The Convention on Cybercrime

by Pagona Markopoulou

Graduate of the Law School of Aristotle University of Thessaloniki

translated by Adam Kennard

Abstract: *The punishable actions which take place online create a multitude of legal problems due to both the complex operation of computers and the intricacies of the internet. It is precisely these problems that the Convention on Cybercrime, which is analysed in this article, attempts to resolve. However, at present the Convention has not been ratified by Greece.*

Introduction

The exponential evolution in the fields of information technology and computer science has led to a series of technological achievements bearing multiple consequences. On the one hand they facilitate many aspects of social life, but, on the other hand, they provide the necessary prerequisites for the emergence of a novel form of criminal activity. A variety of terms are used to describe this new form of crime,[1] such as electronic crime, IT crime, cybercrime, crime with computers, high-tech crime, etc.

The punishable actions described by these terms bring together a series of unique attributes due to their direct relationship with technical issues: the media for the dispersion and exchange of information, in most instances the computer, which often constitute either the medium or target of the criminal activity, function complicatedly. Consequently, crimes associated with Information Technology often cause discomfiture to those from the legal world who seek to confront them, as they require, at a minimum, an elemental familiarity with Information Technology, on the part of the legal analyst.

On the other hand, computers allow the transmission of information on a global scale within seconds, largely through use of the internet. This fact creates a variety of problems, as both the 'scene of the crime' and Court jurisdiction remain undefined, whilst the legal provisions of various states seek application. The stage for the execution of punishable acts, as we currently know it, is changing, and the need for international cooperation is proving ever more imperative.

In an attempt to resolve the issues which emerge in the area of electronic crime, and in recognising that the field requires international understanding, the Council of Europe drafted the Convention on Cybercrime[2] which was signed[3] by the majority of Council members, including Greece, but also the USA, Canada, Japan, and South Africa, on 23/11/2001. However, Greece has yet to ratify the Convention.

The Convention on Cybercrime moves in three directions: harmonisation of Substantive Criminal Law, harmonisation of Procedural Law, and enactment of the rules of International Judicial Cooperation. The substantive law provisions are found in the first Section of the second Chapter of the Convention and include the following categories of criminal activity:

1. Crimes against the Confidentiality, Integrity and Availability of Computer Data and Systems. (articles 2-6)
2. Computer-related offences. (articles 7-8)
3. Content-related offences. (article 9)
4. Offences related to infringements of Copyright and Related Rights. (article 10)

This article shall attempt to present a part of the substantive law provisions adopted by the Convention, as well as the responsibilities of Greece towards complying thereto. Specifically, crimes against the confidentiality, integrity, and availability of computer data and systems, as well as computer-related offenses, shall be referred to.

I. Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems.

Article 2: Illegal Access

The countries which are signatory to the Convention are called to criminalise the premeditated, and unrightful, access to the totality, or sections of information systems. The objective of the provision is the protection of every individual's right to maintain the confidentiality of certain information, far from the public eye.[4]

There already exist within the Greek 'legal order' several provisions regarding the protection of confidentiality:

- ➔ Section 4 in combination with Section 15 of statute 3471/2006 which amended statute 2472/1997 regarding personal data, with the prerequisite that the confidentiality in question protects *personal* data.
- ➔ Section 370B of the Greek Criminal Code which punishes access to classified/confidential data of particular types (data classified by the State,

confidential scientific or professional data, or data belonging to either state or private enterprises) or data which its owner treats as confidential.

- ➔ Section 370C§2 of the Criminal Code which punishes the mere access to data input into a computer, without further prerequisites, and is therefore an adequately broad provision which encompasses all instances not covered by the aforementioned provisions.[5]

In view of the above, it would appear that Greece is already meeting its responsibilities regarding the second Article of the Convention.

Article 3: Illegal Interception

Article 3 calls on the Convention's signatory states to criminalise the illegal interception of computer data in instances of its non-public transfer from, to, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. The provision aims for the protection of the confidentiality of communication by way of information systems, and especially computers.

