ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΓΕΝΙΚΟ ΤΜΗΜΑ ΔΙΚΑΙΟΥ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Δίκαιο και Ευρωπαική ενωποίηση

Κατεύθυνση: Ποινικό Δίκαιο και Φιλοσοφία του Δικαίου

Διπλωματική Εργασία

ΘΕΜΑ

Η ΗΛΕΚΤΡΟΝΙΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙ ΕΙΔΙΚΟΤΕΡΑ Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΗΣ ΔΙΑΤΑΞΗΣ 386^{A} Π.Κ (ΑΠΑΤΗ ΜΕ ΗΛΕΚΤΡΟΝΙΚΟ ΥΠΟΛΟΓΙΣΤΗ)

ΕΙΣΗΓΗΤΗΣ: ΚΩΣΤΑΝΤΙΝΟΣ Δ. ΑΛΕΞΑΝΔΡΟΠΟΥΛΟΣ

Τριμελής επιτροπή:

Επίκουρος καθηγητής:

ΑΓΑΠΙΟΣ ΠΑΠΑΝΕΟΦΥΤΟΥ

Λέκτωρ: ΓΕΩΡΓΙΟΣ ΤΖΩΡΤΖΗΣ

Λέκτωρ: ΟΛΓΑ ΤΣΟΛΚΑ

Αθήνα

Έτος 2007

Η ΗΛΕΚΤΡΟΝΙΚΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙ ΕΙΔΙΚΟΤΕΡΑ Η ΠΡΟΒΛΗΜΑΤΙΚΗ ΤΗΣ ΔΙΑΤΑΞΗΣ 386^{A} Π.Κ (ΑΠΑΤΗ ΜΕ ΗΛΕΚΤΡΟΝΙΚΟ ΥΠΟΛΟΓΙΣΤΗ)

ΠΕΡΙΕΧΟΜΕΝΑ

Summary: In this paper the author tries to set boundaries between economic and cyber crime and examine specifically the notion and the costititutive elements of computer fraud prescribed by the article 386A Greek Penal Code. He also expresses his serious preoccupation concerning the assimilation or the separation of this kind of fraud from the "common" fraud prescribed by the article 386 Greek Penal Code.

More specifically, the traditional formulation of the fraud provision presupposes that the offender influences the mind of another person by false information or by illegal concealment or suppression of facts. Consequently, computer manipulations constitute fraud only in cases in which a person checking the data has been deceived. Therefore, Law No 1805/1988 added a specific provision which punishes as fraud, (COMPUTER FRAUD) computer manipulations made with the intent of enriching the offender or another with unlawful gain even if no person has been deceived. Protected legal interest is property.

The opinion that general financial interests, are additionally protected cannot be approved because of the comparison of the new provision with the traditional fraud offence.

The enumeration of the modes of perpetration has indicative character. Improperly programmed is a computer when the results do not correspond to the will and the intention of the right holder.

Interventions of a program are all the manipulations during the run of a program.

With the use of incorrect or incomplete data the legislator covers most of the cases that were not punished by the traditional provision of fraud. Incorrect is the data if it does not correspond with the reality, and incomplete when it expresses only a part of the reality to which it refers.

The element of interference with the course of data processing has been considered to include every intervention which is not covered by the above mentioned ways of perpetration. This includes any intervention with the hardware of the systems as well as all consol-or output manipulations. This modus operandi is very valuable because it can cover abuses of cash dispensers since there is no other penal provision which punishes them.

In the traditional crime of fraud it is important that the person deceived makes a disposition of property. In Art. 386A Greek Criminal Code such an element does not exist and the question arised whether or not this disposition is necessary. A disposition of property is an element connected with the concept of fraud. And because the expressed will of the legislator was to create a provision similar to the traditional fraud crime, the disposition of property remains a *conditio sine qua non* of the provision.

If we accept that the disposition of property is not a necessary element of Art 386A the new crime does not contain a very important characteristic of fraud: the victim suffers damage through its own action.

In the case of computer fraud the "victim" is the computer and the relation between the criminal behavior and the damage of a property consists of the disposition which is the result of the manipulated data processing. In accordance with the traditional crime of fraud, it is not necessary that the computer which makes the disposition of property belongs to the person who suffers the loss (e.g. in case that a manipulated computer of a bank charges its clients with non-existing bills, so-called triangular fraud).

By closing this summary we must say that a consequence of the development of information technology is that in a lot of cases the existing provisions can not solve the new legal problems arising and

that's because the technology runs faster than the law. Therefore, an adoption of specific provisions in some parts of the law (legislation on the protection of trade secrets, copyright law) and the addition of new parts is indispensable. Additionally, the transborder character of information makes an international cooperation and coordination for the solutions proposed and adopted necessary and the assistance of the information technology industry during the empirical researches of academics and scientists valuable.

The Author: *Constantinos D. Alexandropoulos.*

ΠΡΟΛΟΓΟΣ

Αντικείμενο της παρούσας μελέτης είναι, όπως εξάλλου αναφέρεται και στον τίτλο της, η σύγχρονη ηλεκτρονική (οικονομική) εγκληματικότητα και ειδικότερα η σχέση-σύνδεσή της με ένα διαρκώς αυξανόμενο και γνωστό στους περισσότερους έγκλημα την απάτη με ηλεκτρονικό υπολογιστή, η οποία προβλέπεται ως αυτοτελώς αξιόποινη πράξη στον Ποινικό μας Κώδικα στο άρθρο 386^{A} Π.Κ

Ήδη ωστόσο, από τον τίτλο της μελέτης αντιλαμβάνεται κανείς την ευρήτητα ενός τέτοιου εγχειρήματος, τους κινδύνους που αναφύονται στην διπραγμάτευσή του, αλλά και τις περιορισμένες δυνατότητες ανάπτυξής του στα πλαίσια μιας διπλωματικής εργασίας.

Η παρούσα προσπάθεια στόχο έχει να εξαντλήσει θεματικά τις επιμέρους ενότητες όσο αυτό είναι δυνατόν, να αναδείξει τις εξελίξεις στην σύγχρονη ηλεκτρονική εγκληματικότητα και τη διασύνδεσή τους με ποινικά κολάσιμες συμπεριφορές, να συγκρίνει αντίστοιχες διατάξεις με το 386^{α} Π.Κ, ώστε να μπορέσουν να εξαχθούν ορισμένα ασφαλή συμπεράσματα σε σχέση με την αποτελεσματικότητα των κανόνων δικαίου αλλά και του ευρύτερου νομικού πλαισίου που διέπει το διαδίκτυο αλλά και τους Η/Υ στη χώρα μας αλλά και διεθνώς.

1. ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

(Α).ΕΛΛΗΝΙΚΕΣ:

Αιτιολ.	Αιτιολογική έκθεση
Α.Κ	Αστικός Κώδικας
Α.Ν	Αναγκαστικός Νόμος
Α.Π	Άρειος πάγος
Αρ.	Αριθμός
Αρθρ.	Άρθρο
Αρμ.	Αρμενόπουλος
Αρχ.Νομ	Αρχείο Νομολογίας
ΑΤΜ	Αυτόματη ταμειακή μηχανή
Α.υ.ε	Αντικειμενική υπόσταση του εγκλήματος
Βλ.	βλέπε
Βουλ.	Βούλευμα
Γεν.Μ.	Γενικό μέρος
Γερμ.	Γερμανικό
Γνμδ	Γνωμοδότηση
Διατ	Διάταξη
ΕΕΝ	Εφημερίδα Ελλήνων Νομικών
Ε.Ε.Π.Δ	Ελληνική Εταιρεία Ποινικού Δικαίου

Ειδ.Μ	Ειδικό μέρος
Εις.	Εισαγγελέας
Εκδ.	Έκδοση
ΕλλΔνη	Ελληνική Δικαιοσύνη
ΕΝΟΒΕ	Ένωση Νομικών Βορείου Ελλάδος
Επ.	Επόμενα
Ε.Σ.Δ.Α	Ευρωπαϊκή Σύμβαση Των Δικαιωμάτων του Ανθρώπου (1950)
Εφ.	Εφετείο
Θ.	Θέμις
Η/Υ	Ηλεκτρονικός υπολογιστής
Η.ε	Ηλεκτρονική εγκληματικότητα
Κ.Π.Δ	Κώδικας Ποινικής Δικονομίας
Κ.Πολ.Δ.	Κώδικας Πολιτικής Δικονομίας
Μον.	Μονομελές
Ν.	Νόμος
Ν.Δ	Νομοθετικό Διάταγμα
ΝΟΒ	Νομικό Βήμα
Ολ	Ολομέλεια
Οπ. παρ.	Όπως παραπάνω
Παρ.	παράγραφος
Παραπ.	Παραπάνω

Παρακ.	Παρακάτω
Π.Κ	Ποινικός Κώδικας
ΠΝΑΠ	Ποινική Νομολογία Αρείου Πάγου
ΠοινΔικ	Ποινική Δικαιοσύνη
ΠοινΛογ	Ποινικός Λόγος
Πλημ.	Πλημμελειοδικείο
Ποιν.Χρον.	Ποινικά χρονικά
Πρβλ.	Παράβαλε
Σ.	σελίδα
Σημ.	σημείωση
Στοιχ	στοιχείο
Συμβ.	Συμβούλιο
Τ.	Τόμος
Τριμ.	Τριμελές
Τχ.	Τεύχος
Το Σ	Το Σύνταγμα
Υπερ.	Υπεράσπιση
Φ.Ε.Κ	φύλλο εφημερίδας της κυβέρνησης

(B).ΞΕΝΕΣ:

Art.	Artikel, Articolo.
AT	Allgemeiner Teil
Aufl.	Auflage
BT	Besonderer Teil
BGHst	Entscheidungen des Bundesgerichtshofes in Strafsachen
C.P	Codice Penale
C.P.P	Codice di Procedura Penale
Ed.	Edition
JZ	Juristenzeitung
LG	Landgericht
LK	Leipziger Kommentar
LM	Entischeidungen des BGH in Nachschlagewerk des Bundesgerichtshofes
NJW	Neue Juristische Wochenschrift
NSTZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
PIN	Personal identification number
Zst.W	Zeitschrift für die gesamte Strafrechtswissenschaft

2. Εισαγωγή

Η ραγδαία ανάπτυξη, διάδοση και χρήση νέων τεχνολογιών, ιδιαίτερα τεχνολογιών πληροφόρησης, αλλάζει τα δεδομένα της επικοινωνίας σε όλους τους τομείς της κοινωνικής ζωής, από την πολιτική, την οικονομία και τα μέσα ενημέρωσης έως τις επιστήμες, την εκπαίδευση και την τέχνη. Η μεταφορά δεδομένων σε μεγάλους όγκους μέσω των «λεωφόρων της επικοινωνίας»[1], η δημιουργία αποκεντρωμένων δικτύων με παγκόσμια διάσταση, όπως τα δορυφορικά συστήματα, η ασύρματη τηλεφωνία ή το διαδίκτυο, οι εφαρμογές της ταυτόχρονης μεταφοράς κειμένων, εικόνων και δεδομένων (πολυμέσα) και οι νέες τηλεπικοινωνιακές υπηρεσίες που συνδέονται με αυτά αλλά και γενικά οι πρωτόγνωρες δυνατότητες της ψηφιακής τεχνολογίας ανοίγουν εντελώς νέες προοπτικές στην επικοινωνία και την καθημερινή μας ζωή, αλλά συγχρόνως διαγράφουν και σοβαρούς κινδύνους για την ελεύθερη έκφραση και την όλη διαμόρφωση της ζωής μας.

Ο χώρος του δικαίου δεν θα μπορούσε βεβαίως να μείνει ανεπηρέαστος από αυτές τις μεταβολές. Πράγματι, η μετάβαση σε μια κοινωνία των πληροφοριών απασχολεί όλο και περισσότερο τη νομική επιστήμη και πράξη, ιδιαίτερα στο πεδίο του Δημοσίου και του Ποινικού Δικαίου, όπου αναζητούνται τα κατάλληλα νομικά – δικαιικά πλαίσια, για να μπορέσουν να τεθούν οι νέες υποδομές πληροφόρησης και επικοινωνίας σε μια αποτελεσματική κανονιστική τάξη.

Ιδιαίτερα στο χώρο του ποινικού Δικαίου το ερώτημα που προκύπτει από τη σχέση διαδικτύου και ποινικής νομοθεσίας είναι: α) Αν ο παγκόσμιος ιστός (internet) μπορεί να ελεγχθεί από απόψεως

[1] Βλ. ενδεικτικά Hiltry, Reto M., Information Highway, Bern Műnchen 1996.

ποινικής συμπεριφοράς β) Αν η εν γένει χρήση ενός ηλεκτρονικού υπολογιστή ή ενός δικτύου Η/Υ που συνδέεται ενσύρματα ή ασύρματα μπορεί να προκαλέσει κινδύνους που ενδεχομένως τυποποιούν εγκληματικές συμπεριφορές ήδη γνωστές ή και πρωτόγνωρες στο χρήστη. γ) Αν αυτές οι συμπεριφορές είναι ικανές από μόνες τους να επιφέρουν βλάβη στο θύμα δ) Αν μπορούν να τιμωρηθούν και σύμφωνα με ποιο δίκαιο αφού ο τόπος τέλεσης των συγκεκριμένων πράξεων δεν είναι εύκολο να εντοπιστεί.

Η απάντηση στα παραπάνω ερωτήματα είναι πάρα πολύ δύσκολη και εκτείνεται σε πολύ περιορισμένο τομέα. Και αυτό γιατί η τεχνολογία εξελίσσεται τόσο γρήγορα, που η νομοθεσία όσο και αν προσπαθεί αδυνατεί να την προφτάσει. Επιπλέον για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο απαιτούνται εξειδικευμένες γνώσεις τόσο σε τεχνικό όσο και σε νομικό επίπεδο. Η απόκτηση των γνώσεων αυτών από νομικούς, που έχουν σχέση με την έρευνα, δίωξη και εκδίκαση των σχετικών υποθέσεων, αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε πολιτείας.

Αντικείμενο των επόμενων αναπτύξεων συνεπώς θα αποτελέσει η σχέση Ποινικού Δικαίου και διαδικτύου, η ποινική προσέγγιση του εγκλήματος στον κυβερνοχώρο, η σύνδεση της ηλεκτρονικής με την οικονομική εγκληματικότητα και κυρίως η σύνδεση της ηλεκτρονικής εγκληματικότητας με μια συνεχώς εξελισσόμενη μορφή απάτης αυτή της απάτης με υπολογιστή που ήδη οριοθετείται ποινικά από το άρθρο 386Α του Ποινικού μας Κώδικα.

Το εν λόγω άρθρο προστέθηκε στον Ελληνικό Ποινικό Κώδικα με τον Ν.1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του Ποινικού Κώδικα (άρθρα: 13γ, 370Β, 370Γ, 386Α Π.Κ) οι οποίες αφορούν τα εγκλήματα που διαπράττονται με ηλεκτρονικούς

υπολογιστές (Computer crimes).[2] Για την εποχή του θεωρήθηκε αρκετά πρωτοποριακό. Διαμορφώθηκε ακολουθώντας ως πρότυπο την αντίστοιχη γερμανική διάταξη του άρθρου 263Α του Γερμανικού Ποινικού Κώδικα (263a StGB), η οποία με τη σειρά της είχε εισαχθεί στην Γερμανία μόλις δύο χρόνια νωρίτερα το έτος 1986.

Σκοπός της θέσπισης της διάταξης και πρόβλεψής της ως ιδιώνυμου εγκλήματος, ήταν, όπως άλλωστε και σε αυτή την ίδια την εισηγητική αυτής έκθεση αναφέρεται, να καλυφθεί το νομοθετικό κενό που ανέκυψε στην πράξη, με τη ραγδαία ανάπτυξη συστημάτων ηλεκτρονικών πληρωμών, που συνίστατο στο ότι η διάταξη της κλασικής απάτης δεν μπορούσε να καλύψει παράνομες συμπεριφορές που διαπιστώνονταν ολοένα και συχνότερα στις σύγχρονες ηλεκτρονικές μορφές συναλλαγών, όπου η μετάθεση της περιουσίας γίνεται αυτόματα (ηλεκτρονικά) μέσω ηλεκτρονικού υπολογιστή, χωρίς την παραμικρή παρεμβολή στην ολοκλήρωση της διαδικασίας της περιουσιακής μετάθεσης οιουδήποτε φυσικού προσώπου, αρμοδίου να λαμβάνει αποφάσεις, να διενεργεί προληπτικό έλεγχο, να εγκρίνει, να χορηγεί και εν πάσει περιπτώσει να διενεργεί την περιουσιακή διάθεση. Ο λόγος που οι συμπεριφορές αυτές δεν μπορούσαν να αντιμετωπιστούν με τη διάταξη της κοινής απάτης,

[2] Αξίζει μεταξύ άλλων να σημειωθεί ότι ο Ν.1805/88 προσέθεσε στον Ποινικό μας Κώδικα και την διάταξη του άρθρου 370Γπ.κ αλλά και στο άρθρο 13 γ την έννοια του «ηλεκτρονικού εγγράφου» αναφέρεται έτσι στο εν λόγω άρθρο ότι « Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα , όπως επίσης , και κάθε μαγνητικό , ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία ή εικόνα , σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό , εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.» Η δυνατότητα αποθήκευσης και επεξεργασίας στοιχείων , τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα περιλαμβάνει βέβαια και πολλά απόρρητα. Επειδή υπάρχει κίνδυνος όχι μόνο διείσδυσης σε αυτά αλλά και αντιγραφής τους καθώς και άλλων τρόπων παραβίασης αυτών των απορρήτων , οι μορφές αυτές συμπεριφοράς, που ονομάζονται συνήθως «κατασκοπεία υπολογιστών» (computer espionage), προβλέπονται και τιμωρούνται στο άρθρο 370 β Π.Κ αρ.1 που προστέθηκε στον Π.Κ με το Ν. 1805/88.

καθίσταται σαφής ήδη από την απλή ανάγνωση της διάταξης του άρθρου 386 Π.Κ και εκδηλώνεται σε δύο στοιχεία της αντικειμενικής υπόστασης: α) «*Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία πείθοντας κάποιον….*» Άγραφο στοιχείο της αντικειμενικής υπόστασης του εγκλήματος της απάτης, αλλά λογικό προαπαιτούμενο αυτής, είναι η δημιουργία πλάνης σε εκείνον που προβαίνει στην περιουσιακή διάθεση. Αυτή προϋποθέτει νοητική επικοινωνία μεταξύ δράστη και πλανώμενου. Άρα πλανώμενος μπορεί να είναι μόνο άνθρωπος, φυσικό πρόσωπο.

β) «*……..πείθοντας κάποιον σε πράξη παράλειψη ή ανοχή….*» Ο πλανώμενος πρέπει να είναι κάποιος, ο οποίος δύναται να προβεί σε πράξη, παράλειψη ή ανοχή που ενέχει περιουσιακή διάθεση. Και ως προς το στοιχείο αυτό είναι σαφές ότι μόνο άνθρωπος μπορεί να εννοείται από την εν λόγω διάταξη, αφού εξ ορισμού και κατά το γλωσσικό νόημα της διάταξης, μόνο άνθρωποι μπορούν να προβαίνουν σε πράξη, παράλειψη ή ανοχή. Συνεπώς κατά το γλωσσικό νόημα του άρθρου 386 Π.Κ η κοινή απάτη περιορίζεται μόνο στις περιπτώσεις που α) η ξένη περιουσία βλάπτεται με την παραπλάνηση κάποιου φυσικού προσώπου και β) η περιουσιακή διάθεση με πράξη παράλειψη ή ανοχή γίνεται επίσης από φυσικό πρόσωπο.[3] Στο παρελθόν και ιδίως στη Γερμανία, είχε από κάποιους υποστηριχθεί ότι περιπτώσεις ανάλογες με τις εδώ ερευνώμενες θα μπορούσαν να υπαχθούν και να αντιμετωπιστούν με τη διάταξη της κοινής απάτης, με το επιχείρημα ότι το προγραμματισμένο από άνθρωπο μηχάνημα μπορεί εν μέρει να τον υποκαταστήσει στην λειτουργία του και υπό αυτήν την έννοια είναι και το μηχάνημα αφενός δεκτικό παραπλάνησης και εξαπάτησης και αφετέρου ικανό

[3] Βλ. ΑΠ 1277/98 Ποιν Δικ 2/1999 σελ 113.

να προβεί σε περιουσιακή διάθεση σύμφωνα με τον προγραμματισμό του.[4] Η υπαγωγή ωστόσο των εδώ ερευνώμενων περιπτώσεων στη διάταξη περί κοινής απάτης ορθά κατά τη γνώμη του γράφοντος απορρίπτεται σχεδόν ομόφωνα στη θεωρία και τη νομολογία αφού αδυνατεί να απαντήσει πειστικά στις παραπάνω εύλογες ενστάσεις. Δεν είναι δε τυχαίο ότι πολλοί συγγραφείς παραλείπουν οιαδήποτε αναφορά στον προβληματισμό αυτό και στην αντικειμενική υπόσταση της κοινής απάτης, η στοιχειοθέτηση της οποίας θεωρείται αυτονοήτως ότι πρέπει να αποκλειστεί.[5] Εκ των ανωτέρω προκύπτει ότι η θεσμοθέτηση της διάταξης του άρθρου 386Α Π.Κ κρίθηκε και είναι πράγματι αναγκαία για να καλύψει την τυπολογία των ολοένα και συχνότερα πλέον εμφανιζόμενων περιπτώσεων, στις οποίες ο δράστης – για να χρησιμοποιήσουμε έναν μη δόκιμο αλλά περιγραφικό όρο – «εξαπατά μηχάνημα».

Προβληματικές ωστόσο εμφανίζονται οι περιπτώσεις της ανάληψης χρημάτων από ΑΤΜ με χρήση κλεμμένης κάρτας, της τραπεζικής συναλλαγής μέσω internet banking (home banking), οι περιπτώσεις εκτροπής κλήσεων μέσω προγραμμάτων ιών (dialers) σε χώρες με υψηλό κόστος τηλεφωνικής συνδιάλεξης, οι περιπτώσεις ηλεκτρονικού «ψαρέματος δεδομένων (phising)» και άλλες τις οποίες θα αναλύσουμε διεξοδικά στα κεφάλαια που ακολουθούν.

Πρόσθετο στόχο του παρόντος πονήματος θα αποτελέσει η αποτελεσματικότητα του ως άνω νομοθετήματος σήμερα τόσο σε σχέση με το συνεχώς αυξανόμενο ηλεκτρονικό έγκλημα, τις διαστάσεις του οποίου θα αναλύσουμε παρακάτω, όσο και σε σχέση με τα νομοθετήματα άλλων χωρών αλλά και τα διεθνή κείμενα που

[4] Για τις μεμονωμένες αυτές απόψεις βλ. *Σάμιο* σε ΠοινΧρ ΜΘ/1999 σελ.1061 υποσημ. 22.
[5] Βλ.*Οββαδία Σ. Νομμία* Σύγχρονες μορφές ηλεκτρονικής απάτης στις τραπεζικές συναλλαγές . Σε Τιμητικό Τόμο για το *Νικόλαο Ανδρουλάκη* Αθήνα 2003 σελ 474 επ. αλλά και *Σάμιου* Σσελ.1061 υποσημ 27.

αφορούν το συγκεκριμένο θέμα και από τα οποία προκύπτουν και διεθνείς δεσμεύσεις συμμόρφωσης της χώρας μας ως προς την τυποποίηση συγκεκριμένων εγκληματικών υποστάσεων (τα οποία παρατίθενται στο παράρτημα νομοθετικών κειμένων στο τέλος της εργασίας), και τα οποία θα προσπαθήσουμε να προσεγγίσουμε τόσο συγκριτικά όσο και κριτικά.

3.Διαδίκτυο και Δίκαιο

Η προσέγγιση των νομικών θεμάτων που αφορούν τον κυβερνοχώρο ενέχει τη δυσκολία ότι προϋποθέτει όχι μόνο νομικές, αλλά ως ένα βαθμό τουλάχιστον και τεχνικές γνώσεις. Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του εγκλήματος στον κυβερνοχώρο όπως και στα εγκλήματα με ηλεκτρονικούς υπολογιστές χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Εξίσου σημαντική παρουσιάζεται η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων και αυτό διότι το έγκλημα στον κυβερνοχώρο αποτελεί από ποινική έποψη σχετικά νέα μορφή εγκλήματος. Αντίθετα η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση από την αντίστοιχη ποινική πλευρά και αυτό εξηγείται λόγω της μεγάλης επιρροής του κυβερνοχώρου τόσο στον αστικό (σύναψη συμβάσεων δια του κυβερνοχώρου κ.λπ.) όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο κ.λπ.).[6]

Πρόβλημα επίσης δημιουργείται και όσον αφορά στην ελληνική νομική ορολογία, γιατί κατά κανόνα τόσο η τεχνική όσο και η νομική

[6] Βλ. Σχετικό άρθρο του Αγγελή στην ηλεκτρονική διεύθυνση: http://www.lawnet.gr/pages/eofn/2/cybercrime.asp.

ορολογία είναι διατυπωμένη στα αγγλικά με αποτέλεσμα η αντίστοιχη μεταφορά των όρων αυτών στα ελληνικά να μην είναι ούτε εύκολη ούτε δόκιμη.

Στην καθημερινή πρακτική όμως πολλοί όροι χρησιμοποιούνται στην ξενόγλωσση διάστασή τους, κατά τρόπο που τείνουν να ενσωματωθούν και στο ελληνικό λεξιλόγιο. Έτσι σχετικοί με το θέμα ξενόγλωσσοι όροι είναι[7]: cyber crime, Internet crime, Crime in cyberspace, On line crime, On line computer communication crime, Digital crime, Electronic evidence κ.λ.π. Σχετικοί όροι με το δράστη είναι: Hacker, Cracker, Internet freak, Cyber crook, Cyber freak. [8]

3.1 Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή

Το έγκλημα που τελείται στον κυβερνοχώρο (cyber crime) είναι ειδικότερη μορφή του ηλεκτρονικού εγκλήματος (computer crime), το οποίο με τη σειρά του συνιστά ειδικότερη μορφή του κοινού εγκλήματος, όπως αυτό προσδιορίζεται από το άρθρο 14 Π.Κ.[9] Ως ηλεκτρονικό έγκλημα μπορεί να οριστεί αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών.[10] Ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί κάθε

---

[7] Βλ.*Δ.Κιούπη*, Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της Ελληνικής Νομοθεσίας, Υπερ. 2000,σελ.959.

[8] Βλ.επίσης για τη σχέση των ηλεκτρονικών υπολογιστών με την Ελληνική γλώσσα από τεχνική άποψη Λέων Πολυχρονίου, Ηλεκτρονικοί υπολογιστές και Ελληνική Γλώσσα , Εκδόσεις Γεωργιάδη, Αθήνα 1999.

[9] Βλ. *Ε. Αγγελή* «Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο η σχέση της με την Ελληνική έννομη τάξη» στην ηλεκτρονική διεύθυνση: http://www.lawnet.gr/pages/eofn/2/cybercrime.asp

[10] Βλ.*Θ. Γιαννόπουλου*, Όψεις και προβλήματα Ηλεκτρονικής Εγκληματικότητας, ΝοΒ 1986, σελ 170 επ..

παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων.[11] Στο σημείο αυτό πρέπει να σημειωθεί ότι ο ορισμός αυτός είναι πολύ ευρύς και είναι αυτονόητο ότι μόνο ως οδηγός μπορεί να χρησιμοποιηθεί. Η συγκεκριμενοποίησή του επαφίεται στον εθνικό νομοθέτη και την νομολογία των δικαστηρίων.

3.2. Ορισμός του εγκλήματος στον κυβερνοχώρο

Τα νομικά προβλήματα στον χώρο του ηλεκτρονικού εγκλήματος είναι πολλά και ξεκινούν ήδη από τον ίδιο τον ορισμό του ηλεκτρονικού εγκλήματος. Ο Έλληνας νομοθέτης, όπως και οι περισσότεροι εθνικοί νομοθέτες, περιορίζεται να ρυθμίσει τα επιμέρους εγκλήματα εντάσσοντάς τα στα κεφάλαια των ποινικών κωδίκων ή των ειδικών ποινικών νόμων, όπου ανήκει το προσβαλλόμενο κάθε φορά έννομο αγαθό.

Στη σχετική σύμβαση του Συμβουλίου της Ευρώπης[12] γίνεται λόγος για κυβερνοέγκλημα ή έγκλημα στον κυβερνοχώρο (cyber crime), ενώ η απόφαση-πλαίσιο 2005/222/ΔΕΥ της ΕΕ αναφέρεται μόνο στις «επιθέσεις κατά των συστημάτων πληροφοριών».[13] Στη διεθνή βιβλιογραφία συναντά κανείς ακόμη τους όρους έγκλημα με υπολογιστή (computer crime), έγκλημα υψηλής τεχνολογίας (hi-tech crime), e-έγκλημα κ.λπ. Θα πρέπει να σημειωθεί ότι οι όροι χρησιμοποιούνται συχνά χωρίς διάκριση και οι ειδικότερες περιπτώσεις εντάσσονται σε περισσότερες κατηγορίες. Αν και το ηλεκτρονικό έγκλημα εν στενή εννοία αναφέρεται σε περιπτώσεις

---

[11] Βλ.*Χ. Μυλωνόπουλου* "Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», Σειρά Ποινικά , Νο 33,σελ.14.

[12] *Σύμβαση του Συμβουλίου της Ευρώπης αριθμ. 185* (Βουδαπέστη 23/11/2001). Έχει υπογραφεί, αλλά δεν έχει ακόμη κυρωθεί από την Ελλάδα.

[13] Δημοσιεύθηκε στην εφημερίδα της ΕΕ L 69 16/3/2005, σελ. 67

όπου ο υπολογιστής ή το δίκτυο υπολογιστών αποτελεί αναγκαίο χαρακτηριστικό του εγκλήματος, συχνά μιλώντας για ηλεκτρονικό έγκλημα συμπεριλαμβάνονται και «παραδοσιακά» εγκλήματα, όπως η απάτη, η εκβίαση, η νομιμοποίηση εσόδων από παράνομες δραστηριότητες, η συκοφαντική δυσφήμηση κ.λπ., τα οποία, στην συγκεκριμένη περίπτωση, τελούνται μέσω υπολογιστή.

Σύμφωνα με μια ευρέως διαδεδομένη αντίληψη, οι ηλεκτρονικοί υπολογιστές δεν δημιουργούν συνήθως νέες μορφές εγκληματικότητας, αλλά καθιστούν απλώς δυνατή την τέλεση παραδοσιακών εγκλημάτων με νέες μεθόδους. Σε αυτήν την κατηγορία, ανήκουν π.χ. περιπτώσεις τέλεσης συκοφαντικής δυσφήμησης μέσω μιας ηλεκτρονικής επιστολής (e-mail) ή πλαστογραφίας μέσω της νόθευσης ενός ηλεκτρονικού εγγράφου. Στις περιπτώσεις αυτές, υποστηρίζεται, το ηλεκτρονικό έγκλημα δεν είναι παρά μία νέα μορφή εμφάνισης ενός «παραδοσιακού» εγκλήματος. Μια άλλη κατηγορία ηλεκτρονικού εγκλήματος είναι εκείνη, όπου το περιεχόμενο της αξιόποινης πράξης διαφοροποιείται τόσο πολύ από το παραδοσιακό έγκλημα, ώστε, ενόψει και της απαγορευμένης αναλογικής ερμηνείας των κανόνων του ποινικού δικαίου, διαμορφώνεται ένα νέο έγκλημα που συνδέεται αναγκαία με τον ηλεκτρονικό υπολογιστή, και ειδικότερα, με το λογισμικό του (software). Εδώ, θα μπορούσαν να ενταχθούν περιπτώσεις αλλοίωσης ή καταστροφής δεδομένων μέσω ιών. Τέλος, μια τρίτη κατηγορία περιπτώσεων αναφέρεται σε υπολογιστές που είναι συνδεδεμένοι μεταξύ τους (π.χ. αθέμιτη πρόσβαση σε δεδομένα υπολογιστών ή παραβίαση του απορρήτου μιας ηλεκτρονικής επικοινωνίας).[14]

[14] Για τις διακρίσεις των εγκλημάτων του κυβερνοχώρου βλ. και *Ι. Αγγελής*, Διαδίκτυο και ποινικό δίκαιο, Έγκλημα στον κυβερνοχώρο, ΠοινΧρον Ν΄, 675 επ., 676.

Η σχετικότητα τέτοιων διακρίσεων γίνεται πάντως προφανής π.χ. στην περίπτωση της παιδικής πορνογραφίας, ενός εγκλήματος που γνωρίζει ιδιαίτερη άνθηση στο Διαδίκτυο με αποτέλεσμα να θεωρείται συχνά ως κατ' εξοχήν γνήσιο έγκλημα του κυβερνοχώρου.[15] Στην πραγματικότητα πρόκειται για ένα κοινό-«παραδοσιακό» έγκλημα, του οποίου η τέλεση διευκολύνεται αποφασιστικά από τα τεχνικά χαρακτηριστικά του Διαδικτύου και των υπολογιστών (εξασφάλιση ανωνυμίας, ευχέρεια στην κυκλοφορία και διανομή του υλικού, κρυπτογράφηση, αποθήκευση δεδομένων, τεχνική επεξεργασία κ.λπ.). Αυτό οδήγησε, άλλωστε, τον Έλληνα νομοθέτη στο άρθρο 348 Α Π.Κ. να τυποποιήσει το έγκλημα χωρίς οποιαδήποτε αναφορά στα χρησιμοποιούμενα τεχνικά μέσα, όπως άλλωστε και η αντίστοιχη γερμανική ρύθμιση (παρ.184b ΓερμΠΚ).[16]

Η διάκριση ηλεκτρονικού εγκλήματος και εγκλήματος στον κυβερνοχώρο ή διαδικτυακού εγκλήματος φαίνεται σαφέστερη, καθώς ο πρώτος όρος είναι ευρύτερος και καλύπτει κάθε περίπτωση που χρησιμοποιείται έστω και ένας μεμονωμένος υπολογιστής, ενώ το διαδικτυακό έγκλημα ή έγκλημα στον κυβερνοχώρο αναφέρεται μόνο σε περιπτώσεις περισσότερων υπολογιστών που συνδέονται μεταξύ τους, όπως κυρίως στην περίπτωση του Διαδικτύου.[17] Παρ' όλα αυτά, η επέκταση του Διαδικτύου με τη ραγδαία αύξηση των χρηστών του,[18] τη διόγκωση του περιεχομένου του και τη συχνότητα της χρήσης του μειώνει συνεχώς τον αριθμό των ηλεκτρονικών εγκλημάτων που δεν είναι ταυτοχρόνως και διαδικτυακά εγκλήματα ή εγκλήματα

[15] Έτσι *Ι. Αγγελής* ό.π., σελ. 677.

[16] Με τη διάταξη της παραγρ. 184c ΓερμΠΚ ο Γερμανός νομοθέτης τιμωρεί τις πράξεις παιδικής πορνογραφίας της παραγρ. 184b και όταν τελούνται δια των μέσων μαζικής επικοινωνίας ή τηλευπηρεσιών, προβλέποντας απλώς εξαίρεση για τη μετάδοση πορνογραφίας ενηλίκων που μεταδίδεται κωδικοποιημένα.

[17] Για την ιστορία και τον τρόπο λειτουργίας του Διαδικτύου βλ. *Δ.Κιούπης*, Ποινικό Δίκαιο και Internet 1999, 21 επ.

[18] Σύμφωνα με την ιστοσελίδα http://www.internetworldstats.com/stats.htm, οι χρήστες του διαδικτύου τον Μάρτιο του 2007 ανέρχονται σε πάνω από 1,1 δισ. ανθρώπους

κυβερνοχώρου.[19] Όπως είναι φυσικό, η διευρυμένη χρήση των υπολογιστών και του Διαδικτύου έχει οδηγήσει και σε αντίστοιχη αύξηση των ηλεκτρονικών εγκλημάτων.[20]

Παρά τις δυσκολίες ενός γενικού ορισμού του ηλεκτρονικού εγκλήματος, που ήδη επισημάνθηκαν, μπορούμε να χρησιμοποιήσουμε ως σημεία αναφοράς: α) τις τροποποιήσεις του Π.Κ. που έγιναν με το Ν. 1805/1988[21] και β) τον κατάλογο αξιόποινων πράξεων που περιέχεται στα άρθρα 2-10 της σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο. Σύμφωνα με τον Π.Κ, στην έννοια του ηλεκτρονικού εγκλήματος υπάγονται η απάτη με υπολογιστή (άρθρο 386Α Π.Κ.), η παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που συνιστούν απόρρητα (άρθρο 370Β Π.Κ.), η χωρίς δικαίωμα πρόσβαση σε στοιχεία υπολογιστή (άρθρο 370Γ παρ.2 Π.Κ.), η χωρίς δικαίωμα αντιγραφή ή χρήση προγραμμάτων υπολογιστών (άρθρο 370 Γ παρ. 1 Π.Κ), καθώς και όλα τα εγκλήματα (άρθρα 216 επ. Π.Κ.) που συνδέονται με τη διευρυμένη έννοια του εγγράφου του άρθρου 13 γ΄εδ. β΄ Π.Κ.

Σύμφωνα με τη Σύμβαση του Συμβουλίου της Ευρώπης, εγκλήματα κυβερνοχώρου ή διαδικτυακά εγκλήματα θεωρούνται η παράνομη πρόσβαση σε δεδομένα (άρθρο 2), η υποκλοπή διαβιβαζόμενων δεδομένων (άρθρο 3), η παρέμβαση (διαγραφή-αλλοίωση-βλάβη) σε δεδομένα (4), η παρέμβαση σε συστήματα υπολογιστών (5), η κακή χρήση συσκευών με σκοπό την τέλεση των προηγούμενων εγκλημάτων (6), η πλαστογραφία που σχετίζεται με υπολογιστές (7), η απάτη σχετιζόμενη με υπολογιστές (8) εγκλήματα

[19] Για μια τέτοια περίπτωση ηλεκτρονικού εγκλήματος (παραβίαση επιχειρηματικού απορρήτου με αντιγραφή αρχείων από το σκληρό δίσκο ηλεκτρονικού υπολογιστή σε δισκέτα) βλ. ΑΠ 121/2003 ΠΛογ 2003, 161 επ. ΠοινΧρον ΝΓ 910 επ., με παρατ. *Α. Κωνσταντινίδη*

[20] Βλ. σχετικά. *Ν. Κουράκης*, Το οικονομικό έγκλημα στην Ελλάδα σήμερα σε: *του ιδίου* Εγκληματολογικοί ορίζοντες Β΄, 2005, σελ. 163 επ., 183.

[21] Αναλυτικά για το Ν. 1805/1988 βλ. *Χ. Μυλωνόπουλος*, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο, 1991

σχετικά με την πορνογραφία ανηλίκων (9) και εγκλήματα σχετικά με την πνευματική ιδιοκτησία (10).

Αντίστοιχες περιπτώσεις εγκληματικής συμπεριφοράς καλύπτουν και οι συχνά χρησιμοποιούμενοι όροι hacking (παρέμβαση), phishing («ψάρεμα»), pharming («καλλιέργεια»), ID theft (κλοπή ταυτότητας) κ.λπ.

Παρά το γεγονός ότι πολλές από τις ανωτέρω αναφερθείσες αξιόποινες συμπεριφορές φαίνεται να πλήττουν, κυρίως ή αποκλειστικά, άλλα έννομα αγαθά (π.χ. απόρρητο επικοινωνιών, υπομνήματα, ανηλίκους[22]), δεν είναι υπερβολικό να λεχθεί ότι τα οικονομικά εγκλήματα συνιστούν τον πυρήνα των ηλεκτρονικών εγκλημάτων.[23] Η σύνδεση των υπολογιστών στο Διαδίκτυο έχει οδηγήσει μάλιστα στη θέση ότι η αθέμιτη πρόσβαση σε δεδομένα (hacking) έχει αναχθεί σε ένα είδος «βασικού εγκλήματος»,[24] το οποίο τελείται συχνά προκειμένου να τελεσθεί κάποιο οικονομικό έγκλημα.

Πριν προχωρήσουμε στην ειδικότερη εξέταση ορισμένων ηλεκτρονικών οικονομικών εγκλημάτων, σκόπιμο είναι να τονίσουμε δύο κεντρικά χαρακτηριστικά των ηλεκτρονικών εγκλημάτων:

Α) Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία, που περιέχουν τα ηλεκτρονικά δεδομένα και προσβάλλει την ψηφιακή μας δραστηριότητα. Οι όποιες βλάβες, αλλοιώσεις, φθορές προκαλούνται σε ενσώματα αντικείμενα ή υλικούς φορείς δεδομένων (δισκέτες, σκληρούς δίσκους, μνήμες κ.λπ.) δεν αποτελούν παρά

---

[22] Στην περίπτωση της πορνογραφίας ανηλίκων του άρθρου 348 Α ΠΚ πρόκειται για έγκλημα οικονομικής εκμετάλλευσης της γενετήσιας ζωής, αφού ο Έλληνας νομοθέτης, αντίθετα με άλλες εθνικές νομοθεσίες και την Σύμβαση του Συμβουλίου της Ευρώπης, απαιτεί ο αυτουργός του εγκλήματος να ενεργεί από κερδοσκοπία.

