. Sieber, F.A.R., p. 42.
77. Sieber, *Computerkriminalität*, p. 12/75.
78. Sieber, F.A.R., p. 47.
79. Hass (N 28), Nr. 33.
80. Schlüchter (N. 28), p. 131.
81. Cf. Möhrenschlager, wistra 86, 138.
82. Cf. Schafheutle, (N. 75), p. 93, Kisslming, *Der nach par. 17 VWG strafbare Verrat von Wirtschaftsgeheimnissen*, 1957, p. 74.
83. In this case the offence is a so-called «crime of expression» (Äusserungsdelikt) cf. Kern, *Die Äusserungsdelikte*, 1919, p. 23 et seq.

ment this element has been equated to «absence of any legal right»[84], it is beyond any doubt that it cannot depend on the existence of an explicit legal permission: if, for example, the legal holder of the data has the right to dispose of them, his *consent* excludes conceptually any «violation». Consequently, we have to distinguish: since some of the modi operandi (e.g. use or copying of data) are social adequate acts[85], the element «unlawfully» belongs to the statutory definition of the offence and limits the extent to which the provision applies. In this case consent already negates an element of the offence. Other acts, however, as for example disclosure of secret software to a third party after violation of security measures or copying of state secrets, are socially intolerable and constitute a prima facie offense. In such cases consent *justifies* the act and by the term «unlawfully» a general element of illicity is meant, which emphasizes that the aforementioned modi operandi are not conform to the Law unless a ground of justification is given[86]. The practical significance of the distinction is great, because the presuppositions of consent are less in the first case than in the second[87].

5.5.1. The wide protection of secret programmes and data by Art. 370 B P.C. fills most of the gaps existing under Law 146/1914 and avoids a casuistic enumeration of punishable acts. According however to the wording of Art. 370 B para. 1 P.C., the breach of secret programmes or computer data is unlimitedly punishable (i.e. regardless of whether the perpetrator has acted with a blameworthy intent or not) despite the warnings of experts, emphasizing that unrestricted protection of trade secret would lead to an undesirable «monopolization of stored information» which might «impair the mobility and the professional advancement of employees» as well as the free flow of information[88]. This problem is unavoidable under the formulation of the Greek provision, since the latter protects not only trade secrets but also «state, scientific and professional secrets». Consequently, in cases of violation of industrial and trade secrets the provision must apply, according to its scope, only if the competitiveness of the enterprise is concerned. Mere unauthorized access to secret data or acquisition of their knowledge is, thus, not punishable according to Art. 370 B, if the offender did not intend to cause harm to the enterprise. Here punishment would be contrary to the scope of protection of the legal rule (Normschutzzweck).

---

84. By Minister A. Kaklamanis (Session of 27.7.88, p. 557 of the Records).
85. Cf. already Schlüchter (N. 28), p. 131.
86. Cf. Schönke-Schröder-Leckner, Nr. 65 before par. 13 et seq.
87. Androulakis, *Criminal Law,* General Part, vol. 3 (1986), p. 49, 52.
88. Sieber, *Int. Handbook* 59, F.A.R., p. 47, cf. the Declaration on Transborder Data Flow of the OECD (April 11, 1985).

On the other hand, the above mentioned provisions do not protect secret hardware, which is thus protected only by the Unfair Competition Act. As far as the acquisition of secret data is concerned, punishability is questionable when a person merely receives stolen secret data on his own carrier without using them. The applicability of Art. 394 P.C. (receiving the proceeds of an offence) depends on whether the carrier of the violated data itself has been resulted from an offense or not.

5.5.2. It must be underlined that the application of Art. 370 B P.C. depends on whether a piece of information is stored or not in the memory of a computer. That is, the secrets mentioned by the provision are only protected under condition that they are stored data or that they constitute programmes. This regulation, which is not accompanied by a respective revision of the Unfair Competition Act, poses many questions concerning the scope of the provision[89]. The disclosure, e.g., of an industrial secret stored in a computer memory or the mere hacking in it by an employee is punished by imprisonment for *not less than one year* (Art. 370 B para. 2 P.C.) whilst, if the same secret is not stored, only imprisonment for *up to six months* and pecuniary penalty not exceeding three thousand drs. can be imposed (Art. 10 para. 1 of Law 146/1914). Likewise, if the above industrial secret has been violated by a third person, the act is punished by imprisonment for *not less than three months* in case the secret is stored but *no punishment* can be inflicted if it is not stored.