The interception of computer data is only partially covered under Greek Law, and specifically when the interception refers to personal data from the respective special criminal law.[6] However, due to the constant increase in the proliferation of communication by means of electronic messaging (e-mails), there is an evident need for the enactment of a provision compatible with article 3 of the Convention, and will constitute the necessary supplement for Section 370A of the Greek Criminal Code regarding breaches in the confidentiality of telephone and verbal communication.

It is noteworthy here that the term 'non-public transfer' in article 3 of the Convention refers to the form of communication and not to the computer data. In other words, what should not be 'public' is the manner in which the elements chose to communicate. It is irrelevant whether or not the information conveyed is confidential or open-access data from another source, such as, e.g., the Media, or a particular website.[7]

Article 4: Data Interference

Article 4 of the Convention on Cybercrime regards illegal data interference. To date, deterioration, alteration, deletion, or other forms of data interference are not punishable as computer data does not constitute a 'thing', as defined in Section 381 of the Criminal code, regarding damage to third-party property.[8] Only the damage to the data's physical carrier is punishable.

Regarding the specific adulteration of computer data, there are two, albeit conditional, routes for protection. In dealing with personal data, this can be achieved by way of the law for the protection of personal data, and in dealing with 'documents', as defined in Section 13(c) of the Greek Criminal Code via the document's theft (Section 222 of the Criminal Code). However, the definition of a 'document' is particularly narrow, as it demands that the data have a everlasting, guaranteeing, and evidentiary function.[9] Therefore, interference with data which does not meet the qualifications of a 'document', nor constitute personal data, remains unpunished, even though it incurs significant damages onto the legal owners of the data. This legal gap will be covered by the enactment of a Section which protects electronic data as an independent 'legally protected good', regardless of the damage

to its physical carrier, and punishes all incursions thereto, as in, for example, the highly common distribution of computer viruses.

Article 5: System Interference

Article 5 calls on the Convention's signatory states to criminalise illegal system interference, namely the interception of a computer system's function. Activities which can come under this provision include, for example, 'mail bombing', namely the sending of a tremendous mass of electronic messages toward the end of overloading the system and causing it to collapse, as well as the 'denial of service', or the either temporary, or permanent, interception of system function, usually by means of using codes which 'congest' it.[10]

There is no similar provision in the Greek Criminal Code. Consequently, towards the end of falling in line with the Convention, a new provision which will cover these forms of punishable activities shall have to be enacted, ultimately raising information systems to the level of a 'legally protected good'.

Article 6: Misuse of Devices

Article 6 of the Convention on Cybercrime demands of the signatory states that they criminalise the production, sale, procurement for use, import, or distribution of devices, software, or computer access codes which were developed, or adapted, for the purpose of the execution of the punishable activities outlined in articles 2-5 of the Convention.

The provision, as it is formulated, is exceptionally broad, and, in the event of its transfer into Greek Law, it will create a multitude of problems.

Firstly, it punishes preparatory actions which take place long before the stage of attempt, thus overtly widening the scope of culpability.

Furthermore, it focuses on the *mens rea*, namely the intent to commit another punishable act, without examining the danger the devices and codes themselves pose for 'legally protected goods'. It is a case of punishing objects of everyday use, and, as such, the mere possibility of their use in the execution of punishable acts in combination with *intent* (which as a part of *mens rea* is exceptionally difficult to prove), are insufficient grounds for their criminalisation, even within the context of a provision for the foundation, or containment of a threat.[11] This is because even these provisions require, if only on an abstract level, the existence of a threat, open, 'live', and accessible to 'legally protected goods'.[12] The devices and access codes as they are described in article 6, however, do not objectively pose any threat. The result is essentially the punishment of belief, which infringes on the Constitution (article 7).[13]

Finally, whilst the aim of article 6 of the Convention is the protection of systems, it ends up with the opposite results, as it appears to ignore the fact that many of the devices and access codes to which it refers are used for the fortification of systems against such attacks. It refers to the so-called 'hacking tools', which constitute necessary instruments for the protection of computers and, if article 6 of the Convention is incorporated into Greek law, it would no longer be available for use.[14]

In view of the aforementioned, Greek legislators should probably uphold the reservation included in article 6 regarding devices and programmes and incorporate the provision only in regard to access codes (which is mandatory for the signatory states), whilst, however, paying attention to the wording of the new provision so that

it is specifically access codes which are designated as dangerous to 'legally protected goods', in order to avoid the unacceptable punishment of belief.