[23] Έτσι *U.Sieber σε T.Hoeren, U.Sieber (Hsg.),* Handbuch Multimedia Recht, 1999, κεφ.19, αριθμ. 29

[24] *U.Sieber*, ό.π.. Στην ίδια κατεύθυνση και ο *Ν. Κουράκης*, ό.π. σελ.185-187. που εντοπίζει επτά περιπτώσεις παραβίασης δεδομένων (hacking) που σχετίζονται με το οικονομικό έγκλημα (φθορά προγραμμάτων, δυσφήμηση-παράνομη συγκριτική διαφήμιση, βιομηχανική κατασκοπία, ηλεκτρονική κλοπή πιστωτικών καρτών, ηλεκτρονική κλοπή τραπεζικών κωδικών, ηλεκτρονική απάτη σε χρηματιστηριακές συναλλαγές)

παρακολουθηματικές- δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά στα δεδομένα.

Β) Το ηλεκτρονικό έγκλημα δεν απαιτεί συνήθως την τοπική συνύπαρξη θύματος και δράστη, ούτε καν την τοπική τους εγγύτητα. Χαρακτηριστικό του είναι ότι ο δράστης συνήθως είναι μακριά, άγνωστος, αθέατος. Αυτό δημιουργεί μια νέα κατάσταση όχι μόνο στο δικονομικό επίπεδο της συλλογής αποδείξεων, αλλά και σε επίπεδο άσκησης ποινικής δικαιοδοσίας. Ως προς το αποδεικτικό σκέλος, ο εντοπισμός και η σύλληψη του δράστη του ηλεκτρονικού εγκλήματος προϋποθέτει συχνά την έγκαιρη και αποτελεσματική συνεργασία περισσότερων εθνικών αστυνομικών και διωκτικών αρχών, καθώς και αντίστοιχες διαδικασίες δικαστικής συνδρομής. Ως προς το ζήτημα της ποινικής δικαιοδοσίας, ο τόπος τέλεσης του ηλεκτρονικού εγκλήματος είναι συχνά κρίσιμος για το ζήτημα της ποινικής ευθύνης του δράστη. Ο διασυνοριακός χαρακτήρας του Διαδικτύου συχνά οδηγεί σε διαφορετική αξιολόγηση του περιεχομένου, καθώς αυτό μπορεί να είναι καθ' όλα νόμιμο στο κράτος όπου βρίσκεται ο δράστης ή είναι αποθηκευμένα τα δεδομένα και παράνομο στο κράτος όπου λαμβάνονται τα δεδομένα ή βρίσκεται ο αποδέκτης τους.

3.3. Η ηλεκτρονική οικονομική εγκληματικότητα

3.4 Οι ηλεκτρονικοί υπολογιστές ως μέσο τέλεσης «οικονομικών εγκλημάτων»

Στην χώρα μας οικονομικά εγκλήματα[25] τα οποία έχουν ως μέσο κυρίως το «λογισμικό» και σε σπανιότερες περιπτώσεις το μηχανικό μέρος του υπολογιστή θα μπορούσαν να αναφερθούν η απάτη με υπολογιστή του άρθρου 386Α Π.Κ, η παραβίαση απορρήτων στοιχείων ή προγραμμάτων υπολογιστών που προβλέπονται από τα άρθρα 370Β και Γ του Π.Κ, η πλαστογραφία του άρθρου 216 Π.Κ που αναφέρεται σε «ηλεκτρονικό έγγραφο» του άρθρου 13 Π.Κ και άλλα. Δεσπόζουσα θέση μεταξύ των εγκλημάτων της πληροφορικής και μάλιστα με μέσο τέλεσης το λογισμικό καταλαμβάνει το έγκλημα της απάτης και τούτο διότι το τμήμα αυτό του ηλεκτρονικού υπολογιστή

[25] Για τον ορισμό ενός εγκλήματος ως οικονομικού Βλ. *Β.Ζησιάδη* Η Οικονομική εγκληματικότητα σελ 44 επ. κατά τον οποίο τρία είναι τα ασφαλή κριτήρια προκειμένου να χαρακτηριστεί ένα έγκλημα ως οικονομικό α) Η προσβολή του οικονομικού συστήματος β) Το μέγεθος της ζημίας το οποίο προκαλείται από τη συμπεριφορά του δράστη γ) η κατεύθυνση προς την οποία προκαλείται η ζημία.
Ειδικότερα, για να θεωρηθεί ένα έγκλημα ως οικονομικό θα πρέπει η ζημία την οποία προκαλεί το υποκείμενο να είναι μεγάλη προκειμένου να επέλθει βλάβη στο οικονομικό σύστημα. Δεν είναι όμως μόνο η ζημία η οποία έχει σημασία για το χαρακτηρισμό ενός εγκλήματος ως οικονομικού. Σημασία έχουν επίσης τα «τεχνάσματα» που χρησιμοποιεί ο οικονομικός εγκληματίας για να προκληθεί η ζημία και τα οποία κλονίζουν την εμπιστοσύνη του κοινού και των άλλων επιχειρήσεων στην αξιοπιστία του οικονομικού συστήματος, αν μάλιστα ληφθεί υπόψη ότι πολλές φορές, μια αιφνίδια άνοδος μιας επιχείρησης εξαιτίας οικονομικών εγκλημάτων, μπορεί να δημιουργήσει πρόσφορο έδαφος για τέλεση τέτοιων παράνομων πράξεων όταν υποψήφιοι δράστες διαβλέπουν δυνατότητες «επεμβάσεων» στο οικονομικό σύστημα λόγω αδυναμιών του και έλλειψης ασφαλιστικών δικλείδων. Το δεύτερο κριτήριο είναι η κατεύθυνση προς την οποία προκαλείται η ζημία. Το κατά πόσον δηλαδή ο υφιστάμενος τη ζημία διαδραματίζει σημαντικό ρόλο στο οικονομικό σύστημα του κράτους, όπως π.χ το Δημόσιο, οι τράπεζες, βιομηχανίες αλλά και ομάδες προσώπων, τα οποία επιδρούν στην οικονομική ζωή, όπως το καταναλωτικό κοινό. Η πρόκληση της ζημίας στην οικονομία μπορεί να είναι είτε άμεση, π.χ μεγάλης έκτασης φοροδιαφυγή από επιχείρηση είτε έμμεση, όταν π.χ η ζημία προκαλείται αρχικά σε μία επιχείρηση η οποία είναι ενταγμένη στο οικονομικό σύστημα, διαδραματίζοντας σημαντικό ρόλο στους κόλπους του και εν συνεχεία υφίσταται πλήγμα η οικονομία Σε κάθε περίπτωση πάντως η ζημία δεν θα πρέπει να περιορίζεται και να παραμένει μέσα στα πλαίσια της προσωπικής ζωής του θύματος αλλά να διοχετεύεται στο οικονομικό σύστημα στο οποίο εντάσσεται ο παθών. Χαρακτηριστικό είναι το παράδειγμα το οποίο χρησιμοποιεί ο Μανωλεδάκης (Η τυποποίηση των οικονομικών εγκλημάτων, σελ 266), σύμφωνα με το οποίο, μεμονωμένη απάτη μεγάλου οικονομικού μεγέθους, σε βάρος νεόπλουτου δήθεν φιλότεχνου, από έμπορο έργων τέχνης, με την εμφάνιση και πώληση ενός ζωγραφικού πίνακα ασήμαντης καλλιτεχνικής αξίας σαν έργο μεγάλου ζωγράφου, δεν συνιστά οικονομικό έγκλημα και τούτο διότι η περιουσιακή ζημία, έστω και μεγάλη, δεν έχει καμία σχέση με την καλή λειτουργία της οικονομίας. Τα εγκλήματα της σελίδας 20 του παρόντος ο *Ζησιάδης* τα εντάσσει σαφώς στην ως άνω κατηγορία.

είναι περισσότερο επιρρεπές στο να δεχθεί την εφαρμογή τεχνασμάτων ώστε, αν συντρέξουν και άλλες προϋποθέσεις, το έγκλημα του άρθρου 386Α Π.Κ να λάβει το χαρακτήρα οικονομικού εγκλήματος.

Με τη διάταξη του άρθρου 386Α Π.Κ είναι φανερή η βούληση του νομοθέτη να παρακολουθήσει την εξέλιξη της τεχνολογίας στο χώρο της πληροφορικής, διότι διαφορετικά το αξιόποινο της σχετικής συμπεριφοράς θα εξαρτιόταν από το τυχαίο ζήτημα, αν στην όλη αλληλουχία παρέμβασης του υπολογιστή είχε εμφιλοχωρήσει ή όχι κάποιο φυσικό πρόσωπο ως δέκτης παραπλάνησης.[26]

4.ΜΕΡΟΣ (Α) ΜΟΡΦΕΣ ΕΜΦΑΝΙΣΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

4.1 Παράνομη παρέμβαση σε δεδομένα (hacking)

Στη σημερινή πραγματικότητα των υπολογιστών που είναι συνδεδεμένοι στο Διαδίκτυο το πρώτο βήμα για την τέλεση του ηλεκτρονικού οικονομικού εγκλήματος είναι η παραβίαση της «ψηφιακής οικιακής ειρήνης» του θύματος.[27] Ο hacker εξασφαλίζει πρώτα την είσοδο στον υπολογιστή του θύματος και κατόπιν εντοπίζει στοιχεία-δεδομένα του θύματος με τη χρήση των οποίων θα βλάψει την περιουσία του. Παρ' όλο, λοιπόν, που η συμπεριφορά αυτή δεν

[26] Ο Α.Π διατυπώνει μια γενική θέση οριοθέτησης μεταξύ των εγκλημάτων της κοινής απάτης του άρθρου 386Π.Κ και της απάτης με υπολογιστή του άρθρου 386Α Π.Κ, κατά την οποία το άρθρο 386 Π.Κ περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση κάποιου φυσικού προσώπου, ενώ στο άρθρο 386Α Π.Κ η ξένη περιουσία βλάπτεται *ασχέτως παραπλανήσεως* με αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή. Οι διαφορές μεταξύ των δύο εγκλημάτων εντοπίζονται σύμφωνα με τον Α.Π σε δύο επίπεδα: Α) στο επίπεδο της πλάνης και Β) στο επίπεδο της βλάβης ξένης περιουσίας, η οποία στην απάτη με υπολογιστή πρέπει να προκύπτει άμεσα ως αποτέλεσμα του επηρεασμού των στοιχείων του υπολογιστή και όχι ως αποτέλεσμα περιουσιακής διάθεσης στην οποία προβαίνει ένα φυσικό πρόσωπο Βλ. Α.Π 1277/1998 , Υπερ. 4/1999, σελ 916 επ.

[27] Για τις αναλογίες hacking και διατάραξης οικιακής ειρήνης βλ. ήδη *Δ.Κιούπης*, όπ., σελ. 125

συνιστά οικονομικό έγκλημα, έχει παρατηρηθεί πως αποτελεί συχνά την πρώτη φάση μιας σύνθετης εγκληματικής δραστηριότητας, η οποία τελικά κατατείνει στο οικονομικό όφελος του δράστη. Η συμπεριφορά του δράστη μπορεί να εντάσσεται στο άρθρο 370 Β ή στο άρθρο 370 Γ παρ.2[28] ανάλογα με το περιεχόμενο των δεδομένων στα οποία αποκτά πρόσβαση ο δράστης και μπορεί να αποτελεί, κατά τις διακρίσεις της Σύμβασης του Συμβουλίου Ευρώπης, παράνομη πρόσβαση σε δεδομένα (άρθρο 2) ή υποκλοπή διαβιβαζόμενων δεδομένων (άρθρο 3)[29], ανάλογα με τη θέση των δεδομένων (αποθηκευμένα σε υπολογιστή ή διαβιβαζόμενα δεδομένα).

Η οικονομική διάσταση της συγκεκριμένης εγκληματικής συμπεριφοράς εμφανίζεται εναργέστερα στην περίπτωση της αντιγραφής, χρήσης, παραβίασης κ.λπ. δεδομένων που συνιστούν επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα, όπου η συμπεριφορά του δράστη (παραβίαση του απορρήτου) στοχεύει εξ αρχής στην απόσπαση στοιχείων που αποτελούν σημαντικό περιουσιακό στοιχείο της επιχείρησης ή του επαγγελματία. Χαρακτηριστική είναι η περίπτωση που αντιμετώπισε η ΑΠ 121/2003[30], όπου οι κατηγορούμενοι αντέγραψαν σε δισκέτες το πελατολόγιο γραφείου τουρισμού, προκειμένου να το χρησιμοποιήσουν σε δική τους επιχείρηση με το ίδιο αντικείμενο που ίδρυσαν στη συνέχεια.

Στη σύγχρονη εκδοχή της η αξιόποινη συμπεριφορά συνίσταται στην αποστολή ειδικών προγραμμάτων (δούρειων ίππων) στον

[28] Για τα προβλήματα ερμηνείας των δύο διατάξεων βλ. *Χ.Μυλωνόπουλος*, ό.π., σελ.71 επ., *Δ.Κιούπης* ό.π. 128 επ.

[29] Στην περίπτωση της αθέμιτης πρόσβασης σε διαβιβαζόμενα δεδομένα που μεταδίδονται με συστήματα επικοινωνιών δεν εφαρμόζεται πλέον η διάταξη του άρθρου 370Γ παρ.2 Π.Κ., αλλά η νεότερη διάταξη του άρθρου 10 Ν. 3115/2003 («Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης τουλάχιστον ενός (1) έτους και χρηματική ποινή από δεκαπέντε χιλιάδες (15.000) έως εξήντα χιλιάδες (60.000) ευρώ, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις..»)

[30] ΑΠ 121/2003 ΠΛογ 2003, 161 επ. ΠοινΧρον ΝΓ', 910 επ., με παρατ. *Α. Κωνσταντινίδη*.

υπολογιστή του θύματος,[31] που τα ενεργοποιεί ακούσια και έτσι ο δράστης εξασφαλίζει πολύτιμα στοιχεία, όπως αριθμούς φορολογικού μητρώου, κοινωνικής ασφάλισης, τραπεζικών λογαριασμών, προσωπικούς κωδικούς πρόσβασης σε μηχανήματα αυτόματης ανάληψης τραπεζών ή διενέργειας ηλεκτρονικών τραπεζικών συναλλαγών, τα οποία κατόπιν χρησιμοποιεί για να αποκομίσει περιουσιακό όφελος ζημιώνοντας αντίστοιχα το ανυποψίαστο θύμα του.

Από τη στιγμή που δεδομένα με οικονομική λειτουργία (κωδικοί λογαριασμών κ.λπ) ευρίσκονται αποθηκευμένα σε υπολογιστές είναι αυτονόητο ότι η παράνομη παρέμβαση σε αυτά και η γνώση τους από το δράστη συνιστά το αναγκαίο προστάδιο για την τέλεση του οικονομικού εγκλήματος.

4.2 Απάτη με υπολογιστή (386 Α Π.Κ.) και απάτη μέσω υπολογιστή (386 Π.Κ.)[32]

Το κεντρικό οικονομικό έγκλημα που τελείται –με ή χωρίς hacking– και που θα μας απασχολήσει ειδικότερα στην παρούσα μελέτη είναι η απάτη με υπολογιστή (άρθρο 386 Α Π.Κ.). Με τη ρύθμιση αυτή ο νομοθέτης επεδίωξε να καλύψει όλες εκείνες τις περιπτώσεις, όπου ο δράστης βλάπτει ξένη περιουσία με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος χωρίς όμως να παραπλανά κάποιο φυσικό πρόσωπο, όπως στην απάτη του άρθρου 386 Π.Κ., αλλά «επηρεάζοντας τα στοιχεία

[31] Η συμπεριφορά αυτή μπορεί να συνιστά, ανάλογα με τον τρόπο λειτουργίας αυτών των προγραμμάτων κατά περίπτωση, είτε έγκλημα του άρθρου 370 Γ παρ.2 Π.Κ., είτε φθορά ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.) υπό την έννοια της βλάβης του αποθηκευτικού μέσου λόγω αλλοίωσης των αποθηκευμένων δεδομένων. Για αυτά βλ. αναλυτικότερα στην συνέχεια στα σχετικά με το έγκλημα της απάτης με υπολογιστή και την φθορά ξένης ιδιοκτησίας.

[32] Βλ. Και πίνακες εμφάνισης ηλεκτρονικής εγκληματικότητας στην παρ 6. και συγκεκριμένα πίνακα (α).

υπολογιστή». Αντί της πράξης εξαπάτησης του θύματος με «εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων», δηλ. την επίδραση στο νοητικό ενός άλλου ανθρώπου, στην απάτη με υπολογιστή ο δράστης επηρεάζει τα δεδομένα του υπολογιστή «είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλον τρόπο». Η προσπάθεια του νομοθέτη να προσαρμοσθεί στις ραγδαίες τεχνολογικές εξελίξεις τον οδήγησε στην επιλογή[33] να συμπεριλάβει και τη γενική αναφορά σε επηρεασμό των δεδομένων με οποιονδήποτε τρόπο, χωρίς ταυτόχρονα να περιλαμβάνει ρητά και την χρησιμοποίηση ορθών στοιχείων χωρίς δικαίωμα, πράγμα που συμβαίνει λ.χ στην περίπτωση της κλεμμένης μαγνητικής κάρτας αναλήψεως μετρητών.[34]

Οι περιπτώσεις αυτές εμφανίζονται στην πράξη πολύ συχνά λόγω και της διευρυνόμενης χρήσης μαγνητικών καρτών για ανάληψη μετρητών. Στην απλούστερη μορφή της, η εν λόγω αξιόποινη συμπεριφορά συνίσταται σε κλοπή της κάρτας από το θύμα και σε ταυτόχρονη αποκάλυψη του PIN (προσωπικού αριθμού αναγνώρισης ταυτότητας), το οποίο το θύμα έχει σημειώσει στην κάρτα ή σε χαρτί που βρίσκεται στο πορτοφόλι που έχει αφαιρέσει ο δράστης. Σήμερα, μετά τις αλλεπάλληλες ανακοινώσεις των τραπεζών ότι το PIN θα πρέπει να φυλάσσεται χωριστά και τη σχετική ευαισθητοποίηση των χρηστών, οι δράστες κατέφυγαν στη χρήση προηγμένων τεχνικών μέσων για την απόσπαση της κάρτας και την αποκάλυψη του PIN.

[33] Βλ. σχετικά *Δ.Κιούπης*, ό.π. 114 επ., *Χ. Μυλωνόπουλος*, ό.π. σελ. 58 επ.

[34] Οι συγκεκριμένες περιπτώσεις αποτελούν το μεγαλύτερο τμήμα ηλεκτρονικής απάτης (βλ. σχετικά ΚΑΘΗΜΕΡΙΝΗ 30/3/2007 με αναφορά στα πορίσματα έρευνας για την τραπεζική απάτη στην Ευρώπη, τη Μέση Ανατολή και την Αφρική). Σύμφωνα με τη στατιστική της γερμανικής ομοσπονδιακής αστυνομίας για το 2005, μόνο οι περιπτώσεις αυτές αποτελούν το 51,8% του ηλεκτρονικού εγκλήματος, ενώ μαζί με τις υπόλοιπες περιπτώσεις ηλεκτρονικής απάτης αποτελούν περί το 86% του ηλεκτρονικού εγκλήματος. Βλ. την ετήσια έκθεση σε www.bka.de.

Αναφορικά με την κάρτα, χρησιμοποιούν συνήθως ειδικά συστήματα (θήκες) που εγκαθιστούν στα ATM των τραπεζών, έτσι ώστε να μπλοκάρουν τις κάρτες στο μηχάνημα, ενώ ο κάτοχος απομακρύνεται αποδίδοντας το μπλοκάρισμα σε τεχνική βλάβη του ATM και, σε σχέση με το PIN, εγκαθιστούν στο ATM μικροσκοπική κάμερα, η οποία καταγράφει τους αριθμούς που πληκτρολογεί ο ανυποψίαστος κάτοχος της κάρτας. Το ζήτημα που ανακύπτει εδώ είναι, πέρα από την ποινική αξιολόγηση της περιφερειακής συμπεριφοράς του δράστη (κλοπή της κάρτας ως αντικειμένου, φθορά ξένης ιδιοκτησίας με την επέμβαση στο ATM, παράνομη εγκατάσταση κάμερας και παραβίαση προσωπικών δεδομένων), πώς θα αξιολογηθεί ποινικά η κύρια συμπεριφορά του δράστη που συνίσταται στη μετέπειτα ανάληψη ποσού από τον λογαριασμό του θύματος. Στη θεωρία και τη νομολογία έχουν υποστηριχθεί δύο βασικές θέσεις. Σύμφωνα με την πρώτη[35], η συμπεριφορά αυτή υπάγεται στο άρθρο 386 Α Π.Κ. με κύρια επιχειρήματα, την ευρεία διατύπωση της ελληνικής διάταξης (επηρεασμός στοιχείων υπολογιστή με οποιονδήποτε τρόπο), την αντίστοιχη λύση που δίνεται σε άλλες νομοθεσίες (όπως η γερμανική παραγρ. 263a και η αμερικανική διάταξη Computer Fraud and Abuse Act (US) 18 USC 1030(a) παρ.4), καθώς και τη δομική ομοιότητα της συμπεριφοράς με εκείνη του δράστη που εμφανίζεται στο ταμείο της τράπεζας με το βιβλιάριο τρίτου παριστάνοντας ψευδώς στον υπάλληλό της ότι είναι ο νόμιμος δικαιούχος. Σύμφωνα με τη δεύτερη, δεν υπάρχει επηρεασμός. διότι η εκτέλεση του προγράμματος γίνεται κανονικά από τρίτο πρόσωπο και όχι το νόμιμο

[35] *Μυλωνόπουλου* ό.π., 66 επ., *Ε.Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών 1993, 213, *Δ.Κιούπς* ό.π. 116, *Γ. Νούσκαλη*, Απάτη με ηλεκτρονικό υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386 Α Π.Κ., ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, ΠοινΔικ 2003, 188, *Μυλωνόπουλο*, Ποινικό Δίκαιο, ειδικό μέρος, εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, 2η έκδοση, 2006, 603 και από τη νομολογία το ΣυμβΝαυτΠειρ418/1996, Υπερ 1997, 103.

κάτοχο της κάρτας και άρα εδώ πρόκειται περί κλοπής[36] ή υπεξαίρεσης.[37] Αν και μια σαφέστερη διατύπωση του άρθρου 386Α θα διευκρίνιζε το ζήτημα, η πρώτη άποψη φαίνεται περισσότερο υποστηρίξιμη ενόψει μάλιστα και του γεγονότος ότι αυτές οι συχνότατες στην πράξη περιπτώσεις αντιμετωπίζονται διεθνώς ως απάτες με υπολογιστή, όπως δείχνει άλλωστε και η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.[38]

Στο χώρο του διαδικτυακού εγκλήματος αρκετά συχνή είναι και η περίπτωση της απάτης με υπολογιστή με παρέμβαση στο λογισμικό του υπολογιστή, η οποία επηρεάζει την σύνδεση του υπολογιστή στο Διαδίκτυο μέσω τηλεφώνου. Από τα μέσα της δεκαετίας του 1990 μέχρι σήμερα έχουν καταγραφεί χιλιάδες περιπτώσεις αυτής της μορφής ηλεκτρονικής απάτης[39].

Ειδικότερα, ενώ το θύμα επισκέπτεται κάποια ιστοσελίδα (συχνά πορνογραφικού περιεχομένου) καλείται συνήθως να κατεβάσει κάποιο πρόγραμμα που θα του προσφέρει περισσότερες δυνατότητες (μεγέθυνση εικόνων, πρόσθετες επιλογές κ.λπ.). Άλλοτε πάλι, το πρόγραμμα εγκαθίσταται «στο παρασκήνιο», χωρίς να το αντιληφθεί καν το θύμα. Στη συνέχεια, το πρόγραμμα διακόπτει την τηλεφωνική σύνδεση του θύματος με την εταιρεία παροχής πρόσβασης στο διαδίκτυο και συνδέει το θύμα με άλλο τηλεφωνικό αριθμό (στο

[36] *Η. Αναγνωστόπουλου*, Παρατηρήσεις στην ΕφΑΘ 1904/1991, ΠοινΧρον ΜΒ, 197 και *Σ. Παύλου*, Παρατηρήσεις στην ΣυμβΝαυτΠειρ 418/1996, Υπερ 1997, 113.
[37] *Α.Παπαδαμάκη*. Τα περιουσιακά εγκλήματα, 2000 σελ. 191.

[38] Στο άρθρο 8 αναφέρεται «Κάθε Συμβαλλόμενο Μέρος θα λάβει τα νομοθετικά και άλλα μέτρα που είναι αναγκαία για να ποινικοποιηθεί στο εσωτερικό του δίκαιο, η εκ προθέσεως και άνευ δικαιώματος πρόκληση βλάβης ξένης περιουσίας δια της *α. εισαγωγής, αλλοίωσης, διαγραφής ή καταστολής δεδομένων υπολογιστή*, β. παρέμβασης στη λειτουργία ενός συστήματος υπολογιστή με δόλια ή αθέμιτη πρόθεση όπως, άνευ δικαιώματος, προσπορισθεί οικονομικό όφελος για τον ίδιο ή για άλλο πρόσωπο». Εντάσσεται δηλ. στην έννοια της απάτης με υπολογιστή και η εισαγωγή (ορθών) δεδομένων χωρίς δικαίωμα.
[39] Για μια τέτοια περίπτωση βλ. *Δ.Κιούπη* ό.π. 111 με παραπομπή στο δημοσίευμα της ΖΕΙΤ της 31/10/1997

εξωτερικό) προκαλώντας υπερβολικές χρεώσεις στον τηλεφωνικό λογαριασμό του.

Ιδιαίτερα επικίνδυνη είναι και μια άλλη παραλλαγή της ανωτέρω συμπεριφοράς. Στις περιπτώσεις αυτές, οι δράστες αποστέλλουν ένα σύντομο μήνυμα (SMS) στα κινητά τηλέφωνα των θυμάτων προσκαλώντας να τηλεφωνήσουν σε ένα συγκεκριμένο αριθμό. Με την βοήθεια ειδικού λογισμικού κατορθώνουν να αποκτήσουν πρόσβαση στα στοιχεία της κάρτας (SIM card) του θύματος και κατόπιν πραγματοποιούν τηλεφωνικές κλήσεις με χρέωση του δικού του λογαριασμού.[40]

Οι πιο σύγχρονες μορφές ηλεκτρονικής απάτης σχετίζονται άμεσα με τη διευρυνόμενη χρήση του Διαδικτύου σε συνδυασμό με τη χρήση πιστωτικών καρτών και την επέκταση των ηλεκτρονικών τραπεζικών εργασιών (το λεγόμενο e-banking,win-banking κ.λπ.) και είναι γνωστές στην γλώσσα των χρηστών ως phishing και pharming.

Ο πρώτος όρος (phishing) αποτελεί παραφθορά του fishing (ψάρεμα)[41] και περιγράφει την ακόλουθη συμπεριφορά. Το θύμα λαμβάνει ηλεκτρονική επιστολή, που υποτίθεται ότι προέρχεται από το τμήμα μηχανογράφησης-ασφάλειας-διοίκησης μιας τράπεζας, στην οποία καλείται να απαντήσει στέλνοντας τα στοιχεία της πιστωτικής του κάρτας ή του λογαριασμού του στο πλαίσιο δήθεν αναβάθμισης λογισμικού, αλλαγής κωδικών ασφαλείας που πρέπει επειγόντως να αντικατασταθούν κ.λπ. Πέρα από την πειστικότητα του ίδιου του κειμένου,[42] μπορούν να χρησιμοποιούνται λογότυπα τραπεζών,

[40] Βλ. σχετική είδηση του Γερμανικού Πρακτορείου Ειδήσεων (dpa) της 25/5/2000.

[41] Στους κύκλους των χάκερς, αλλά και άλλων εγκληματιών του κυβερνοχώρου (διακινητών πειρατικών προγραμμάτων, παιχνιδιών, ταινιών, λαθρεμπόρων κ.λπ.) είναι πολύ διαδεδομένη η δημιουργία λέξεων-όρων με αλλαγή ενός γράμματος σε σχέση με μια λέξη της αγγλικής. Στον χώρο της παράνομης διακίνησης προϊόντων πνευματικής ιδιοκτησίας συχνή είναι η αντικατάσταση του τελικού s με το γράμμα z (π.χ. filmz, moviez, recordz)

[42] Οι πρώτες προσπάθειες phishing είχαν λίγες πιθανότητες επιτυχίας, καθώς προέρχονταν από χάκερς ανατολικών χωρών και ήταν συντεταγμένες σε μέτρια αγγλικά, είχαν εμφανή συντακτικά ή γραμματικά λάθη με εντελώς ερασιτεχνική σχεδίαση που δύσκολα μπορούσε να παραπλανήσει. Σταδιακά, το

ονόματα υπαρκτών προσώπων που πράγματι κατέχουν διοικητικές θέσεις στην τράπεζα[43] κ.λπ. Με τον τρόπο αυτό ο δράστης παραπλανά το θύμα του[44] και αποκτά τα στοιχεία που χρειάζεται, ώστε κατόπιν να προχωρήσει σε χρήση τους ζημιώνοντας την περιουσία του θύματος και αποκομίζοντας παράνομο περιουσιακό όφελος. Στη δεύτερη φάση, αυτή της χρήσης του αριθμού κάρτας και των κωδικών που έχει αποκτήσει, τελεί, σύμφωνα, με την ορθότερη άποψη, απάτη με υπολογιστή.

Το ερώτημα που γεννιέται είναι αν στην πρώτη φάση της συμπεριφοράς του δράστη θεμελιώνεται ήδη απάτη (386 Π.Κ.)[45] και ειδικότερα αν ήδη η υφαρπαγή με παραπλάνηση του PIN ή άλλων στοιχείων λογαριασμού συνιστά περιουσιακή διάθεση. Ορθότερη εμφανίζεται η αρνητική απάντηση ενόψει της διαπίστωσης ότι λείπει η αμεσότητα της περιουσιακής διάθεσης υπό την έννοια ότι απαιτείται μια περαιτέρω ενέργεια (του δράστη) για να επέλθει περιουσιακή ζημία.[46] Συνεπώς, πρόκειται κατ' αρχήν, για μια προπαρασκευαστική πράξη απάτης με υπολογιστή, εκτός αν από τις περιστάσεις προκαλείται τουλάχιστον κίνδυνος για την ξένη περιουσία. Η αντίθετη άποψη οδηγεί, κατά την άποψη του γράφοντος, σε υπερβολική διεύρυνση του αξιοποίνου και καταλήγει να τιμωρεί τον δράστη για ολοκληρωμένη απάτη, (απάτη μέσω υπολογιστή) ακόμα και αν αυτός

περιεχόμενο βελτιώθηκε, το κείμενο έγινε πειστικό και η τεχνική σχεδίαση επαγγελματική με αποτέλεσμα ο αριθμός των θυμάτων να αυξηθεί πολύ. Βλ. σχετικά *M. Gercke,* Die Strafbarkeit von " Phishing" und Identitätsdiebstahl, CR 2005, 606.

[43] Το ζήτημα της ενδεχόμενης τέλεσης πλαστογραφίας θα μας απασχολήσει κατωτέρω.

[44] Στην φάση αυτή δηλ. δεν παρεμβαίνει στα στοιχεία του υπολογιστή αλλά επιχειρεί να δημιουργήσει πλάνη στο νοητικό του θύματος (social engineering).

[45] Βλ. σχετικά *M. Gercke*, ό.π., σελ. 607 επ.

[46] Έτσι *Μυλωνόπουλου* Ποινικό Δίκαιο (υποσημ.21), σελ. 488, *M.Gercke*,ό.π., 608, *S/S/Cramer-Perrron*[27] §263, αριθμ.145. Επίσης, *W.Buggisch & C.Kerling*. „Phishing", „Pharming" und ähnliche Delikte, Kriminalistik 2006, 531 επ., 534 με την επισήμανση, όμως, ότι κατά τη γερμανική νομολογία υφίσταται σε τέτοιες περιπτώσεις μια κατάσταση συγκεκριμένης διακινδύνευσης για την περιουσία και συνεπώς περιουσιακή βλάβη (σχετικά BGH St 33,246 και 47,167). Για τον κίνδυνο της περιουσίας ως περιουσιακή βλάβη βλ. αναλυτικά . *Μυλωνόπουλου* ό.π., 507 επ.

μετά την απόκτηση των κωδικών δεν τους χρησιμοποιεί καθόλου, δεν τελεί δηλαδή καν απόπειρα απάτης με υπολογιστή.[47]

Συμπερασματικά, κατά την ορθότερη άποψη, ο δράστης του phishing τιμωρείται ως αυτουργός απάτης με υπολογιστή όταν προχωρεί σε ανάληψη χρημάτων χάρις στους κωδικούς που έχει προηγουμένως αποσπάσει, ενώ στην προηγούμενη φάση της απόσπασης των κωδικών από το θύμα η ποινική του ευθύνη εστιάζεται στην πλαστογραφία που τελεί καταρτίζοντας το πλαστό e-mail, που αποστέλλει στο θύμα.

Η ενεργοποίηση των τραπεζών που οργάνωσαν εκστρατείες ενημέρωσης των πελατών τους για αυτά τα παραπλανητικά e-mail καθώς και η αντίστοιχη αφύπνιση των πελατών, οι οποίοι δεν παραχωρούν αφελώς τέτοια στοιχεία μέσω ηλεκτρονικού ταχυδρομείου ώθησαν τους δράστες σε μια εξελιγμένη τεχνική phishing, το λεγόμενο pharming (παραφθορά της λέξης farming=καλλιέργεια). Στις περιπτώσεις αυτές, ο δράστης δεν επιζητεί να πείσει το θύμα, αλλά χρησιμοποιεί προγράμματα που στην πραγματικότητα επαναδρομολογούν την κυκλοφορία των δεδομένων. Απλουστευτικά, με παρεμβάσεις στο λογισμικό του υπολογιστή του θύματος ή και σε άλλους υπολογιστές ο χρήστης που θέλει να επισκεφθεί μια ιστοσελίδα και να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται σε άλλη σελίδα που είναι αντίγραφο της γνήσιας. Έτσι, ο χρήστης καταχωρίζει τα στοιχεία του νομίζοντας ότι βρίσκεται στην γνήσια ιστοσελίδα, ενώ στην πραγματικότητα τα «παραδίδει» στην ιστοσελίδα του δράστη. Σε άλλες περιπτώσεις, ο δράστης αποστέλλει μέσω e-mail προγράμματα τα οποία μετά την

[47] Και κατά τη δεύτερη άποψη, σε περίπτωση που ο δράστης πραγματοποιήσει τελικά ανάληψη χρηματικού ποσού με χρήση των κωδικών θα πρέπει, θεωρώ, να τιμωρηθεί μόνο για την απάτη με υπολογιστή αφού η προηγούμενη απάτη με περιεχόμενο την διακινδύνευση της περιουσίας θα συρρέει φαινομενικά με την απάτη με υπολογιστή που έχει ως περιεχόμενο τη βλάβη της περιουσίας.

εγκατάστασή τους στον υπολογιστή του θύματος συλλέγουν και αποστέλλουν τα στοιχεία (PIN, κωδικούς κ.λπ.) τα οποία ενδιαφέρουν τον δράστη, ο οποίος κατόπιν τα χρησιμοποιεί προκαλώντας περιουσιακή ζημία στο θύμα.[48]

Το pharming διαφοροποιείται δηλ. από το phishing, διότι ο δράστης δεν επιδρά στο νοητικό του θύματος, αλλά επηρεάζει το πρόγραμμα του υπολογιστή, τελεί δηλ. πάντοτε πριν από την απάτη με υπολογιστή κάποια ή όλες τις ακόλουθες αξιόποινες πράξεις: πλαστογραφία (216 Π.Κ), παραβίαση απορρήτου (370 Β Π.Κ.), αθέμιτη πρόσβαση σε δεδομένα (370 Γ Π.Κ), παραβίαση απορρήτου επικοινωνιών (άρθρο 10 Ν. 3115/2003), ενώ δεν τίθεται σε καμιά περίπτωση ζήτημα εφαρμογής της διάταξης περί κοινής απάτης (άρθρο 386 Π.Κ.).

Σε διεθνές επίπεδο, οι περιπτώσεις απάτης με υπολογιστή που έχουν την μορφή του phishing και του pharming αποκτούν συνεχώς ευρύτερες διαστάσεις,[49] οι οποίες σε σχέση με την «παραδοσιακότερη» μορφή της παράνομης χρήσης κλεμμένων ή πλαστών καρτών αυτόματης ανάληψης διακρίνονται για το διασυνοριακό χαρακτήρα τους, την επικινδυνότητα των δραστών που διαθέτουν υψηλό επίπεδο τεχνικών γνώσεων και την ένταξή τους στον χώρο της οργανωμένης εγκληματικότητας. Στον αγγλοσαξωνικό χώρο, και όχι μόνον, όλες οι περιπτώσεις ηλεκτρονικής απάτης που συνδυάζονται με απόκτηση στοιχείων που επιτρέπουν στον δράστη να διενεργεί συναλλαγές επ' ονόματι άλλου (του θύματος) ονομάζονται

[48] Πρόσφατη είναι υπόθεση pharming με την σύλληψη Ουκρανού υπηκόου στην Ελλάδα, ο οποίος είχε με αυτό τον τρόπο αποσπάσει χρήματα από τραπεζικό λογαριασμό. Βλ. ΚΑΘΗΜΕΡΙΝΗ 4/4/2007.

[49] Σύμφωνα με τα στατιστικά στοιχεία που δημοσιεύονται στην ιστοσελίδα www.antiphishing.org (Φεβρ. 2007), οι χώρες από τις οποίες ενεργούν οι δράστες είναι, κυρίως, η Κίνα και οι ΗΠΑ και ακολουθούν η Ν. Κορέα και διάφορες μεγάλες ευρωπαϊκές χώρες. Κύριος στόχος τέτοιων επιθέσεων είναι ο χώρος των οικονομικών υπηρεσιών (92,6%).

κλοπή ταυτότητας (ID theft)[50] και αποτελούν πλέον σημαντικότατο τμήμα οικονομικού ηλεκτρονικού εγκλήματος[51] με μεγάλο σκοτεινό αριθμό, καθώς οι τράπεζες και άλλοι μεγάλοι οργανισμοί αποφεύγουν να δημοσιοποιούν στοιχεία, που αποδεικνύουν τις αδυναμίες των συστημάτων και μπορούν να δημιουργήσουν ανασφάλεια στους πελάτες τους.

Η ένταξη πολλών περιπτώσεων ηλεκτρονικής απάτης στο χώρο του διαδικτυακού εγκλήματος έφερε στο προσκήνιο και μια άλλη κατηγορία προσώπων που εντάσσονται στο κύκλωμα, ως ενδιάμεσοι μεταξύ θύματος και δράστη. Ο δράστης του phishing και του pharming, αφού εξασφαλίσει τους αριθμούς αναγνώρισης και άλλα στοιχεία του λογαριασμού του θύματος επιχειρεί να αποκομίσει περιουσιακό όφελος, χωρίς όμως να γίνει αντιληπτός από τις αρχές. Συχνά, λοιπόν, χρησιμοποιεί τρίτα πρόσωπα, τους αποκαλούμενους οικονομικούς διαχειριστές (finance managers), με τους οποίους συνάπτει την εξής συμφωνία: Χρησιμοποιώντας τα στοιχεία του θύματος εμβάζει χρηματικό ποσό στο λογαριασμό του οικονομικού διαχειριστή, ο οποίος αφαιρεί ένα ποσοστό ως προμήθεια και μεταβιβάζει το υπόλοιπο στον δράστη μέσω υπηρεσιών διεθνούς διαβίβασης χρημάτων. Έτσι, ο μεν οικονομικός διαχειριστής εισπράττει προμήθεια άκοπα, χωρίς καμιά δική του ενέργεια, ο δε δράστης της απάτης με υπολογιστή διασφαλίζει μέσω της παρεμβολής του τρίτου προσώπου την ανωνυμία του. Σε πολλές από αυτές τις περιπτώσεις ο οικονομικός διαχειριστής δεν είναι πρόσωπο που συμμετέχει εξ αρχής στο εγκληματικό σχέδιο, αλλά τρίτος που απλώς

[50] Για τις μεθόδους της κλοπής ταυτότητας βλ. αναλυτικά *A.M. Marshall & B.C. Tompsett, Identity theft in an online world*, Computer law & security report , 2005, 128 επ.

[51] Σύμφωνα με την Federal Trade commission-Identity Theft Survey Report σε http://www.ftc.gov/os/2003/09/synovatereport.pdf, το 2003 υπήρχαν στις ΗΠΑ 3,3 εκατομμύρια θύματα και ζημία που ανερχόταν σε άνω των 30 δις. δολαρίων., ενώ στην Βρετανία η ζημία για το 2004 υπολογίσθηκε σε 1,3 δις. λίρες. Βλ. σχετικό δημοσίευμα του BBC σε http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/4311693.stm της 3/3/2005

εξασφαλίζει την προμήθειά του πειθόμενος (με σχετική ευκολία) στις διαβεβαιώσεις του δράστη ότι πρόκειται για σοβαρή επένδυση που πρέπει να ξεπεράσει συναλλαγματικά, γραφειοκρατικά και άλλα οργανωτικά προβλήματα.[52]

Η νομική αξιολόγηση της συμπεριφοράς των οικονομικών διαχειριστών συνδυάζεται με το γενικότερο ζήτημα αν είναι δυνατή η συμμετοχή σε κύρια πράξη στο χρονικό διάστημα μεταξύ της τελείωσης της απάτης και μέχρι την ουσιαστική αποπεράτωσή της. Ο οικονομικός διαχειριστής δρα μετά την τυπική τελείωση της απάτης με υπολογιστή (έχει ήδη επέλθει η περιουσιακή ζημία), αλλά πριν από την ουσιαστική αποπεράτωση (δεν έχει επιτευχθεί ακόμη το παράνομο περιουσιακό όφελος, το οποίο ο δράστης αποκτά μετά την ενέργεια του τρίτου-οικονομικού διαχειριστή).