Similarly, if someone attempts to induce another to disclose secret software or data, the act shall be punished according to Art. 18 para. 2 of Law 146/1914 (under the further condition that it was committed for the purpose of competition) if the disclosure concern trade or industrial secrets (sentence: *imprisonment for up to three months* and a fine) but according to Art. 186 P.C. («inciting to commit felony or a misdemeanor») if the disclosure concerns a state or professional secret.

In other words: punishability and heaviness of penalty depend on the way the secrets are stored and not (according to the wording) on their nature and importance. Art. 370 B P.C. punishes breach of secrecy only with regard to the «computer dimension» as a mode of perpetration and not according to the blameworthiness of the act. A narrow interpretation of the provision, so that it protects only objective secrets, is therefore indicated also by this reason. Otherwise, Art. 370 C P.C. which protects *formal* secrecy would be unnecessary.

5.5.3. Some problems are further created by the aggravating circumstances provided for in para. 2 of Art. 370 B P.C. The provision punishes for

89. Cf. Deputy Kappos, Session of 27.7.88 p. 545 and 552.

example in the same way the employee who «*discloses*» secret software by abusing the confidence of his employer (and thus causing considerable harm to him) and the apprentice who merely acquires access to («violates») the data without blameworthy intent and without any prejudice of the enterprise. On the contrary, the members of the Board of Directors or former employees can be punished only according to para. 1 (unless the second alternative is given). Finally, it is questionable whether scientific secrets which do not simultaneously constitute state, professional or trade secrets, should be protected by Art. 370 B, especially when secret scientific research is prohibited by Law (Art. 2 para. 2 of Law 1268/1982). These cases of infrigement are therefore punishable only according to Art. 370 C para. 2 P.C.

VI. UNAUTHORIZED COPYING OR USE OF COMPUTER PROGRAMMES AND UNAUTHORIZED ACCESS TO DATA (ART. 370 C P.C.)

6.1. Art. 370 C P.C., added by Art. 4 of Law 1805/1988, aims at the suppression of illegal copying and use of software as well as at the punishment of unauthorized access to computer data. According to the new provisions:

«1. Everyone who, without right, copies or uses computer programmes shall be punished by imprisonment for up to six months and by a pecuniary penalty from one hundred to two million drachmas.

2. Everyone who obtains access to data recorded in a computer or in the *external memory* of a computer or transmitted by *telecommunication* systems shall be punished by imprisonment for up to three months or by a pecuniary penalty not less than ten thousand drachmas, under condition that these acts have been committed without right, especially in violation of prohibitions or of security measures taken by their legal holder. If the act concerns the international relations or the security of the State, he shall be punished according to Art. 148.

3. If the offender is in the service of the legal holder of the data, the act of the preceding paragraph shall be punished only if it has been explicitely prohibited by internal regulations or by a written decision of the holder or of one of his competent employees.

4. The acts of para. 1 to 3 shall be prosecuted only upon complaint».

6.2.1. The main feature of Art. 370 C para. 1 consists in the fact that it *disconnects* the protection granted to software from the copyright protection provided for by the Copyright Act (Law 2387/1920, as subsequently amended) and gives the impression that it is applied regardless of the restrictions emanating from the concept of «work of intellect» which presupposes a certain «level of originality». The violation of para. 1 seems, therefore, to be reprimandable even if the infringed programmes are totally common and

conventional and consequently not protectable by virtue of the Greek Copyright Law. The great advantage of the latter, (that is avoidance of monopolization of the ideas[90] contained in a work) is, thus, in danger *to be lost*. The provision punishes, therefore, without any differentiation, any case of software copying, such as private copying for personal use, production of back-up copies or copying of the simplest and most conventional programmes.

6.2.2. Similarly the *use* of another's programme is punishable in every case where it is unauthorized, in a way allowing the conclusion that not only serious infringements (such as public performance of a programme) are sanctioned, but also insignificant cases, e.g. «the use of a colleague's desk-top calculator» or pocket calculator or the overtime use of computers by students[91] as well as the adaptation of the programme by the purchaser, according to his personal needs. The above view, however, leads not only to an unbearable criminalization of minor breaches; it also has further unacceptable consequences. The most important consists in a contradiction: copying of a common programme is permitted by Copyright Law but prohibited by Law 1805/1988. The evaluations, however, expressed by the Greek Copyright Act do not cease to be enforceable also with regard to computer programmes. The same applies in the case of the International Convention of Berne-Paris concerning intellectual property, which has been ratified by Greece (Law 100/1975) and thus constitutes a law of higher rank with regard to Law 1805/1988. The copying of a work, therefore, which does not have the features of a «work of intellect» and cannot be protected by Copyright Law, is free. Otherwise the constitutional rule of free development of the personality is violated too[92]. The application of Art. 370 C para. 1 P.C. is therefore limited by the conditions provided for by the Copyright Act[93].