II. Computer-related Offences

Article 7: Computer-related Forgery

This provision calls the signatory states to criminalise the forgery of computer data with the intent to use it as authentic, regardless or not whether the data is directly readable or intelligible.

In regard to this article, it must be noted that under current law, forgery of computer data is not penalised, unless the data incorporates the elements of a 'document' as defined in Section 13(c) of the Criminal Code. In such a case, the *actus reus* of Section 216 of the Criminal Code, regarding forgery, is coved.[15]

In this manner, however, many instances of data forgery are not covered. For example, in the case of 'phishing',[16] the perpetrator creates a false electronic message misleading the victim to visit a fake website where the victim supplies personal data, such as access codes and credit card details, which will be used later by the perpetrator for illegal objectives. In this case, whilst the fraud could be punished under Section 386 of the Criminal Code,[17] the forgery of both the electronic message and website remain unpunished should the data not constitute a 'document'.[18] Compliance with article 7 of the Convention will cover these gaps.

Article 8: Computer-related Fraud

Computer-related fraud is already formulated in Section 386A of the Greek Criminal Code. Therefore, the question posed, in view of Greece's promised compliance with article 8 of the Convention, is to which degree Section 386A of the

Criminal Code complies with this obligation, whether it should be abolished and a new provision then passed, or whether it should simply be amended.

Before attempting to give an answer to this question, it would be useful to refer to the problem which arose regarding Section 386A of the Criminal Code, which has divided theory and legislation. This refers to instances of the theft of an ATM card, and the illegal withdrawal of money by means of the input of correct data into the system. In this case, the provisions regarding theft (Section 372 of the Criminal Code), misappropriation (Section 375 of the Criminal Code), and computer-fraud (Section 386A of the Criminal Code), may be applied.[19] The extent to which the illegal input of correct data into the system can be viewed as affecting computer data 'by any other means' remains a source of disagreement.

According to article 8 of the Convention, this case falls under the provision regarding computer fraud. Therefore, in order for Section 386A of the Criminal Code to be compatible with the Convention, it would suffice to add the phrase "with the use of correct data". Hence, the amendment of Section 386A of the Criminal Code would solve the disagreement between theory and legislation, and cover the requirement of Greece's compliance with article 8 of the Convention.[20]

Conclusion

The leaping progress which has marked technology throughout the past decades is one of the largest challenges which Law and Criminal Law more specifically are faced. Although the problems which arise preemptively seek solutions, the legal world must progress with stable and careful steps, without

exaggeration, toward securing the correct dispensation of justice and effective protection of citizens, whilst simultaneously duly respecting human rights.

With its incorporation into the Greek legal order, the Convention of the Council of Europe on Cybercrime will cover many gaps in current legislation. Greek legislators, however, should critically examine and adapt it to the needs and particularities of Greek society and legal culture, paying especial attention to the formulation of the new provisions, so that they serve their purpose and comply with the Constitution.