Κατά μία άποψη, που υποστηρίζεται ισχυρά στην ελληνική θεωρία[53] αλλά και στη γερμανική νομολογία και θεωρία[54], είναι δυνατή η συμμετοχή (συνέργεια) και σε αυτό το στάδιο, οπότε στη συγκεκριμένη περίπτωση ο οικονομικός διαχειριστής θα πρέπει να τιμωρηθεί για συνέργεια σε απάτη με υπολογιστή.[55] Σύμφωνα με άλλη άποψη, επίσης ισχυρά υποστηριζόμενη στην ελληνική[56] και γερμανική θεωρία[57], δεν είναι δυνατή συνέργεια στο στάδιο μετά την τελείωση της πράξης και προ της ουσιαστικής αποπεράτωσης. Στην περίπτωση αυτή, ο οικονομικός διαχειριστής του phishing ή του pharming δεν μπορεί να τιμωρηθεί ως συνεργός σε απάτη με υπολογιστή, αλλά θα

---

[52] Τα γερμανικά δικαστήρια δέχονται ότι λόγω αυτής της συμπεριφοράς (είσπραξη σημαντικής προμήθειας ως αντιπαροχή για μια απλή υλική ενέργεια που συνίσταται στη διαβίβαση του υπόλοιπου ποσού σε άλλο πρόσωπο) οι οικονομικοί διαχειριστές δρουν (τουλάχιστον) με ενδεχόμενο δόλο.

[53] Βλ. αναλυτικά τις παραπομπές σε *Α.Δημάκης* ΣυστΕρμΠΚ άρθρο 47 αριθμ. 23.

[54] Βλ. επ' αυτού παραπομπές σε *S/S- Cramer/Heine*[27] §27 αριθμ.17.

[55] Έτσι in concreto η απόφαση *AG Hamm* CR 2006, 70 επ.

[56] Ειδικά για την απάτη *Ν. Μπιτζιλέκη,* Συμμετοχική πράξη 1990, σελ. 204 και *Μυλωνόπουλου,* (υποσημ.21) , 543. Αναλυτική και εμπεριστατωμένη ανάπτυξη αυτής της θέσης σε *Α..Δημάκη* ΣυστΕρμΠΚ άρθρο 47 αριθμ.23 με περαιτέρω παραπομπές.

[57] Βλ. σχετικά *C.Roxin,* Strafrecht Allg.Teil Τόμος ΙΙ 2003, 221 με περαιτέρω παραπομπές.

πρέπει να τιμωρηθεί για νομιμοποίηση εσόδων από παράνομες δραστηριότητες.[58]

Κλείνοντας αυτή την ενότητα, θα πρέπει να επισημάνουμε ότι σε πολλές περιπτώσεις γίνεται καταχρηστικά λόγος για ηλεκτρονικό έγκλημα απάτης, ενώ πρόκειται για κοινή απάτη που απλώς τελείται μέσω υπολογιστή. Πρόκειται για περιπτώσεις, όπου ο δράστης επικοινωνεί με το θύμα μέσω του υπολογιστή (του αποστέλλει e-mail ή το θύμα επισκέπτεται ιστοσελίδα με παραπλανητικό περιεχόμενο)[59], καθώς και για περιπτώσεις όπου ο δράστης εισάγει δεδομένα στον υπολογιστή τα οποία κατόπιν δημιουργούν πλάνη σε φυσικό πρόσωπο, το οποίο προβαίνει σε περιουσιακή διάθεση.[60] Αποφασιστικό στοιχείο είναι κατά πόσον τελικά η περιουσιακή ζημία επέρχεται ως αποτέλεσμα πλάνης φυσικού προσώπου που προβαίνει σε περιουσιακή διάθεση (οπότε έχουμε κοινή απάτη με απλή χρήση του υπολογιστή ως εργαλείου) ή απλή εκτέλεση της συναλλαγής σε τελικό στάδιο από το φυσικό πρόσωπο, το οποίο δεν προβαίνει σε οποιονδήποτε, ουσιαστικό έλεγχο της συναλλαγής η περιουσιακή ζημία είναι άμεσο αποτέλεσμα του επηρεασμού των δεδομένων, άρα απάτη με υπολογιστή. Με δεδομένη τη διαφορετική διαμόρφωση της αντικειμενικής υπόστασης είναι αυτονόητο ότι οι δύο διατάξεις τελούν σε σχέση αμοιβαίου αποκλεισμού.[61]

[58] Έτσι in concreto η απόφαση AG Darmstadt της 15/2/2006 σε http://www.jurpc.de. Ομοίως και ο D.Werner παρατηρήσεις στην AG Hamm CR 2006, 72 . Η απάτη με υπολογιστή προβλέπεται ρητά στον σχετικό κατάλογο εγκληματικών δραστηριοτήτων του νόμου για τη νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες (άρθρο 1 α i) στστ) Ν. 2331/1995).

[59] Βλ. τέτοια παραδείγματα σε *Δ.Κιούπη*, όπ., 110.

[60] Βλ. σχετ. ΑΠ 1152/1999, ΠοινΧρον Ν', 597 επ.

[61] *Μυλωνόπουλου* ό.π., 605.

4.3 Αλλοίωση δεδομένων

Μια άλλη διαδεδομένη μορφή οικονομικού ηλεκτρονικού εγκλήματος είναι η αλλοίωση των δεδομένων υπολογιστή. Πρόκειται για συμπεριφορά που είναι αντίστοιχη με εκείνη της φθοράς ξένης ιδιοκτησίας, με τη διαφορά ότι εδώ δεν πλήττεται κάποιο πράγμα αλλά τα δεδομένα που είναι αποθηκευμένα στον υλικό φορέα αποθήκευσης. Ο Έλληνας νομοθέτης δεν ρύθμισε νομοθετικά αυτή τη μορφή εγκληματικότητας[62], ίσως γιατί κατά το χρόνο ψήφισης του Ν. 1805/1988 δεν είχε συνειδητοποιήσει τις διαστάσεις του προβλήματος.

Η γεωμετρική αύξηση του αριθμού των υπολογιστών και η διεύρυνση των χρήσεών τους δημιούργησε έναν ευαίσθητο χώρο, όπου η παρέμβαση (με την έννοια της διαγραφής, αλλοίωσης, αχρήστευσης) των δεδομένων (προγραμμάτων και δεδομένων χρήστη) αποδεικνύεται καταστροφική. Σε τέτοιες περιπτώσεις η ζημία που προκαλείται είναι πολλαπλάσια της φθοράς των μηχανικών τμημάτων του υπολογιστή (hardware).

Αυτό που πρέπει να προστατευθεί είναι η ιδιοκτησία στα δεδομένα. Αν κατά το χρόνο ψήφισης του Ν. 1805/1988 ο δράστης ήταν κυρίως κάποιο πρόσωπο που είχε φυσική πρόσβαση στον υπολογιστή (υπάλληλος της επιχείρησης, ο διαρρήκτης που είχε εισέλθει παράνομα στον χώρο), τα τελευταία χρόνια ο κίνδυνος προέρχεται από την αποστολή ιών, δούρειων ίππων και άλλων επιβλαβών προγραμμάτων που εγκαθίστανται κρυφίως στον υπολογιστή του θύματος και διαγράφουν αρχεία, μπλοκάρουν τα

[62] Στην γερμανική νομοθεσία, προβλέπεται ειδική διάταξη η § 303a (αλλοίωση δεδομένων), ενώ στην Αγγλία ρυθμίζεται από την Computer Misuse Act 1990 section 3 .

προγράμματα, αχρηστεύουν τον υπολογιστή συνολικά, προκαλώντας τεράστια οικονομική ζημία.[63]

Στο πλαίσιο του ισχύοντος δικαίου, η αξιόποινη αυτή συμπεριφορά αντιμετωπίζεται ως φθορά ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.), με σημείο αναφοράς δηλ. την έμμεση βλάβη που συνίσταται σε μεταβολή του υλικού φορέα.[64] Η έμμεση αυτή ποινική προστασία προσανατολίζεται εσφαλμένα στη βλάβη του υλικού φορέα και παραβλέπει τον πυρήνα της αξιόποινης συμπεριφοράς, μη δυνάμενη να καλύψει τις περιπτώσεις εκείνες παρέμβασης στη λεγόμενη «διαβιβαστική φάση» (φάση κατά την οποία τα δεδομένα διαβιβάζονται χωρίς ενσωμάτωση σε υλικό φορέα), ενώ και για την εφαρμογή της διακεκριμένης φθοράς ιδιαίτερα μεγάλης αξίας σημείο αναφοράς μπορεί να είναι μόνο το υλικό αντικείμενο και όχι η αξία των δεδομένων.[65]

Για όλους αυτούς τους λόγους, αλλά και διότι το φαινόμενο της αλλοίωσης δεδομένων έχει αποκτήσει ανησυχητικές διαστάσεις, η ανάγκη νομοθετικής παρέμβασης είναι επιτακτική.[66]

Στο ίδιο πλαίσιο συμπεριφοράς, εντάσσεται η περαιτέρω παρακώλυση της λειτουργίας του υπολογιστή,[67] που προκαλείται σε ορισμένες περιπτώσεις από την μόλυνση του υπολογιστή με ιούς ή την εγκατάσταση άλλων επιβλαβών προγραμμάτων και μπορεί, υπό προϋποθέσεις, να οδηγήσει σε παράλυση των επικοινωνιών ή την πρόκληση εκτεταμένων δυσλειτουργιών σε συγκοινωνιακά και

---

[63] Οι ιοί και τα άλλα επιβλαβή προγράμματα, όπως ήδη αναφέρθηκε, μπορούν να λειτουργούν ως μέσα για την τέλεση απάτης με υπολογιστή ή να λειτουργούν κατά τρόπο ώστε να τελούνται τα εγκλήματα των άρθρων 370 Β και 370 Γ Π.Κ.

[64] *Μυλωνόπουλου*, (υποσημ. 10), 26, *Δ.Κιούπη*, ό.π. 139, *Μυλωνόπουλου* (υποσημ. 21), 348.

[65] *Δ.Κιούπης*, ό.π. 140.

[66] Βλ. και την σχετική ρύθμιση στο άρθρο 4 της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο και τις σχετικές επισημάνσεις στην επεξηγηματική έκθεση (explanatory report) της Σύμβασης (αριθμ.60,61).

[67] Πρόκειται για τις λεγόμενες επιθέσεις που οδηγούν σε αναστολή λειτουργίας του συστήματος (denial of service attacks) και ρυθμίζονται στο άρθρο 5 της Σύμβασης του Συμβουλίου της Ευρώπης για τον Κυβερνοχώρο.

επικοινωνιακά δίκτυα, αεροδρόμια, νοσοκομεία[68] και άλλες κρίσιμες κρατικές υποδομές[69].

4.4 Πλαστογραφία

Όπως ήδη σημειώθηκε, ο Ν. 1805/1988, πέρα από την εισαγωγή διατάξεων στο ειδικό μέρος του ΠΚ για τα εγκλήματα που τελούνται με υπολογιστές , προχώρησε και σε διεύρυνση της έννοιας του εγγράφου με την προσθήκη β΄ εδαφίου στο άρθρο 13 περ.γ΄ (έννοια του εγγράφου) με το ακόλουθο περιεχόμενο «Έγγραφο είναι και κάθε μέσο στο οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία».

Αυτή η διευρυμένη έννοια του εγγράφου έχει ως συνέπεια την εφαρμογή των διατάξεων που αναφέρονται στα εγκλήματα περί τα υπομνήματα (άρθρα 216 Π.Κ.) και στα ηλεκτρονικά έγγραφα. Η γενική αυτή επέκταση των διατάξεων περί τα υπομνήματα στα ηλεκτρονικά δεδομένα έχει ορθά επικριθεί καθώς οδηγεί, σε αρκετές

---

[68] Προβλήματα στη λειτουργία νοσοκομείου προκάλεσε η περίπτωση Maxwell στις ΗΠΑ, όπου ο δράστης εγκατέστησε ένα πρόγραμμα με το οποίο κατόρθωσε να ελέγχει τους υπολογιστές νοσοκομείου (370Γ και 381 Π.Κ.) για να αποκομίσει περιουσιακό όφελος (386Α Π.Κ.). Η περαιτέρω συνέπεια αυτής της χρήσης των πόρων του συστήματος ήταν η πρόκληση δυσλειτουργιών στο νοσοκομείο με μπλοκάρισμα θυρών ασφαλείας, απενεργοποίηση βομβητών ειδοποίησης προσωπικού και διακοπή παροχής ρεύματος σε μονάδες εντατικής θεραπείας, όπου τα χειρότερα αποφεύχθηκαν μόνο χάρις στη λειτουργία εφεδρικού συστήματος ενέργειας. Βλ. αναλυτικά σε http://www.cybercrime.gov/maxwellPlea.html .

[69] Μπορεί, δηλαδή .να αποτελέσει τρομοκρατική ενέργεια ή ενέργεια που υπηρετεί την οργανωμένη εγκληματικότητα

περιπτώσεις, σε αξιολογικές αντινομίες, σε συνύπαρξη ετερόκλητων εννόμων αγαθών και σε σύγχυση.[70]

Σε κάθε περίπτωση, η τέλεση πλαστογραφίας ηλεκτρονικού εγγράφου δεν αποτελεί κατ' αρχήν οικονομικό έγκλημα, αφού σύμφωνα με την κρατούσα άποψη το προστατευόμενο έννομο αγαθό (τουλάχιστον για τη βασική διάταξη της παραγρ. 1) δεν έχει οικονομικό περιεχόμενο, αλλά εντοπίζεται στην προστασία της εμπιστοσύνης στην ακεραιότητα της έγγραφης απόδειξης στις συναλλαγές, τη δημόσια πίστη, την ακεραιότητα της αποδεικτικής διαδικασίας και στην προστασία του θεσμού του εγγράφου.[71] Βέβαια, ορθά επισημαίνεται[72] ότι μαζί με τα υπερατομικά έννομα αγαθά προσβάλλονται και ατομικά έννομα αγαθά, και ειδικότερα η ελευθερία διαθέσεως του δικαιώματος ή σχέσης, τα οποία εξαρτώνται από το πραγματικό γεγονός, ως προς το οποίο σκοπείται η παραπλάνηση με την χρήση του πλαστού. Αυτή η ελευθερία διάθεσης στις περισσότερες περιπτώσεις έχει οικονομική διάσταση.

Η πλαστογραφία, ως οικονομικό ηλεκτρονικό έγκλημα, εμφανίζεται κατεξοχήν στο πλαίσιο της εγκληματικής δραστηριότητας που κατατείνει τελικά στη διάπραξη της απάτης με υπολογιστή με την μορφή του phishing ή του pharming. Στην περίπτωση του phishing, που περιγράψαμε πιο πάνω, ο δράστης επικοινωνεί με το θύμα του αποστέλλοντας μια ηλεκτρονική επιστολή, δηλ. ένα πλαστό έγγραφο, το οποίο παραπλανά ως προς την ταυτότητα του εκδότη του. Προκειμένου δηλ. να παραπλανήσει το θύμα του και να αποσπάσει τους κωδικούς του λογαριασμού (PIN και άλλα στοιχεία) καταρτίζει ένα πλαστό έγγραφο, το οποίο φέρεται να προέρχεται από την

[70] Βλ. αναλυτικά *Μυλωνόπουλου*, (υποσημ.10), 50 επ. και *Δ.Κιούπη*, ό.π. 165.
[71] Βλ. σχετικά *.Μυλωνόπουλου*, Ποινικό Δίκαιο, Ειδικό Μέρος, Τα εγκλήματα σχετικά με τα υπομνήματα, 2005, 38 επ., *Α.Τζαννετή*, Το πλαστό έγγραφο 1998, 5 επ.
[72] *.Μυλωνόπουλου*, ό.π., 40.

τράπεζα ή από άλλο πιστωτικό οργανισμό ή εταιρεία ασφάλειας συστημάτων κ.λπ.. Η ηλεκτρονική επιστολή εντάσσεται στην έννοια του εγγράφου[73] κατ' άρθρο 13 γ΄ Π.Κ. και επιτελεί και τις τρεις λειτουργίες του (αποδεικτική, διαιωνιστική, εγγυητική).[74] Μάλιστα, όπως έχει επισημανθεί, τα στοιχεία που δηλώνουν την ταυτότητα του εκδότη (ηλεκτρονική διεύθυνση και λοιπά στοιχεία επικοινωνίας) εμφανίζουν, σε σχέση με άλλες μορφές επικοινωνίας (π.χ. φαξ), υψηλότερο βαθμό ασφάλειας.[75]

Πλαστογραφία τελείται και σε αρκετές περιπτώσεις pharming, πριν από την τέλεση της απάτης με υπολογιστή. Συγκεκριμένα, ο δράστης σε κάποιες περιπτώσεις με την εγκατάσταση ειδικού προγράμματος αναδρομολογεί τις διευθύνσεις των ιστοσελίδων με τις οποίες επικοινωνεί το θύμα. Το θύμα, λόγω αυτής της παρέμβασης, επισκέπτεται μια άλλη ιστοσελίδα, η οποία συνιστά και αυτή πλαστό έγγραφο, υπό την έννοια ότι με το περιεχόμενό της και την εμφανιζόμενη διεύθυνσή της παραπλανά το θύμα ως προς τον δημιουργό της –εκδότη του εγγράφου.[76]

Πλαστογραφία, έχουμε επίσης στις περιπτώσεις που ο δράστης αντιγράφει κάρτα ανάληψης μετρητών ή πιστωτική κάρτα[77], αλλά και στην περίπτωση της επαναφόρτισης κάρτας που ενσωματώνει αξία τηλεφωνικού χρόνου[78].

---

[73] Για τις λειτουργίες του εγγράφου βλ. *Μυλωνόπουλου* Ποινικό Δίκαιο Ειδικό Μέρος εγκλήματα σχετικά με τα υπομνήματα σελ 8 επ.

[74] *Δ.Κιούπη* ό.π., 157, *Α. Κωνσταντινίδη,* Η έννοια και λειτουργία του εγγράφου στο ουσιαστικό και δικονομικό ποινικό δίκαιο 2000, 117 επ., *.Μυλωνόπουλου* ό.π.,31. Έτσι και ειδικά για την περίπτωση του phishing *M. Gercke*, ό.π. 611.

[75] Βλ. *.Κιούπη* ό.π., 158.

[76] Για την ιστοσελίδα ως έγγραφο βλ. *Δ.Κιούπη* ό.π. 161 επ. και *Μυλωνόπουλο υό.π.*31. Επίσης για την ιστοσελίδα ως έγγραφο στο pharming *W.Buggisch & C. Kerling* ό.π. 532

[77] *.Μυλωνόπουλουό.π.*, 23.

[78] BGH, απόφαση 3StR 128/03 της 13/5/2003.

4.5 Παραβάσεις του Νόμου περί πνευματικής ιδιοκτησίας.

Σημαντικό τμήμα του ηλεκτρονικού εγκλήματος αποτελούν οι παραβάσεις του νόμου περί πνευματικής ιδιοκτησίας.[79] Η αναπαραγωγή διαφόρων κατηγοριών δεδομένων (μουσικής, ταινιών, εικόνων κ.λπ.) με προγράμματα που λειτουργούν στους ηλεκτρονικούς υπολογιστές έχει οδηγήσει σε εκτεταμένη παράνομη διάθεση αυτών των δεδομένων στο διαδίκτυο, ενώ ταυτόχρονα η δυνατότητα ψηφιακής αντιγραφής προγραμμάτων και άλλων δεδομένων σε ψηφιακούς δίσκους και άλλα αποθηκευτικά συστήματα έχει αντικαταστήσει το γνωστό από παλαιότερες εποχές φαινόμενο της «κασετοπειρατείας». Η διάθεση τέτοιων πειρατικών προϊόντων μέσω του Διαδικτύου διευκολύνεται από δύο κυρίως παράγοντες: α) την εγκατάσταση των σχετικών δικτυακών τόπων σε χώρες, όπου η πνευματική ιδιοκτησία ουσιαστικά δεν προστατεύεται β) τις ευρυζωνικές συνδέσεις που επιτρέπουν την ταχύτατη διαβίβαση των δεδομένων, ώστε να καθίσταται ευχερές το γρήγορο και φθηνό «κατέβασμα» μεγάλων όγκων δεδομένων.

Ακόμη και παραδοσιακά έργα πνευματικής ιδιοκτησίας, όπως ο έντυπος λόγος, δέχονται ισχυρά πλήγματα, καθώς μέσω της σάρωσης (scanning) ψηφιοποιούνται και τίθενται σε κυκλοφορία.[80]

Η ανάλυση του ζητήματος εκφεύγει των ορίων της παρούσης μελέτης. Αξίζει πάντως να σημειωθεί η θέσπιση διοικητικών κυρώσεων ειδικά για την διανομή και αναπαραγωγή προγραμμάτων

[79] Ενδεικτική είναι η σχετική αναφορά στην Στατιστική της Γερμανικής Ομοσπονδιακής Αστυνομίας για το 2005, σύμφωνα με την οποία οι περιπτώσεις αυτές συνιστούν το 8,8% της συνολικής διαδικτυακής εγκληματικότητας, ενώ το 63,4% του συνολικού αριθμού των εγκλημάτων κατά της πνευματικής ιδιοκτησίας τελείται μέσω Διαδικτύου.

[80] Ειδική πρόβλεψη για την ποινική αντιμετώπιση των προσβολών της πνευματικής ιδιοκτησίας περιέχει το άρθρο 10 της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.

Η/Υ,[81] και η άρση του αξιοποίνου αν ο δράστης καταβάλλει ανεπιφύλακτα το διοικητικό πρόστιμο, αν η ποσότητα δεν υπερβαίνει τα 50 προγράμματα.[82] Οι νεοπαγείς αυτές διατάξεις (προστέθηκαν με το Ν. 3524/2007) κινούνται σε διπλή κατεύθυνση: Αφενός καθιερώνουν μια αυστηρή, διοικητική κύρωση που βαρύνει άμεσα τον δράστη, παρακάμπτοντας τον πιο χρονοβόρο, αλλά δικαιοκρατικά εγκυρότερο μηχανισμό της ποινικής δίκης και αφετέρου αναγνωρίζουν de facto την πραγματικότητα του μικρέμπορου-αντιγραφέα, ο οποίος δεν είναι πλέον αξιόποινος, εφόσον συμμορφώνεται στη διοικητική κύρωση.[83]

4.6 Domain grabbing και εκβίαση

Μια ειδικότερη μορφή ηλεκτρονικού οικονομικού εγκλήματος συνιστά η εκβίαση που συνδέεται με το γνωστό στους κύκλους του Διαδικτύου domain grabbing (αρπαγή πεδίου) ή cybersquatting (κυβερνοσφετερισμό). Στην ουσία, δεν πρόκειται για ηλεκτρονικό έγκλημα εν στενή εννοία, διότι τα εγκλήματα που δυνατόν να τελούνται είναι κοινά εγκλήματα που απλώς τελούνται σε συνδυασμό με ένα ειδικότερο χαρακτηριστικό του Διαδικτύου.

---

[81] Άρθρο 65 Α παρ. 1 Ν. 2121/1993 : «Όποιος χωρίς δικαίωμα και κατά παράβαση των διατάξεων του παρόντος νόμου αναπαράγει, πωλεί ή κατ' άλλον τρόπο διανέμει στο κοινό ή κατέχει με σκοπό διανομής πρόγραμμα ηλεκτρονικού υπολογιστή, ανεξαρτήτως άλλων κυρώσεων, υπόκειται σε διοικητικό πρόστιμο ίσο με χίλια (1.000) ευρώ για κάθε παράνομο αντίτυπο προγράμματος ηλεκτρονικού υπολογιστή.»

[82] Άρθρο 66 παρ.11 Ν. 2121/1993: « Όταν το αντικείμενο της προσβολής αφορά σε προγράμματα ηλεκτρονικού υπολογιστή, η, κατά τη διάταξη της παραγράφου 1 του άρθρου 65Α και υπό τους προβλεπόμενους όρους, ανεπιφύλακτη καταβολή του διοικητικού προστίμου από τον δράστη έχει ως αποτέλεσμα την άρση του αξιοποίνου όταν η προσβολή αφορά σε ποσότητα μέχρι πενήντα (50) προγράμματα».

[83] Δεν προχωράει η ποινική δίωξη με την καταβολή του διοικητικού προστίμου περίπου όπως γίνεται στον ΚΟΚ.

Για να κατανοήσουμε το περιεχόμενο της συγκεκριμένης συμπεριφοράς, πρέπει να αναφερθούμε σε ορισμένα τεχνικά χαρακτηριστικά των δικτυακών τόπων (sites) και των ιστοσελίδων. Κάθε δικτυακός τόπος έχει μια ταυτότητα, την διεύθυνση IP (Internet Protocol), η οποία αποτελείται καταρχήν από ένα σύνολο αριθμών. Για να διευκολυνθεί η επικοινωνία στο Διαδίκτυο, αυτή η σειρά αριθμών αντικαθίσταται από μια ηλεκτρονική διεύθυνση που έχει ως περιεχόμενο μια σειρά λέξεων (συνήθως με λατινικούς χαρακτήρες) της μορφής «www. επωνυμία. καταληκτική λέξη» που υποδηλώνει είτε γεωγραφική προέλευση (gr., de, fr. Uk It.), είτε μορφή δραστηριότητας (.com, org.). Με την αύξηση της χρήσης του Διαδικτύου καθίσταται σαφές ότι υπάρχει ένα έντονο ενδιαφέρον με σημαντική περιουσιακή διάσταση φυσικών και κυρίως νομικών προσώπων να κατοχυρώσουν ονόματα ψηφιακών διευθύνσεων που α) θα προσομοιάζουν με την επωνυμία ή τον τίτλο τους και β) θα είναι σύντομα και εύληπτα.

Στη νομολογία και στην επιστήμη, υπάρχει διχογνωμία σχετικά με τη φύση του domain name, το οποίο αντιμετωπίζεται ως σήμα, διακριτικό γνώρισμα, όνομα, εμπορική επωνυμία, αντικείμενο προστασίας στο πλαίσιο του αθέμιτου ανταγωνισμού κ.λπ.[84] Η δυσκολία ένταξής του σε μια από αυτές τις κατηγορίες έχει οδηγήσει και στην άποψη ότι πρόκειται για κάτι διαφορετικό που επιτελεί οιονεί λειτουργία διακριτικού τίτλου και σήματος.[85]

Το ενδιαφέρον ποινικά ερώτημα είναι πώς θα αντιμετωπισθεί η συμπεριφορά εκείνου που σπεύδει να κατοχυρώσει δεκάδες ή χιλιάδες τέτοια ονόματα, πληρώνοντας το συμβολικό αντίτιμο στους

[84] Βλ. την σχετική παρουσίαση σε *Ι. Καράκωστα* Το Δίκαιο των ΜΜΕ[3], 2005, 482 και αναλυτικά *Γ. Γεωργιάδη*, Η προστασία των διακριτικών γνωρισμάτων στο διαδίκτυο - Domain names, ΔΕΕ 1999, 1243 επ.

[85] *ΠολΠρωτΑθ 3359/2003*, ΔΙΜΕΕ 2004, 100 επ.

διαχειριστές των domain names και κατόπιν απευθύνεται στις εταιρείες των οποίων τις επωνυμίες έχει δεσμεύσει ζητώντας τους χρηματικά ποσό για να τους μεταβιβάσει το domain name. Ανεξαρτήτως της τυχόν ευθύνης του κατά τις διατάξεις της νομοθεσίας περί σήματος ή αθεμίτου ανταγωνισμού ανακύπτει και ενδεχόμενη ποινική του ευθύνη για εκβίαση. Τέτοια συμπεριφορά αντιμετώπισε η απόφαση LG München II της 14/09/2000[86] που καταδίκασε για εκβίαση και απόπειρα εκβίασης τον κατηγορούμενο, ο οποίος ζήτησε από εταιρείες και έλαβε από μερικές από αυτές χρήματα για να τους παραχωρήσει τις διευθύνσεις που ο ίδιος είχε φροντίσει να καταχωρήσει στο όνομά του και οι οποίες ήταν οι ίδιες με τις επωνυμίες αυτών των εταιρειών. Είναι προφανές, ότι στις περιπτώσεις αυτές η συμπεριφορά της μαζικής καταχώρησης των domain names από ένα άσχετο πρόσωπο, που επιδιώκει να αποσπάσει οικονομικό όφελος είναι καταχρηστική και αντιβαίνει στα χρηστά ήθη, είναι όμως εξαιρετικά αμφισβητούμενο κατά πόσον μια τέτοια συμπεριφορά είναι παράνομη στο πλαίσιο της εκβίασης. Πέραν τούτου, ο δράστης εφόσον νόμιμα έχει κατοχυρώσει το domain name δεν απειλεί ούτε με πράξη, ούτε με παράλειψη άλλον, αλλά απαιτεί ένα (υπέρογκο) τίμημα για το όνομα που κατοχύρωσε. Αν και στη συγκεκριμένη περίπτωση η καταδίκη για εκβίαση στηρίχθηκε σε προγενέστερες αστικές αποφάσεις που χαρακτήριζαν παράνομη την καταχώρηση και ο δράστης δεν επιχείρησε να πωλήσει τα domain names, αλλά απαιτούσε χρήματα προκειμένου να τα απελευθερώσει, όπως ήταν υποχρεωμένος βάσει των αποφάσεων των αστικών δικαστηρίων, απειλώντας μάλιστα ότι θα τα πωλήσει σε ανταγωνιστές, η παραδοχή ότι έχει τελεσθεί εκβίαση σε άλλες περιπτώσεις εμφανίζεται προβληματική.

[86] Βρίσκεται στην διεύθυνση www.jurpc.de καταχωρημένη με τα στοιχεία JurPC Web-Dok. 228/2000.

Θα πρέπει, γενικότερα, να σημειωθεί ότι σε ορισμένες περιπτώσεις τα όρια της θεμιτής ή αθέμιτης χρήσης ενός domain name είναι ρευστά, όταν δηλαδή δεν πρόκειται για την επωνυμία μιας ευρύτερα γνωστής εταιρείας, όταν στον ίδιο χώρο δραστηριοποιούνται περισσότεροι με το ίδιο όνομα, έστω και σε διαφορετικές επιχειρηματικές δραστηριότητες, όταν χρησιμοποιούνται συντομογραφίες, σύνολα γραμμάτων παύλες, κόμματα ή άλλα σημεία στίξης κ.λπ.[87]

Τα ζητήματα του domain grabbing αντιμετωπίζονται αποτελεσματικότερα στο επίπεδο του ελέγχου των προϋποθέσεων καταχώρησης ονομάτων. Στην Ελλάδα αρμόδια είναι πλέον η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) που είναι Ανεξάρτητη Αρχή. Τα σχετικά ζητήματα ρυθμίζονται ήδη από τον Κανονισμό Διαχείρισης και Εκχώρησης Ονομάτων Χώρου[88] (όπως αποκαλούνται τα domain names), όπου προβλέπονται πλέον και οι περιπτώσεις απόρριψης αίτησης εκχώρησης και διαγραφής εκχωρηθέντος ονόματος χώρου[89] με κατάληξη gr.

[87] Για τα θέματα αυτά βλ. από την πρόσφατη γερμανική νομολογία ενδεικτικά στην διεύθυνση www.bundesgerichtshof.de την απόφαση BGH I ZR 207/01, 2/12/2004 (weltonline.de) και την απόφαση BGHI ZR 65/02 9/9/2004 (mho.de).

[88] απόφαση ΕΕΤΤ 351/76 ΦΕΚ Β 717/ 27-5-2005

[89] Άρθρα 8 και 9 αντίστοιχα του κανονισμού, όπου προβλέπεται και η περίπτωση της αίτησης εκχώρησης που γίνεται με προφανή κακοπιστία.

4.7 Spamming

Το spamming[90] είναι μια δραστηριότητα που κατακλύζει τα τελευταία χρόνια το διαδίκτυο, προκαλώντας διάφορες παρενέργειες και οδηγεί σε μια ευρύτερη διεθνή συζήτηση για την ενδεχόμενη ποινικοποίησή του. Αν και δεν υπάρχει κάποιος κοινά αποδεκτός ορισμός, γίνεται δεκτό ότι καλύπτει οπωσδήποτε τις περιπτώσεις μαζικής αποστολής ηλεκτρονικών επιστολών, συνήθως με εμπορικό-διαφημιστικό περιεχόμενο προς παραλήπτες, οι οποίοι ουδέποτε εξεδήλωσαν διάθεση να τους σταλούν αυτές οι επιστολές, και των οποίων οι ηλεκτρονικές διευθύνσεις έχουν συλλεγεί παράνομα με την βοήθεια προγραμμάτων. Τα περισσότερα από αυτά τα μηνύματα έχουν, συνήθως, περιεχόμενο την πώληση φαρμακευτικών σκευασμάτων, απομιμήσεων επωνύμων προϊόντων, μετοχών, επενδυτικών προϊόντων, προγραμμάτων και συσκευών. Παρά το γεγονός ότι μεγάλο μέρος αυτών το μηνυμάτων περιέχει ψευδές περιεχόμενο, που στοχεύει στην εξαπάτηση του θύματος (παραγγελία προϊόντων που ουδέποτε παραδίδονται, ή προϊόντων που παραδίδονται αλλά είναι ελαττωματικά και δεν έχουν καμία σχέση με τις αρχικώς εμφανιζόμενες προδιαγραφές τους)[91], έχει διαπιστωθεί ότι σημαντικό τμήμα χρηστών αγοράζει προϊόντα που διαφημίζονται με τέτοιον τρόπο (μέσω spamming).[92] Έτσι οι spammers καταλήγουν να

[90] Η λέξη spam προέρχεται από ένα χιουμοριστικό σκέτς των Μόντυ Πάυθον, όπου διακωμωδείτο η επαναλαμβανόμενη χρήση της λέξης spam στον κατάλογο ενός εστιατορίου, όπου προσφερόταν spam, spam και,.... spam. Η χρήση του όρου αυτού στο Διαδίκτυο σκοπό έχει να αποδώσει τον κατακλυσμό από σκουπιδοταχυδρομείο (junk mail).

[91] Βλ. σχετικά *S.Hedley*, A brief history of spam, Information & Communication Technology Law, 2006, 223 επ..

[92] Σε έρευνα που διεξήχθη στις ΗΠΑ το 2003, υπολογίσθηκε ότι 11 εκατομμύρια Αμερικανοί (δηλ. το 9% των χρηστών είχε αγοράσει προϊόντα που διαφημίζονταν με μαζικά e-mail. Τα σχετικά στοιχεία σε http://www.the-dma.org/cgi/disppressrelease?article 484.

κερδίζουν σημαντικά χρηματικά ποσά[93] μέσα από την ενοχλητική, επιβλαβή και συχνά αξιόποινη συμπεριφορά τους.

Από πλευράς ποινικού δικαίου, το spamming μπορεί να συνδέεται με τις ήδη αναφερθείσες περιπτώσεις απάτης (απάτη σε βάρος του καταναλωτή), παράνομης πρόσβασης σε δεδομένα υπολογιστή και παραβίασης απορρήτου (άρθρα 370Β και 370 Γ Π.Κ., όταν μέσω αυτών των μηνυμάτων και των συνημμένων σε αυτά αρχείων ο δράστης αποκτά πρόσβαση σε αρχεία και απόρρητα που είναι αποθηκευμένα στον υπολογιστή του θύματος), απάτης με υπολογιστή (άρθρο 386 Α Π.Κ., όταν με προγράμματα γίνεται επηρεασμός δεδομένων υπολογιστή, με σκοπό να αποκομίσει ο δράστης περιουσιακό όφελος), πλαστογραφίας (άρθρο 216 Π.Κ., όταν καταρτίζεται πλαστή ηλεκτρονική επιστολή) και αλλοίωσης δεδομένων (τιμωρούμενης ως φθορά ιδιοκτησίας 381 Π.Κ., όταν αποστέλλονται ιοί και άλλα επιβλαβή προγράμματα που αλλοιώνουν, καταστρέφουν ή διαγράφουν δεδομένα από τον υπολογιστή).

Βεβαίως, το spamming δεν συνδέεται πάντοτε με όλες ή μερικές από αυτές τις αξιόποινες πράξεις και η ποινική αξιολόγηση θα πρέπει να γίνεται με βάση τα δεδομένα της κάθε συγκεκριμένης περίπτωσης. Ωστόσο, είναι αλήθεια ότι το spamming προσφέρει ένα φθηνό και αποτελεσματικό εργαλείο εγκληματικής δραστηριότητας, καθώς επιτρέπει στους δράστες να προσεγγίζουν μεγάλο αριθμό θυμάτων, με πολύ μικρό οικονομικό κόστος και εξασφάλιση της ανωνυμίας τους ή, σε κάθε περίπτωση, ουσιώδη δυσχέρεια εντοπισμού τους. Είναι, λοιπόν, εύλογο ότι το spamming χρησιμοποιείται, τα τελευταία χρόνια, και από εγκληματικές

[93] *K.M. Rogers,* Viagra, Viruses and virgins: A pan-Atlantic comparative analysis on the vanquishing of spam, Computer law & security report 2006, 228-240, 229.

οργανώσεις οι οποίες στήνουν δίκτυα απάτης ή επιχειρούν να εκβιάσουν τους χρήστες.[94]

Η πιο πρόσφατη, και εξαιρετικά επικίνδυνη, μορφή spamming είναι η λεγόμενη χρήση του botnet[95]. Πρόκειται για μια εξαιρετικά ευφυή μέθοδο απόκρυψης των ιχνών των δραστών και ταυτόχρονης μαζικής αναπαραγωγής του spamming. Οι δράστες, σε αυτή την περίπτωση, αποστέλλουν μαζικά μηνύματα στα θύματα (α΄ φάση - παραδοσιακή μέθοδος spamming), στα οποία εμπεριέχονται προγράμματα που καθιστούν τους υπολογιστές των θυμάτων botnets, δηλ. συσκευές ελεγχόμενες από τους δράστες. Οι δράστες, στην δεύτερη φάση, χρησιμοποιούν πλέον τους ελεγχόμενους υπολογιστές-botnets για να διαδώσουν πλέον μέσω αυτών τα μηνύματά τους. Με αυτό τον τρόπο και τα δικά τους ίχνη συγκαλύπτουν (αφού το spamming δεν προέρχεται από τους δικούς τους υπολογιστές) και την επέκταση της δραστηριότητάς τους εξασφαλίζουν, χρησιμοποιώντας τους υπολογιστές των θυμάτων ως εργαλεία της δραστηριότητάς τους.[96]

Ανεξάρτητα από την ποινική αντιμετώπιση των ειδικότερων πράξεων που τελούνται μέσω του spamming, η ίδια η μαζική αποστολή ηλεκτρονικών μηνυμάτων-σκουπιδιών, που κυριολεκτικά ταλανίζει τους χρήστες και καταναλώνει σημαντικό τμήμα των πόρων του Διαδικτύου απασχολεί το νομοθέτη, ο οποίος προσπαθεί να

---

[94] *S.Hendley*, ό.π. σελ. 228. Τέτοιες περιπτώσεις οργανωμένης εγκληματικότητας συνδυάζονται με την λεγόμενη νιγηριανή απάτη ή απάτη 419, όπου δηλ. αποστέλλονται μηνύματα στα θύματα, τα οποία καλούνται να συνδράμουν κάποια (ανύπαρκτη) εταιρεία να αποφύγει τους συναλλαγματικούς περιορισμούς που υφίστανται στη Νιγηρία βοηθώντας στο άνοιγμα κάποιου λογαριασμού στο εξωτερικό και καταθέτοντας ένα μικρό σχετικά οικονομικό ποσό για να λάβουν στην συνέχεια μια πολύ μεγαλύτερη προμήθεια. Σε περίπτωση που το θύμα πεισθεί και καταθέσει τα χρήματα, οι μεν δράστες τα εισπράττουν και εξαφανίζονται, αυτό δε αναμένει ματαίως την προμήθεια. Σε άλλες περιπτώσεις, η εγκληματική οργάνωση μέσω spamming εγκαθιστά στους υπολογιστές των θυμάτων λογισμικό που «κλειδώνει» τα αρχεία τους και κατόπιν απαιτεί χρηματικό ποσό για να τους στείλει το «κλειδί», ώστε να μπορούν να τα χρησιμοποιήσουν και πάλι.

[95] *S.Hendley*, ό.π. 231 επ.

[96] Με αυτή τη μέθοδο παρακάμπτουν την αμυντική δραστηριότητα των διαχειριστών συστημάτων, που εγκαθιστούν φίλτρα για την τεχνική αντιμετώπιση του spamming.

περιορίσει το φαινόμενο χωρίς να παρεμβαίνει στην ελεύθερη διακίνηση πληροφοριών ή να περιορίζει την θεμιτή εμπορική διαφήμιση. Στο πλαίσιο αυτό, εντάσσεται η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12/ 7/2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[97] που ενσωματώθηκε στην ελληνική νομοθεσία με το Ν. 3471/2006. Το spamming ρυθμίζεται στο άρθρο 11 του Νόμου (μη ζητηθείσα επικοινωνία), όπου προβλέπονται και οι προϋποθέσεις, υπό τις οποίες αυτή η δραστηριότητα είναι νόμιμη, ενώ φαίνεται κατ' αρχήν[98] να ποινικοποιείται αυτοτελώς και μια όψη του spamming που συνίσταται στη συλλογή, λήψη γνώσης ή αποθήκευση δεδομένων προσωπικού χαρακτήρα συνδρομητών ή χρηστών (άρθρο 15 παρ.1 Ν. 3471/2006 σε συνδυασμό με άρθρο 2 α) Ν. 2472/1997), στα οποία θα πρέπει να ενταχθεί και η διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη, εφόσον ο χρήστης δεν την έχει γνωστοποιήσει στον δράστη και ο τελευταίος την έχει αποκτήσει παράνομα.