The provision treats further in the same way – as illegal use – both time theft and illegal exploitation of software and data, although these criminal activities are of a different nature and blameworthiness.

On the other hand, Art. 370 C para. 1 does not increase punishment in cases where the offence is committed by profession or habitually and thus it treats in the same way first offenders (e.g. a student copying a programme for his personal use) and criminals systematically violating the law. The narrow limit of six months does not permit an appropriate differentiation in

90. Cf. Sieber, *Int. Handbook*, p. 69.
91. Cf. Sieber, *Int. Handbook*, p. 85.
92. Marinos (N. 16), p. 88.
93. Cf. Sieber, F.A.R., p. 41: The committee suggests that unauthorized reproduction must only concern protected computer programmes, i.e. programmes worthy of intellectual property right protection. In this sense also C.E.C. LAB, p. 3 and Green Paper (N. 36), p. 200.

sentencing and the dispositions about forgery do not always apply. Consequently the above problem is not just a fictive one.

6.3.1. The provisions contained in paras. 2 and 3 of Art. 370 C P.C., punish unauthorized access to data processing or storage systems as well as unauthorized interception of data communications. The fact that criminalization of such activities by a separate provision has been characterized as advisable (because of the increasing frequency of wiretapping and unauthorized access to computer systems) and the suggestion that wiretap provisions should not be limited to the description of contemporary transmission techniques, have been taken into consideration by the legislator, who has thus chosen a wide formulation of the wording. Consequently, paras. 2 and 3 cover unauthorized wiretapping of electronic mail boxes, interception of digitally transmitted information, access to data banks through telephone networks by using another's password etc. Protected *legal interest* is the formal sphere of secrecy, that is, the formal right of the legitimate data holder to exclude others from having access to them. The provision also protects an aspect of privacy and not secret data of mere economic value. Access to an electronic mail box, e.g., corresponds clearly to violation of a closed letter[94]. Notwithstanding this subjective character of secrecy, the holder must have expressed his will objectively to secure data from unauthorized infringements.

6.3.2. Despite the danger of overcriminalization, the provision punishes mere unauthorized access to computer systems, that is, not only «the entering into a computer system without causing any damage other than retrieving information for no particular purpose»[95], but also any entering which enables the perpetrator to retrieve information directly and without obstacles. However, cases in which data are not yet or no longer registered or transmitted remain uncovered[96].

6.3.3.1. Since the provision protects the holder's formal right to designate the persons who may have access to the data, the element «*without right*» means the absence of any consent from the part of the legitimate holder of the data. The consent excludes therefore the objective elements of the offence and it does not merely justify it, since in such cases the protected legal interest is not afflicted[97].

For the same reason, by the term «without right» is not meant a negative external condition of punishability («objektive Strafbarkeitsbedingung»)

---

94. Schlüchter (N. 28), p. 59.

95. Sieber, *Int. Handbook*, p. 87.

96. Cf. Schönke-Schröder-Leckner, art. 202 a Nr. 4.

97. Cf. Schlüchter (N. 28), p. 68. Contra, Schönke-Schröder-Leckner, art. 202a Nr. 11, Hass (N. 28), p. 26.

since, if it is given, the act is not even prima facie unlawful.

If, on the contrary, the violation of the data has been committed against the holder's will, but was permitted by law, the act is merely justified, because the legal interest has been affected.

6.3.3.2. If the right to access to the data is derivative[98] and the data holder, in violation of the permission granted, procures to a third party access to the data, the latter acts without any right, and consequently is punishable according to Art. 370 C para. 2. The data holder is namely not entitled to enlarge the extent of the original authorization. In this case, however, the data holder is not a principal, since *he* had obtained access by virtue of a valid authorization. However, he is an immediate accomplice to the act of the third party. Similarly, if the holder of a programme has merely the right to *use* it but not to obtain *knowledge* of it, the offence is accomplished too[99], provided that the contrary will of the right holder has been sufficiently expressed. Punishability of such cases, however, clearly shows the danger of overcriminalization. In this context it is worth noting that the provision of para. 3, requiring an explicit prohibition by internal enterprise regulations in case of the employer – employee relationship, constitutes an exception *only with regard to para.* 2 of Art. 370 C P.C., although the restriction has been originally proposed[100] in order to limit punishability to unauthorized use of computer systems.