Endnotes

[1] *For the terminology used see: Kaiafa-Gbandi M., Criminal Law and Abuses of Information Technology[(Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής], Armen 2007, pp. 1061 et sub., see also Kioupi D., Electronic Financial Crimes [Ηλεκτρονικά Οικονομικά Εγκλήματα] in Kourakis N., "Financial Crimes II Special Section" ["Τα Οικονομικά Εγκλήματα ΙΙ Ειδικό Μέρος"], Ant. N. Sakkoula Editions, p. 405.*

[2] *See also Angeli, I., The Convention of the Council of Europe for the Fight against Crime in Cyberspace (Convention on Cybercrime)[Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο], Poiniko Dikaio 2001, p. 1218.*

[3] *For the signatory states of the Convention, see also http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, retrieved at 7/3/2008.*

[4] *It could be supported that apart from confidentiality, the provision also protects the 'legally protected good' of property (or the Legal Right to Property), especially when the legal owner of the system is a 'legal entity'. This is largely attributable to the fact that access to a certain corporation's system will cost it in terms of both time and money, as an investigation will have to be conducted in order to locate the access point, to correct the fault in the firewall, and most likely change the security software, whilst, simultaneously, an audit of files and folders will be conducted to assess whether something is missing or has been degraded, all of which make up a series of actions which require increased spending. See also Carr, I. and Williams, S. K., Draft Cybercrime Convention, Criminalization and the Council of Europe (Draft) Convention on Cybercrime, Computer Law & Security Report 2002, p. 84.*

[5] *However, reservations have been put forward regarding the question of whether the relatively lenient sentence incurred by Article 370§2 can achieve its crime-deterrent goal, see Kioupi, D.., Criminal Law and the Internet (Ποινικό Δίκαιο και Internet), Ant. N. Sakkoula Editions 1999, p. 127.*

[6] *Section 370 of the Criminal Code could also be applied, in line with its prerequisites and as long as the data in question meets the requirements of Section 13(c) of the Criminal Code, as could Section 10 of statute 3115/2003 regarding the protection of communication confidentiality, a less specific provision which punishes any form of the breaching of communication confidentiality.*

[7] *See Carr I. and Williams S. K., p. 84.*

[8] *See Manoledaki, I., Bitzileki, N., Crimes against Property [Εγκλήματα κατά της Ιδιοκτησίας], Sakkoula Editions 2004, 12th edition, p. 269, Kioupi, D., p. 140, and Milonopoulou, H., Criminal Justice – Special Section [Ποινικό Δίκαιο – Ειδικό Μέρος], 2nd Edition, P. N. Sakkoula Editions, Athens 2006, p. 11 and p. 343, who, however, accepts that infection with computer viruses includes a*

decrease in the optimal utility of the physical carrier, and therefore constitutes damage to third-party property, p. 348.

[9] *For the three functions of a 'document' see Milonopoulou, H., Computers and Criminal Law [Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο], N. Sakkoula Editions, 1991, p. 42, and Janetti, A., The Forged Document [Το Πλαστό Έγγραφο], P. N. Sakkoula Editions, p. 9.*

[10] *Spamming, namely the mailing electronic messages with promotional /advertising content (junk mail), does not fall under this provision, except in cases where it is proven that there existed an intent to intercept the system's function. See also Carr, I., and Williams, S. K., p. 85.*

[11] *Also referred to as 'provision of unintentional endangerment'.*

[12] *For the problem of crimes of endangerment, see Kaiafa-Gbandi, M., Common Dangerous Crimes [Κοινώς Επικίνδυνα Εγκλήματα], 3rd edition, Sakkoula Editions 2005, p. 40.*

[13] *See Kaiafa-Gbandi, M., Criminal Law and Abuses of Information Technology [(Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής], Armen 2007, p. 1086.*

[14] *See Carr, I., and Williams, S. K., p. 85. As a resolution for the problem, the composition of a registry and the licensing of 'hacking tools' have been proposed, in a similar fashion with what happens with the use of weapons. Nonetheless, valid doubts have been expressed regarding the extent to which something like this could be effective and in the financial interest of the State. Besides, it could be added that 'hacking tools' do not present the same danger as weapons, and, therefore, do not need to be faced with the same measures.*

[15] *See note 8, above.*

[16] *For a closer analysis of 'phishing' see Vlahopoulou, K., Electronic Crime [Ηλεκτρονικό Έγκλημα], Library of Law Editions [Εκδόσεις Νομική Βιβλιοθήκη]*