[97] ΕΕ L 201/37 της 31/7/2002.

[98] Επισημαίνεται πάντως, και πάλι η προβληματική τακτική του Έλληνα νομοθέτη να ρυθμίζει στους ειδικούς νόμους περισσότερες πράξεις και με μία μόνη διάταξη περί ποινικών κυρώσεων να ρυθμίζει ζητήματα ποινικής ευθύνης, αντί της συγκεκριμένης και αναλυτικής κατάστρωσης των ειδικών υποστάσεων που επιβάλλει η αρχή nullum crimen sine lega certa.

5. ΜΕΡΟΣ (Β) Ειδικότερα η σκοπιμότητα ψήφισης της διάταξης του άρθρου 386Α ΠΚ

Όπως αναφέρθηκε προηγουμένως, με το ν. 1805/1988 προστέθηκε στον Π.Κ το άρθρο 386Α με τίτλο «Απάτη με υπολογιστή», σύμφωνα με το οποίο: «Οποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο τιμωρείται με τις ποινές του προηγούμενου άρθρου" δηλαδή του άρθρου 386 Π.Κ.

Η συγκεκριμένη διάταξη διατυπώθηκε σχεδόν κατ' αντιγραφή της αντίστοιχης παραγράφου 263a του γερμανικού ποινικού κώδικα, με σκοπό να καλύψει τα κενά εφαρμογής των διατάξεων της κλασσικής απάτης, ενόψει των προσβολών της περιουσίας με τη χρήση ηλεκτρονικού υπολογιστή στις οποίες δεν παρεισφρύει παραπλάνηση ανθρώπου.[99] Υπάρχουν βέβαια και κάποιες διαφορές ανάμεσα στις δύο διατάξεις οι οποίες θα επισημανθούν στη συνέχεια. Ακριβώς λόγω της παραπάνω ομοιότητας, χρησιμοποιούνται συχνά από την ελληνική θεωρία πορίσματα της γερμανικής θεωρίας και νομολογίας, αναφορικά με τα προβλήματα που κάθε φορά προκύπτουν.

Τη χρονική περίοδο ψήφισης του νόμου 1805/1988 το κυρίαρχο φαινόμενο προσβολής της περιουσίας με τη χρήση Η/Υ και

[99] Βλ. *Γ. Νούσκαλη* «Απάτη με ηλεκτρονικό υπολογιστή το παρελθόν και το μέλλον του άρθρου 386Α Π.Κ ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση" ΠοινΔικ 2/2003, 178.,αλλά και *Ε.Βασιλάκη,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών ,1993,201 επ., *Μυλωνόπουλου,* Ηλεκτρονικοί υπολογιστές και ποινικό Δίκαιο ,1991,56, *Παπαδαμάκη,* Τα περιουσιακά εγκλήματα,2000,183.

αποκόμισης περιουσιακού οφέλους, συνίστατο στη χωρίς δικαίωμα χρήση κωδικών καρτών αυτόματης τραπεζικής ανάληψης και αυτό διότι το διαδίκτυο, τουλάχιστον με τη σημερινή του μορφή, δεν είχε κάνει ακόμη την εμφάνισή του.

Στα τέλη της δεκαετίας του 1980 αποτελούσε κρατούσα αντίληψη ότι ο Η/Υ αποτελεί απλώς το μέσο για την τέλεση προσβολών ήδη γνωστών εννόμων αγαθών. Γύρω στα μέσα της δεκαετίας του 1990 με την ανάπτυξη του διαδικτύου στη σημερινή του μορφή άρχισε να εμπεδώνεται η άποψη ότι υπάρχουν πράξεις που διευκολύνονται απλώς με τη χρήση Η/Υ και άλλες που συνιστούν «εγκλήματα του κυβερνοχώρου» και προσβάλουν νέα έννομα αγαθά, ή ότι σε κάθε περίπτωση, χρήζουν ειδικής ρύθμισης. Ήδη, με τη σύγκλιση των τεχνολογιών που συνδυάζουν τον Η/Υ και το διαδίκτυο η τελευταία θεώρηση φαίνεται μάλλον παρωχημένη. Σήμερα γίνεται λόγος για πράξεις που στρέφονται εναντίον συστημάτων πληροφοριών[100], τα οποία περιλαμβάνουν τον Η/Υ, τα προγράμματα για Η/Υ και τα δίκτυα επικοινωνίας μεταξύ των υπολογιστών. Τα ανωτέρω θα πρέπει να ληφθούν υπόψη ώστε να εξηγηθεί καλύτερα η δομή της αντικειμενικής υπόστασης του άρθρου 386Α Π.Κ αλλά και να διαγραφούν τα όρια αυτής ενόψει των τρεχουσών νομοθετικών εξελίξεων στα πλαίσια της Ευρώπης αλλά και παγκοσμίως.

[100] Βλ. *Νούσκαλη*, Απάτη με Η/Υ το παρελθόν και το μέλλον του άρθρου 386Α Π.Κ ιδίως υπό το πρίσμα των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, Ποιν Δικ 2/2003, 178 με περαιτέρω παραπομπές.

5.1 Το πρόγραμμα Η/Υ ως μέσο διακίνησης και διασφάλισης της περιουσίας.

Το πρόγραμμα Η/Υ λειτουργεί στην παραγωγική διαδικασία και ως μέσο διασφάλισης και διακίνησης περιουσιακών στοιχείων. Η χρήση κωδικής κάρτας (cashcard) και του μυστικού της κωδικού αριθμού (PIN) με σκοπό την ανάληψη χρημάτων από τερματικό υπολογιστή τράπεζας ήταν από τις πρώτες περιπτώσεις όπου εμφανίστηκε αυτή η λειτουργία του προγράμματος. Ο χρήστης της κάρτας και του μυστικού αριθμού της χρεώνει τον αντίστοιχο τραπεζικό λογαριασμό χωρίς την παρεμβολή ανθρώπου. Οι τραπεζικές εργασίες από απόσταση (homebanking, telebanking), με τις οποιες είναι δυνατή η μεταφορά οποιουδήποτε χρηματικού ποσού από ένα λογαριασμό σε άλλον χωρίς τη μεσολάβηση ανθρώπου παρά μόνο εκείνου που αποφασίζει και εκτελεί τη μεταφορά, αποτελούν ακόμα μία περίπτωση. Η χρήση μίας ιστοσελίδας στο διαδίκτυο και ενός μυστικού κωδικού αριθμού καθιστούν εικονική την παρουσία ενός πελάτη σε μια τράπεζα, αφού υπάρχει και λειτουργεί μόνο μέσα στο διαδίκτυο.

Με τον τρόπο αυτό διενεργούνται χρεοπιστώσεις ενός ή περισσότερων τραπεζικών λογαριασμών με οποιοδήποτε ποσό χωρίς την παρεμβολή ανθρώπινου στοιχείου. Η από απόσταση πρόσβαση σε αγαθά και υπηρεσίες, μέσω υπολογιστή και προγράμματος το οποίο υποκαθιστά τον πωλητή, είναι ένας άλλος τομέας όπου το πρόγραμμα λειτουργεί ως μέσο διακίνησης και διασφάλισης της περιουσίας. Όταν κάποιος κάνει χρήση στο διαδίκτυο μίας ιστοσελίδας «εικονικής» βιτρίνας καταστήματος, μπορεί να αγοράσει ένα αγαθό, π.χ ένα βιβλίο, και να χρεώσει έναν τραπεζικό λογαριασμό πιστωτικής

κάρτας, χωρίς την παραμικρή παρεμβολή ανθρώπινου στοιχείου. Το πιστωτικό όριο της κάρτας ελέγχεται από το κατάλληλο πρόγραμμα που συνδέει την εκδότρια τράπεζα της κάρτας και την επιχείρηση που πουλάει το αγαθό. Εφόσον εγκριθεί η χορήγηση πίστωσης, θεωρείται συναφθείσα η σύμβαση, ο λογαριασμός της κάρτας χρεώνεται και έπειτα παρεμβαίνει το ανθρώπινο στοιχείο, το οποίο, αφού ελέγξει τα παραπάνω, αποστέλλει το αγαθό στον αγοραστή.

Σήμερα, αναπτύσσονται διεθνώς όλο και περισσότερα συστήματα διακίνησης περιουσιακών στοιχείων, κυρίως χρήματος, με πλήρη αυτοματισμό, όπως για παράδειγμα η λειτουργία της ηλεκτρονικής φορτωτικής[101] και το σύστημα των άϋλων τίτλων[102] . Η τάση είναι η περαιτέρω αυτοματοποίηση όλων των συστημάτων πληρωμών. Τα κύρια χαρακτηριστικά αυτών των συστημάτων είναι η πλήρης αυτοματοποίηση των περιουσιακών μετατοπίσεων και η διασφάλιση της νομιμότητας χρήσης αυτών μόνο με τη χρήση ενός μυστικού κωδικού που «διαβάζεται» και «αναγνωρίζεται» από το πρόγραμμα του Η/Υ.[103] Στα ηλεκτρονικά αυτά συστήματα παράγονται και διακινούνται ανθρώπινες δηλώσεις βουλήσεως μέσω του κατάλληλου προγραμματισμού.[104] Ο παράγων άνθρωπος δεν παρεμβαίνει για την ανταλλαγή των σχετικών δηλώσεων, παρά μόνο στην αρχική φάση του προγραμματισμού και κατόπιν για τον έλεγχο της ήδη επελθούσης περιουσιακής μετατόπισης.

Έπεται, ότι τα ανωτέρω αυτοματοποιημένα συστήματα διακίνησης της περιουσίας μέσω Η/Υ έχουν αποκτήσει ιδιαίτερη

[101] Για τα ειδικότερα ζητήματα που ανακύπτουν στο εμπορικό και εν γένει στο αστικό δίκαιο από τα συστήματα αυτά, βλ. *Κουσούλη,* Ζητήματα Ηλεκτρονικής Φορτωτικής, Ελληνική Ένωση Ναυτικού Δικαίου, Δημοσιεύματα, 1,1992,σελ.35 επ.

[102] Βλ. *Μιχαλόπουλου,* Αποϋλοποίηση τίτλων κυρίως μετοχών, 1999, σελ 63-65.

[103] Βλ. *Bandekow* An introduction to the com Phenomenon. Recognition of Electronic Documents and Signatures σε http://profs.lp.findlaw.com/e-commerce/ecommerce 1.html.

[104] Βλ. *Ψούνη-Ζορμπά,* Δήλωση βουλήσεως μέσω ηλεκτρονικού υπολογιστή. Ένταξη στο σύστημα του ΑΚ, δυνατότητες ακύρωσης, Θεσσαλονίκη, 1988,σελ.66 επ., όπου και περαιτέρω παραπομπές στη διεθνή βιβλιογραφία.

σημασία στη σύγχρονη κοινωνία. Καταλαμβάνουν μεγάλο μέρος των συναλλαγών και είναι βέβαιο ότι θα εκτοπίσουν εξολοκλήρου τα παραδοσιακά συστήματα διακίνησης χρήματος. Το κυρίαρχο υλικό στοιχείο των σύγχρονων αυτοματοποιημένων συστημάτων διακίνησης χρήματος είναι το πρόγραμμα Η/Υ, υπό την ιδιότητά του να διακινεί και να διασφαλίζει την περιουσία. Η ιδιότητα αυτή του προγράμματος θα μπορούσε αναμφίβολα να χαρακτηριστεί ως ουσιώδες στοιχείο του σύγχρονου κοινωνικού χώρου, ώστε να μπορεί να συζητηθεί και η προστασία του ως εννόμου αγαθού.[105] Η διαφύλαξη της ακεραιότητας αυτής της ιδιότητας- λειτουργίας του προγράμματος Η/Υ αποτελεί προϋπόθεση για την ασφαλή διακίνηση αγαθών και υπηρεσιών σε ολόκληρο τον πλανήτη. Συνεπώς, θα νομιμοποιούνταν ο Έλληνας και διεθνής νομοθέτης να τυποποιήσουν ως έγκλημα τη χωρίς δικαίωμα χρήση της ιδιότητας του προγράμματος να διακινεί και να διασφαλίζει την περιουσία.[106]

Η πράξη που συνιστά βλάβη για την ανωτέρω ιδιότητα του προγράμματος είναι η χρήση του χωρίς δικαίωμα. Η χρήση αυτή μπορεί να αφορά είτε την εξωτερική είτε την εσωτερική λειτουργία του προγράμματος. Η επίδραση στην εσωτερική λειτουργία του συνίσταται στην αλλαγή της προσχεδιασμένης ροής του προγράμματος, με τη χρησιμοποίηση προγραμμάτων-ιών ή με ηλεκτρομαγνητικά μέσα. Κατά μία άποψη,[107] η επίδραση στην εξωτερική λειτουργία αφορά την τροφοδοσία του προγράμματος με δεδομένα, ανεξάρτητα εάν αυτά ανταποκρίνονται στην πραγματικότητα ή όχι, αρκεί να γίνεται η εισαγωγή τους χωρίς δικαίωμα. Η βλάβη που προκαλείται για το προστατευόμενο έννομο

[105] Βλ. *Νούσκαλη*, οπ.παρ. σελ 179.
[106] Για την αναγκαιότητα να αποτελεί ένα υλικό αντικείμενο-ουσιώδες στοιχείο του κοινωνικού χώρου, ώστε να τυποποιηθεί ως αξιόποινη η προσβολή του, βλ. *Μανωλεδάκη*, Το έννομο αγαθό ως βασική έννοια του ποινικού δικαίου, 1998,σελ.105 επ.
[107] Βλ. *Νούσκαλη*, όπ. παρ. σελ. 179 επ.

αγαθό «πρόγραμμα» από τις ανωτέρω πράξεις, αποτελεί όρο συγκεκριμένου κινδύνου για άλλα έννομα αγαθά που συνδέονται με αυτό, όπως η περιουσία, το υπόμνημα, το απόρρητο και άλλα.

Έπεται λοιπόν η δυνατότητα του νομοθέτη να τυποποιήσει τη χωρίς δικαίωμα χρήση του προγράμματος, είτε με είτε χωρίς την απαίτηση να προσβάλλει αυτή και άλλο έννομο αγαθό.

5.2 Αντικειμενική υπόσταση 386Α Π.Κ.

Απάτη με υπολογιστή (αρθρ.386Α Π.Κ)[108] τελεί όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία ηλεκτρονικού υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιοδήποτε άλλο τρόπο. Η εγκληματική συμπεριφορά συνίσταται στον επηρεασμό των στοιχείων του ηλεκτρονικού υπολογιστή, ο οποίος μπορεί να τελεστεί είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιοδήποτε άλλο τρόπο [109].

Αναλύοντας την αντικειμενική υπόσταση του άρθρου 386^Α Π.Κ μπορούμε να επισημάνουμε αρχικά τις εξής δυσχέρειες: Όσον αφορά το υποκείμενο του συγκεκριμένου εγκλήματος, αυτό μπορεί να είναι σύμφωνα με τη διάταξη του νόμου οποιοσδήποτε (όποιος), με την

[108] Βλ. *Α Κονταξή* Ποινικός Κώδικας κατ΄άρθρο ερμηνεία « Πρόκειται για ιδιώνυμο έγκλημα απάτης και ειδική μορφή αυτής . Σωρευτική συνδρομή των εγκλημάτων 386 και 386 Α Π.Κ δεν είναι δυνατή.

[109] Από το κείμενο του άρθρου 386^α Π.Κ.

έννοια ότι το έγκλημα δεν είναι ιδιαίτερο, δεν χρειάζεται δηλαδή το πρόσωπο να ανήκει σε ορισμένο κύκλο προσώπων με ιδιαίτερα χαρακτηριστικά γνωρίσματα. Η δυσχέρεια έγκειται εδώ στο ότι κάθε προγραμματιστής ηλεκτρονικού υπολογιστή δεν έχει πάντοτε και τις γνώσεις[110] εκείνες, οι οποίες να τον καθιστούν ικανό ώστε κάθε επέμβασή του στο σύστημα επεξεργασίας δεδομένων του υπολογιστή να έχει ως αποτέλεσμα την απάτη, χωρίς βέβαια αυτό να σημαίνει ότι για το λόγο αυτό το έγκλημα του άρθρου 386^{A}.Π.Κ θα μπορούσε να χαρακτηριστεί ιδιαίτερο.

Αντικείμενο της πράξης είναι η συγκεκριμένη περιουσία, υπολογιζόμενη όμως σε χρήμα. Το θύμα όμως το οποίου μειώθηκε η περιουσία δεν εξειδικεύεται, αλλά ο δράστης της απάτης με υπολογιστή, προσβάλλει την περιουσία όχι ενός ατόμου αλλά μιας συλλογικής ομάδας προσώπων, εταιρειών ή πιστωτικών ιδρυμάτων, οπότε η απάτη συγκεντρώνει και κατά την άποψη του γράφοντος τι περισσότερες πιθανότητες να χαρακτηριστεί ως οικονομικό έγκλημα.

Η ενδεικτική απαρίθμηση των τρόπων τέλεσης όχι μόνο εξασφαλίζει την αποτελεσματικότητα της διάταξης που δεν επηρεάζεται από τις ραγδαίες τεχνολογικές εξελίξεις αλλά και επιτρέπει την ικανοποιητική επίλυση πρακτικών προβλημάτων, όπως εκείνων που ανακύπτουν στην περίπτωση χρησιμοποίησης ορθών στοιχείων χωρίς δικαίωμα (πχ κλεμμένη πιστωτική κάρτα)[111] αφού ο

---

[110] Οι ιδιαίτερες γνώσεις τις οποίες πρέπει να έχει ο δράστης προκειμένου να χρησιμοποιήσει τεχνάσματα, φαίνονται για παράδειγμα και από τις ανησυχητικές διαστάσεις τις οποίες έχει πάρει τα τελευταία χρόνια στη Δανία η ηλεκτρονική οικονομική απάτη με θύματα δεκάδες κατόχους τραπεζικών λογαριασμών, οι οποίοι ανακάλυψαν ξαφνικά ότι οι λογαριασμοί τους υπερχρεώθηκαν εν αγνοία τους. Συγκεκριμένα οι δράστες τοποθετούσαν ένα πλαστό καντράν στη θέση του γνησίου σε τραπεζικό μηχάνημα αυτόματης ανάληψης πάνω στο οποίο ο πελάτης πληκτρολογεί τον κωδικό αριθμό του .Το καντράν πιθανώς να είναι εξοπλισμένο με μίκρο-υπολογιστή ο οποίος επιτρέπει στο δράστη να διαβάσει τις πληροφορίες που περιέχουν οι τραπεζικές κάρτες όπως και τους κωδικούς τους. Οι πληροφορίες αυτές μεταφέρονται σε νέες αχρησιμοποίητες μαγνητικές κάρτες , τις οποίες και χρησιμοποιούν οι δράστες στα μηχανήματα αυτόματων συναλλαγών (Βλ. σχετικά Ζησιάδη όπ.παρ σελ 100 υποσημείωση 138)

[111] βλ. *Μυλωνόπουλου* « Ποινικό Δίκαιο Ειδικό Μέρος» Π.Ν Σάκκουλα Αθήνα 2000 σελ 550. Αλλά και *Δ.Κιούπη* οπ.παρ «Η Απάτη με ηλεκτρονικό υπολογιστή» σελ 54 επ.

επηρεασμός μπορεί να επιτευχθεί όχι μόνο με μία από τις πράξεις που εξειδικεύονται στο νόμο αλλά και με οποιοδήποτε άλλο τρόπο.

5.2.1. Μη ορθή διαμόρφωση του προγράμματος

Πρόγραμμα είναι σύνολο δεδομένων με τα οποία παρέχονται εντολές στον υπολογιστή.[112] Άρα η μη ορθή διαμόρφωση του προγράμματος αποτελεί ειδικότερη περίπτωση του τρίτου τρόπου τέλεσης «χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων» αφού και το πρόγραμμα αποτελεί κατηγορία δεδομένων.[113] Μπορεί να πραγματωθεί με την εκπόνηση ενός νέου, ολικά η μερικά, προγράμματος ή με την αλλοίωση του ήδη υπάρχοντος προγράμματος ή με την απόκρυψη δεδομένων (holding back).

Η αλλοίωση μπορεί να επιτευχθεί με την προσθήκη ή την εξάλειψη λογικών βημάτων (με απομάκρυνση δεδομένων). Η απόκρυψη δεδομένων πραγματοποιείται σε κάθε συμπεριφορά εξ αιτίας της οποίας δεν εισάγονται στη διαδικασία επεξεργασίας στοιχεία απαραίτητα για την ορθή εφαρμογή του προγράμματος.

«Μη ορθή» είναι η διαμόρφωση του προγράμματος όταν αυτό είναι πρόσφορο να προκαλέσει βλάβη στην περιουσία άλλου ή να επαυξήσει αυτήν, σύμφωνα με την αρχή της επίτασης του κινδύνου (Risikoerhöhungsprinzip)[114] και έτσι η λειτουργία του προγράμματος αποκλίνει από την κοινωνικά αποδεκτή αποστολή του για την οποία προορίζεται.[115]Κατά την αντίθετη (αντικειμενική) θεωρία ένα πρόγραμμα είναι ορθό όταν εκπληρώνει την αποστολή του. Βασική

---

[112] Έτσι και *Μυλωνόπουλου* σελ 551 Ποινικό Δίκαιο Ειδικό Μέρος.

[113] Tiedemann LK§263A num.27.

[114] Η συγκεκριμένη αρχή αποτελεί πεδίο της θεωρίας του αντικειμενικού καταλογισμού βλ *Ν. Ανδρουλάκη,* Ποινικό Δίκαιο Γενικό Μέρος, Π.Ν Σάκκουλα Αθήνα 2000 αλλά και *C.Roxin,* Ο αντικειμενικός καταλογισμός, εκδόσεις Ποινικά Χρονικά Αθήνα 1991.

[115] Κανονιστικό κριτήριο, *Μυλωνόπουλου* οπ. παρ, πρβλ. *Βασιλάκη,* Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 204, όπου μη ορθή είναι η διαμόρφωση όταν αυτή αντιτίθεται σε μια νόμιμη κατάσταση.

αδυναμία της άποψης αυτής είναι να θεωρεί ορθό και το πρόγραμμα που καταρτίστηκε ή με επεμβάσεις τροποποιήθηκε με σκοπό την παραπλάνηση του χρήστη, όταν επιτυγχάνει το σκοπό του.

5.2.2. Επέμβαση κατά την εφαρμογή του προγράμματος

Επέμβαση κατά την εφαρμογή του προγράμματος συνιστά κάθε πράξη που επηρεάζει τη διαδικασίας επεξεργασίας των δεδομένων από το πληκτρολόγιο καθώς και κάθε επέμβαση στα μηχανικά μέρη του υπολογιστή που επηρεάζουν τη λειτουργία του προγράμματος.[116]

5.2.3 Χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων

«Μη ορθά» είναι τα δεδομένα του υπολογιστή που δεν ανταποκρίνονται στην πραγματικότητα ενώ «ελλιπή» εκείνα που εκφράζουν ανακριβώς την πραγματικότητα στην οποία αναφέρονται και η οποία έχει αποφασιστική σημασία για την επεξεργασία των δεδομένων.

Παράδειγμα 1: η συμπλήρωση μηχανογραφικού δελτίου όπου ο υπαίτιος παραλείπει με πρόθεση να μνημονεύσει το διαζύγιο του, με αποτέλεσμα να εξακολουθεί να εισπράττει επίδομα συζύγου.

Παράδειγμα 2: Η τροφοδότηση του υπολογιστή με το δεδομένο, ότι ο δράστης είναι πολύτεκνος ενώ δεν είναι.[117]

Τα χρησιμοποιούμενα δεδομένα πρέπει να αναφέρονται σε γεγονότα και όχι σε προγνώσεις ή αξιολογικές κρίσεις. Συνεπώς η

[116] Έτσι και *Μυλωνόπουλου*, σελ 551 σημ 11 .
[117] βλ. *Βασιλάκη*, οπ. παρ.205, *Παπαδαμάκη* , 188, *Μυλωνόπουλου*, 552 σημ 14.

παρεμβολή κάποιου φυσικού προσώπου στις περιπτώσεις αυτές που απλώς παραλαμβάνει χωρίς έλεγχο τα δεδομένα δεν αποκλείει την στοιχειοθέτηση απάτης με υπολογιστή 386Α Π.Κ, αφού αυτό δεν παραπλανάται ούτε αποτελεί εμπόδιο που πρέπει να παρακαμφθεί. Αν όμως τα στοιχεία ελέγχονται σε κάποια φάση της επεξεργασίας τους, πριν από την περιουσιακή διάθεση, από φυσικό πρόσωπο, το οποίο και παραπλανάται, στοιχειοθετείται κοινή απάτη του άρθρου 386 Π.Κ.[118]

5.2.4 Επηρεασμός των στοιχείων του υπολογιστή «με οποιοδήποτε άλλο τρόπο»

Ο επηρεασμός των στοιχείων του υπολογιστή μπορεί να γίνει και με «οποιοδήποτε άλλο τρόπο». Η ευρεία διατύπωση του νόμου, επιτρέπει την υπαγωγή σε αυτήν και περιπτώσεων επηρεασμού ακόμη και με μη νόμιμη χρήση ορθών στοιχείων.[119] Σε αυτή την περίπτωση υπάγεται και η ανάληψη χρημάτων από ΑΤΜ από μη δικαιούμενο πρόσωπο, είτε με κλεμμένη μαγνητική κάρτα (cash card) είτε με υπέρβαση του πιστωτικού ορίου (overdraft).

Ο δράστης επηρεάζει τα στοιχεία του υπολογιστή όταν το αποτέλεσμα της επεξεργασίας των δεδομένων, λόγω της συμπεριφοράς του, αποκλίνει από εκείνο που θα επιτυγχάνονταν με κανονική και σύννομη εκτέλεση του προγράμματος.[120] Ο επηρεασμός των δεδομένων ως εγκληματική συμπεριφορά μπορεί να πραγματωθεί

---

[118] Βλ. *Βασιλάκη,* οπ. παρ 217, *Καϊάφα Γκμπάντι,* παρατ. στην ΑΠ 1277/1998, Υπερ 99, 917. Ασαφής σύμφωνα με *Μυλωνόπουλο,* σελ.552 σημ 17 η ΑΠ 1059/1995, ΠΧ ΜΣΤ/97 Οι δράστες καταχώρισαν σε ηλεκτρονικό υπολογιστή ημερήσιες αποδοχές των ιδίων και του τρίτου προσώπου μεγαλύτερες από τις πραγματικές και εισέπρατταν παράνομα τα ποσά αυτά από τον εργοδότη τους . Αν η ανωτέρω διαδικασία διεξήγετο αυτόματα, στοιχειοθετείται όντως απάτη με υπολογιστή. Αν όμως παρεμβάλλονταν φυσικό πρόσωπο το οποίο και επλανάτο στοιχειοθετείται απάτη. Contra η ΕφΑθ 678, 751/1998 (ΠοινΔικ 99 , 817).

[119] Κανονική αλλά χωρίς δικαίωμα εκτέλεση προγράμματος.

[120] Έτσι και η Οριστική Έκθεση Πεπραγμένων του Συμβουλίου της Ευρώπης (F.A.R) P.28.

σε κάθε στάδιο της εξέλιξης της ανάλυσής τους, όπως για παράδειγμα κατά την εισαγωγή στοιχείων, κατά την εφαρμογή του προγράμματος, κατά την έξοδο των στοιχείων, καθώς και με επέμβαση στα μηχανικά μέρη του Η/Υ (hardware).

Επηρεασμό συνιστά επομένως, και κάθε χωρίς δικαίωμα επεξεργασία των δεδομένων του υπολογιστή που οδηγεί σε αποτέλεσμα διαφορετικό από εκείνο που προσδοκάται με νόμιμη χρήση.[121] Συνεπώς, αρκεί ο δράστης να προσδιορίσει με οποιονδήποτε παράνομο τρόπο την επεξεργασία των στοιχείων του υπολογιστή και να προκαλέσει περιουσιακή βλάβη.

Δεν είναι απαραίτητο να βρίσκεται ήδη σε λειτουργία ο υπολογιστής. Επηρεασμό συνιστά και η έναρξη της κανονικής διαδικασίας επεξεργασίας των στοιχείων, εφόσον αυτή δεν γίνεται με νόμιμο τρόπο, π.χ από μη δικαιούμενο πρόσωπο.[122]

5.2.5 Η διάκριση με βάση το στοιχείο της πλάνης

Είναι γενικά αποδεκτή η άποψη ότι το άρθρο 386Α Π.Κ καλύπτει το κενό τιμώρησης που άφηνε η διάταξη της κοινής απάτης στην περίπτωση που η περιουσιακή διάθεση και συνακόλουθα η περιουσιακή βλάβη προέρχεται αποκλειστικά από την επέμβαση του δράστη στο σύστημα επεξεργασίας των δεδομένων του Η/Υ και όχι από πρόκληση πλάνης σε ορισμένο φυσικό πρόσωπο, το οποίο για παράδειγμα διενεργεί έλεγχο της ορθής επεξεργασίας των στοιχείων,

[121] Έτσι και *Μυλωνόπουλου* σελ 553 επ..

[122] Πρβλ. BGHSt 38 ,121 ΠΧ ΜΒ/468 (Αποδ. *Α Τζανεττή*) το αποτέλεσμα της επεξεργασίας των δεδομένων επηρεάζει και αυτός που θέτει σε κίνηση μία αιτιώδη διαδρομή χρησιμοποιώντας συγκεκριμένα μέσα τα οποία δημιουργήθηκαν από τρίτους για την επίτευξη ενός διαφορετικού αποτελέσματος. Όμοια OLG Köln NJW 92, 125 *Wessels-Hillenkamp* BT/2 , 234 αλλά και BGH 10.11.1994, NStZ 95 , 135 σε ΠΧ ΜΕ/379 ο δράστης έθεσε σε λειτουργία αυτόματα το ηλεκτρονικό παίγνιο Triamint-Jacky-Jackpot χρησιμοποιώντας παράνομα πρόγραμμα και κέρδισε έτσι 105 DM.

λαμβάνει αποφάσεις για την πραγματοποίηση της περιουσιακής διάθεσης κλπ. Όπως είναι γνωστό η πρόκληση πλάνης απαιτεί επενέργεια στο νοητικό φυσικού προσώπου, η οποία ως αποτέλεσμα έχει είτε την δημιουργία εξ αρχής εσφαλμένης είτε την τροποποίηση μιας εξαρχής ορθής παράστασης είτε την παρακώλυση της ορθής μεταβολής μιας αρχικά εσφαλμένης παράστασης για την πραγματικότητα[123].

Δεν πρέπει να παραβλέπεται ότι όταν συντρέχει αποκλειστικά περίπτωση επενέργειας στα δεδομένα Η/Υ δεν μπορεί να θεωρηθεί ότι υπάρχει πλάνη του χειριστή ή του εντολέα επεξεργασίας ή του νόμιμου δικαιούχου του προγράμματος με την έννοια ότι διαψεύδονται οι προσδοκίες τους για κανονική και σύννομη εκτέλεση του προγράμματος.[124] Η εντύπωσή τους ότι «όλα πάνε καλά» δεν αρκεί για την στοιχειοθέτηση της κοινής απάτης γιατί αυτή η νοητική κατάσταση, εφόσον δεν στηρίζεται σε συγκεκριμένα δεδομένα του εξωτερικού κόσμου, αποτελεί ignorantia facti, δηλαδή απλή άγνοια της επελθούσης μεταβολής στο αντικείμενο της γνώσης, η οποία όμως δεν συνοδεύεται και από σχετική επίδραση στο νοητικό του δράστη. Επιπλέον η οποιαδήποτε εντύπωση-γνώση του χειριστή ότι όλα τα δεδομένα είναι ορθά προϋπάρχει της οποιασδήποτε επέμβασης του δράστη στα δεδομένα Η/Υ και συνεπώς δεν προκαλείται από αυτήν, δηλαδή ελλείπει ο εννοιολογικά απαραίτητος αιτιώδης σύνδεσμος μεταξύ της απατηλής συμπεριφοράς του δράστη και της πλάνης του παθόντος. Επίσης ούτε πλάνη με τη μορφή της εκ μέρους του δράστη παράλειψης της μεταβολής της εξαρχής εσφαλμένης παράστασης για την πραγματικότητα του παθόντος μπορεί να γίνει δεκτή, εφόσον

[123] Βλ μεταξύ άλλων όσον αφορά στην πλάνη *Ν. Κ Ανδρουλάκη* « Ποινικό Δίκαιο Γενικό Μέρος» σελ 494 επ. βλ. επίσης *Λ Κοτσαλή* «Ποινικό Δίκαιο Γενικό Μέρος» σελ 529 επ. αλλά και *Μπούρμα Γ.*, «Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386ΑΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386Π.Κ», ΠοινΧρον ΝΑ/2001 470 επ.

[124] Βλ. *Μυλωνόπουλου,* Ηλεκτρονικοί υπολογιστές οπ'παρ. σελ 55.

λαμβάνει αποφάσεις για την πραγματοποίηση της περιουσιακής διάθεσης κλπ. Όπως είναι γνωστό η πρόκληση πλάνης απαιτεί επενέργεια στο νοητικό φυσικού προσώπου, η οποία ως αποτέλεσμα έχει είτε την δημιουργία εξ αρχής εσφαλμένης είτε την τροποποίηση μιας εξαρχής ορθής παράστασης είτε την παρακώλυση της ορθής μεταβολής μιας αρχικά εσφαλμένης παράστασης για την πραγματικότητα[123].

Δεν πρέπει να παραβλέπεται ότι όταν συντρέχει αποκλειστικά περίπτωση επενέργειας στα δεδομένα Η/Υ δεν μπορεί να θεωρηθεί ότι υπάρχει πλάνη του χειριστή ή του εντολέα επεξεργασίας ή του νόμιμου δικαιούχου του προγράμματος με την έννοια ότι διαψεύδονται οι προσδοκίες τους για κανονική και σύννομη εκτέλεση του προγράμματος.[124] Η εντύπωσή τους ότι «όλα πάνε καλά» δεν αρκεί για την στοιχειοθέτηση της κοινής απάτης γιατί αυτή η νοητική κατάσταση, εφόσον δεν στηρίζεται σε συγκεκριμένα δεδομένα του εξωτερικού κόσμου, αποτελεί ignorantia facti, δηλαδή απλή άγνοια της επελθούσης μεταβολής στο αντικείμενο της γνώσης, η οποία όμως δεν συνοδεύεται και από σχετική επίδραση στο νοητικό του δράστη. Επιπλέον η οποιαδήποτε εντύπωση-γνώση του χειριστή ότι όλα τα δεδομένα είναι ορθά προϋπάρχει της οποιασδήποτε επέμβασης του δράστη στα δεδομένα Η/Υ και συνεπώς δεν προκαλείται από αυτήν, δηλαδή ελλείπει ο εννοιολογικά απαραίτητος αιτιώδης σύνδεσμος μεταξύ της απατηλής συμπεριφοράς του δράστη και της πλάνης του παθόντος. Επίσης ούτε πλάνη με τη μορφή της εκ μέρους του δράστη παράλειψης της μεταβολής της εξαρχής εσφαλμένης παράστασης για την πραγματικότητα του παθόντος μπορεί να γίνει δεκτή, εφόσον

[123] Βλ μεταξύ άλλων όσον αφορά στην πλάνη *Ν. Κ Ανδρουλάκη* « Ποινικό Δίκαιο Γενικό Μέρος» σελ 494 επ. βλ. επίσης *Λ Κοτσαλή* «Ποινικό Δίκαιο Γενικό Μέρος» σελ 529 επ. αλλά και *Μπούρμα Γ.*, «Στοιχεία απάτης με υπολογιστή κατ'άρθρο 386ΑΠΚ και διάκριση αυτής από την κοινή απάτη του άρθρου 386Π.Κ», ΠοινΧρον ΝΑ/2001 470 επ.

[124] Βλ. *Μυλωνόπουλου,* Ηλεκτρονικοί υπολογιστές οπ'παρ. σελ 55.

κατά κανόνα δεν υπάρχει ιδιαίτερη νομική υποχρέωση του δράστη προς άρση της πλάνης του παθόντος.[125]

Έπεται και με βάση τα μέχρι τώρα πορίσματα της θεωρίας ότι όταν τα εξαχθέντα από τον ειδικευμένο υπάλληλο[126] στοιχεία είναι απευθείας γραμμένα σε κώδικα μηχανής (δηλαδή κωδικοποιημένα και κατανοητά από τον υπολογιστή, δια μέσου του χρησιμοποιηθέντος προγράμματος-γλώσσας του Η/Υ και επομένως δεν απαιτείται επεξεργασία και μεταβολή των αρχικών εισερχομένων στοιχείων σε άλλα κωδικοποιημένα και κατανοητά από τον υπολογιστή, δια μέσου της διατρητικής ή άλλης μεθόδου) τότε συντρέχει πρωτογενής εγγραφή στοιχείων.[127]

Στην παραπάνω εγγραφή στοιχείων δεν μεσολαβεί άλλος έλεγχος της ουσιαστικής ορθότητας των εισερχομένων στοιχείων (πλην εκείνου που διενεργεί ο διευθυντής του υποκαταστήματος), μέχρι την τελική είσπραξη-ανάληψη των φαινομενικά κατατιθέμενων ποσών από τρίτο δια μέσω ενός υπαλλήλου (teller) της τράπεζας. Στην περίπτωση αυτή, ο καλόπιστος υπάλληλος εφόσον διαπιστώνει πιστωτικό υπόλοιπο στον λογαριασμό του φαινομενικού καταθέτη από το σύστημα on line της τράπεζας προβαίνει σε εκταμίευση του φαινομενικά κατατιθέμενου ποσού (περιουσιακή διάθεση), από την οποία προκαλείται, περιουσιακή βλάβη του παθόντος.

Το κρίσιμο ερώτημα που τίθεται για την εφαρμογή στην περίπτωση αυτή της κοινής τριγωνικής απάτης είναι αν ο διαθέτης υπάλληλος της τράπεζας βρίσκεται σε πλάνη σχετικά με την ουσιαστική ορθότητα των εισερχόμενων στοιχείων, ή αν αντίθετα

[125] Βλ. *Ανδρουλάκη*, Ποιν Δικ, Γεν μέρος 1 ,1991,242 αλλά και *Μυλωνόπουλου*, Εφαρμογές Ποινικού δικαίου 1997 σελ134 επ.
[126] Βλ. τα πραγματικά της ΑΠ 1152/1999 στο παράρτημα νομολογίας· στη συγκεκριμένη περίπτωση τον teller αρχικά και τον διευθυντή του υποκαταστήματος ως ελεγκτή μεταγενέστερα.
[127] Βλ. *Βασιλάκη*, οπ. παρ, σελ. 192.

διακατέχεται από άγνοια των κρίσιμων γεγονότων (ignorantia facti), η συνδρομή της οποίας αποκλείει τη στοιχειοθέτηση απάτης.

Από τη θεωρία γίνεται δεκτό ότι πλάνη είναι κάθε παράσταση γεγονότων στη συνείδηση του θύματος, η οποία δεν ανταποκρίνεται ολικώς ή μερικώς στην πραγματικότητα και πρέπει να διακρίνεται από την έλλειψη οποιασδήποτε παράστασης της πραγματικότητας από το θύμα (άγνοια).[128]

Συνεπώς, εκ των προηγηθέντων προκύπτει ότι ο έλεγχος στον οποίο προβαίνει τελικά ο υπάλληλος της τράπεζας και που σαν αποτέλεσμα έχει να προβεί στην περιουσιακή διάθεση είναι καθαρά τυπικός και ως περιεχόμενο έχει τη διαπίστωση της μαθηματικής-λογιστικής συμφωνίας μεταξύ των στοιχείων του λογαριασμού του εκάστοτε καταθέτη, τα οποία αναγράφονται στο βιβλιάριο καταθέσεων και αυτών που αναγράφονται στο on line σύστημα της τράπεζας. Συνακόλουθα ο εν λόγω υπάλληλος δεν αποτελεί, κατά την χαρακτηριστική έκφραση του Μυλωνόπουλου,[129] «τοποτηρητή» της περιουσίας του παθόντος (της τράπεζας), ούτε εμπόδιο που θα πρέπει με δόλο να παρακαμφθεί. Δεν έχει επίσης σχηματίσει στη συνείδησή του καμία άμεση παράσταση σχετικά με την ουσιαστική ορθότητα των στοιχείων του λογαριασμού του εκάστοτε καταθέτη.

Από την κρατούσα στη θεωρία άποψη γίνεται περαιτέρω δεκτό ότι η πλάνη δεν είναι αναγκαίο να είναι αποτέλεσμα μιας τεκμηριωμένης νοητικής διεργασίας αλλά αρκεί και μια λανθάνουσα παράσταση στο περιθώριο της γνώσης («συν-γνώση», Mitbewusstsein) ή μια γενική παράσταση ότι «όλα είναι εντάξει», η οποία όμως στηρίζεται σε συγκεκριμένα γεγονότα.[130]

---

[128] Βλ. *Κονταξή*, Ερμ ΠΚ σελ 210 επ, *Σπινέλλη*, Ποιν Δίκαιο Ειδ Μερ. ΣΕΛ 82 επ. αλλά και *Γάφο*, Ποιν Δικ Ειδ Μέρος Τομ ΣΤ1967 137 επ.
[129] Ηλεκτρονικοί υπολογιστές, οπ. παρ, σελ. 65.
[130] Βλ. σχετικά *Lackner:* LK § 263 αριθ. 78.