6.3.3.3. Since the provision emphasizes that the offender acts without right «particularly» in case of «violation of prohibitions or of security measures», it can be concluded that the offence is accomplished in any case where the data holder has objectively manifested his will to maintain the data secret. The above mentioned *indicative* enumeration, however, does not fulfil the purpose for which security measures have been considered as necessary in order to limit punishability to a reasonable extent[101]. In the system of Greek law they have a rather evidentiary function: they indicate the holder's will to exclude others from access to the data. Unauthorized access to them is therefore punished in any case this will has been objectively manifested. Consequently it is not necessary, as e.g. it is according to German law[102], that the security measure was *active* during the infringement, provid-

---

98. About this problem cf. Schüchter (N. 28), p. 63, BT-Drs 10/5058/29, Schönke-Schröder-Lenckner, art. 202a Nr. 6.

99. Cf. *Lenckner-Winkelbauer,* CuR 86, p. 486.

100. Sieber, *Int. Handbook,* p. 85.

101. Cf. Sieber, *Int. Handbook,* p. 90: «In order to avoid the criminalization of minor breaches... unauthorized access should be made punishable only in cases in which data are protected by security measures.

102. Schönke-Schröder-Lenckner, art. 202 a Nr. 3.

ed that the holder's will is sufficiently documentated. On the other hand, however, a security measure which is not *objectively* adequate and *subjectively* destined to impair unauthorized access (as e.g. security measures protecting data carriers from fire or from copying but not from access) cannot be subsumed under the provision.

VII. COMPUTER-RELATED INFRINGEMENTS OF PRIVACY

7.1. As far as the protection of the citizen's right to privacy is concerned, a proposal for a Bill has been prepared by an experts committee, pertaining to «the protection of the individual from personal data processing». The Bill differentiates between strict personal and confidential personal data: *confidential* data refer to nationality, religion, race, family relations, professional status, health, penal or administrative prosecutions and imposed sentences (Art. 1 para. 2), while *strict* personal data concern political and philosophical opinions, feelings and sexual life, as well as political activities (Art. 1 para. 3).

According to Art. 2 para. 1 of the Bill, the processing of strict personal data is absolutely prohibited (unless it is explicitly permitted by law) while the processing of confidential data is possible under the conditions described in paras. 2 and 3 of Art. 2. The willful violation of these provisions shall be punished by imprisonment for not less than one year (i.e. 1-5 years) and a pecuniary penalty of not less than 250.000 drs. If the offender, however, has acted with the intent of unlawful gain, imprisonment for not less than two years and pecuniary penalty of not less than 500.000 drs. shall be inflicted. (Art. 22 para. 1 of the Bill). The above acts are punishable even if committed through negligence, but in this case the provided sanction is lenient.

7.2. According to Art. 22 para. 1 of the Bill, the above mentioned penalties also have to be imposed on anyone who, in violation of its provisions:

- establishes or operates a register of confidential personal data without licence (Art. 3 paras. 1-5).
- grants the use of the register to a third party without authorization (Art. 4 para. 5b).
- stores personal data collected by deception, threat or duress (Art. 5 para. 2b).
- collects and stores false or unnecessary confidential personal data (Art. 5 paras. 3-4) or fails to destroy such data (Art. 5 para. 6).
- fails to destroy such data after the expiration of the license time (Art. 6).

- unlawfully transmits confidential personal data to a third party (Art. 7).
- unlawfully connects a register to another one (Art. 8) or violates the provisions concerning the citizen's right to have access to the data (Art. 10).

The same Art. 22 provides in para. 2 that everyone who, unlawfully and by any means, interferes with the programming of a data register or obtains knowledge of, alters, uses, exploits or transmits registered data to a third party, shall be punished by imprisonment for up to five years. If, however, danger to the democratic principles or to national security results from the aforementioned acts, the punishment is increased to confinement from five to twenty years (Art. 22 para. 3).

7.3. It is worth noting that the Bill also provides the establishment of a standing commission supervising the observance of its dispositions. (Art. 11f. of the Bill). The criminal liability of the members of this Commission, as well as of the administrative personnel, is regulated according to Art. 259 P.C. («breach of duty»).

CONCLUSIONS

The hesitation of the Greek legislator with regard to criminal law protection in case of infringements of privacy, is accompanied by a decisive intervention in the field of economic crimes, which is, nevertheless, both wider and narrower than it should be. Although the experiences of the German legislation and the recommendations of the OECD and the Council of Europe have been taken into consideration to a large extent, they did not avert the Greek legislator from reprimanding the main cases of programme piracy or computer sabotage by the provisions protecting reliability of written evidence. Furthermore, the Greek legislator has not proceeded to a respective modification of the Copyright Act and the Law of Unfair Competition, although the topics the new provisions concern are inherently linked to them. It would be, therefore, desirable, for the above aspects to constitute a subject of consideration by the legislator in the future.