[17] *Common fraud, and not computer fraud (Section 386A of the Criminal Code) as it involves the misleading of an individual, and does not affect machine functioning. The element which must be noted is that in phishing, financial damage is indirect, as the victim supplies information and not money. Hence, it remains uncertain whether or not the* actus reus *of Section 386 of the Criminal Code will be covered.*

[18] *Should they meet the requirements of Section 13(c) of the Criminal Code, forgery is established following Section 216 of the Criminal Code.*

[19] *For the various opinions which have been supported, see, amongst others, Manoledaki, I., Bitzileki, N., p. 40, supporting the application of misappropriation, Milonopoulou, H., p. 65 and Nouskali, G., Computer Fraud: The past and future of Section 386A of the Criminal Code, especially in the context of events at the Council of Europe and in the European Union [Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386Α ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση], Criminal Law [ΠοινΔικ] 2003, p. 189, supporting the application of computer fraud, and Papadamaki, A., Crimes of Fortune [Τα περιουσιακά εγκλήματα], Sakkoula Editions 2000, p. 190, supporting the application of theft.*

[20] *It has also been claimed that Section 386A of the Criminal Code already covers the State's commitments toward the Convention, see Nouskali, G., as it includes the use of correct data. This, however, is not accepted by the majority of legislators and theorists, and consequently the article as it stands today does not solve the disagreement or serve the 'continuity of law'.*

Bibliography

- *Vlachopoulou, K., Electronic Crime [Ηλεκτρονικό Έγκλημα], Library of Law Editions [Εκδ. Νομική Βιβλιοθήκη] 2007.*
- *Kaiafa-Gbandi, M., Popular Dangerous Crimes [Κοινώς Επικίνδυνα Εγκλήματα], 3rd edition, Sakkoula Editions 2005.*
- *Kioupi, D.., Criminal Law and the Internet (Ποινικό Δίκαιο και Internet), Ant. N. Sakkoula Editions 1999.*
- *Manoledaki, I., Bitzileki, N., Crimes against Property [Εγκλήματα κατά της Ιδιοκτησίας], Sakkoula Editions 2004, 12th edition.*
- *Milonopoulou, H., Criminal Justice – Special Section [Ποινικό Δίκαιο – Ειδικό Μέρος], 2nd Edition, P. N. Sakkoula Editions, Athens 2006.*
- *Milonopoulou, H., Computers and Criminal Law [Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο], N. Sakkoula Editions, 1991.*

- *Papadamaki, A., Crimes of Fortune [Τα περιουσιακά εγκλήματα], Sakkoula Editions 2000.*
- *Janetti, A., The Forged Document [Το Πλαστό Έγγραφο], P. N. Sakkoula Editions.*

Articles

- *Carr, I. and Williams, S. K., Draft Cybercrime Convention, Criminalization and the Council of Europe (Draft) Convention on Cybercrime, Computer Law & Security Report 2002, p. 83.*
- *Angeli, I., The Convention of the Council of Europe for the fight against crime in cyberspace (Convention on Cybercrime)[Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο], Poiniko Dikaio 2001, p. 1218.*
- *Kaiafa-Gbandi M., Criminal Law and Abuses of Information Technology[(Ποινικό Δίκαιο και καταχρήσεις της Πληροφορικής], Armen 2007, 1058.*
- *Kioupi D., Electronic Financial Crimes [Ηλεκτρονικά Οικονομικά Εγκλήματα] in Kourakis N., "Financial Crime II Special Section" ["Τα Οικονομικά Εγκλήματα ΙΙ Ειδικό Μέρος"], Ant. N. Sakkoula Editions.*
- *Nouskali, G., Computer Fraud: The past and future of article 386A of the Criminal Code, especially within the context of events at the Council of Europe and European Union [Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ): Το παρελθόν και το μέλλον του άρθρου 386^{A} ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση], Criminal Law [ΠοινΔικ] 2003, p. 178.*