Βάσει όμως των παραπάνω το αρχικό ερώτημα σχετικά με την πλάνη του διαθέτοντος υπαλλήλου αναφορικά με την ουσιαστική ορθότητα των εισερχόμενων στοιχείων δυσχεραίνεται και μετατρέπεται σε ερώτημα αναφορικά με το αν ο εν λόγω υπάλληλος έχει εσφαλμένη συν-γνώση των πιο πάνω κρίσιμων γεγονότων και συνεπώς πλανάται-εξαπατάται άμεσα από την ύπαρξη και το περιεχόμενο προγενέστερων σχετικών ελέγχων. Πιο συγκεκριμένα, αν υπάρχουν προγενέστεροι έλεγχοι της ουσιαστικής ορθότητας των λογιστικών εγγραφών (καταθέσεων-αναλήψεων) του λογαριασμού του εκάστοτε καταθέτη και όχι απλά μόνο τεχνικοί, τυπικοί έλεγχοι της μαθηματικής ακρίβειας της αντιγραφής-μεταφοράς ή επεξεργασίας στοιχείων πριν ή και μετά την μηχανική κωδικοποίησή τους από τον Η/Υ, τότε είναι λογικό να γεννάται στον διαθέτοντα υπάλληλο η εύλογη γενική πεποίθηση ότι «όλα είναι εντάξει».

Η πεποίθηση αυτή στηρίζεται στο γεγονός του προγενέστερου ελέγχου, από τον διευθυντή του υποκαταστήματος, της ουσιαστικής ορθότητας των λογιστικών εγγραφών του υπαλλήλου με βάση τα γραμμάτια που εκδίδει ο τελευταίος. Είναι άλλωστε γνωστό ότι ο έλεγχος διενεργείται καθημερινά, μετά το πέρας των συναλλαγών (κλείσιμο ταμείου). Άρα υφίσταται πράξη εξαπάτησης και κατ' επέκταση πλάνη του εν λόγω προσώπου, το οποίο έχει αποφασιστική συμβολή και αρμοδιότητα στη διαδικασία λήψης της απόφασης που επιφέρει τελικά την περιουσιακή διάθεση.

Σε αυτή την περίπτωση – πάντα με βάση τα πραγματικά της απόφασης (ΑΠ 1152/1999 ΠοινΧρον Ν/597)- η «χρησιμοποίηση» των στοιχείων γίνεται από το παρένθετο πρόσωπο του υπαλλήλου και του διευθυντή του υποκαταστήματος, οι οποίοι εκ προθέσεως ενέγραψαν ψεύτικα στοιχεία, και η περιουσιακή βλάβη δεν προέρχεται από τη χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων από

το δράστη αλλά από την εξαπάτηση ενός προσώπου, το οποίο έχει τη νομική ή την πραγματική εξουσία να επεμβαίνει σε ξένη περιουσία. Αφού λοιπόν προκαλείται πλάνη σε τρίτο πρόσωπο, το οποίο επιφέρει περιουσιακή διάθεση (αιτιώδης σύνδεσμος μεταξύ της δημιουργίας πλάνης και της περιουσιακής διάθεσης), εφαρμόζεται το άρθρο 386 Π.Κ (τριγωνική απάτη) και όχι το 386Α Π.Κ (απάτη με Η/Υ).

5.2.6. Περιουσιακή ζημία[131]

Ο επηρεασμός των στοιχείων πρέπει να προκαλεί άμεσα μείωση ξένης περιουσίας. Δεν αρκεί δηλαδή αιτιώδης σύνδεσμος μεταξύ του επηρεασμού και της περιουσιακής βλάβης, αλλά απαιτείται και αμεσότητα στην πρόκληση της τελευταίας. Η περιουσιακή ζημία είναι άμεση όταν δεν απαιτείται παρεμβολή ανθρώπινης συμπεριφοράς μεταξύ της επεξεργασίας των στοιχείων και της μείωσης της περιουσίας. Αντίθετα δεν στοιχειοθετείται περιουσιακή ζημία αν το αποτέλεσμα της επεξεργασίας των στοιχείων απλώς διευκολύνει το δράστη να επιτύχει περιουσιακό όφελος με άλλη πράξη του π.χ. με απάτη.

Η περιουσιακή βλάβη στοιχειοθετείται ακόμη «αν τα πρόσωπα που την υπέστησαν είναι άδηλα» ενώ για τον υπολογισμό της ζημίας «είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα».[132]

---

[131] Πρβλ. *Κονταξή* ερμ.ΠΚ σελ 3566. « Η ζημία είναι το οριστικό αποτέλεσμα της επεξεργασίας των στοιχείων μετά τον επηρεασμό των δεδομένων του υπολογιστή. Εάν όμως το αποτέλεσμα αυτό δεν είναι οριστικό αλλά αποτελεί προϋπόθεση για περαιτέρω λήψη αποφάσεως τότε υπάρχει κανονική απάτη με παραπλανηθέν το πρόσωπο που έλαβε υπόψη το άνω αποτέλεσμα. Βλ. *Παπαδαμάκη* 186,188

[132] Εδάφια β και γ του άρθρου 386Α Π.Κ.

Απάτη με υπολογιστή στοιχειοθετείται επομένως και όταν με την πράξη βλάπτεται η περιουσία απεριόριστου αριθμού προσώπων, τα οποία δεν είναι απαραίτητο να είναι γνωστά.[133] Αυτό έχει σημασία για την αιτιολόγηση της καταδικαστικής απόφασης, αφού δεν είναι πρακτικά δυνατό να προσδιορίζονται σε αυτή τα άπειρα πρόσωπα που υπέστησαν αυτοτελώς το καθένα ελάχιστη ζημία, η οποία όμως αντιστοιχεί συνολικά σε σημαντικό περιουσιακό όφελος για το δράστη.

Επομένως η καταδικαστική απόφαση για απάτη με υπολογιστή (386Α Π.Κ) δεν πάσχει από έλλειψη αιτιολογίας αν δεν αναφέρει το πρόσωπο του παθόντος, όπως απαιτείται ως προς την κοινή απάτη του άρθρου 386 Π.Κ.

5.3. Υποκειμενική υπόσταση

Η απάτη με υπολογιστή είναι έγκλημα σκοπού.[134] Για την θεμελίωση του αρχικού αδίκου πέραν της πλήρωσης των στοιχείων της αντικειμενικής υποστάσεως προαπαιτείται σκοπός του δράστη να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος. Απαιτείται δηλαδή «επιδίωξη» (άμεσος δόλος Α΄ βαθμού) ως προς το περιουσιακό όφελος για το οποίο ο δράστης τελεί την πράξη, ενώ ως προς τα πραγματικά περιστατικά που θεμελιώνουν το «παράνομο» του περιουσιακού οφέλους, αρκεί και ενδεχόμενος δόλος (γ' είδος δόλου).

Ενδεχόμενος δόλος αρκεί και ως προς τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος. Αρκεί για παράδειγμα ο

[133] Έτσι και *Κιούπης*, οπ. παρ., 62.

[134] Αυτό πρακτικά σημαίνει ότι ο δόλος σκοπού που εμφαίνεται στο σκοπό παράνομης ιδιοποίησης αποτελεί υποκειμενικό στοιχείο του αδίκου και αναφέρεται στην αντικειμενική υπόσταση του εν λόγω εγκλήματος. Αν ελλείπει, δεν μπορεί να υπάρχει τέλεση κατά φυσική αυτουργία από τον συγκεκριμένο δράστη.

δράστης να προβλέπει ως ενδεχόμενη την πρόκληση περιουσιακής ζημίας και να την αποδέχεται.[135]

5.3.1. Ποινικές κυρώσεις

Σύμφωνα με όσα προβλέπονται στο πρώτο εδάφιο του άρθρου 386Α Π.Κ η απάτη με υπολογιστή «τιμωρείται με τις ποινές του προηγούμενου άρθρου» δηλαδή της απάτης (άρθρο 386 Π.Κ).

Άρα η βασική απάτη με υπολογιστή τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών (και άρα υπάγεται στην καθ ύλη αρμοδιότητα του τριμελούς πλημμελειοδικείου κατά το άρθρο 112 Κ.Π.Δ), ενώ επιβάλλεται φυλάκιση τουλάχιστον δύο ετών αν η ζημία που προκλήθηκε από την πράξη είναι ιδιαίτερα μεγάλη.[136]

Αν όμως ο δράστης τελεί απάτες με υπολογιστή κατ επάγγελμα ή κατά συνήθεια[137] και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των 15.000 € (ευρώ) ή αν το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν συνολικά τα 73.000 € (ευρώ), επιβάλλεται κάθειρξη μέχρι δέκα ετών (ποινική δίωξη σε βαθμό κακουργήματος και άρα διακεκριμένη παραλλαγή αφού τιμωρείται βαρύτερα).[138]

Αξιοσημείωτο είναι εδώ ότι ως προς την απάτη με υπολογιστή δεν χωρεί εφαρμογή του Ν.1608/1950[139] διότι η απαρίθμηση των εγκλημάτων στα οποία αυτός εφαρμόζεται είναι περιοριστική[140] και η

---

[135] Έτσι και *Φ.Ανδρέου,* Ερμηνεία Ποινικού Κώδικα Ειδικό Μέρος, Α.Σάκκουλας Αθήνα 2005, άρθρο 386[α] Π.Κ. Όμοια *Κονταξή* και *Μυλωνόπουλου,* Ποινικό Δίκαιο Ειδικό Μέρος Π.Ν Σάκκουλας Αθήνα 2000 σελ 556 επ.

[136] Αρμόδιο για τον προσδιορισμό της ιδιαίτερα μεγάλης ζημίας είναι το πρωτοβάθμιο δικαστήριο χωρίς περαιτέρω δυνατότητα αναιρετικού ελέγχου.

[137] Πρόκειται για περίπτωση αθροιστικού εγκλήματος. Για το κατ' επάγγελμα και κατά συνήθεια τέλεση βλ. άρθρο 13 εδ.στ Π.Κ.

[138] Όπως ισχύει μετά το Ν.2721/1999.

[139] Τίτλος « *περί αυξήσεως των ποινών των προβλεπομένων δια τους καταχραστάς του δημοσίου*» Ν.1608/50.

[140] 1. Στον ένοχο των αδικημάτων που προβλέπονται στα άρθρ. 216, 218, 235, 236, 237, 242, (256), 258, 372, 375 και 386 του Ποινικού Κώδικα, εφόσον αυτά στρέφονται κατά του Δημοσίου

τυχόν εφαρμογή του θα συνιστούσε απαγορευμένη αναλογία εις βάρος του κατηγορουμένου.[141]

Η παράλειψη αυτή του νομοθέτη οφείλεται σε προφανή παραδρομή διότι η δυνάμενη να προκληθεί από το έγκλημα (απάτη με υπολογιστή 386^{A} Π.Κ) ζημία μπορεί να φτάσει σε δυσθεώρητα ύψη. Ευνόητο είναι ότι η μη κάλυψη του ζητήματος αυτού είναι μια πρόσθετη ένδειξη ότι υπήρξαν αβλεψίες και ατέλειες από το νομοθέτη κατά τη ψήφιση του νόμου με τον οποίο εισήχθη στο δίκαιό μας η απάτη με υπολογιστή.

5. 3.2 Προνομιούχες περιπτώσεις απάτης με υπολογιστή

Οι διατάξεις των άρθρων 387 Π.Κ (απάτη ευτελούς αξίας) και 393 παρ 1 Π.Κ (δίωξη κατ΄έγκληση σε περίπτωση απάτης μεταξύ συγγενών κατά τα στοιχεία α΄και γ΄ του άρθρου 378 Π.Κ και εξάλειψη του αξιοποίνου λόγω έμπρακτης μετάνοιας κατά άρθρο 379 Π.Κ) εφαρμόζονται σύμφωνα με την ορθότερη και κρατούσα στη θεωρία άποψη[142] και εδώ κατ΄αναλογία in bonam partem διότι η παράλειψη των σχετικών διατάξεων να ρυθμίσουν το άρθρο 386^{α} Π.Κ

ή των νομικών προσώπων δημοσίου δικαίου ή κατά άλλου νομικού προσώπου από εκείνα που αναφέρονται στο άρθρ. 263Α του Ποινικού Κώδικα και το όφελος που πέτυχε ή επιδίωξε ο δράστης ή η ζημία που προξενήθηκε ή οπωσδήποτε απειλήθηκε στο Δημόσιο ή στα πιο πάνω νομικά πρόσωπα υπερβαίνει το ποσό των "50.000.000" δραχμών, επιβάλλεται η ποινή της κάθειρξης και, αν συντρέχουν ιδιαζόντως ιδιάζοντος επιβαρυντικές περιστάσεις, ιδίως αν ο ένοχος εξακολούθησε επί μακρό χρόνο την εκτέλεση του εγκλήματος ή το αντικείμενό του είναι ιδιαίτερα μεγάλης αξίας, επιβάλλεται η ποινή της ισόβιας κάθειρξης". "Στον ένοχο του αδικήματος που προβλέπεται ειδικώς από το άρθρ. 256 του Ποινικού Κώδικα, τα παραπάνω εφαρμόζονται μόνο όταν το αδίκημα στρέφεται κατά του Δημοσίου, των οργανισμών τοπικής αυτοδιοίκησης και των νομικών προσώπων δημοσίου δικαίου".

[141] Βλ. ΑΠ 1152/1999, ΠΝΑΠ 99 ,352 ΠΧ Ν/597.,1270/93 ΠοινΧρ ΜΓ΄1026.

[142] *Μυλωνόπουλου* σελ 559 επ. αλλά και *Δ. Σπινέλλης* Ποινικό Δίκαιο Ειδικό Μέρος εγκλήματα κατά περιουσιακών εννόμων αγαθών. Α Σάκκουλας Αθήνα –Κομοτηνή 1992.

δεν οφείλεται σε συνειδητή επιλογή του νομοθέτη αλλά σε παραδρομή.[143]

Έτσι αν η συνολική ζημία που προκλήθηκε από την απάτη με υπολογιστή είναι ευτελούς αξίας, η πράξη διώκεται μόνο κατ' έγκλιση και τιμωρείται με χρηματική ποινή ή με φυλάκιση από δέκα μέρες μέχρι έξι μήνες. Αν μάλιστα η πράξη τελέστηκε από ανάγκη για άμεση ανάλωση, η οποία δεν εμπίπτει στις περιπτώσεις της κατάστασης ανάγκης της Π.Κ 25, η πράξη μπορεί να μείνει ατιμώρητη (αρθρ 387 σε συνδ με 377 Π.Κ)[144]

Εννοείται ότι η διάταξη του άρθρου 377Π.Κ δεν εφαρμόζεται αν η συνολική ζημία που προκλήθηκε από τη μία πράξη δεν είναι ευτελής, έστω και αν η βλάβη των επί μέρους προσώπων είναι μηδαμινή.

Κατ' έγκλιση διώκεται η απάτη με υπολογιστή (χωρίς όμως να τιμωρείται ηπιότερα) και όταν τελείται κατά προσώπου από τα αναφερόμενα ως θύματα της απάτης. Έτσι για παράδειγμα κατά την κρατούσα στη νομολογία άποψη η απόπειρα κακουργηματικής απάτης με υπολογιστή απορροφάται από την κακουργηματική πλαστογραφία με χρήση, ενώ η τετελεσμένη συρρέει με αυτήν αληθινά.[145]

5. 3. 3 Κατ' εξακολούθηση τέλεση

[143] Σύμφωνος ο*Παπαδαμάκης*, 194 , αλλά και ΑΠ 1059/1995, ΠΧ ΜΣΤ/97 , που εμμέσως πλήν σαφώς δέχεται δυνατότητα εφαρμογής του άρθρου 379 Π.Κ στην απάτη με υπολογιστή εφόσον ο ισχυρισμός για έμπρακτη μετάνοια δεν είναι αόριστος.

[144] Βλ το παράδειγμα του *Μυλωνόπουλου* Ποινικό Δίκαιο Ειδικό μέρος σελ 560 Ο ενδεής φοιτητής πληροφορικής Α διεισδύει στο πρόγραμμα μιας τράπεζας και εγγράφει στο λογαριασμό του 1500 δρχ. με τις οποίες εξασφαλίζει το μεσημεριανό του γεύμα.

[145] ΑΠ 75/1999, ΠΧ ΜΘ/319, ΑΠ329/1988, ΠΧ ΜΗ/975, ΑΠ 1300/1997, ΠΧ ΜΗ/468, ΑΠ 292/1990, ΠΧ Μ/1038, ΑΠ 912/1980,ΠΧ ΛΑ/49, ΑΠ 1017/1980, ΠΧ ΛΛ/158, ΑΠ 1300/1997, ΠΧ ΜΗ/468, ΑΠ 1819/1997, ΠΧ ΜΗ/607, ΑΠ 100/1983, ΠΧ ΛΓ/713, ΑΠ 1444/1983, ΠΧ ΛΔ/421, ΑΠ 1292/1984, NoB 32,1781, ΑΠ 552/1989, ΠΧ Μ/47, ΑΠ 1706/1988, ΠΧ Μ/829, ΑΠ 57/1998, ΠΧ ΜΗ/730, ΑΠ329/1988, ΠΧ ΜΗ/975.

Σε περίπτωση κατ' εξακολούθηση τέλεσης, το περιουσιακό όφελος ή η περιουσιακή βλάβη λαμβάνονται συνολικά υπόψη μόνον αν ο δράστης με τις μερικότερες πράξεις του απέβλεπε στο αποτέλεσμα αυτό(αρθρ. 98 παρ.2 που προστέθηκε με το άρθρο 14 Ν.2721/1999). Η εφαρμογή της εν λόγω διάταξης δεν εμποδίζεται από εκείνη του τρίτου εδαφίου του άρθρου 386ΑΠ.Κ διότι αυτή η τελευταία αναφέρεται σε πρόκληση ζημίας με μία πράξη και όχι με πλείονες.[146]

5.4 Απάτη με Η/Υ386Α Π.Κ και απάτη του άρθρου 386 Π.Κ μέσω υπολογιστή

5.4.1 Οι απόψεις που υποστηρίζονται ως προς τα βασικά ζητήματα:

Το αξιόποινο αποτέλεσμα που τιμωρείται ρητά από το άρθρο 386Α Π.Κ είναι η βλάβη ξένης περιουσίας. Και για το λόγο αυτό οι μέχρι σήμερα διατυπωμένες απόψεις θεωρούν ότι προστατευόμενο έννομο αγαθό σε αυτή τη διάταξη είναι μόνο η περιουσία.[147] Ωστόσο, έχουν διατυπωθεί και απόψεις που μιλούν για προστασία, δευτερευόντως ή επικουρικώς, και άλλων έννομων αγαθών, όπως τα συστήματα συναλλαγών χωρίς μετρητά χρήματα ή η εμπιστοσύνη στην ασφάλεια και αξιοπιστία της μεταφοράς κεφαλαίων μέσω της επεξεργασίας δεδομένων.

---

[146] Βλ. *Μυλωνόπουλο* οπ.παρ σελ 560 .

[147] Βλ. για το ελληνικό Δίκαιο, *Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, 1993, 201 επ., *Μυλωνόπουλου*, Ηλεκτρονικοί υπολογιστές και ποινικό δίκαιο ο.π σελ 59, *Παπαδαμάκη*, σελ 184, *Νούσκαλη*, όπ. παρ., 180 επ. Για το γερμανικό δίκαιο βλ. *Schoencke/ Schroeder- Cramer*, StGB, 25, 1997, §263A αριθ 27, *Lackner/Koehl*, StGB,23 , 1999§263a, αριθ. 25, *Sieber*, Computerkriminalitaet im Strafrecht, 2, 1980, σελ. 32. Για το Ολλανδικό Δίκαιο, βλ. *Kleve/Mudler*, Computer and law in the Netherlands, Revue europeene de droit public, 1991, σελ. 11 επ. Για το ελβετικό δίκαιο βλ. *Schubarth/Albrecht*, Kommentar zum schweizerischen Strafrecht. Schweizerisches Strafgesetzbuch, B.T.2.

Η άποψη που επικρατεί όμως δέχεται ότι στην απάτη με Η/Υ προστατευόμενο έννομο αγαθό είναι η περιουσία και ότι η απάτη με υπολογιστή δομήθηκε ως έγκλημα κατ΄αντιστοιχία με την απάτη του άρθρου 386 Π.Κ. Συνεπώς θα πρέπει να μεταφερθούν στη διάταξη του άρθρου 386Α Π.Κ όλα τα θεωρούμενα ως απαραίτητα στοιχεία της πράξης της απάτης του άρθρου 386 Π.Κ.[148] Πράγματι σύμφωνα με την εισηγητική έκθεση του νόμου 1805/1988, αλλά και του γερμανικού δεύτερου νόμου για την καταπολέμηση της ηλεκτρονικής εγκληματικότητας, η απάτη με Η/Υ θεσπίστηκε για να καλύψει τα κενά νόμου που υπήρχαν (δευτερογενή κενά) και εμπόδιζαν την εφαρμογή της διάταξης της απάτης.[149] Ο όρος «επηρεασμός των στοιχείων» ερμηνεύεται ως το αποτέλεσμα μιας ηλεκτρονικής επεξεργασίας δεδομένων το οποίο αποκλίνει από εκείνο που θα προερχόταν από την κανονική και σύννομη εκτέλεση του προγράμματος, κατ΄αντιστοιχία προς την παραπλάνηση ανθρώπου και την περιουσιακή διάθεση στην απάτη, οι οποίες ταυτίζονται με τον «επηρεασμό των στοιχείων».[150] Σύμφωνα πάντα με την ίδια άποψη θα πρέπει η βλάβη της περιουσίας να επέρχεται άμεσα ως αποτέλεσμα του «επηρεασμού» των στοιχείων του υπολογιστή, ήτοι την «παραπλανητική κατάσταση», η οποία οδηγεί σε μία περιουσιακή διάθεση σε αντιστοιχία με την απάτη του άρθρου 386 Π.Κ.[151] Οι παραπάνω αποδοχές έχουν οδηγήσει τη θεωρία να καταλήξει στο συμπέρασμα ότι παρόλο τον παραλληλισμό απάτης και απάτης με

[148] Βλ. *Μυλωνόπουλο*, όπ. παρ. 56 , *Παπαδαμάκη*, όπ. παρ 182. Από τους θεωρητικούς του γερμανικού ποινικού δικαίου Βλ *Cramer* σε: Schoenke/Scroeder, Kommentar , σελ 1881 , αριθ 2 και σελ 1886 αριθ 21, Maurach/Scroeder/Maiwald, Strafrecht, σελ 490 αριθ 228.

[149] Βλ. *Νούσκαλη*, όπ. παρ. 180 επ. *Μυλωνόπουλο*, όπ. παρ. 58.

[150] Βλ. *Μυλωνόπουλο* όπ. παρ., *Παπαδαμάκη*, Τα περιουσιακά εγκλήματα σελ 185.

[151] Βλ. *Νούσκαλη* οπ. παρ. 180, *Βασιλάκη* οπ. παρ. σελ 217, *Καϊάφα-Γκπάντι*, Παρατηρήσεις στην ΑΠ 1277/1998 Υπερ 1999, 912 Contra *Κουράκη*, Παρατηρήσεις στην νομολογία σχετικά με την απάτη με Η/Υ , Πλογ 6/2001, 2593, ο οποίος θεωρεί ότι δεν είναι αναγκαίος ο συσχετισμός οφέλους και βλάβης ξένης περιουσίας.

Η/Υ, υπάρχει σχέση αλληλοαποκλεισμού[152] μεταξύ των δύο αυτών διατάξεων και ότι η απάτη με Η/Υ αποτελεί ιδιώνυμο έγκλημα.[153]

Στο μέτρο δε που η επίδραση στα στοιχεία υπολογιστή αντιστοιχεί στην «παραπλάνηση», αναγκαστικά δέχεται η παραπάνω άποψη ότι και οι τρόποι επίδρασης των στοιχείων υπολογιστή που τυποποιεί ο νομοθέτης θα πρέπει να προκαλούν μία κατάσταση αντίστοιχη με εκείνη της εξαπάτησης ανθρώπου στην απάτη του άρθρου 386 Π.Κ.[154]

Η διαμόρφωση του προγράμματος θεωρείται «μη ορθή» όταν τα αποτελέσματα που προκύπτουν από την εφαρμογή του έρχονται σε αντίθεση με μία νόμιμη κατάσταση[155] ή όταν το πρόγραμμα είναι πρόσφορο να επιφέρει περιουσιακή βλάβη.[156] Η «επέμβαση κατά την εφαρμογή του προγράμματος» νοείται ως μεταβολή στη λειτουργία του προγράμματος.[157] Η «χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων» παραλληλίζεται τέλος προς την απόκρυψη και την παρασιώπηση αληθών γεγονότων κατά το άρθρο 386 Π.Κ. Ως συνέπεια αυτού του παραλληλισμού, ως «μη ορθά» θεωρούνται τα στοιχεία που δεν ανταποκρίνονται προς την πραγματικότητα και ως «ελλιπή» εκείνα που ανταποκρίνονται εν μέρει προς αυτήν[158] , ώστε η τελική εντύπωση που προκαλείται από τη χρήση τους να είναι διαφορετική από την πραγματικότητα. Σχετικά δε με τον «επηρεασμό» των στοιχείων του υπολογιστή με «οποιοδήποτε άλλο τρόπο» η παραπάνω άποψη δέχεται ότι αποκλείονται οι περιπτώσεις που δεν δημιουργούν μία κατάσταση αντίστοιχη προς την παραπλάνηση ανθρώπου, όπως αυτό συμβαίνει στο άρθρο 386 Π.Κ.[159]

---

[152] Βλ. *Βασιλάκη*, οπ.παρ. 217, *Καϊάφα-Γκπάντι*, οπ.παρ.σημ 146.
[153] Βλ. *Κουράκη*, οπ.παρ. σελ 2591, *Παπαδαμάκη*, οπ.παρ σελ 186.
[154] Βλ. *Βασιλάκη*, οπ.παρ σελ 214.
[155] Βλ. *Νούσκαλη*, οπ.παρ 180. *Βασιλάκη*, οπ.παρ 214.
[156] Βλ *Μυλωνόπουλου,(Ηλεκτρονικοί υπολογιστές)* σελ 59-62, *Παπαδαμάκη* ο.π.σελ 187.
[157] Βλ. *Μυλωνόπουλου*, οπ.παρ σελ 63.
[158] Βλ. *Μυλωνόπουλου*, οπ.παρ σελ 64, *Βασιλάκη* οπ.παρ σελ 205, *Παπαδαμάκη*, οπ.παρ σελ 188.
[159] Βλ. *Μυλωνόπουλου*, οπ.παρ σελ 57 , *Βασιλάκη* οπ.παρ. σελ 214.

Ως απόρροια των ανωτέρω, θα πρέπει, να αποκλείονται από το πεδίο εφαρμογής του 386Α Π.Κ πράξεις που αποτελούν εκμετάλλευση[160] απλώς των δυνατοτήτων της νέας τεχνολογίας, χωρίς να ασκούν καμία επίδραση στα στοιχεία του υπολογιστή και πράξεις που συνιστούν «ετεροπροσβολή» της περιουσίας και όχι «αυτοπροσβολή»του εννόμου αγαθού από τον φορέα του όπως στην κλασική απάτη.[161]

5.4.2 Η θέση της ελληνικής νομολογίας.

Στην ελληνική νομολογία, τόσο των δικαστηρίων της ουσίας όσο και του Άρειου Πάγου, επιχειρήθηκε σχετικά πρόσφατα ο καθορισμός των ορίων μεταξύ απάτης και απάτης με Η/Υ. Το Εφετείο Αθηνών το 1998, δέχτηκε την ταύτιση του περιεχομένου των δύο διατάξεων, εκτός του τρόπου βλάβης της ξένης περιουσίας, η οποία στην απάτη με υπολογιστή δεν προκαλείται από εξαπάτηση φυσικού προσώπου αλλά από την «επέμβαση σε Η/Υ».[162] Κατά τα ανωτέρω, το Δικαστήριο θεώρησε την απάτη με Η/Υ ειδική μορφή απάτης και δέχτηκε την πραγμάτωση των όρων αυτής, ακόμη και όταν «οι αθέμιτες επεμβάσεις στον Η/Υ είναι το αναγκαίο μέσο για την πραγματοποίηση του σκοπού αυτού». Η περίπτωση που κρίθηκε από

---

[160] Βλ. *Παπαδαμάκη*, οπ.παρ σελ 190. Διαφοροποιημένη είναι η άποψη του *Κουράκη* οπ.παρ 2593. Η γερμανική νομολογία πάντως φαίνεται να προσανατολίζεται τελευταία όλο και περισσότερο στην ιδέα ότι πράξεις που «θέτουν σε κίνηση» την επεξεργασία δεδομένων είναι δυνατόν να θεωρηθεί ότι «επηρεάζουν» την ηλεκτρονική επεξεργασία δεδομένων και το εξαυτής παραγόμενο αποτέλεσμα. Πρόσφατα παραδείγματα γι αυτό αποτελούν οι περιπτώσεις της χρήσης εξομειωτών τηλεφωνικών καρτας («Telefonkartensimulationen" στην απόφαση LG Wuerzburg Urteil v. 29.7.1999, Wistra 1999.429) και της επίδρασης ηλεκτρονικού παιχνιδιού μέσω παρανόμως κτηθέντος σχετικού προγράμματος Η/Υ, ώστε το συγκεκριμένο παιχνίδι να αποδώσει κέρδη σε συγκεκριμένη χρονική στιγμή(BGH Beshcluss v.10.11.1994,wistra 1995.105). Κρίθηκε πάντως ότι δεν συνιστά απάτη με υπολογιστή το «ξεγέλασμα» μηχανήματος που αλλάζει χαρτονομίσματα με κέρματα από το δράστη ο οποίος έθεσε στο μηχάνημα αυτό μια ειδική ταινία αντί για χαρτονόμισμα, την οποία και ξαναπήρε πίσω όταν πήρε τα κέρματα χωρίς να βάλει κάποιο χαρτονόμισμα στη θέση τους. (OLG Duesseldorf 29.6.1999, Wistra 1999.471).

[161] Βλ. .*Νούσκαλη* οπ.παρ 181, *Βασιλάκη* οπ.παρ σελ 215-216.

[162] ΠεντΕφΑθ 751/1998 ΠοινΔικ 1999.817.

το Δικαστήριο ως απάτη με Η/Υ αφορούσε την πράξη κάποιου ο οποίος, αφού ενέγραψε στη μνήμη του Η/Υ ανύπαρκτες καταθέσεις σε υπαρκτό λογαριασμό τρίτου, εμφάνισε προς πληρωμή στον ταμία της τράπεζας επιταγή με χρέωση του ανωτέρω λογαριασμού και σε συνεννόηση με τον κάτοχο του λογαριασμού.

Ο Άρειος Πάγος το 1995 έκρινε ως απάτη με Η/Υ την περίπτωση εκείνων που καταχωρούσαν στη μνήμη Η/Υ ανύπαρκτες μισθολογικές αποδοχές από την υπηρεσία τους και στη συνέχεια εισέπρατταν τα ποσά αυτά.[163] Στην περίπτωση αυτή το Δικαστήριο δεν διατύπωσε κάποια ιδιαίτερη αιτιολογία για την υπαγωγή των κρινόμενων περιστατικών στην απάτη με Η/Υ ούτε και κατέστησε σαφές εάν η είσπραξη του μη δικαιούμενου ποσού έγινε με ή χωρίς την παρεμβολή ανθρώπινου παράγοντα. Το 1998 ο Άρειος Πάγος δέχθηκε ότι η απάτη με Η/Υ είναι «διαφορετικό έγκλημα» από την απάτη που αποτελεί «ειδικό έγκλημα»[164] Το Δικαστήριο διαχώρισε την απάτη με Η/Υ με τη βασική σκέψη ότι «το άρθρο 386 Π.Κ περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση φυσικού προσώπου, ενώ στο άρθρο 386Α Π.Κ η ξένη περιουσία βλάπτεται, ασχέτως παραπλανήσεως, με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή».

Έτσι λοιπόν, σύμφωνα με την ανωτέρω απόφαση, όποτε συνυπάρχουν στα πραγματικά περιστατικά τόσο η πράξη επέμβασης «στη μνήμη ηλεκτρονικού υπολογιστή» όσο και η παράσταση ψευδών περιστατικών σε τρίτους, τότε θα πρέπει να γίνει σαφής διάκριση εάν

[163] ΑΠ 1059/1995, ΠοινΧρ 1996, 97.Βλ. και παράρτημα νομοθετικών κειμένων στο τέλος.
[164] ΑΠ 1277/1998 Υπερ 1999,912 (παρατ. *Καϊάφα-Γκπάντι*)

καταφάσκεται η απάτη με Η/Υ ή η απάτη του άρθρου 386 Π.Κ.[165] Κατά τα ανωτέρω, το Δικαστήριο αναίρεσε την προσβαλλόμενη απόφαση της ουσίας για το λόγο ότι δεν περιείχε σαφείς αιτιολογίες περί τη μορφή της απάτης που τέλεσε ο δράστης (άρθρο 510 στοιχ δ΄ Κ.Π.Δ) ο οποίος συνέδεσε στη μνήμη Η/Υ τον αριθμό πλαστογραφημένων επιταγών με υπαρκτό λογαριασμό όψεως και στη συνέχεια εισέπραξε χωρίς να δικαιούται χρηματικά ποσά από τον ανωτέρω λογαριασμό, εμφανίζοντας στον ταμία της τράπεζας τις σχετικές επιταγές.

Το 1999 Ο Άρειος Πάγος[166] έκανε και πάλι αποδεκτή τη θεώρηση της απάτης με υπολογιστή ως εγκλήματος διαφορετικού από την απάτη του άρθρου 386 Π.Κ. Τόνισε όμως ότι το έγκλημα του άρθρου 386Α Π.Κ τελείται «αποκλειστικά και μόνο με τον επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του συστήματος και την επεξεργασία δεδομένων σε οποιαδήποτε φάση της λειτουργίας του υπολογιστή» και όχι «με την παραπλάνηση ενός φυσικού προσώπου που είναι αρμόδιο να λαμβάνει αποφάσεις ή να διενεργεί έλεγχο ή να εγκρίνει ή να χορηγεί κλπ» «...Όταν όμως, χωρίς να γίνεται επέμβαση στη διαμόρφωση του προγράμματος ή στην εφαρμογή του, χρησιμοποιείται ο υπολογιστής ως μέσο ή όργανο με την πληκτρολόγηση αναληθών ποσών και παραπλανάται με τον τρόπο αυτό τρίτος που προβαίνει σε πράξη, παράλειψη ή ανοχή η οποία επιφέρει την περιουσιακή βλάβη, τότε στοιχειοθετείται κοινή απάτη του άρθρου 386Α Π.Κ».

---

[165] Ο *Κουράκη*, ο.π.παρ. σελ 2595, θεωρεί ότι , σε περίπτωση αμφιβολίας περί την ύπαρξη φυσικού προσώπου που παρεμβάλλεται και ελέγχει το αποτέλεσμα επεξεργασίας των δεδομένων Η/Υ, θα πρέπει να εφαρμόζεται το άρθρο 386 Α Π.Κ.

[166] ΑΠ 1152/1999 ΠοινΔικ 2000,141.

Με βάση τις ανωτέρω σκέψεις ο Άρειος Πάγος αναίρεσε την απόφαση του Εφετείου Αθηνών του 1998 (ΠεντΕφΑθ 751/1998), η οποία προαναφέρθηκε, για έλλειψη αιτιολογίας (άρθρο 510 στοιχ δ Κ.Π.Δ) αφού δέχθηκε ότι η συνδρομή τόσο της επέμβασης στα στοιχεία υπολογιστή όσο και η παραπλάνηση φυσικού προσώπου που προβαίνει σε περιουσιακή διάθεση επιβάλλουν τον σαφή διαχωρισμό μεταξύ απάτης και απάτης με υπολογιστή.[167]

Ενδιαφέρουσα επίσης παρουσιάζεται η εισαγγελική πρόταση προς το συμβούλιο πλημμελειοδικών Αθηνών 4742/2004[168], η οποία καίτοι δεν κατέληξε σε παραπεμπτικό βούλευμα αναφέρεται με βάση τα πραγματικά της περιστατικά στην παγίδευση μηχανήματος αυτόματης τραπεζικής ανάληψης (ΑΤΜ) τράπεζας με μηχάνημα που διάβαζε τον μυστικό αριθμό των καρτών και μηχάνημα αντιγραφής μαγνητικού πεδίου κάρτας με αποτέλεσμα να μπορεί να προβαίνει σε αναλήψεις ποσών από τους λογαριασμούς των χρηστών του συγκεκριμένου μηχανήματος.

Με βάση το σκεπτικό της παραπεμπτικής διάταξης λοιπόν ο δράστης που χρησιμοποιεί ξένη κάρτα αυτόματης συναλλαγής στα ΑΤΜ παριστά ψευδώς ότι είναι αφενός νόμιμος κάτοχος της κάρτας[169] και αφετέρου δικαιούχος του συνδεδεμένου με αυτή λογαριασμού. Με την ενέργεια αυτή ο δράστης επιδιώκει να παραπλανήσει την τράπεζα αφενός ως προς το εξωτερικό γεγονός της νομιμοποίησής του για

[167] Σημαντική απόφαση κατά τη γνώμη του γράφοντος και η ΑΠ 201/2205 NoB 2005/53, 1482 σύμφωνα με την περίληψη της οποίας: Αν μετά την υπεξαίρεση ο δράστης προς συγκάλυψή της ή διατήρηση της κατοχής του υπεξαιρεθέντος τελέσει απάτη με υπολογιστή υπάρχει φαινόμενη συρροή υπεξαιρέσεως και μη τιμωρητής μεταγενέστερης πράξης απάτης, εκτός αν η δεύτερη είναι βαρύτερη της πρώτης, οπότε απορροφά την υπεξαίρεση. Στην προκειμένη περίπτωση (ΤριμΕφΚαουργ. 37/2002) το Δικαστήριο δέχθηκε ότι: «Όταν η απάτη τιμωρείται σε βαθμό κακουργήματος και η υπεξαίρεση σε βαθμό πλημμελήματος τότε η απάτη απορροφά την υπεξαίρεση διότι η απαξία της τελευταίας υπολείπεται της απαξίας της πρώτης .»

[168] ΣυμβΠλημΑθ 4742/2004 σε ΠοινΔικ 2005/407 (Τράπεζα νομικών πληροφοριών INTRACOM-ΝΟΜΟΣ)

[169] Όχι όμως και κύριος καθώς η κάρτα ανήκει στην εκδότρια τράπεζα, βλ. και τον όρο «εκδότη κάρτας» στον Κώδικα Τραπεζικής Δεοντολογίας.

πραγματοποίηση συναλλαγών με τη χρήση της κάρτας και αφετέρου ως προς το εσωτερικό γεγονός της ετοιμότητάς του να ισοφαρίσει την υλοποιούμενη ανάληψη χρημάτων με μια αντίστοιχη μείωση των απαιτήσεών του (ως δήθεν δικαιούχος του συνδεδεμένου λογαριασμού) έναντι της τράπεζας. Η συμπεριφορά αυτή του δράστη περιέχει «πράξη εξαπάτησης», η οποία πραγματοποιείται με μια συναγόμενη παράσταση με βάση την οποία η τράπεζα θα πρέπει να δεχθεί ένα γεγονός. Αντίστοιχη σκέψη μπορεί να γίνει και σε περίπτωση όπου επιδιώκεται η άνευ δικαιώματος πραγματοποίηση συναλλαγής σε ΑΤΜ με πλαστή κάρτα που επιχειρεί να παραπλανήσει την τράπεζα, τόσο ως προς τη γνησιότητα της κάρτας, όσο και ως προς τη νομιμοποίησή του για την πραγματοποίηση της συναλλαγής. Αυτές οι παραστάσεις (σιωπηρώς-συμπερασματικώς συναγόμενες-ανακοινώσεις του χρήστη ΑΤΜ) Θα μπορούσαν να αντιμετωπισθούν ως πράξεις εξαπάτησης τότε μόνο, εφόσον δια της επιδράσεως τους στη συνείδηση κάποιου άλλου ανθρώπου θα μπορούσε να προκληθεί πλάνη.

Η πρόκληση πλάνης όμως στο ΑΤΜ είναι αδιανόητη, το ίδιο και η διατήρησή της. Και αυτό διότι η συσκευή δεν έχει συνείδηση δεν σχηματίζει παράσταση επί της οποίας θα μπορούσε κανείς να επενεργήσει ή να διατηρήσει καθώς τα μηχανήματα ΑΤΜ απλώς μεταθέτουν και προωθούν δεδομένα κατά τρόπο αυτοματοποιημένο σε μια επόμενη φάση της διαδικασίας επεξεργασίας αυτών, βάσει προκαθορισμένων και ενσωματωμένων στο μηχάνημα εντολών. Οι εντολές αυτές έχουν βεβαίως δοθεί από φυσικά πρόσωπα, τα οποία όμως δεν είναι σωματικώς παρόντα κατά το χρόνο επεξεργασίας των εισαγόμενων στο μηχάνημα δεδομένων.

Για το πρόβλημα αυτό υποστηρίχθηκε μεμονωμένα στην γερμανική θεωρία[170] ότι στο μέτρο που η τράπεζα προβαίνει σε ένα γνήσιο επιμερισμό εργασίας με τον υπολογιστή, στο μέτρο δηλαδή που «εξουσιοδοτεί» τον υπολογιστή να διεκπεραιώνει αλλεπάλληλες εργασίες κάθε φορά που πληρούνται οι εκάστοτε προαπαιτούμενες προϋποθέσεις, οποιαδήποτε εξαπάτηση του υπολογιστή συνεφέλκεται μια αναγκαία πρόκληση πλάνης στο φυσικό πρόσωπο του εξουσιοδοτούμενου με τον έλεγχο των εγγράφων υπαλλήλου. Η άποψη όμως αυτή δεν μπορεί να γίνει δεκτή καθώς η αποδοχή του μορφώματος προκλήσεως πλάνης σε άνθρωπο διαμέσου του υπολογιστή θα είχε νόημα τότε μόνο εάν η πρόοδος της διαδικασίας ανάληψης ή από την πλευρά της τράπεζας απόδοσης των χρημάτων είχε ως αιτία την προκληθείσα διαμέσου του υπολογιστή πλάνη.

Για να γίνει όμως κάτι τέτοιο θα έπρεπε κάθε φορά που ο πελάτης ζητά την υλοποίηση μιας συναλλαγής να μεσολαβεί ένα νεκρό διάστημα έως ότου τα στοιχεία της συναλλαγής διαβιβαστούν στον αρμόδιο υπάλληλο της τράπεζας που έχει την ικανότητα σχηματισμού παράστασης ως προς αυτά (και κατά τούτο είναι πρόσφορο αντικείμενο παραπλάνησης) και ο οποίος, εγκρίνοντας την αθέμιτη συναλλαγή, προβαίνει σε μια περιουσιακή διάθεση σε βάρος της τράπεζας, ώστε να πληρούται και το τελευταίο στοιχείο της αντικειμενικής υπόστασης της απάτης. Όμως η πλάνη του υπαλλήλου της τράπεζας που ώρες ή μέρες μετά τη διενέργεια της συναλλαγής ελέγχει το πρωτόκολλο των συναλλαγών που πραγματοποιήθηκαν μέσω του ATM είναι σύμφωνα πάντα με την εισαγγελική διάταξη, κάθε άλλο παρά αιτιώδης της γενόμενης ήδη περιουσιακής διάθεσης και ως εκ τούτου δεν πληρούται το στοιχείο προκλήσεως της πλάνης, διότι ο υπάλληλος δεν αποκτά γνώση των αποτελεσμάτων στα οποία

[170] *Knecht* kriminalistik 1971,467 , *Steinke*, Kriminalistik 1987,74

κατέληξε ο ηλεκτρονικός υπολογιστής, ούτως ώστε η περιουσιακή διάθεση να συνιστά προϊόν ανθρώπινης βούλησης.[171]

Αντίθετα η συμπεριφορά του δράστη κάλλιστα μπορεί να υπαχθεί στην έννοια της απάτης με υπολογιστή.[172]

5.4.3 Η χωρίς δικαίωμα χρήση κωδικών καρτών αυτόματης τραπεζικής ανάληψης

Στη γερμανική θεωρία και νομολογία είχε ανακύψει έντονη αμφισβήτηση ήδη πριν την ψήφιση του άρθρου που αφορά την απάτη με υπολογιστή σχετικά με τη λήψη χρημάτων από μηχάνημα αυτόματης τραπεζικής συναλλαγής ΑΤΜ με τη χρήση ξένης μαγνητικής κωδικής κάρτας και του μυστικού αριθμού της χωρίς εξουσιοδότηση από το δικαιούχο καθ' υπέρβαση του πιστωτικού υπολοίπου της ίδιας κάρτας.[173]

Υπήρξε έντονη διαμάχη γύρω από το θέμα της κατάφασης της κλοπής ή της υπεξαίρεσης για τον τρίτο που χρησιμοποιεί την ξένη μαγνητική κάρτα και τον κωδικό της χωρίς τη συναίνεση του δικαιούχου αλλά και για τον δικαιούχο που υπερβαίνει το πιστωτικό του υπόλοιπο.

---

[171] Βλ. *Θ. Σαμίου*, Παρατηρήσεις στην ΣυμβΠλημΚαστ 196/1999 ΠοινΧρ ΜΘ΄,1061 επ.

[172] Βλ. ΣυμβΝαυτΠειρ 418/1996 Υπερ 1997, 102 επ. Βλ. επίσης *Μυλωνόπουλου*, Ηλεκτρονικοί υπολογιστές και Ποινικό Δίκαιο –Συμβολή στην ερμηνεία των άρθρων 13γ,370Β,370Γκαι 386^{Α} Π.Κ (άρθρο 2-5 Ν 1805/1988), 1991, σελ 66-67, *Βασιλάκη*, Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών-Η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν 1805/1988, σειρά Ποινικά αρ.40 ,1993,σελ 209.

[173] Βλ. *Νούσκαλη*, όπ. παρ με περεταίρω παραπομπές για την αναλυτική παρουσίαση της συζήτησης στο γερμανικό δίκαιο, σελ 182 επ. .

Σχηματίστηκαν τρεις κατευθύνσεις. Η πρώτη[174] δέχτηκε ότι στοιχειοθετείται το έγκλημα της κλοπής και για τις δύο παραπάνω περιπτώσεις. Κατά τη δεύτερη[175] πραγματώνεται το αδίκημα της υπεξαίρεσης, ενώ μια τρίτη άποψη[176] θεώρησε ότι με το ισχύον ποινικό οπλοστάσιο οι παραπάνω συμπεριφορές μένουν ατιμώρητες. Και στη νομολογία εμφανίστηκαν οι παραπάνω απόψεις αλλά μόνο για την περίπτωση τρίτου που χρησιμοποιεί την κάρτα χωρίς τη συναίνεση του δικαιούχου, ενώ για την περίπτωση του νόμιμου χρήστη που υπερβαίνει το πιστωτικό του όριο μόνο οι απόψεις περί κλοπής και υπεξαίρεσης.[177]

Μετά τη θέσπιση της διάταξης περί απάτης με η/υ το 1986 στην Γερμανία (263a StGB) συνεχίστηκαν οι διχογνωμίες που προαναφέρθηκαν αλλά η άποψη που παρουσιάζεται ως μάλλον κρατούσα ως προς την περίπτωση της χρήσης της κάρτας και του μυστικού αριθμού της από τρίτο χωρίς δικαίωμα είναι εκείνη που καταφάσκει απάτη με υπολογιστή,[178] δεχόμενη επίδραση στη ροή της ηλεκτρονικής επεξεργασίας δεδομένων από την αθέμιτη χρήση

[174] Βλ, *Gropp,* Die Codekarte: der Schluessel zum Diebstahl, JZ 1987, σελ. 487 και αυτό σε *Νούσκαλη* οπ.παρ σελ 182.

[175] Βλ. *Kleb-Braun,* Codekartenmissbrauch und Sparbuchfaelle aus Volljuristischer Sicht, JA 1986, 249 σε Νούσκαλη οπ.παρ. 218.

[176] Βλ. οπ.παρ σε *Νούσκαλη* 182 *Lenckner,* Computerkriminalitaet und Vermoegensdelikte 1981, 25, Ahrens, Automatenmissbrauch und Rechtschutz moderner Automatensystemen,1985,100, *Huff,* Die Strafbarkeit im Zusammenhang mit Geldautomaten, NStZ 1985,438, *Steinhilper,* Ist die Bedienung von Bargeldautomaten unter missbrauchlichen Vermendung fremder Codekarten strafbar? GA 1985 ,114.

[177] Βλ. οπ.παρ σε *Νούσκαλη.* Για την περίπτωση της κλοπής όταν η πράξη γίνεται από τρίτο: BayObLG,14.11.1986, Wistra 1987. 108, BayObLG 20.1.1986, Wistra 1987.110 ,StV 1987.204, OLG Koblenz 16.4.1987, Wistra 1987.261, AG Giessen 24.5.1985,NJW 1985.2283. Για τον χαρακτηρισμό της ίδιας πράξης ως υπεξαίρεσης : BGH 16.12.1987 ,NJW 1988.979, OLG Stuttgart 18.12.1986, Wistra 1987.114, LG Oldenburg Urt 1.12.1986, NJW 1987.667, LG Koeln 22.8.1986,NJW 1987.667, AG Hamburg 22.1.1986, NJW 1986.945. Ως προς την άποψη περί ατιμώρητου : BGH, Beschl 16.12.1987, JA 1988.461, OLG Hamburg 7.11.1986 ,Wistra 1987.112, AG Berlin-Tiergarten 18.4.1986,NStZ 1987.122, AG Muenchen, Urt 12.3.1986,Wistra 1986.268. Περι χαρακτηρισμού της πράξης ως κλοπής όταν τελείται από τον δικαιούχο της πιστωτικής κάρτας : LG Karlsruhe 18.3.1985,NStZ 1986.71, AG Berlin-Tiergarten 31.5.1983, Wistra 1984.114. Για τη θεώρηση της πράξης ως υπεξαίρεσης όταν τελείται από το δικαιούχο της κάρτας : OLG Stuttgart 13.12.1983,Wistra 1984.114.

[178] Βλ.*Tiedemann* o.p.869, *Ehrilcher* Der Bankomatenmissbrauch 89, *Bandekow,* Strafbarer Missbrauch 242, *Cramer* in *Schonke/Scrhroder,* StGb 26 Aufl §263 a Rdn, *Maurach/Schroeder/Maiwald,* Strafrecht, Besonderer Teil , T. 1,8 Auf, 1995 ,494

δεδομένων που ανταποκρίνονται στην πραγματικότητα και αφορούν την τυπική νομιμοποίηση του χρήστη της κάρτας. Ο αντίλογος που εκφράστηκε στηρίζεται στο γεγονός ότι από την παραπάνω πράξη δεν επηρεάζεται η ηλεκτρονική επεξεργασία των δεδομένων απλά τίθεται σε λειτουργία και ο δράστης εκμεταλλεύεται παράνομα το παραγόμενο αποτέλεσμα αυτής.

Εάν λοιπόν θεωρηθεί ως επίδραση στη ροή της επεξεργασίας δεδομένων ακόμη και η θέση αυτής σε λειτουργία, τότε έχουμε να κάνουμε με αναλογική ερμηνεία και στην ουσία εξαφάνιση των ορίων της διάταξης. Στο τελευταίο αυτό επιχείρημα δόθηκε απάντηση ότι η θέση σε λειτουργία της ηλεκτρονικής επεξεργασίας των δεδομένων θα μπορούσε να θεωρηθεί ως η πιο έντονη περίπτωση επηρεασμού της και ότι εν πάσει περιπτώσει, το σύστημα της ηλεκτρονικής επεξεργασίας δεδομένων σε αυτές τις περιπτώσεις βρίσκεται ήδη σε λειτουργία και ετοιμότητα χρήσης.

Όσον αφορά δε, στην περίπτωση του νόμιμου χρήστη της κωδικής κάρτας που πραγματοποιεί υπεραναλήψεις χωρίς να δικαιούται αυτές[179], υποστηρίχτηκαν και οι δύο εκδοχές εξίσου ισχυρά. Όσοι υποστηρίζουν την κατάφαση της απάτης με υπολογιστή βασίζουν την άποψή τους ότι και σε αυτή την περίπτωση επηρεάζεται η διαδικασία της ηλεκτρονικής επεξεργασίας δεδομένων και ειδικότερα στο δέον αυτής. Το κύριο επιχείρημα της αντίθετης άποψης συνίσταται στο ότι δεν υφίσταται πυρήνας απατηλής συμπεριφοράς στην πράξη που μας

[179] Αυτό μπορεί να συμβεί είτε με ανάληψη όλου του υπολοίπου ταυτόχρονα με πίστωση του λογαριασμού για αγορά ενός αγαθού, π.χ Αν υποθέσουμε ότι ο Α έχει υπόλοιπο λογαριασμού 1000 ευρώ την 1/1/2007 , το ίδιο βράδυ πλήρώνει με την κάρτα λογαριασμό σε κέντρο διασκέδασης 1000 ευρώ και στις 2/1/2007 κάνει ανάληψη 1000 ευρώ. Πως γίνεται αυτό θα ρωτήσει εύλογα κανείς α) είτε διότι το κατάστημα δεν έστειλε έγκαιρα τον λογαριασμό στην τράπεζα είτε διότι η τράπεζα είναι κλειστή και στο σύστημα η πληρωμή θα καταχωρηθεί τρεις ημέρες μετά οπότε για μικρό χρονικό διάστημα θα φαίνεται πιστωτικό υπόλοιπο στον λογαριασμό. Είτε διότι η τράπεζα έχει χορηγήσει στον δικαιούχο κάρτα υπερανάληψης μετρητών η οποία εύκολα με τους πιο πάνω τρόπους μπορεί να ξεπεράσει το συμφωνημένο όριο μεταξύ τράπεζας και δικαιούχου.

απασχολεί αντίστοιχης προς εκείνη της κλασικής απάτης, αλλά απλά μια αντισυμβατική συμπεριφορά του νόμιμου κατόχου της κάρτας η οποία εάν θεωρούνταν απάτη θα διεύρυνε υπερβολικά το αξιόποινο καθιστώντας τη σχετική διάταξη ελαστικό εργαλείο προς εξυπηρέτηση της ιδιωτικής βούλησης των τραπεζών. Άποψη που βρίσκει απόλυτα σύμφωνο και τον γράφοντα.[180]

Οι αμφισβητήσεις αυτές απασχόλησαν και την νομολογία των γερμανικών δικαστηρίων τόσο σε επίπεδο δικαστηρίων της ουσίας[181] όσο και στο Ανώτατο Ακυρωτικό[182]. Το δικαστήριο αυτό δέχθηκε ότι τελείται απάτη με υπολογιστή και ειδικότερα στον τρόπο τέλεσης που αφορά στην παράνομη χρησιμοποίηση δεδομένων, μόνο όταν η λήψη των χρημάτων γίνεται με χρήση κάρτας από τρίτον[183] και όχι από τον δικαιούχο αλλά με ανάληψη πέραν του επιτρεπόμενου ορίου.[184] Η άποψη αυτή ξεπερνά το επιχείρημα της αντίθετης γνώμης ότι στην περίπτωση αυτή δεν υπάρχει επίδραση στο αποτέλεσμα της ηλεκτρονικής επεξεργασίας των δεδομένων, επειδή δήθεν προϋποτίθεται για την εφαρμογή της διάταξης μία ήδη λειτουργούσα διαδικασία επεξεργασίας, με το να προτείνει ότι επίδραση των στοιχείων του υπολογιστή υπάρχει και όταν κάποιος προκαλεί μια αιτιώδη εξέλιξη με μέσα που τέθηκαν από κάποιον τρίτο με σκοπό

---

[180] Η ίδια προβληματική συναντάται και στο Ελβετικό Ποινικό Δίκαιο, παρά την υπαγωγή του «λογιστικού χρήματος» στην έννοια του κινητού πράγματος, όπου αμφισβητείται έντονα η υπαγωγή της πράξης αυτής στην έννοια της απάτης. Για τη σχετική συζήτηση Βλ. *Schmidt,* Das neueschweizerische Computerstrafrecht vom 17 Juni 1994, Computer und Recht 1996, SchwZStR 1996 ,36 σε Νούσκαλη υποσημείωση 49 οπ.παρ σελ 183.

[181] Βλ. OLG Koeln Urteil v.9.7.1991, με σύμφωνες παρατηρήσεις του Otto, BayObIG 24.6.1993, για την περίπτωση όπου την κωδική κάρτα χρησιμοποιεί τρίτος χωρίς δικαίωμα και όχι για την περίπτωση τρίτου που υπερβαίνει την δοθείσα εξουσιοδότηση ή εκείνου που χρησιμοποιεί αντίγραφο κάρτας, με το επιχείρημα ότι στις τελευταίες αυτές περιπτώσεις δεν υπάρχει πράξη «εξαπάτησης». Όμοια OLG Dusseldorf 5.1.1998 STV 1998,266.

[182] BGH Urt.vom 22.11.1991, JZ 1992.1031, με σύμφωνες παρατηρήσεις Cramer, ο οποίος ωστόσο σημειώνει ότι η αοριστία της διάταξης της απάτης με υπολογιστή μπορεί να θεραπευθεί μόνο εάν αυτή ερμηνευθεί συμπληρωματικά προς την κλασική απάτη.

[183] BGH Beschluss vom 30.01.2001, JurPCWeb-Dok 109/2001 http://www.jurpc.de/rechtspr/2000109.htm

[184] BGH Beschluss vom 21.11.2001, JurPCWeb-Dok 55/2002 1-39 http://www.jurpc.de/rechtspr/2002055.htm

την πρόκληση ενός διαφορετικού αποτελέσματος (την πληρωμή μόνο του νόμιμου χρήστη της κάρτας) από εκείνο που προξενεί ο δράστης. Σε συνάφεια με τα παραπάνω, η ίδια άποψη του γερμανικού Ακυρωτικού υποστηρίζει ότι ο τρόπος τέλεσης που αφορά την παράνομη χρησιμοποίηση δεδομένων δεν προσκρούει στην επιταγή του συντάγματος για το ορισμένο του ποινικού νόμου. Στη συνέχεια απορρίπτει την εφαρμογή της διάταξης για την κλοπή και για τις δύο παραπάνω περιπτώσεις με το βασικό επιχείρημα ότι δεν υπάρχει θραύση της ξένης κατοχής καθώς πληρούνται όλοι οι τυπικοί όροι που έχει θέσει το οικείο τραπεζικό ίδρυμα για να γίνει η πληρωμή.[185]

Την ελληνική θεωρία απασχόλησε το πρόβλημα της χωρίς δικαίωμα χρήσης της κωδικής κάρτας και του κωδικού της αριθμού καθώς και το πρόβλημα της υπέρβασης του πιστωτικού ορίου της κάρτας από το δικαιούχο της. Εκείνοι που αρνούνται να υπαγάγουν τις ανωτέρω περιπτώσεις στη με «οποιονδήποτε άλλο τρόπο επίδραση των στοιχείων του υπολογιστή», ως προς την ελληνική διάταξη της απάτης με υπολογιστή, χρησιμοποιούν ως κυρίαρχα επιχειρήματα την έλλειψη «απατηλής» συμπεριφοράς και την απουσία «επίδρασης» στα στοιχεία υπολογιστή.[186] Ως αποτέλεσμα της παραπάνω σκέψης οι πράξεις αυτές χαρακτηρίζονται είτε ως κλοπή[187] (372 Π.Κ) είτε ως υπεξαίρεση[188] (375 Π.Κ), ανάλογα με το συμβατικό πλαίσιο που διέπει τις σχέσεις τράπεζας και κατόχου της κάρτας. Αντίθετα, οι υποστηρικτές της τέλεσης απάτης με υπολογιστή, βασίζονται σε μια

[185] Βλ. *Νούσκαλη* οπ.παρ σελ 183.
[186] Βλ. *Παπαδαμάκη* οπ.παρ.190.
[187] Βλ. *Αναγνωστόπουλου*, παρατηρήσεις στην ΕφΛθ 1904/1991 ΠοινΧρ 1992,197, *Παύλου*, παρατηρήσεις στη ΣυμβΝαυτΠειρ 418/1996 Υπερ 1997,113 ο οποίος θεωρεί ότι από τις ανωτέρω ενέργειες δεν προκύπτει γενικά ζημία της περιουσίας αλλά αφαίρεση των συγκεκριμένων χαρτονομισμάτων από το μηχάνημα αυτόματης συναλλαγής της τράπεζας. Ωστόσο, θα μπορούσε να παρατηρηθεί στο σημείο αυτό ότι είναι αμφίβολο αν δεν υπάρχει περιουσιακή ζημία και στην περίπτωση που αφαιρούνται τα συγκεκριμένα χαρτονομίσματα.
[188] Βλ. *Μανωλεδάκη* Εγκλήματα κατά της ιδιοκτησίας εκδ 9η 2000 σελ 36 σημ 9, *Παπαδαμάκη* οπ.παρ. σελ 191 σημ 22.

διευρυμένη θεώρηση της έννοιας «επίδραση» στα στοιχεία υπολογιστή, στην οποία περιλαμβάνεται και η χρησιμοποίηση της διαδικασίας και όχι μόνο η αλλαγή ροής δεδομένων.[189] Κατά την ανωτέρω διαδικασία ο δράστης «εξαπατά»[190] τον υπολογιστή με μία ψευδή πληροφόρηση για δικαιώματα που δεν έχει.

Η ελληνική νομολογία πριν τη θέση σε ισχύ του άρθρου 386Α Π.Κ ασχολήθηκε μία φορά με τον ανωτέρω προβληματισμό. Το Στρατοδικείο Θεσσαλονίκης αποφάνθηκε το 1986 ότι συνιστά κλοπή η υπέρβαση του πιστωτικού υπολοίπου από τον δικαιούχο χρήσης της κάρτας, με το επιχείρημα ότι υπάρχει συναίνεση της τράπεζας για την χρήση της κάρτας αλλά όχι και για την υπέρβαση του πιστωτικού υπολοίπου.[191] Μετά τη θέση σε ισχύ του νόμου 1805/1988, η ελληνική νομολογία ασχολήθηκε με τα υπό εξέταση παραδείγματα αρκετές φορές χωρίς έως τώρα να φαίνεται ότι έχει διαμορφώσει πάγια άποψη.

Το Εφετείο Αθηνών έκρινε το 1991 ότι η πράξη της χωρίς δικαίωμα χρήσης ξένης κωδικής κάρτας και του μυστικού αριθμού αυτής συνιστά κλοπή, χωρίς ωστόσο να εισέλθει καθόλου στον προβληματισμό της υπαγωγής στη διάταξη της απάτης με υπολογιστή.[192]

Περισσότερο αναλυτικές σκέψεις παρουσίασε το Στρατοδικείο Αθηνών το 1994. Χαρακτήρισε κλοπή και όχι απάτη με υπολογιστή την πράξη της χωρίς δικαίωμα χρήσης της ξένης κωδικής κάρτας. Το δικαστήριο δέχθηκε ότι η παραπάνω πράξη δεν προκαλεί επηρεασμό των στοιχείων υπολογιστή κατά το άρθρο 386Α Π.Κ, ως «απόκλιση από την κανονική και σύννομη εκτέλεση του προγράμματος», διότι ο

[189] Βλ. *Μυλωνόπουλου* οπ.παρ σελ 66, *Του ίδιου*, Ποινικό Δίκαιο Ειδικό Μέρος , Εγκλήματα κατά της περιουσίας και της ιδιοκτησίας, 2001 σελ 548 επ.
[190] Βλ. *Βασιλάκη*, οπ.παρ 213, *Κιούπη*, Ποινικό Δίκαιο και Ιντερνετ 1999 σελ 116.
[191] ΔιαρκΣτρατΘες 401/1986 ΠοινΧρ 1986,114 (με πρόταση *Παπαδαμάκη*).
[192] ΕφΑθ 1904/1991 ΠοινΧρ 1992, 196 (παρατ. *Αναγνωστόπουλου*)

«υπολογιστής με βάση τα δεδομένα και τον προγραμματισμό του αναγνωρίζει ως δικαιούχο κάθε χρήστη ορθών δεδομένων...».[193] Υπέρ της κατάφασης της απάτης με υπολογιστή για την πράξη της χωρίς δικαίωμα χρήσης ξένης κωδικής κάρτας τάχθηκε το Ναυτοδικείο Πειραιώς το 1996. Το δικαστήριο αποδέχθηκε τη συλλογιστική της συμπερασματικά συναγόμενης πληροφόρησης του υπολογιστή από τον δράστη για ένα δικαίωμα που δεν έχει στην πραγματικότητα.[194]

5.4.4 Η χωρίς δικαίωμα χρήση συστημάτων πληρωμών στο internet

Οι διατραπεζικές εργασίες εξ αποστάσεως και οι πράξεις ηλεκτρονικού εμπορίου συντελούνταν παλαιότερα με τη χρήση του κειμένου οθόνης τηλεόρασης και αποκωδικοποιητή τηλεφωνικών σημάτων (modem). Σήμερα, επικρατεί το σύστημα χρήσης ιστοσελίδων στο διαδίκτυο. Ο πυρήνας του προβληματισμού παραμένει ο ίδιος και στα δύο ανωτέρω συστήματα. Το παραπάνω σύστημα αποτελείται από μία απλή τηλεφωνική γραμμή, μία συσκευή τηλεόρασης μαζί με έναν αποκωδικοποιητή των ηλεκτρονικών σημάτων σε γραφικά (modem) ή από έναν υπολογιστή και ένα modem στο internet.[195] Τα παραπάνω συνδέονται με την κεντρική μονάδα επεξεργασίας του υπολογιστή της τράπεζας, με την οποία συμβάλλεται ο χρήστης του συστήματος, και με έναν ιδιωτικό οργανισμό (πάροχο), ο οποίος εκτελεί τη διαμεσολάβηση προς την τράπεζα και προσφέρει στον πελάτη πρόσβαση, αντί χρέωσης, σε

[193] ΔιαρκΣτρατΑθ 2897/1994 ΠοινΧρ 1994,1465 (με σύμφωνη πρόταση *Κ. Κονιδάρη*).
[194] ΣυμβΝαυτΠειρ 418/1996 Υπερ 1997, 103 (με σύμφωνη πρόταση *Παπαδαμάκη* και παρατηρήσεις *Παύλου*).
[195] Βλ. *Νούσκαλη* οπ.παρ. 184.

ποικίλες βάσεις δεδομένων που αναφέρονται σε αγαθά ή υπηρεσίες. Στα πλαίσια του Ποινικού Δικαίου περισσότερο συζητείται η χρήση ιστοσελίδων στις εξ αποστάσεως τραπεζικές συναλλαγές[196] (telebanking, homebanking) και στις αγορές αγαθών και υπηρεσιών εξ αποστάσεως. Οι πράξεις εκείνες που απασχολούν περισσότερο είναι τα τραπεζικά εμβάσματα από μη δικαιούχο με χρέωση άλλου, παραγγελίες αγαθών σε ξένο όνομα χωρίς δικαίωμα, κλήση και χρέωση στο όνομα άλλου για ιστοσελίδες που αφορούν διάφορες βάσεις δεδομένων, π.χ βιβλιοθήκες, με σκοπό αποφυγής των εξόδων για κάποιο χρήστη, αλλαγή ξένων κωδικών λέξεων με αποτέλεσμα ο νόμιμος χρήστης του συστήματος να μην μπορεί να χρησιμοποιήσει τη σύνδεσή του, μεθοδεύσεις στο πρόγραμμα του αποκωδικοποιητή των τηλεφωνικών σημάτων ώστε να χρεώνεται υπέρμετρα ο τηλεφωνικός λογαριασμός του νόμιμου χρήστη της ιστοσελίδας εν αγνοία του.[197]

Τα παραπάνω συστήματα είναι εφοδιασμένα συνήθως με συστήματα προστασίας τα οποία συνίστανται, είτε διαζευκτικά είτε σωρευτικά: α) Στη χρήση ενός κωδικού εισόδου που αποτελείται από γράμματα και αριθμούς ή μόνο από γράμματα ή μόνο από αριθμούς και β) στην ηλεκτρονική-ψηφιακή υπογραφή του νόμιμου χρήστη του συστήματος, η οποία πιστοποιείται[198] με τη βοήθεια ενός κατάλληλου προγράμματος Η/Υ και κρυπτογραφικών συστημάτων γραφής μεταξύ του αποστολές και του παραλήπτη της ψηφιακής υπογραφής.[199] Οι προσβολές της περιουσίας από τη χρήση του παραπάνω συστήματος

[196] Βλ. *Goode,* Electronic banking: The legal implications, Institute of Bankers, London, 1985 p.57.
[197] Βλ. *Κιούπη,* οπ. παρ σελ 112.
[198] Βλ. *Μανιώτη,* Η ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των εγγράφων στο Αστικό Δικονομικό Δίκαιο, 1988, σελ 79, *Κιούπη,* οπ.παρ.σελ 160, *Αγγελή,* Διαδίκτυο και ποινικό δίκαιο, Έγκλημα στον Κυβερνοχώρο, ΠοινΧρ 2000,686
[199] Για τη λειτουργία των συστημάτων αυτών με τη μορφή των λεγόμενων «δημόσιων» και «ιδιωτικών» κλειδιών με σκοπό τη συναλλακτική κίνηση των εγγράφων στα πλαίσια της ηλεκτρονικής φορτωτικής , Βλ. *Κουσούλη,* οπ. παρ., σελ 32 επ.

έχουν απασχολήσει έντονα τόσο τη θεωρία όσο και τη γερμανική ποινική νομολογία.

Στη Γερμανία έγινε δεκτή[200] η υπαγωγή στην απάτη με υπολογιστή της χωρίς δικαίωμα χρήσης του ως άνω συστήματος, τόσο από την πλευρά του δικαιούχου που υπερβαίνει το χορηγηθέν δικαίωμα όσο και από εκείνη του τρίτου που χωρίς δικαίωμα χρησιμοποιεί το σύστημα σε βάρος του δικαιούχου. Η πράξη έχει ενταχθεί στον ειδικότερο τρόπο τέλεσης του εγκλήματος που συνίσταται στη «χωρίς δικαίωμα χρησιμοποίηση δεδομένων» της παραγράφου 263a (StGB). Κατά μία άλλη άποψη[201] στον ειδικότερο τρόπο της απάτης με υπολογιστή που συνίσταται στη «χωρίς δικαίωμα χρησιμοποίηση δεδομένων», υπάγεται μόνο η χρήση των συστημάτων τραπεζικών εργασιών από απόσταση (telebanking) που γίνεται από κάποιον χωρίς εξουσιοδότηση από το νόμιμο χρήστη του συστήματος και όχι από το δικαιούχο χρήσης καθ' υπέρβαση του δικαιώματος χρήσης. Η πράξη αυτή αφορά απλώς μία παράβαση των εσωτερικών συμβατικών σχέσεων μεταξύ τράπεζας και δικαιούχου χρήσης του συστήματος.

Από τη νομολογία των γερμανικών δικαστηρίων έχει κριθεί[202] ότι σχετικά με την αντισυμβατική χρήση από δικαιούχο του συστήματος η μόνη δυνατή περίπτωση εφαρμογής της διάταξης για την απάτη με υπολογιστή είναι η υπαγωγή της πράξης αυτής στον ειδικότερο τρόπο τέλεσης του εγκλήματος αυτού που συνίσταται στη «χωρίς δικαίωμα χρησιμοποίηση (αληθινών) δεδομένων».[203] Όμως

---

[200] Βλ. *Frey*, 163, *Bandekow*, 297, *Buehler*, 450, αλλά και *Νούσκαλη*, οπ. παρ. σελ. 184 σημ.67.
[201] *Cramer Schoenke/Schroeder*, StGB Kommentar, 25 Auf, 1997,1886,20
[202] OLG Zweibruecken, Urteil vom 30.09.1992, StV 1993.196.
[203] Βλ § 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch

κατά την ίδια άποψη της νομολογίας αυτό δεν θα μπορούσε τελικά να γίνει δεκτό διότι η ίδια συμπεριφορά νοούμενη απέναντι σε έναν άνθρωπο δεν θα προκαλούσε εξαπάτηση, κριτήριο που η παραπάνω άποψη ανάγει σε βασικό ερμηνευτικό άξονα λόγω του παραλληλισμού αυτού προς την κοινή απάτη.

5.4.5 Συγκριτική επισκόπηση

Στην Ιταλία αντίστοιχη διάταξη του 386Α Π.Κ είναι η (640ter c.p) Ιταλικού Ποινικού κώδικα[204], η οποία ετέθη σε ισχύ με το άρθρο 4 του Νόμου 547 23.12.1993 και που προβλέπει ακριβώς τους ίδιους τρόπους τέλεσης με την Γερμανική 263 α αλλά και την ελληνική 386Α Π.Κ. Αξίζει επίσης να σημειωθεί ότι στο άρθρο 3 του ίδιου νόμου υπήρξε προσθήκη για την αντιμετώπιση του ηλεκτρονικού

unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend

[204] «Οποιος με οποιονδήποτε τρόπο επηρεάζει την λειτουργία ενός ηλεκτρονικου ή τηλεματικού συστήματος υπολογιστή ή παρεμβαίνει χωρίς δικαίωμα και με οποιονδήποτε τρόπο σε στοιχεία πληροφορίες η προγράμματα που περιέχονται σε ηλεκτρονικό υπολογιστή ή αφορούν αυτόν και το τηλεματικό σύστημα και με τον τρόπο αυτό παρέχει στον εαυτό του ή σε άλλον κέρδος (αχρεώστητο) τιμωρείται με φυλάκιση από έξι μήνες έως τρία χρόνια και με πρόστιμο από 51 έως 1032,91 ευρώ. Αν το έγκλημα έγινε με κατάχρηση θέσης υπευθύνου τότε αυτό αποτελεί επιβαρυντική περίσταση» βλέπε και παρακάτω όπου και ολόκληρο το πρωτότυπο κείμενο υποσημείωση αριθ.197.

εγγράφου αντίστοιχη με την προσθήκη στο άρθρο 13 του ελληνικού ποινικού κώδικα που έγινε με την εισαγωγή του νόμου 1805/1988 που χαρακτηρίζει ως «έγγραφο» οποιοδήποτε ηλεκτρονικό βοήθημα που περιέχει δεδομένα στοιχεία ή προγράμματα. Επίσης η απάτη που τελείται με κλεμμένες πιστωτικές κάρτες ή προπληρωμένες πιστωτικές κάρτες προβλέπεται ειδικά σε ειδικό ποινικό νόμο που την τιμωρεί αυτοτελώς.[205] Αντίστοιχη προβληματική στην Ιταλική Νομολογία έχει προκύψει όσον αφορά τη χρήση μαγνητικής κάρτας από δικαιούχο χωρίς δικαίωμα αλλά και από δικαιούχο καθ' υπέρβαση του πιστωτικού του ορίου με πάνω κάτω ίδιες διαπιστώσεις σε επίπεδο θεωρητικής προσέγγισης δηλαδή κλοπή, υπεξαίρεση αλλά και απάτη με ηλεκτρονικό υπολογιστή. Η ιταλική νομολογία[206] όμως όσον αφορά τις μαγνητικές κάρτες που χρησιμοποιούνται για παράδειγμα για αγορά βενζίνης από βενζινάδικο, μαγνητικές κάρτες που χρησιμοποιούνται σε φωτοτυπικά μηχανήματα, αλλά και κάρτες που επαναφορτίζουν κινητά τηλέφωνα πάγια αποδέχεται κλοπή που απλά τελείται με απατηλά μέσα[207] δεχόμενη ότι οι απάτες σε βάρος μηχανημάτων που χρησιμοποιούν μαγνητικές κάρτες τιμωρούνται ως απάτη με υπολογιστή (frode informatica art.640 ter codice penale) μόνο στην περίπτωση που η συσκευή διαθέτει-παρέχει υπηρεσίες όπως για παράδειγμα το ATM τράπεζας ενώ στην περίπτωση μηχανημάτων που λειτουργούν με μαγνητικές κάρτες αλλά διαθέτουν αγαθά όπως για παράδειγμα βενζίνη, μηχανήματα καφέ ή αναψυκτικών δέχεται τη θεμελίωση κλοπής με την επιβαρυντική

[205] Βλ.Decreto legislativo d.l. 3 maggio1991, n.143.
[206] Βλ Tribunale di Roma 20.06.1995,141 αλλά και Cass pen 44362/2003, 12732/2000, 3065/1999, 3067/1999, σε *Borruso* , 693 επ.
[207] Βλ. *Pecorella* , Il diritto penale dell informatica, Milano 1996, σελ 63

περίπτωση της χρήσης απατηλού μέσου (624,625, codice penale "furto aggravato").[208]

Στις περιπτώσεις αντίστοιχα των τραπεζικών συναλλαγών από απόσταση (home banking) η Ιταλική νομολογία δέχεται απάτη με υπολογιστή στην περίπτωση που κάποιος χρησιμοποιεί τραπεζικό κωδικό άλλου προκειμένου από απόσταση να πραγματοποιήσει τραπεζική συναλλαγή όπως μεταφορά χρημάτων από το λογαριασμό του δικαιούχου σε άλλο λογαριασμό ή την πληρωμή λογαριασμών. Όταν όμως οι ίδιες πράξεις πραγματοποιούνται από υπάλληλο τράπεζας (operator,operatore) τότε δέχεται την επιβαρυντική περίσταση του άρθρου 640ter (frode qualificata) με το σκεπτικό ότι ένας τρίτος προκειμένου να διεισδύσει στο ηλεκτρονικό σύστημα της τράπεζας χρειάζεται κωδικούς (passwords) που συνήθως δίνονται από ους ίδιους τους υπαλλήλους της τράπεζας ή από τεχνικούς που αναλαμβάνουν την συντήρηση του δικτύου της τράπεζας. Στην παραπάνω περίπτωση πρέπει να γίνει διάκριση για το εάν ο δικαιούχος του τραπεζικού λογαριασμού έχει δώσει την συναίνεσή του ή όχι. Εάν δεν υπάρχει συναίνεση του δικαιούχου, τότε δεν υπάρχει και αξιόποινο. Στην αντίθετη περίπτωση και ο δικαιούχος βαρύνεται με τη διακεκριμένη παραλλαγή της απάτης με υπολογιστή του Ιταλικού ποινικού κώδικα.[209]

---

[208] Βλ. *Pedrazzi* , Inganno ed errore nei delitti contro il patrimonio, Milano ,1995 σελ 85.

[209] **640ter. Frode informatica.** (1) — Chiunque, **alterando** in qualsiasi modo il funzionamento di un **sistema informatico** o **telematico** o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o **programmi** contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto **profitto** con altrui danno, è punito con la **reclusione** da sei mesi a tre anni e con la **multa** da cinquantuno euro a milletrentadue euro.
La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema (2).
Il delitto è punibile a **querela** della **persona offesa**, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra **circostanza aggravante**.

Χάριν πληρότητας στο σημείο αυτό θα πρέπει να επισημάνουμε ότι διατάξεις παρόμοιες με το 386Α Π.Κ συναντούμε α) Στις ΗΠΑ τη διάταξη: Computer fraud and Abuse act (US) 18 usc 1030 (a) παρ.4 που τιμωρεί την πράξη απάτης η οποία τελείται μέσω της χωρίς δικαίωμα πρόσβασης σε υπολογιστή ή της υπέρβασης νόμιμης πρόσβασης, β) στην Αγγλία το νόμο Computer Misuse Act section 2 (με τη λογική της αθέμιτης πρόσβασης σε δεδομένα), γ) στη Γαλλία το άρθρο 323-3 του Γαλλικού Ποινικού Κώδικα (που τιμωρεί την απατηλή εισαγωγή δεδομένων σε αυτοματοποιημένο σύστημα Η/Υ καθώς και την απατηλή διακοπή – επηρεασμό στοιχείων Η/Υ), δ) στην Ελβετία αντίστοιχα το άρθρο 143bis Ελβετικού Ποινικού Κώδικα διάταξη παρόμοια με τη γερμανική που τιμωρεί τη χωρίς δικαίωμα είσοδο στο σύστημα με σκοπό παράνομου περιουσιακού οφέλους, ενώ πολλές ομοιότητες με την Ελληνική παρουσιάζει η Αυστριακή διάταξη 197 Α Αυστριακού Π.Κ.

5.4.6 Το άρθρο 386Α Π.Κ και η συμβατότητά του σε σχέση με τη Σύμβαση του Συμβουλίου για το έγκλημα στον κυβερνοχώρο και της απόφασης - πλαίσιο του Συμβουλίου της Ε.Ε για τις επιθέσεις εναντίον των πληροφορικών συστημάτων

Στις 23.11.2001 ψηφίστηκε η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Convention on Cybercrime). Η Σύμβαση έχει τεθεί σε ισχύ, ήδη από τα τέλη

Φεβρουαρίου 2002, σύμφωνα με το άρθρο 36 παρ.2 αυτής, καθώς έχει υπογραφεί από τα περισσότερα μέλη του Συμβουλίου της Ευρώπης, αλλά και από τις ΗΠΑ, τον Καναδά, την Ιαπωνία και τη Νότιο Αφρική.

Στην Ελλάδα η υποστηριζόμενη ερμηνευτική θεώρηση της διάταξης του άρθρου 386Α Π.Κ συμβαδίζει με τα οριζόμενα στο άρθρο 8[210] της ανωτέρω Σύμβασης του Συμβουλίου της Ευρώπης.

Σύμφωνα με το άρθρο αυτό, τα Κράτη Μέρη υποχρεούνται να υιοθετήσουν μέτρα ποινικής τιμώρησης: Της πράξης της χωρίς δικαίωμα και με πρόθεση, πρόκλησης απώλειας περιουσίας σε κάποιον, η οποία συντελείται: α) με οποιαδήποτε εισαγωγή, διαγραφή ή απόκρυψη δεδομένων Η/Υ και β) με οποιαδήποτε επέμβαση στη λειτουργία ενός συστήματος Η/Υ, εφόσον συνοδεύεται από σκοπό εξαπάτησης ή αθέμιτο σκοπό πρόκλησης οικονομικού οφέλους στο δράστη ή τρίτο.[211] Θα πρέπει να σημειωθεί πάντως, ότι, σύμφωνα με το αρχικό σχέδιο της Σύμβασης, ήταν προαιρετική για τα Κράτη Μέρη η απαίτηση να υπάρχει σκοπός εξαπάτησης ή αθέμιτος σκοπός ως προϋπόθεση του αξιοποίνου.[212] Το τελικό κείμενο της Σύμβασης διέπεται από την αντίληψη που διακρίνει αφενός μεταξύ εγκλημάτων

---

[210] Βλ. **Article 8 – Computer-related fraud**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

[211] Για το τελικό κείμενο της Σύμβασης , βλ. την ηλεκτρονική διεύθυνση: http://conventions.coe.int/treaty/EN/cadreprincipal.htm

[212] Για το αρχικό σχέδιο της Σύμβασης βλ. την ηλεκτρονική διεύθυνση: http://conventions.coe.int/treaty/EN/projects/cybercrime25.htm

που τελούνται εναντίον της ακεραιότητας των συστημάτων και δεδομένων Η/Υ (computer system, compiuter data),[213] χωρίς να απαιτείται ο σκοπός πρόκλησης οικονομικού οφέλους ή ζημίας και αφετέρου εκείνων που σχετίζονται με Η/Υ (computer related crimes).[214] Οι δύο αυτές κατηγορίες προσβολών διακρίνονται από εκείνες που αφορούν εγκλήματα σχετικά με το περιεχόμενο παραδοσιακών εννόμων αγαθών που απλά διευκολύνονται με τη χρήση Η/Υ (computer related offences), όπως για παράδειγμα μια εξύβριση μέσω του διαδικτύου.

Η παραπάνω ρύθμιση της Σύμβασης δεν απαιτεί καμία ενέργεια αντίστοιχη με την παραπλάνηση της κλασικής απάτης. Θεωρεί ως κυρίαρχη ενέργεια τη, χωρίς δικαίωμα, επίδραση στο πρόγραμμα Η/Υ και την απώλεια περιουσίας, ως το αποτέλεσμα αυτής. Μόνο το γεγονός ότι τίθεται ως προϋπόθεση ο σκοπός εξαπάτησης δεν πρέπει να μας οδηγήσει στο συμπέρασμα ότι η προτεινόμενη νέα διάταξη θα δομείται παράλληλα με την κλασική απάτη.[215] Μάλλον το αντίθετο ακριβώς συμβαίνει. Ο σκοπός εξαπάτησης πρέπει να συνοδεύει τις ενέργειες της εισαγωγής, αλλοίωσης, διαγραφής ή απόκρυψης στοιχείων ή της οποιασδήποτε επέμβασης στη λειτουργία Η/Υ (βλ. αντίστοιχα στην ελληνική διάταξη 386Α Π.Κ « ή με οποιοδήποτε άλλο τρόπο»), ώστε να αποκλειστεί η περίπτωση της απλής δολιοφθοράς συστημάτων Η/Υ από το πεδίο του αξιοποίνου. Δεν εξυπηρετεί αντίθετα την άποψη που θέλει να εντάσσει στην απάτη με Η/Υ μόνο τις περιπτώσεις που παραλληλίζονται απόλυτα με τα παραδείγματα της κλασικής απάτης.

[213] Βλ. κεφάλαιο 1 άρθρο 1, κεφάλαιο 2, τίτλος 2, άρθρα 2-5, στην ηλεκτρονική διεύθυνση: http://conventions.coe.int/treaty/en/cadreprincipal.htm
[214] Βλ. κεφάλαιο 2, άρθρα 7 και 8 , οπ.παρ.
[215] Βλ. και *Νούσκαλη*, οπ.παρ σελ 189.

Σύμφωνα με το επεξηγηματικό κείμενο που συνοδεύει τη Σύμβαση γίνεται δεκτό ότι οι μεν ανωτέρω ρυθμίσεις του άρθρου 7 αφορούν σε παραδοσιακά εγκλήματα προσβολής της περιουσίας, αλλά η νέα ρύθμιση τίθεται με σκοπό να συμπεριλάβει οποιαδήποτε, χωρίς δικαίωμα, επέμβαση σε σύστημα Η/Υ, συνοδευόμενη από σκοπό πρόκλησης παράνομου περιουσιακού οφέλους. Τονίζεται μάλιστα, ότι η Σύμβαση έχει κατά νου ιδίως τις περιπτώσεις του «ηλεκτρονικού χρήματος», συμπεριλαμβάνοντας σε αυτές και τις πράξεις απάτης με πιστωτικές κάρτες (παράγραφος 86 επεξηγηματικού κειμένου).[216]

Σύμφωνα με τους ορισμούς της Σύμβασης στο άρθρο 1 περ. β', στην έννοια «δεδομένα υπολογιστή» εντάσσονται γεγονότα, πληροφορίες ή έννοιες, τα οποία περιέχονται σε ένα πρόγραμμα υπολογιστή που προκαλεί τη λειτουργία του υπολογιστή.[217] Εξάλλου, σύμφωνα με το άρθρο 1 περ. α', ως «σύστημα υπολογιστή» θεωρείται κάθε συσκευή ή κάθε σύνολο συνδεόμενων συσκευών, τα οποία διενεργούν επεξεργασία δεδομένων μέσω ενός προγράμματος υπολογιστή. Θα μπορούσε λοιπόν να υποστηρίξει κανείς ότι η δική μας 386ΑΠ.Κ αποτελεί τον «πρόγονο της διάταξης της Σύμβασης του Συμβουλίου της Ευρώπης. Αν κανείς ερμηνεύσει την ισχύουσα διάταξη ανεξάρτητα από την απάτη του άρθρου 386Π.Κ, θα μπορούσε να θεωρήσει ότι το άρθρο 386ΑΠ.Κ καλύπτει τις υποχρεώσεις της Ελλάδας να συμμορφωθεί προς την ανωτέρω Σύμβαση.[218] Ακόμη πιο προωθημένες απόψεις, σχετικά με την τιμώρηση των ανωτέρω συμπεριφορών εξέφρασε η πρόταση της απόφασης –πλαίσιο του Συμβουλίου της Ευρώπης της 27.8.2002, όπως τροποποιήθηκε από το

[216] Για το επεξηγηματικό κείμενο που συνοδεύει τη Σύμβαση, βλ. την ηλεκτρονική διεύθυνση:http://conventions.coe.int/treaty/EN/cadreprincipal.htm
[217] Βλ.Software
[218] Έτσι και ο *Νούσκαλης*, οπ.παρ 189 επ.

Ευρωπαϊκό κοινοβούλιο την 4.11.2002. Στην αιτιολογική έκθεση της πρότασης και των τροπολογιών του Κοινοβουλίου τονίζεται η σκοπιμότητα τιμώρησης κάθε πράξης παράνομης πρόσβασης στα συστήματα πληροφοριών, εφόσον αυτή στρέφεται είτε κατά συστημάτων που συνοδεύονται από μέτρα ασφαλείας είτε γίνεται με σκοπό πρόκλησης ζημίας ή την αποκόμιση περιουσιακού οφέλους.

Η τυποποίηση των ανωτέρω ενεργειών προβλέπεται στο άρθρο 3 της πρότασης. η ευρεία αυτή ποινικοποίηση κατευθύνεται, σύμφωνα με την ανωτέρω έκθεση, στην υπερκέραση ακόμη και των όσων προβλέπονται στη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, ενόψει του μεγέθους του κινδύνου από τις επιθέσεις σε συστήματα πληροφοριών των δικτύων επικοινωνιών αλλά και του ηλεκτρονικού εμπορίου.[219] Ενδεικτική της άποψης όσον αφορά τη σύγκλιση των εγκλημάτων που τελούνται με Η/Υ και των εγκλημάτων που τελούνται στον κυβερνοχώρο σε μια κατηγορία ενιαία αποτελούν οι ορισμοί της πρότασης στο άρθρο 2 αυτής. Στο «σύστημα πληροφοριών» εντάσσονται το λογισμικό και το «υλικό του συστήματος»(hardware) οποιουδήποτε δικτύου επικοινωνίας είτε αυτόνομου είτε διασυνδεδεμένου, ξεπερνώντας τους ορισμούς που περιέχονται από τις διεθνείς συμβάσεις του ΟΑΣΑ το 1992, τους οποίους όμως η πρόταση χρησιμοποιεί ως σημείο εκκίνησης (βλ. άρθρο 2 περ 2 της πρότασης). Στον ανωτέρω ορισμό δεν συμπεριλαμβάνεται όμως κατά το άρθρο 2 της πρότασης το περιεχόμενο της πληροφορίας την οποία διακινούν τα συστήματα.

Η διευκρίνιση αυτή είναι αναγκαία ενόψει του ότι τα εγκλήματα που αφορούν το περιεχόμενο της πληροφορίας θεωρούνται ότι δεν συνιστούν επιθέσεις εναντίον των «συστημάτων πληροφοριών», αλλά πράξεις που εντάσσονται στις αντικειμενικές υποστάσεις

[219] Βλ. παράγραφο 1.1 της αιτιολογικής έκθεσης.

παραδοσιακών εγκλημάτων. Για τις πράξεις αυτές η πρόταση θεωρεί ότι είναι επαρκής η νομοθεσία των κρατών μερών όπως για παράδειγμα για την πνευματική ιδιοκτησία, το απόρρητο των επικοινωνιών, τα προσωπικά δεδομένα[220] κλπ.

Στο ίδιο περίπου πλαίσιο κινείται και η Απόφαση-Πλαίσιο (2001/413/ΔΕΥ) με τον τίτλο: «για την καταπολέμηση της απάτης και της πλαστογραφίας, που αφορούν τα μέσα πληρωμής πλην των μετρητών» και που η χώρα μας υποχρεούτο έως τις 2.6.2003 να διαμορφώσει και διαβιβάσει προς το Συμβούλιο, το κείμενο των διατάξεων, με το οποίο θα προσαρμόζει στις επιταγές της Απόφασης-Πλαίσιο το εθνικό μας Δίκαιο. Συγκεκριμένα κατά το άρθρο 3 της εν λόγω Απόφασης-Πλαίσιο, προβλέπεται ως αξιόποινη πράξη η εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη χωρίς δικαίωμα δεδομένων υπολογιστή και ιδίως δεδομένων αναγνώρισης της ταυτότητας με σκοπό εξασφάλισης παράνομου περιουσιακού οφέλους.

[220] Βλ. παράγραφο 1.4 της αιτιολογικής έκθεσης.

6. Επίλογος – τελικά συμπεράσματα

Είναι νομίζουμε χωρίς καμία αμφιβολία γενικά παραδεκτό ότι το ηλεκτρονικό έγκλημα διογκώνεται καθημερινά λόγω της συνεχώς αυξανόμενης χρήσης των ηλεκτρονικών υπολογιστών, της βελτίωσης των τεχνικών τους δυνατοτήτων και της διασύνδεσής τους στο Διαδίκτυο που επεκτείνεται μέρα με την μέρα ολοένα και περισσότερο. Αποτελεί κοινό τόπο ότι ο ηλεκτρονικός υπολογιστής έχει καταστεί απαραίτητο εργαλείο της καθημερινότητάς μας είτε αυτή αναφέρεται στην εργασία είτε στην καθημερινή επικοινωνία και διασκέδασή μας.

Μπροστά σε αυτή τη ραγδαία εξελισσόμενη πραγματικότητα και την υπερεθνική διάσταση πολλών ηλεκτρονικών εγκλημάτων (ή εγκληματικών συμπεριφορών) ο εθνικός νομοθέτης είναι φυσικό να αντιδρά με καθυστέρηση και να χρησιμοποιεί ευρείες ειδικές υποστάσεις ή να επεκτείνει τις ειδικές υποστάσεις παραδοσιακών εγκλημάτων.

Ταυτόχρονα, επιχειρείται η σύγκλιση κάποιων κεντρικών επιλογών σε υπερεθνικό επίπεδο με νομικά εργαλεία (βλ. αποφάσεις – πλαίσιο) στο πλαίσιο της ΕΕ ή με διεθνείς συμβάσεις του Συμβουλίου της Ευρώπης ή άλλων διεθνών οργανισμών. Λαμβάνοντας υπόψη τις διεθνείς νομοθετικές εξελίξεις θα μπορούσε να υποστηριχθεί με βάση τα όσα παραπάνω αναπτύχθηκαν ότι η διάταξη του άρθρου 386Α ΠΚ, η οποία αποτελεί και αντικείμενο επεξεργασίας της παρούσας μελέτης, καλύπτει τις υποχρεώσεις συμμόρφωσης της χώρας μας προς τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, μόνο όμως ως προς τις προσβολές που σχετίζονται με Η/Υ και όχι εκείνες που αφορούν την ακεραιότητα συστημάτων Η/Υ

και δεδομένων. Για την κάλυψη αυτών των περιπτώσεων θα πρέπει μάλλον να τροποποιηθεί η διάταξη του άρθρου 370Γ Π.Κ.[221]

Όσον αφορά στην ίδια την διάταξη του άρθρου 386Α Π.Κ πρέπει να τονιστεί ότι η ψηφιοποίηση του χρήματος σε συνδυασμό με τη διεύρυνση της χρήσεως του διαδικτύου για την εκτέλεση τραπεζικών εργασιών ή γενικότερα για τη διεξαγωγή οικονομικών εργασιών καθιστά ουσιαστικά τη συγκεκριμένη διάταξη κεντρική διάταξη των οικονομικών εγκλημάτων. Και αυτό διότι επιχειρεί να καλύψει περιπτώσεις αντίστοιχες με εκείνες της απάτης του άρθρου 386 Π.Κ, όπου όμως αντί της διαπροσωπικής σχέσεως δράστη και πλανώμενου προσώπου υπάρχει η σχέση ανθρώπου μηχανής. Ακριβώς λόγω της διαφορετικής φύσεως της σχέσεως αυτής τα στοιχεία της αντικειμενικής υπόστασης που έχουν καθαρά ανθρώπινη διάσταση (δημιουργία *πεποιθήσεως* στο θύμα διαμέσου παραστάσεως-αποκρύψεως και παραπλανήσεως) τροποποιούνται αντίστοιχα σε επίδραση επί των στοιχείων του υπολογιστή διαμέσου μη ορθής διαμόρφωσης του προγράμματος, επέμβασης κατά την εφαρμογή του, χρησιμοποίησης μη ορθών ή ελλιπών στοιχείων ή με οποιοδήποτε άλλο τρόπο. Έτσι, καλύπτονται παρεμβάσεις στα στοιχεία του υπολογιστή που αναφέρονται σε όλα τα στάδια της διαδικασίας δηλαδή και στην παρέμβαση στα εισερχόμενα δεδομένα (Inputmanipulation) και την παρέμβαση στο πρόγραμμα (Programmanipulation) και την παρέμβαση στα εξερχόμενα δεδομένα (Outputmanipulation) καθώς και την επίδραση στα μηχανικά τμήματα του υπολογιστή (Hardware).

Ο τελευταίος τρόπος τέλεσης της διάταξης 386^{A} Π.Κ «επηρεασμός των στοιχείων του υπολογιστή .... με οποιοδήποτε άλλο τρόπο» έχει στο παρελθόν υποστεί άδικη κατά τη γνώμη του γράφοντος κριτική

[221] Βλ. *Νούσκαλη*, όπ. παρ. σελ.190.

τόσο από τη θεωρία[222] όσο και από τη νομολογία δημιουργώντας αμφιβολίες για την ορθή υπαγωγή και αντιμετώπισή του από κάποια ποινική διάταξη με βασικό επιχείρημα ότι και στα νομοθετικά κείμενα του Συμβουλίου της Ευρώπης που παραπάνω μνημονεύθηκαν, ρητά γίνεται λόγος, όπως εξάλλου και στην αντίστοιχη Γερμανική διάταξη στο στοιχείο της «χωρίς δικαίωμα χρήσης». Κατά την άποψη του γράφοντος εφόσον τα δεδομένα υπολογιστή οδηγούν μετά την επεξεργασία τους σε ένα αποτέλεσμα διαφορετικό από το προσδοκώμενο με τη νόμιμη χρήση δεν υπάρχει λόγος να αρνηθεί κανείς ότι έχουν επηρεαστεί. Ο επηρεασμός δε αυτός μπορεί να προκληθεί με «οποιοδήποτε τρόπο», συνακόλουθα η διάταξη του άρθρου 386Α Π.Κ καλύπτει και τις περιπτώσεις της «χωρίς δικαίωμα χρησιμοποίησης». Στο σημείο αυτό δε οφείλουμε να θυμηθούμε ότι η συγκεκριμένη διάταξη εισήχθη το 1988 στον Κώδικά μας και τελικά ακόμη και σήμερα καλύπτει και τις υποχρεώσεις της χώρας μας σε σχέση με τα διεθνή νομοθετικά κείμενα και ακόμα πολύ περισσότερο όλους τους μοντέρνους τρόπους τέλεσης που εμφανίστηκαν, εμφανίζονται και θα εμφανιστούν όπως για παράδειγμα τους dialers.

Ευνόητο είναι δε ότι για τις παραπάνω περιπτώσεις πρέπει να αποκλισθεί η αντιμετώπισή τους με τις διατάξεις της κλοπής και της υπεξαίρεσης, και αντίστοιχα να προτιμηθεί η διάταξη του άρθρου 386Α ΠΚ, αφού πέραν του αυτονόητου συνδετικού στοιχείου με τη διάταξη αυτή, που είναι βεβαίως η μέσω ηλεκτρονικού υπολογιστή πρόκληση περιουσιακής βλάβης, είναι αναμφισβήτητο ότι η άξια κολασμού ποινική συμπεριφορά, με την οποία επέρχεται η ποινικώς ενδιαφέρουσα παράνομη περιουσιακή μετατόπιση, εμφανίζει πολύ

[222] Βλ. *Μαργαρίτη*, οπ. παρ. «διάταξη αμφιβόλου συνταγματικότητας» αλλά και *Ο.Νάμμία*, οπ. παρ. σελ 488 επ.

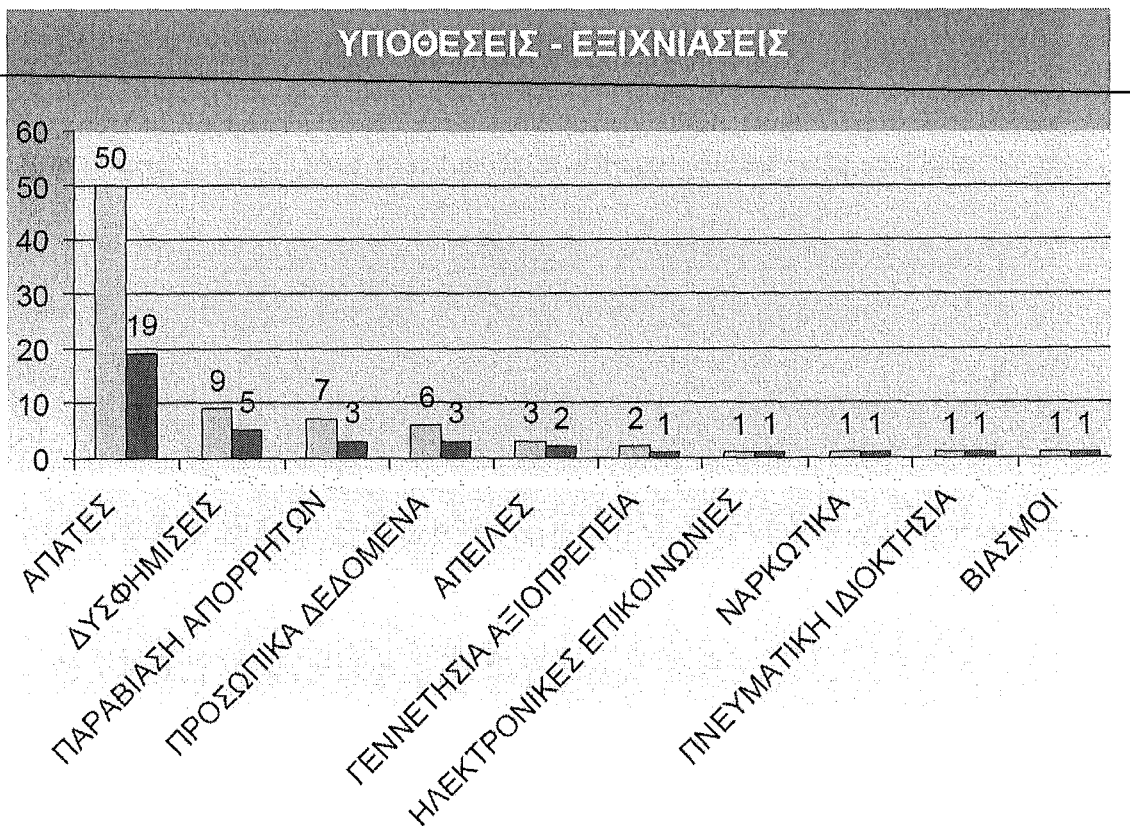
μεγαλύτερη (σχεδόν απόλυτη) δομική ομοιότητα με την απάτη, παρά με την κλοπή ή την υπεξαίρεση.[223]

Πάντως ενώ η τέλεση της απάτης με υπολογιστή που τελείται στο διαδίκτυο για τις περισσότερες περιπτώσεις επέμβασης κατά την εφαρμογή προγράμματος (περίπτωση του hacker που σπάει τα συστήματα ασφαλείας και αποκτά πρόσβαση στα δεδομένα χωρίς να τηρήσει την προβλεπόμενη διαδικασία εισόδου χρήστη με κωδικό εισόδου) καλύπτεται από το άρθρο 386Α Π.Κ, προβλήματα ανακύπτουν στην περίπτωση εκείνου που εμφανίζεται στο πρόγραμμα με «ψευδή» ταυτότητα έχοντας υποκλέψει τον κωδικό εισόδου του νόμιμου χρήστη. Το πρόβλημα, που είναι ήδη γνωστό από την περίπτωση της κλεμμένης κάρτας αυτόματης αναλήψεως και της χρήσεως του σωστού κωδικού εισόδου, εμφανίζεται αντίστοιχα και εδώ. Ο δράστης επηρεάζει τα στοιχεία υπολογιστή αλλά εξωτερικά τουλάχιστον φαίνεται να χρησιμοποιεί απολύτως κανονικά το πρόγραμμα όπως ακριβώς και ο νόμιμος χρήστης-κάτοχος του κωδικού εισόδου. Παρά την απουσία ειδικής αντίστοιχης διάταξης για τη χωρίς δικαίωμα χρήση δεδομένων η ευρεία διατύπωση του νόμου «με οποιοδήποτε άλλο τρόπο» και η αναλογία της συμπεριφοράς αυτής με την απάτη του άρθρου 386 Π.Κ, που τελεί όποιος δια της συναγόμενης συμπεριφοράς του παριστάνει ψευδώς ότι είναι ο δικαιούχος του τραπεζικού λογαριασμού, επιβάλλει να δεχθούμε ότι εφαρμόζεται και εδώ η διάταξη του άρθρου 386Α Π.Κ.

[223] Έτσι π.χ *Ε. Συμεωνίδου-Καστανίδου*, οπ. παρ. σελ. 944, η οποία παρατηρεί ότι «η αφαίρεση των νομισματικών μονάδων με παράνομη διείσδυση στον ηλεκτρονικό υπολογιστή της τράπεζας και η μεταφορά τους σε άλλο λογαριασμό θα πρέπει να χαρακτηριστεί κλοπή…» και προτρέπει σε αντιμετώπιση του θέματος από τον ίδιο το νομοθέτη.

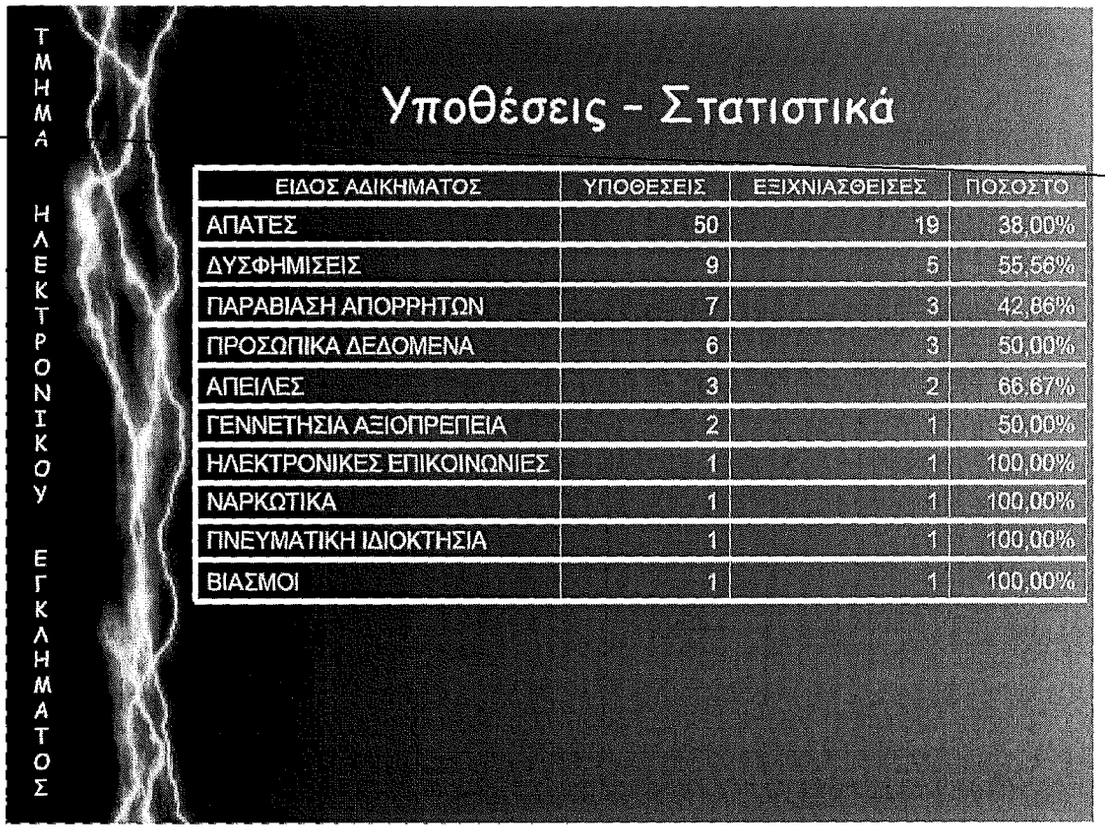
7. Πίνακες Εμφάνισης Ηλεκτρονικής Εγκληματικότητας και ηλεκτρονικής απάτης στην Ελλάδα[224]

Πίνακας (Α)



[224] Στοιχεία από το τμήμα δίωξης ηλεκτρονικού εγκλήματος.

Πίνακας (Β)



ΕΙΔΟΣ ΑΔΙΚΗΜΑΤΟΣ	ΥΠΟΘΕΣΕΙΣ	ΕΞΙΧΝΙΑΣΘΕΙΣΕΣ	ΠΟΣΟΣΤΟ
ΑΠΑΤΕΣ	50	19	38,00%
ΔΥΣΦΗΜΙΣΕΙΣ	9	5	55,56%
ΠΑΡΑΒΙΑΣΗ ΑΠΟΡΡΗΤΩΝ	7	3	42,86%
ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ	6	3	50,00%
ΑΠΕΙΛΕΣ	3	2	66,67%
ΓΕΝΝΕΤΗΣΙΑ ΑΞΙΟΠΡΕΠΕΙΑ	2	1	50,00%
ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ	1	1	100,00%
ΝΑΡΚΩΤΙΚΑ	1	1	100,00%
ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ	1	1	100,00%
ΒΙΑΣΜΟΙ	1	1	100,00%

Όπως εύκολα μπορεί να παρατηρήσει κανείς η «ηλεκτρονική απάτη» είτε με υπολογιστή είτε μέσω υπολογιστή είναι ίσως το πιο σύνηθες οικονομικό ηλεκτρονικό έγκλημα δυστυχώς και στη χώρα μας.

8. ΒΑΣΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Α. ΕΛΛΗΝΙΚΗ

1. ***Αγγελής Ι.*** Διαδίκτυο (internet) και Ποινικό Δίκαιο. Έγκλημα στον κυβερνοχώρο (cybercrime-internet crime), ΠοινΧρον.675-686.

2. ***Του ίδιου*** Ηλεκτρονικό έγκλημα . Ο γνωστός αντίπαλος της Δικαιοσύνης , Τα Νέα 11-11-2000 σελ. Ν34.

3. ***Αναγνωστόπουλος Η.*** παρατηρήσεις στην ΕφΑθ 1904/1991 ΠοινΧρ 1992.

4. ***Ανδρουλάκης Ν.*** Ποινικό Δίκαιο Γενικό Μέρος Τόμοι 1 και 2 Αθήνα 2000, 2005 Εκδόσεις Π.Ν Σάκκουλα

5. ***Του ίδιου***, Ποινικά Varia, ΠοινΧρον. 1995,673 επ.και Σπινέλλη ιδιωτική γνωμοδότηση, ΠοινΧρον.1996,436 Υπεξαίρεση και λογιστικό χρήμα.

6. ***Του ίδιου*** Συστηματική ερμηνεία του Ποινικού Κώδικα (Μαγκάκης , Σπινέλλης, Σταμάτης ,Ψαρούδα-Μπενάκη Εκδόσεις Π.Ν Σάκκουλα Αθήνα 2005.

7. ***Του ίδιου*** Ποινική Νομοθεσία έκδοση Ποινικά Χρονικά Π.Ν Σάκκουλας Αθήνα 2002.

8. ***Αργυρόπουλος Α.*** Ηλεκτρονική εγκληματικότητα. Τα αδικήματα της χωρίς άδεια απόκτησης δεδομένων (202^{α} StGB) της παραποίησης δεδομένων (303a StGB) σε σχέση με το Hacking και τη μετάδοση ηλεκτρονικών ιών στο internet, Εγκληματολογικά 19. Εκδόσεις Α.Σάκκουλα , Αθήνα – Κομοτηνή 2001.

9. ***Βασιλάκη Ε.*** Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών η αντιμετώπιση του προβλήματος ιδιαίτερα μετά την εισαγωγή του Ν.1805/1988, Ποινικά 40, Εκδόσεις Α.Σάκκουλα, Αθήνα-Κομοτηνή 1993.

10.***Βελέντζας Γ.*** Δίκαιο τραπεζικών συμβάσεων (Εργασιών) Θεσσαλονίκη 1996.

11.***Γεωργιάδης Γ.*** Η προστασία των διακριτικών γνωρισμάτων στο διαδίκτυο- Domain names,ΔΕΕ 1999,1243 επ.

12.***Γιαννόπουλος Θ.*** Όψεις και προβλήματα της ηλεκτρονικής εγκληματικότητας ΝοΒ 34(1986) σελ.173 επ.

13.***Ελληνική Εταιρεία Ποινικού Δικαίου***, Πρακτικά Δ Πανελλήνιου Συνεδρίου Εκδόσεις Π.Ν Σάκκουλα 1993.

14.***Ζαννή Α.*** Το διαδικτυακό έγκλημα, Εκδόσεις Α.Σάκκουλα Αθήνα-Κομοτηνή 2005.

15.***Ζησιάδης Β.*** Ι. Η οικονομική εγκληματικότητα το ουσιαστικό και δικονομικό οικονομικό Ποινικό Δίκαιο Εκδόσεις Σάκκουλα Αθήνα-Θεσσαλονίκη 2001.

16.***Καράκωστας Ι.*** Δίκαιο και Internet Νομική αντιμετώπιση του Διαδικτύου, ΝοΒ 46 σελ 1172-1184.

17.***Του ίδιου*** Το Δίκαιο των ΜΜΕ,2005,482

18.***Του ίδιου*** Δίκαιο και Internet Νομικά ζητήματα του διαδικτύου Εκδόσεις Π.Ν Σάκκουλα Αθήνα 2001.

19.***Κιούπης Δ.*** Ποινικό Δίκαιο και Internet, Ποινικά 57, Εκδόσεις Α.Σάκκουλα , Αθήνα-Κομοτηνή 1999.

20.***Του ίδιου*** Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της Ποινικής Νομοθεσίας, Υπερ.2000 σελ.959-972.

21.***Του ίδιου*** Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet ΠοινΧρον. ΜΗ/1998 σελ712 επ.

22.***Κοτσαλής Λ.*** Ποινικό Δίκαιο Γενικό Μέρος Τόμοι 1 και 2 Εκδόσεις Α.Σάκκουλα Αθήνα-Κομοτηνή 2006.

23.***Κουράκης Ν.*** Το οικονομικό Έγκλημα στην Ελλάδα σήμερα ΠοινΔικ 6 2000 644 επ.

24.***Kaiser Gunter*** Ο ποινικός έλεγχος της βαριάς οικονομικής εγκληματικότητας Ποινικά Εκδόσεις Α.Σάκκουλα Αθήνα-Κομοτηνή 1983.

25.***Κονταξή Α.*** Ποινικός Κώδικας Ερμηνεία κατ΄άρθρο, Αθήνα 2000.

26.***Κωστάρας Α.*** Ποινικό Δίκαιο Επιλογές Ειδικού Μέρους Εκδόσεις Α.Σάκκουλα Αθήνα –Κομοτηνή 2006.

27.***Λάζος Γ.*** Πληροφορική και έγκλημα , Εκδόσεις Νομική Βιβλιοθήκη , Αθήνα 2001.

28.***Του ίδιου*** Το οικονομικό έγκλημα στη σύγχρονη Ελλάδα Σκληρά δεδομένα και βασικές συντεταγμένες , ΠοινΔικ 6/2000 655 επ.

29.***Μαγκάκης .Γ.Α.*** Ποινικό Δίκαιο Διάγραμμα Γενικού Μέρους γ εκδ Αθήνα 1984.

30.***Μανιώτης Η*** ψηφιακή υπογραφή ως μέσο διαπιστώσεως της γνησιότητος των εγγράφων στο αστικό δικονομικό δίκαιο 1998.

31.***Μανωλεδάκης Ι.*** Ερμηνεία κατ΄άρθρο βασικών όρων του ειδικού μέρους του ποινικού κώδικα Εκδόσεις Σάκκουλα Θεσσαλονίκη 1996.

32.***Του ίδιου*** Το έννομο αγαθό ως βασική έννοια του Ποινικού Δικαίου, Εκδόσεις Σάκκουλα Θεσσαλονίκη 1998.

33.***Του ίδιου*** Εγκλήματα κατά της ιδιοκτησίας έκδοση $9^{η}$ Θεσσαλονίκη Σάκκουλας 2000.

34.***Μούζουλας Γ.*** Η χρήση της τεχνολογίας της πληροφόρησης ως μέσο τέλεσης αξιόποινων πράξεων, Μέθοδοι τάσεις και προοπτικές της ποινικής καταστολής, ΠοινΧρον.Μ 778-784.

35.***Μπουρμάς Γ.*** Στοιχεία Απάτης με υπολογιστή κατ΄΄αρθρο 386^{α} Π.Κ και διάκριση αυτής από την κοινή απάτη του άρθρου 386 Π.Κ. ΠοινΧρον. ΝΑ/2001 σελ. 468 επ.

36.***Μπόση Μ.*** Ζητήματα ασφαλείας στη Νέα Τάξη Πραγμάτων Εκδόσεις Παπαζήση Αθήνα 1999 299 επ.

37.***Μυλωνόπουλος Χ.*** Ηλεκτρονικοί υπολογιστές και Ποινικό Δίκαιο Συμβολή στην ερμηνεία των άρθρων: 13γ,370Β,370Γ,386^{Α} Π.Κ (Άρθρ.2-5 Ν.1805/1988), Ποινικά 33, Εκδόσεις Α.Σάκκουλα Αθήνα –Κομοτηνή 1991.

38.***Του ίδιου*** Ποινικό Δίκαιο Ειδικό Μέρος τα εγκλήματα κατά της περιουσίας και της ιδιοκτησίας Εκδόσεις Π.Ν Σάκκουλας Αθήνα 2005.

39.***Του ίδιου*** Ποινικό Δίκαιο Γενικό Μέρος Τόμος 1 Εκδόσεις Π.Ν.Σάκκουλας , Αθήνα 2007.

40.***Του ίδιου*** Η ποινική προστασία του λογισμικού κατά το Ελληνικό Ποινικό Δίκαιο , ΠοινΧρον. ΛΗ 3 επ.

41.***Του ίδιου*** Ποινικό Δίκαιο Ειδικό Μέρος Τα εγκλήματα σχετικά με τα υπομνήματα Εκδόσεις Π.Ν.Σάκκουλας Αθήνα 2005.

42.***Ναμμίας Ο.*** Σύγχρονες μορφές απάτης στις τραπεζικές συναλλαγές Ένωση Ελλήνων Ποινικολόγων- Εθνική Τράπεζα της Ελλάδος Επιστημονική διημερίδα με θέμα Εγκλήματα στις τραπεζικές και χρηματιστηριακές συναλλαγές Αθήνα 18,19 Απριλίου 2003 . Επίσης σε Τιμητικό Τόμο Ν.Ανδρουλάκη σελ 467 επ. Εκδόσεις Α.Σάκκουλα 2003

43.***Νούσκαλης Γ.*** Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ) Το παρελθόν και το μέλλον του άρθρου 386^{α} Π.Κ ιδίως υπό το πρίσμα

των εξελίξεων στο συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση. ΠοινΔικ 2/2003 σελ 178 επ.

44.***Του ίδιου*** Ηλεκτρονικά Μπισκότα Δηλητηριώδη για τις ατομικές ελευθερίες (Προκλήσεις της ψηφιακής εποχής. Η προσαρμογή του Ελληνικού Ποινικού Δικαίου στην διαδικτυακή εγκληματικότητα σε http://www.nouskalis.gr/art01.htm.

45.***Παπαδαμάκης Α***. Τα περιουσιακά εγκλήματα Εκδόσεις Σάκκουλα Θεσσαλονίκη 2003.

46.***Παπαθεοδώρου Θ.*** Δημόσια Ασφάλεια και αντεγκληματική πολιτική Συγκριτική προσέγγιση, Εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2002.

47.***Παύλου Σ***. Αποφάσεις- πλαίσια Εκδόσεις Π.Ν Σάκκουλας Αθήνα 2005

48.***Του ίδιου*** Ο Ν. 3074/2002 και η κατ΄εξαίρεση δι΄απευθείας κλήσεως παραπομπή του υπαλλήλου που κατηγορείται για κακούργημα στο αρμόδιο δικαστήριο , ΠοινΔικ 2003, 419.

49.***Του ίδιου*** Παρατηρήσεις στην ΣθμβΝαυτΠειρ 418/1996 Υπερ 1997 113.

50.***Σπυράκης Π***. Έγκλημα στον Κυβερνοχώρο, Το Βήμα 28-12-1997.

51.***Σπινέλλης Δ***. Ποινικό Δίκαιο Ειδικό Μέρος Τεύχος Β Εγκλήματα κατά περιουσιακών εννόμων αγαθών (άρθρα 385-387) εκδόσεις Α.Σάκκουλα Αθήνα Κομοτηνή 1985.

52.***Του ίδιου*** Μελέτες Ποινικών Επιστημών εκδόσεις Α.Σάκκουλα Αθήνα –Κομοτηνή 2001.

53.***Συμμεωνίδου-Καστανίδου Ε***. Υπεξαίρεση και λογιστικό χρήμα Υπερ 1998 940 επ.

54.***Της ίδιας*** Παρατηρήσεις σε ΣυμβΠλημΠατρών 211/2001 ΠοινΔικ 2002,880

55. ***Τσιρίδης Π.*** Μελέτες Ποινικού Δικαίου. εκδόσεις Α.Σάκκουλα Αθήνα-Κομοτηνή 2001

56. ***Φαραντούρης Ν.*** Σύγχρονες εγκληματικές δράσεις στο διαδίκτυο-Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινόμενου της μόλυνσης με ιούς , ΠοινΔικ 2/2003, σελ. 191-196.

57. ***Χλούπης Γ.*** Υπερεθνικό Έγκλημα με τη χρήση Η/Υ, ΑρχΝομ. 1999 σελ 647 επ.

58. ***Ψούνη-Ζορμπά*** Δήλωση βουλήσεως μέσω ηλεκτρονικού υπολογιστή .Ένταξη στο σύστημα του Α.Κ, δυνατότητες ακύρωσης, Θεσσαλονίκη 1988.

59. ***Ψυχομάνη*** Τραπεζικό Δίκαιο, Δίκαιο τραπεζικών συμβάσεων , Γενικό Μέρος καταθέσεις ,πιστώσεις, εγγυητικές επιστολές Θεσσαλονίκη 1997.

60. ***Χάνος Α.*** Δίκαιο και τεχνολογική εξέλιξη στην κοινωνία των πληροφοριών-με παράδειγμα το διοικητικό δίκαιο ΕΕΝ 2000 ΣΕΛ 7-18.

61. ***Χαραλαμπάκης Α.*** Διάγραμμα Ποινικού Δικαίου Εκδόσεις Σάκκουλα Αθήνα- Κομοτηνή 1999.

62. ***Του ίδιου*** Μελέτες Ποινικού Δικαίου Εκδόσεις Σάκκουλα Αθήνα-Κομοτηνή 1999.

Β.ΞΕΝΟΓΛΩΣΣΗ

(Σε Ελληνική Μετάφραση)

1. ***Kaiser Gunter*** Ο ποινικός έλεγχος της βαριάς οικονομικής εγκληματικότητας Απόδοση Λ.Κοτσαλή Σειρά Ποινικά 15, Εκδόσεις Α.Σάκκουλα Αθήνα-Κομοτηνή 1983.

2. ***Hassemer W.*** Προβλεπόμενες εξελίξεις στη δογματική του Ποινικού Δικαίου και στην αντεγκληματική πολιτική (Απόδοση στα ελληνικά Γ.Αραπίδου) Υπερ. 1/2000.

3. ***Roxin C.*** Ο καταλογισμός στην αντικειμενική υπόσταση του εγκλήματος Εκδόσεις Ποινικά αρ.21 Αθήνα-Κομοτηνή 1985 Α.Σάκκουλας.

4. ***Sieber U.*** Η εξέλιξη του Ποινικού Δικαίου στα πλαίσια της Ευρωπαϊκής Ένωσης Υπερ.4/1993.

5. ***Tapscott H*** ψηφιακή οικονομία (μετ. Μ.Σίμου) εκδόσεις .Leader Books Αθήνα 2000.

6. ***Tiedemann K.*** Η εγκληματικότητα στο χώρο των ηλεκτρονικών υπολογιστών και η γερμανική μεταρρύθμιση του Ποινικού Δικαίου του 1986 (Μετάφραση Ν.Μπιτσελέκη) Δημοσιεύματα του Ελληνικού Τμήματος της Διεθνούς Εταιρείας Κοινωνικής Αμύνης τευχ.4/1998.

Γ. ΞΕΝΟΓΛΩΣΣΗ

(Αγγλία)

7.***Great Britain Law Commision*** Computer misuse
The Law Commission London H.M.S.O 1988.

8.*Goode* , Electronic banking: The legal implications, Institute of Bankers , London 1985.

(Ηνωμένες Πολιτείες)

9.*Platt C.* Anarchy online New York Harperprism 1996.

10.*Parker D.B* Computer abuse final report Stanford Research Institute.

11..*Scott A.* H. Computer and intellectual property crime federal and state law Washington D.C Bureau of National Affairs 2001.

12.*Loundy D.* Computer crime information warfere and economic espionage Durhan N.C Carolina Academic Press 2003

13.*Hollinger R..C.* Crime, deviance and the computer Aldershot Brookfield, VT Portsmouth 1997.

14..*Smith R.G.* Cyber criminals on trial New York Cambridge University Press 2004.

15..*Doyle C.*Cybercrime an overview of the federal computer fraud and abuse statute and related federal criminal laws New York Novinkta Books 2006.

16.*Stuckey K.d.* Internet and online law New York , NY, Law Journal Press 1996.

17.*Bequai A.* Technocrimes Lexington Mess Books 1987

18.*Duncan J.* White collar crime Washington D.C 1998.

(Γαλλία)

19.*Martin d.* Cybercrime menaces vulnerabilites rispostes Paris presses universitaires de France 2001.

20.*Chatelain Y.* Cybercriminalite LOICK Roche Paris Hermes Science Pubblications 2000.

(Ιταλία)

21.*Buffa F.* Internet e criminalita Milano Giuffre 2001

22.*Carrera M.* I reati commessi con l' uso del computer banche dei dati e tutela della persona Padova CEDAM 1987.

23.*Del Giudice F.* Frode informatica art 640 ter Simone 1998

24.*Domenico Ammiretti* Internet e legge penale Convegno su Internet e legge penale Empoli 2001 Torino Giappichelli 2001

25.*Lemme F.* Diritto penale dell economia CEDAM Padova 1999.

26.*Picotti L.* Il diritto penale dell' informatica nell' epoca di internet Padova CEDAM 2004.

27. ***Pecorella*** , Il Diritto penale dell' Informatica, Milano 1996

28. ***Pedrazzi*** , Inganno ed errore nei delitti contro il patrimonio , Milano , 1995

29.*Codice penale e di procedura penale* Simone Napoli 2004.

(Γερμανία)

30.*Cramer /Schoenke/Schroeder*, StGB Kommentar, 25 Auf, 1997

31.*Gropp*, Die Codekarte : der Schluessel zum Diebstahl, JZ 1987

32.*Hilgendorf E.* Informatiostrafrecht und Rechtsinformatik Berlin Logos-Verl 2004

33.*Kleb-Braun*, Codekartenmissbrauch und Sparbuchfaelle aus Volljuristischer Sicht, JA 1986, 249

34.*Knecht* kriminalistik 1971

35.*Lackner/Koehl*, StGB,23 Aufl.1999

36.*Lenckner*, Computerkriminalitaet und Vermoegensdelikte 1981
Huff, Die Strafbarkeit im Zusammenhang mit Geldautomaten, NStZ 1985,438,

37.*Marbeth- Kubicki A.* Computer und Internet Strafrecht Műnchen C.H.Beck 2005

38.*Maurach/Schroeder/Maiwald*, Strafrecht, Besonderer Teil , T. 1,8 Auf, 1995

39.*Schoenke/Schroeder/Cramer*, StGB, 25 Aufl.1997

40.*Schoenke/Scroeder*, Strafgesetzbuch, Kommentar,27 Aufl.2006

41.*Schubarth/Albrecht*, Kommentar zum schweizerischen Strafrecht. Schweizerisches Strafgesetzbuch, B.T.2

42.*Schmidt,* Das neueschweizerische Computerstrafrecht vom 17 Juni 1994, Computer und Recht 1996, SchwZStR

43.***Sieber***, Computerkriminalitaet im Strafrecht,2,1980

43.*Steinhilper*, Ist die Bedienung von Bargeldautomaten unter missbrauchlichen Vermendung fremder Codekarten strafbar? GA 1985,114.

44.*Wessels-Hillenkamp* BT/2 , 234 .

9. ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

1. www.bka.de
2. www.antiphishing.org
3. http://www.ftc.gov/os/2003/09/synovatereport.pdf
4. ://www.jurpc.de
5. mho.de
6. www.nouskalis.gr
7. http://dsanet.gr
8. http://nomos0.intrasoftnet.com
9. http://europa.eu.int/eur-lex
10. http://lawnet.gr
11. http://www.rand.org/pubs/technical reports/2006/RAND TR337.pdf
12. www.diritto e diritti.it
13. www.penale.it
14. www.ergaomnes.net
15. http://conventions.coe.int/treaty/EN/cadreprincipal.htm

10. Παράρτημα Νομοθετικών Κειμένων

ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Άρθρα Ποινικού Κώδικα

Άρθρο 348Α - Πορνογραφία ανηλίκων

Άρθρο 370Α - Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας

Άρθρο 370Β - Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα.

Άρθρο 370Γ - Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών.

Άρθρο 386Α - Απάτη με υπολογιστή.

Νόμοι

Ν. 2225/94 – «Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»

Ν. 2472/97 και 2774/99 – «Περί προσωπικών δεδομένων»

Ν. 2472/1997 – «Για την προστασία των προσωπικών δεδομένων στο Διαδίκτυο»

Ν. 2774/1999 – «Για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»

Ν. 2867/2000 - «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών»

Ν. 2819/2000 – «Προσθήκη στο Ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων»

Ν. 2225/1994 όπως τροπ. Με Ν. 3115/2003 – «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις»

Ν. 3411/2006 – «Περί ηλεκτρονικών επικοινωνιών».

Οδηγία 90/387/ΕΟΚ του Συμβουλίου της 28ης Ιουνίου 1990 για τη δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Networt Provision -ONP).

Οδηγία 90/388/ΕΟΚ της Επιτροπής της 28ης Ιουνίου 1990 σχετικά με τον ανταγωνισμό στις αγορές των τηλεπικοινωνιακών υπηρεσιών.

Οδηγία 91/250/ΕΟΚ του Συμβουλίου της 14ης Μαΐου 1991 για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών

Οδηγία 96/9/ΕΟΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 1996, σχετικά με τη νομική προστασία των βάσεων δεδομένων.

Οδηγία 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Μαΐου 1997 για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις.

Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

Οδηγία 2002/19/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους (οδηγία για την πρόσβαση).

Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση).

Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο).

Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας).

Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Οδηγία 2002/77/ΕΚ της Επιτροπής, της 16ης Σεπτεμβρίου 2002, σχετικά με τον ανταγωνισμό στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Διεθνείς Συμβάσεις

Συνθήκη των Βρυξελλών (1968) περί προσδιορισμού της δικαιοδοσίας

Σύμβαση για το Κυβερνοχώρο - Βουδαπέστη 23-11-2001

Η Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ της 10-12-1948

Η Σύμβαση της Ρώμης «για την προάσπιση των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθεριών» της 4-11-1950 (ΕΣΔΑ)

Αποφάσεις

Η Υπουργική Απόφαση με αριθ. 88141/1995 - «Κώδικα Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων».

Η Απόφαση της Ε.Ε.Τ.Τ. με αριθ. 268/73/2002 - «Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr»

Η απόφαση της Ε.Ε.Τ.Τ. με αριθ. 248/71/2002 - «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής»

Α.ΚΟΙΝΟΤΙΚΗ ΝΟΜΟΘΕΣΙΑ

Ηλεκτρονικό Εμπόριο-Ηλεκτρονικές Υπογραφές:
Πρόταση Οδηγίας στις 24 Σεπτεμβρίου 2002 για την τροποποίηση της Οδηγίας 68/151/ΕΟΚ σχετικά με τις απαιτήσεις δημοσιότητας για ορισμένες μορφές εταιριών
Κανονισμός 44/2001 ΕΚ για την διεθνή δικαιοδοσία (σε αντικατάσταση της Σύμβασης των Βρυξελλών), άρθρο 23 παρ.2 που αναγνωρίζει το κύρος της ηλεκτρονικής υπογραφής σε συμφωνίες παρέκτασης της διεθνούς δικαιοδοσίας Τελευταία ενημέρωση 22-05-03
Απόφαση της Επιτροπής (2001) για έγκριση ενός παγκοσμίου δικτύου (Identrus) για την πιστοποίηση των ηλεκτρονικών υπογραφών και άλλων συναλλαγών ηλεκτρονικού εμπορίου
Απόφαση 2000/709 της Επιτροπής για τους φορείς ελέγχου και συμμόρφωσης των διατάξεων δημιουργίας της ηλεκτρονικής υπογραφής στους όρους ασφάλειας του Παραρτήματος ΙΙΙ της Οδηγίας 99/93/ΕΚ
Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά ("Οδηγία για το ηλεκτρονικό εμπόριο").
Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
Οδηγία 98/84/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη νομική προστασία των υπηρεσιών που βασίζονται ή συνίστανται στην παροχή πρόσβασης υπό όρους.
Οδηγία 98/48/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 20ής Ιουλίου 1998 για την τροποποίηση της οδηγίας 98/34/ΕΚ για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών
COM(97) 157 Μια Ευρωπαϊκή Πρωτοβουλία στο Ηλεκτρονικό Εμπόριο και

Ηλεκτρονικές Επικοινωνίες

Οδηγία 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά στα δίκτυα και στις υπηρεσίες ηλκτρονικών επικοινωνιών
Οδηγία 2002/21/ΕΚ για το κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/20/ΕΚ για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών
Οδηγία 2002/19/ΕΚ για την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφής ευκολίες
Οδηγία 96/2/ΕΚ για τροποποίηση της οδηγίας 90/388/ΕΟΚ όσον αφορά τις κινητές και προσωπικές επικοινωνίες.

Ηλεκτρονικά συστήματα πληρωμών-Ηλεκτρονικό Χρήμα:

Οδηγία 2002/65/ΕΚ για την εξ αποστάσεως εμπορία χρηματοπιστωτικών υπηρεσιών προς τους καταναλωτές
Οδηγία 2000/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Σεπτεμβρίου 2000 για την ανάληψη, την άσκηση και την προληπτική εποπτεία της δραστηριότητας ιδρύματος ηλεκτρονικού χρήματος.
Τελευταία ενημέρωση 22-05-03
Οδηγία 2000/28/ΕΚ για την ανάληψη και άσκηση δραστηριοτήτων χρηματοπιστωτικών ιδρυμάτων
Οδηγία 2000/35/ΕΚ για την καταπολέμηση της καθυστέρησης πληρωμών στις εμπορικές συναλλαγές
COM (2000) 650 - Πρόταση Οδηγίας του Συμβουλίου για την τροποποίηση της οδηγίας 77/388/ΕΟΚ με στόχο την απλοποίηση, τον εκσυγχρονισμό και την εναρμόνιση των όρων που επιβάλλονται στην τιμολόγηση όσον αφορά το φόρο προστιθέμενης αξίας.
Ανακοίνωση COM(2001) 66 για το ηλεκτρονικό εμπόριο και τις χρηματοπιστωτικές υπηρεσίες
Ψήφισμα COM(2000) 36 του Ευρωπαϊκού Κοινοβουλίου για τις πληρωμές μικρών ποσών στην εσωτερική αγορά
Ανακοίνωση COM(2001) 11 της Επιτροπής για την πρόληψη της απάτης και της πλαστογραφίας όσον αφορά στα μέσα πληρωμής πλην των μετρητών
97/489/ΕΚ: Σύσταση της Επιτροπής της 30ής Ιουλίου 1997 σχετικά με τις συναλλαγές που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου.
Οδηγία 97/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Ιανουαρίου 1997 για τις διασυνοριακές μεταφορές πιστώσεων
Σύσταση 87/598/ΕΟΚ της Επιτροπής της 8ης Δεκεμβρίου 1987 για ευρωπαϊκό κώδικα δεοντολογίας σε θέματα ηλεκτρονικών πληρωμών.

Ονόματα χώρου (domain names)

Κανονισμός 733/2002 για την υλοποίηση του domain name «.eu» τομέα ανώτατου επιπέδου
Οδηγία 1989/104/ΕΟΚ για την προστασία των σημάτων

Πνευματική Ιδιοκτησία:

Οδηγία 2001/29/ΕΚ της 22ας Μαΐου 2001 για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας.
Οδηγία 96/9/ΕΟΚ της 11ης Μαρτίου 1996 σχετικά με τη νομική προστασία των βάσεων δεδομένων.
Οδηγία 92/100/ΕΟΚ σχετικά με το δικαίωμα εκμίσθωσης το δικαίωμα δανεισμού και ορισμένα δικαιώματα συγγενικά προς την πνευματική ιδιοκτησία στον τομέα των προϊόντων της διανοίας.
Τελευταία ενημέρωση 22-05-03

□ Οδηγία 91/250/ΕΟΚ για τη νομική προστασία των προγραμμάτων ηλεκτρονικών Υπολογιστών

□ ***Ηλεκτρονικό Έγκλημα:***

□ Σύσταση του Συμβουλίου 25 Ιουνίου 2002 για σημεία επαφής που λειτουργούν 24 ώρες το εικοσιτετράωρο για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας
□ Έγγραφο Διαβουλεύσεων της Επιτροπής, Ιούνιος 2002 για την ασφάλεια των ηλεκτρονικών δικτύων
□ Σχέδιο Κανόνων της Επιτροπής, Απρίλιος 2002 για τον κοινό ορισμό ορισμένων αδικημάτων που αφορούν υπολογιστές
□ Ψήφισμα του Συμβουλίου 1 Μαρτίου 2002 για την προστασία των καταναλωτών, ιδίως των νέων, με την επισήμανση ορισμένων βιντεοπαιχνιδιών και ηλεκτρονικών παιγνίων αναλόγως της ηλικίας
□ Έγγραφο Πολιτικής της Επιτροπής, Ιανουάριος 2002 για την καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικού υπολογιστή και την βελτίωση της ασφάλειας των υποδομών πληροφορικής με την λήψη νομοθετικών και μη νομοθετικών μέτρων.
□ Απόφαση – Πλαίσιο 2001/413/ΔΕΥ του Συμβουλίου της 28-5-2001 για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών
□ Ανακοίνωση COM (2000) 890 της Επιτροπής «Για μια ασφαλέστερη Κοινωνία της Πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής».
□ Απόφαση 276/1999/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για ένα πολυετές κοινοτικό πρόγραμμα δράσης για ασφαλέστερη χρήση του Internet μέσω της καταπολέμησης του παράνομου και βλαβερού περιεχομένου στα παγκόσμια δίκτυα

□ **Προστασία δεδομένων:**

□ Οδηγία 2002/58/ΕΚ της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
□ Οδηγία 97/66/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.
□ Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

□ ***Προστασία καταναλωτή:***

Τελευταία ενημέρωση 22-05-03
□ Οδηγία 2002/65/ΕΚ για την εξ αποστάσεως εμπορία χρηματοπιστωτικών υπηρεσιών προς τους καταναλωτές και την τροποποίηση των Οδηγιών 1997/7/ΕΚ και 1998/27/ΕΚ
□ Οδηγία 99/44/ΕΚ της 25ης Μαΐου 1999 σχετικά με ορισμένες πτυχές της πώλησης και των εγγυήσεων καταναλωτικών αγαθών
□ COM (1999) 385 Τροποποιημένη Πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εξ αποστάσεως εμπορία χρηματοπιστωτικών υπηρεσιών προς τους καταναλωτές και την τροποποίηση των οδηγιών 97/7/ΕΚ και 98/27/ΕΚ
□ Οδηγία 98/27/ΕΚ περί των αγωγών παραλείψεως στον τομέα της προστασίας των συμφερόντων των καταναλωτών.
□ Σύσταση 98/257/ΕΚ της Επιτροπής της 30ής Μαρτίου 1998 σχετικά με τις αρχές που διέπουν τα αρμόδια όργανα για την εξώδικη επίλυση των διαφορών κατανάλωσης
□ Οδηγία 97/55/ΕΚ για την τροποποίηση της οδηγίας 84/450/ΕΟΚ σχετικά με την παραπλανητική διαφήμιση προκειμένου να συμπεριληφθεί η συγκριτική διαφήμιση
□ Οδηγία 97/7/ΕΚ για την προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις
□ Σύσταση 97/489/ΕΚ της Επιτροπής της 30ής Ιουλίου 1997 σχετικά με τις συναλλαγές

που γίνονται με μέσα ηλεκτρονικής πληρωμής και ιδίως όσον αφορά τις σχέσεις μεταξύ του εκδότη και του κατόχου.
□ Οδηγία 93/13/ΕΟΚ της 5ης Απριλίου 1993 σχετικά με τις καταχρηστικές ρήτρες των συμβάσεων που συνάπτονται με καταναλωτές.
□ Σύσταση 92/295/ΕΟΚ για τους κώδικες δεοντολογίας αναφορικά στην προστασία των καταναλωτών στις συμβάσεις διαπραγματευόμενες από απόσταση
□ Ενοποιημένο κείμενο: Οδηγία 85/374/ΕΟΚ του Συμβουλίου της 25ης Ιουλίου 1985 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σε θέματα ευθύνης λόγω ελαττωματικών προϊόντων, όπως τροποποιήθηκε από την Οδηγία 1999/34/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 10ης Μαΐου 1999

□ **Φορολογία:**

□ Κανονισμός αριθ. 792/2002/ΕΚ της 7ης Μαΐου 2002 για την προσωρινή τροποποίηση του κανονισμού (ΕΟΚ) αριθ. 218/92 σχετικά με τη διοικητική συνεργασία στον τομέα των έμμεσων φόρων (ΦΠΑ) όσον αφορά πρόσθετα μέτρα για το ηλεκτρονικό εμπόριο
□ Οδηγία 2002/38/ΕΚ της 7ης Μαΐου 2002 για την τροποποίηση και την προσωρινή τροποποίηση της οδηγίας 77/388/ΕΟΚ όσον αφορά το σύστημα φόρου προστιθεμένης αξίας που εφαρμόζεται στις ραδιοφωνικές και τηλεοπτικές υπηρεσίες και σε ορισμένες υπηρεσίες που παρέχονται ηλεκτρονικά
Τελευταία ενημέρωση 22-05-03
□ Οδηγία 2001/115/ΕΚ για την τροποποίηση της Οδηγίας 77/288/ΕΟΚ για την απλοποίηση, τον εκσυχρονισμό και την εναρμόνιση των όρων που επιβάλλονται στην τιμολόγηση αναφορικά με τον ΦΠΑ (ειδικότερα α.28 παρ.3 στοιχ.γ)
□ COM (2000) 650 - Πρόταση Οδηγίας του Συμβουλίου για την τροποποίηση της οδηγίας 77/388/ΕΟΚ με στόχο την απλοποίηση, τον εκσυγχρονισμό και την εναρμόνιση των όρων που επιβάλλονται στην τιμολόγηση όσον αφορά το φόρο προστιθέμενης αξίας.
□ COM (2000) 349 1Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΟΚ) αριθ. 218/92 του Συμβουλίου σχετικά με τη διοικητική συνεργασία στον τομέα των έμμεσων φόρων (ΦΠΑ) και Πρόταση Οδηγίας του Συμβουλίου για την τροποποίηση της οδηγίας 388/77/ΕΟΚ όσον αφορά το σύστημα φόρου προστιθέμενης αξίας που εφαρμόζεται σε ορισμένες υπηρεσίες παρεχόμενες με ηλεκτρονικά μέσα.
□ COM (98) 374. Ηλεκτρονικό Εμπόριο και έμμεση φορολογία

□ **Δικονομικά θέματα:**

□ Κανονισμός (ΕΚ) αριθ. 44/2001 του Συμβουλίου της 22ας Δεκεμβρίου 2000 για τη διεθνή δικαιοδοσία, την αναγνώριση και την εκτέλεση αποφάσεων σε αστικές και εμπορικές υποθέσεις.
□ Κανονισμός (ΕΚ) αριθ. 1348/2000 του Συμβουλίου της 29ης Μαΐου 2000 περί επιδόσεως και κοινοποιήσεως στα κράτη μέλη δικαστικών και εξωδίκων πράξεων σε αστικές ή εμπορικές υποθέσεις.

52007DC0267

[pic] | ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ |

Βρυξέλλες, 22.5.2007

COM(2007) 267 τελικό

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ ΚΑΙ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

{SEC(2007) 641}{SEC(2007) 642}

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ ΚΑΙ ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

1. Εισαγωγή

1.1. Τι είναι το έγκλημα στον κυβερνοχώρο;

Τι είναι το έγκλημα στον κυβερνοχώρο;

Η ασφάλεια των συστημάτων πληροφοριών, τα οποία προσλαμβάνουν στις κοινωνίες μας όλο και μεγαλύτερη σημασία, καλύπτει πολλές πτυχές, μεταξύ των οποίων κεντρική θέση έχει η καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Δεδομένου ότι ο ορισμός του εγκλήματος στον κυβερνοχώρο δεν έχει αποτελέσει αντικείμενο συμφωνίας, οι όροι «έγκλημα στον κυβερνοχώρο», «ηλεκτρονικό έγκλημα», «έγκλημα πληροφορικής» ή «έγκλημα υψηλής τεχνολογίας» χρησιμοποιούνται συχνά αδιακρίτως. Για τους σκοπούς της παρούσας ανακοίνωσης, ο όρος «έγκλημα στον κυβερνοχώρο» νοείται ως «αξιόποινες πράξεις που διαπράττονται με χρήση ηλεκτρονικών δικτύων επικοινωνιών και συστημάτων πληροφοριών ή εναντίον αυτών των δικτύων και συστημάτων».

Στην πράξη, ο όρος έγκλημα στον κυβερνοχώρο εφαρμόζεται σε τρεις κατηγορίες αξιόποινων δραστηριοτήτων. Η πρώτη καλύπτει τις παραδοσιακές μορφές αδικημάτων όπως την απάτη ή την πλαστογραφία, παρόλο που, στα πλαίσια του εγκλήματος στον κυβερνοχώρο, αφορά ειδικά αξιόποινες πράξεις οι οποίες διαπράττονται μέσω δικτύων ηλεκτρονικής επικοινωνίας και συστημάτων πληροφοριών (εφεξής: ηλεκτρονικά δίκτυα). Η δεύτερη μορφή αφορά τη δημοσίευση παράνομου περιεχομένου με χρήση ηλεκτρονικών μέσων (π.χ., υλικό σεξουαλικής κακοποίησης παιδιών ή προτροπή σε φυλετικό μίσος). Η τρίτη κατηγορία περιλαμβάνει αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων , π.χ. επιθέσεις κατά συστημάτων πληροφοριών, άρνηση παροχής υπηρεσιών και παράνομη επέμβαση στο σύστημα πληροφοριών. Αυτά τα είδη επίθεσης μπορεί επίσης να στρέφονται κατά των θεμελιωδών υποδομών κρίσιμης σημασίας στην Ευρώπη και να έχουν επιπτώσεις στα υφιστάμενα συστήματα έγκαιρης προειδοποίησης σε πολλούς τομείς, με ενδεχόμενες καταστροφικές συνέπειες για το κοινωνικό σύνολο. Το κοινό στοιχείο μεταξύ αυτών των κατηγοριών αξιόποινων πράξεων είναι ότι μπορούν να διαπραχθούν σε μαζική κλίμακα και με μεγάλη γεωγραφική απόσταση μεταξύ του τόπου της διάπραξης της αξιόποινης πράξης και των συνεπειών της. Ως εκ τούτου, οι τεχνικές πτυχές των εφαρμοζόμενων ανακριτικών μεθόδων είναι συχνά οι ίδιες. Η παρούσα ανακοίνωση εστιάζεται σ'αυτά τα κοινά στοιχεία.

1.2. Οι τελευταίες εξελίξεις όσον αφορά το έγκλημα στον κυβερνοχώρο

1.2.1. Γενικότητες

Ο συνδυασμός της συνεχούς εξέλιξης των αξιόποινων δραστηριοτήτων και της έλλειψης αξιόπιστης πληροφόρησης καθιστά δυσχερή τη διαμόρφωση επακριβούς εικόνας της σημερινής κατάστασης. Εντούτοις, μπορούμε να διακρίνουμε ορισμένες γενικές τάσεις:

- Ο αριθμός των αξιόποινων πράξεων στον κυβερνοχώρο αυξάνεται, ενώ οι αξιόποινες δραστηριότητες όλο και περισσότερο εκσυγχρονίζονται και προσλαμβάνουν διεθνή χαρακτήρα [1]

- Υπάρχουν σαφείς ενδείξεις σχετικά με την αυξανόμενη συμμετοχή ομάδων οργανωμένου εγκλήματος σε αξιόποινες πράξεις στον κυβερνοχώρο

- Εντούτοις, δεν σημειώνεται αύξηση του αριθμού των ποινικών διώξεων που ασκούνται στην Ευρώπη στο πλαίσιο της διασυνοριακής συνεργασίας μεταξύ των αρχών επιβολής του νόμου

1.2.2. Αξιόποινες πράξεις παραδοσιακής μορφής σε ηλεκτρονικά δίκτυα

Οι περισσότερες αξιόποινες πράξεις μπορεί να διαπράττονται με χρήση ηλεκτρονικών δικτύων, και διάφορες κατηγορίες απάτης και απόπειρας απάτης είναι ιδιαιτέρως συνηθισμένες και αποτελούν μορφή εγκληματικότητας η οποία εμφανίζεται όλο και πιο συχνά στα ηλεκτρονικά δίκτυα. Αξιόποινες τεχνικές όπως η κλοπή ταυτότητας, το «ψάρεμα»[2], ανεπίκλητα ηλεκτρονικά μηνύματα και κακόβουλοι κώδικες μπορεί να χρησιμοποιούνται για τη διάπραξη απάτης μεγάλης κλίμακας. Το παράνομο εμπόριο μέσω του Διαδικτύου σε εθνικό και διεθνές επίπεδο συνιστά επίσης πρόβλημα του οποίου η σοβαρότητα αυξάνεται συνεχώς. Στις δραστηριότητες αυτές περιλαμβάνεται η λαθρεμπορία ναρκωτικών, ειδών απειλούμενων με εξαφάνιση και όπλων.

1.2.3. Παράνομο περιεχόμενο

Στην Ευρώπη, υπάρχει πρόσβαση σε έναν συνεχώς αυξανόμενο αριθμό ιστοτόπων με παράνομο περιεχόμενο. Πρόκειται για ιστοτόπους με υλικό σεξουαλικής κακοποίησης παιδιών, προτροπή σε τρομοκρατικές ενέργειες, παράνομη εξύμνηση της βίας, της τρομοκρατίας, του ρατσισμού και της ξενοφοβίας. Η δράση για την επιβολή του νόμου εναντίον αυτών των ιστοτόπων είναι εξαιρετικά δυσχερής, δεδομένου ότι οι ιδιοκτήτες και οι διαχειριστές τους βρίσκονται συχνά σε χώρες διαφορετικές από τη χώρα–στόχο, και συχνά εκτός της ΕΕ. Οι ιστότοποι αυτοί μπορούν να μετατοπίζονται με μεγάλη ταχύτητα, εντός και εκτός της εδαφικής επικράτειας της ΕΕ, ενώ ο ορισμός του παρανόμου σ' αυτόν τον τομέα παρουσιάζει μεγάλες διαφορές από το ένα κράτος στο άλλο.

1.2.4. Αξιόποινες πράξεις που μπορούν να διαπραχθούν μόνο μέσω ηλεκτρονικών δικτύων

Οι επιθέσεις μεγάλης κλίμακας που στρέφονται εναντίον συστημάτων πληροφοριών ή οργανισμών και ατόμων (συχνά μέσω των επονομαζόμενων «δικτύων προγραμμάτων ρομπότ» (botnets[3])) φαίνεται ότι εμφανίζονται με συνεχώς αυξανόμενη συχνότητα. Επίσης, έχουν σημειωθεί προσφάτως περιστατικά συστηματικών, καλά συντονισμένων και ευρείας κλίμακας άμεσων επιθέσεων κατά των κρίσιμων υποδομών πληροφόρησης ενός κράτους. Το φαινόμενο αυτό έχει επιδεινωθεί εξαιτίας της συγχώνευσης των τεχνολογιών και της επιταχυνόμενης διασύνδεσης των συστημάτων πληροφοριών, στις οποίες οφείλεται το γεγονός ότι τα συστήματα αυτά έχουν γίνει πιο ευάλωτα. Οι επιθέσεις αυτές είναι συχνά καλά οργανωμένες και χρησιμοποιούνται για σκοπούς εκβιαστικής απόσπασης. Μπορούμε να υποθέσουμε ότι τα κρούσματα αυτά παρουσιάζονται έτσι ώστε να μετριάζεται η σοβαρότητά τους, πράγμα που οφείλεται εν μέρει στο ενδεχόμενο ζημιών των εμπορικών συμφερόντων των εμπλεκόμενων επιχειρήσεων σε περίπτωση που θα δινόταν δημοσιότητα σε προβλήματα ασφάλειας.

1.3. Οι στόχοι

Λαμβάνοντας υπόψη αυτές τις συνεχείς εξελίξεις, συμπεραίνουμε ότι υπάρχει επείγουσα ανάγκη να ληφθούν μέτρα – σε εθνικό και σε ευρωπαϊκό επίπεδο –κατά όλων των μορφών εγκλήματος στον κυβερνοχώρο, που συνιστούν όλο και πιο σημαντικές απειλές για την κοινωνία, τις επιχειρήσεις και τους πολίτες. Η προστασία των ατόμων κατά του εγκλήματος στον κυβερνοχώρο περιπλέκεται συχνά εξ αιτίας προβλημάτων που έχουν σχέση με τον προσδιορισμό της αρμόδιας δικαιοδοσίας, με την εφαρμοστέα νομοθεσία, με τη διασυνοριακή επιβολή του νόμου ή με την αναγνώριση και τη χρησιμοποίηση ηλεκτρονικών αποδεικτικών στοιχείων. Η κατ' ουσίαν διασυνοριακή φύση του εγκλήματος στον κυβερνοχώρο οξύνει αυτά τα προβλήματα. Για να αντιμετωπίσει αυτές τις απειλές, η Επιτροπή εγκαινιάζει πρωτοβουλία υπέρ γενικής πολιτικής η οποία αποσκοπεί στη βελτίωση του συντονισμού της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε ευρωπαϊκό και διεθνές επίπεδο.

Σκοπός είναι η ενίσχυση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο. Τα κράτη μέλη και η Επιτροπή εκτιμούν εδώ και πολύ καιρό ότι η περαιτέρω διαμόρφωση συγκεκριμένης πολιτικής της ΕΕ για αυτά τα ζητήματα, ιδίως, αποτελεί προτεραιότητα. Η πρωτοβουλία θα επικεντρωθεί σε δύο από τις διαστάσεις αυτής της καταπολέμησης, την επιβολή του νόμου και το ποινικό δίκαιο· η πολιτική που θα διαμορφωθεί θα συμπληρώσει άλλα μέτρα της ΕΕ τα οποία αποσκοπούν στη βελτίωση της ασφάλειας στον κυβερνοχώρο εν γένει. Μακροπρόθεσμα, η πολιτική αυτή θα περιλαμβάνει: βελτιωμένη επιχειρησιακή συνεργασία μεταξύ των αρχών επιβολής του νόμου· βελτιωμένη πολιτική συνεργασία και συντονισμό μεταξύ των κρατών μελών· πολιτική και νομική συνεργασία με τρίτες χώρες· ευαισθητοποίηση· κατάρτιση· έρευνα· ενισχυμένο διάλογο με τις επιχειρήσεις και ενδεχομένως νομοθετικά μέτρα.

Η πολιτική σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και με τις συναφείς δικαστικές προσφυγές θα καθοριστεί και θα υλοποιηθεί με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων, ιδίως του δικαιώματος έκφρασης της γνώμης, του σεβασμού της ιδιωτικής και οικογενειακής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Κάθε νομοθετικό μέτρο που θα λαμβάνεται στο πλαίσιο αυτής της πολιτικής θα εξετάζεται προηγουμένως για να αξιολογηθεί η συμβατότητά του με τα δικαιώματα αυτά, ιδίως υπό το πρίσμα του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Σημειωτέον επίσης ότι όλες αυτές οι πολιτικές πρωτοβουλίες θα υλοποιηθούν λαμβάνοντας πλήρως υπόψη τα άρθρα 12 έως 15 της επονομαζόμενης οδηγίας για το ηλεκτρονικό εμπόριο[4], στις περιπτώσεις που αυτό το νομικό μέσο είναι εφαρμοστέο.

Ο στόχος της παρούσας ανακοίνωσης μπορεί να υποδιαιρεθεί σε τρείς κύριες λειτουργικές πτυχές, οι οποίες μπορούν να συνοψιστούν ως εξής:

- Βελτίωση και διευκόλυνση του συντονισμού και της συνεργασίας μεταξύ των μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο, άλλων αρμόδιων αρχών και άλλων εμπειρογνωμόνων στην Ευρωπαϊκή Ένωση

- Διαμόρφωση, σε συνεργασία με τα κράτη μέλη, με τους αρμόδιους ευρωπαϊκούς και διεθνείς οργανισμούς και με άλλα ενδιαφερόμενα μέρη, ενός συνεκτικού πλαισίου πολιτικών της ΕΕ για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

- Ευαισθητοποίηση σχετικά με το κόστος και τους κινδύνους που συνεπάγεται το έγκλημα στον κυβερνοχώρο.

2. Υφιστάμενα νομικα μεσα για την καταπολεμηση του εγκληματοσ στον κυβερνοχωρο

2.1. Υφιστάμενα μέσα και μέτρα στο επίπεδο της ΕΕ

Η παρούσα ανακοίνωση σχετικά με την πολιτική για το έγκλημα στον κυβερνοχώρο παγιώνει και αναπτύσσει την ανακοίνωση του 2001 για μια ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής[5] (εφεξής: η ανακοίνωση του 2001). Η ανακοίνωση του 2001 πρότεινε κατάλληλες ουσιαστικές και διαδικαστικές νομοθετικές διατάξεις για την αντιμετώπιση τόσο των εγχώριων όσο και των

διεθνικών αξιόποινων ενεργειών. Η ανακοίνωση αυτή είχε ως επακόλουθο πολλές σημαντικές προτάσεις, μεταξύ των οποίων, ιδίως, αυτές οι οποίες περιλάμβαναν την πρόταση που οδήγησε στην οδηγία πλαίσιο 2005/222/ΔΕΥ για τις επιθέσεις κατά των συστημάτων πληροφοριών[6]. Σημειωτέον σχετικά με τα προαναφερόμενα ότι έχουν επίσης ληφθεί και άλλα, γενικότερα νομοθετικά μέτρα τα οποία καλύπτουν επίσης πτυχές της καταπολέμησης του εγκλήματος στον κυβερνοχώρο, όπως η απόφαση πλαίσιο 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών[7].

Η *απόφαση* Πλαίσιο 2004/68/ΔΕΥ για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών[8] είναι ένα καλό παράδειγμα της ιδιαίτερης έμφασης που δίνει η Επιτροπή στην προστασία των παιδιών , ιδίως σε σχέση με την καταπολέμηση κάθε μορφής υλικού σεξουαλικής κακοποίησης παιδιών το οποίο δημοσιεύεται παράνομα με χρήση συστημάτων πληροφοριών· πρόκειται για οριζόντια προτεραιότητα που θα εξακολουθήσει να ισχύει και μελλοντικά.

Για να απαντήσει στις προκλήσεις που αφορούν την κοινωνία της πληροφορίας, η Ευρωπαϊκή Κοινότητα έχει διαμορφώσει τρίπτυχη προσέγγιση σχετικά με την ασφάλεια των δικτύων και της πληροφόρησης: ειδικά μέτρα για την ασφάλεια των δικτύων και της πληροφόρησης, το κανονιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Παρόλο που οι τρεις αυτές πτυχές μπορούν, ως έναν ορισμένο βαθμό, να αναπτυχθούν ξεχωριστά, οι πολυάριθμες αλληλεξαρτήσεις μεταξύ τους συνιστούν επιχείρημα υπέρ της στενής συνεργασίας. Στον συναφή τομέα της ασφάλειας των δικτύων και των πληροφοριών έχει εκδοθεί, εκ παραλλήλου με την ανακοίνωση του 2001 για το έγκλημα στον κυβερνοχώρο, πρόταση ευρωπαϊκής πολιτικής[9]. Η οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών ορίζει υποχρέωση για τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών διαθέσιμων στο κοινό να κατοχυρώνουν την ασφάλεια των υπηρεσιών τους. Σ' αυτή την οδηγία προβλέπονται επίσης διατάξεις για την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων και των κατασκοπευτικών λογισμικών. Η ασφάλεια των δικτύων και των πληροφοριών έχει έκτοτε αναπτυχθεί μέσω ενός αριθμού δράσεων, πιο πρόσφατα με τις ανακοινώσεις σχετικά με μια στρατηγική για ασφαλή κοινωνία της πληροφορίας[10]στην οποία παρουσιάζεται η αναζωογονημένη στρατηγική και ορίζεται το πλαίσιο που επιτρέπει την εμβάθυνση και τη διευκρίνιση συνεκτικής προσέγγισης όσον αφορά την ασφάλεια των δικτύων και των πληροφοριών, καθώς επίσης και στην ανακοίνωση σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού [11], και με τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών το 2004[12]. Ο κύριος στόχος του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών είναι να αποκτήσει την εμπειρογνωμοσύνη που χρειάζεται για την προώθηση της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα και για να παρέχει αρωγή στην Επιτροπή και τα κράτη μέλη. Τα πορίσματα των ερευνών στον τομέα των τεχνολογιών για την εξασφάλιση της ασφάλειας των συστημάτων πληροφοριών θα διαδραματίσουν επίσης σημαντικό ρόλο κατά την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Συνεπώς, οι τεχνολογίες πληροφοριών και επικοινωνιών καθώς επίσης και η ασφάλεια περιλαμβάνονται μεταξύ των στόχων του Έβδομου Ερευνητικού Προγράμματος Πλαισίου της ΕΕ (7ο ΠΠ), που θα ισχύει για την περίοδο 2007-2013[13]. Η αναθεώρηση του κανονιστικού πλαισίου το οποίο διέπει τις ηλεκτρονικές επικοινωνίες θα μπορούσε να συνεπάγεται τροποποιήσεις έτσι ώστε να ενισχυθεί η αποτελεσματικότητα των σχετικών με την ασφάλεια διατάξεων της οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία[14].

2.2. Τα υφιστάμενα διεθνή μέσα

Λόγω της παγκόσμιας φύσης των δικτύων πληροφοριών, καμία πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο δεν μπορεί να είναι αποτελεσματική αν οι προσπάθειες περιορίζονται εντός της ΕΕ. Οι κακοποιοί μπορούν

όχι μόνο να επιτίθενται σε συστήματα πληροφοριών ή να διαπράττουν αξιόποινες πράξεις από το ένα κράτος μέλος στο άλλο, αλλά μπορούν να τις διαπράττουν επίσης με ευκολία όταν βρίσκονται εκτός της δικαιοδοσίας της ΕΕ. Συνεπώς, η Επιτροπή έχει συμμετάσχει ενεργά σε διεθνείς συζητήσεις και δομές συνεργασίας, όπως στην ομάδα Λυών-Ρώμη του G 8 για το έγκλημα υψηλής τεχνολογίας και σε έργα που διαχειρίζεται η Ιντερπόλ. Η Επιτροπή παρακολουθεί στενά, ιδίως, τις εργασίες του δικτύου 24ωρων επαφών σχετικά με το διεθνές έγκλημα υψηλής τεχνολογίας (το δίκτυο 24/7)[15], μέλη του οποίου είναι ένας σημαντικός αριθμός κρατών παγκοσμίως, συμπεριλαμβανομένων των περισσότερων κρατών μελών της ΕΕ. Το δίκτυο του G8 είναι μηχανισμός ο οποίος επιτρέπει την επιτάχυνση των επαφών μεταξύ των συμμετεχόντων κρατών, με σημεία επαφής που λειτουργούν 24 ώρες το 24ωρο για υποθέσεις για τις οποίες υπάρχουν ηλεκτρονικά αποδεικτικά στοιχεία, και για υποθέσεις για τις οποίες απαιτείται κατεπείγουσα αρωγή από αρχές επιβολής του νόμου άλλων χωρών.

Σ' αυτόν τον τομέα, το κυριότερο ευρωπαϊκό και διεθνές μέσο είναι αναμφισβήτητα η Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης το 2001[16]. Η Σύμβαση αυτή, η οποία έχει εκδοθεί και τεθεί σε ισχύ το 2004, περιλαμβάνει κοινούς ορισμούς διαφόρων ειδών εγκλήματος στον κυβερνοχώρο και θέτει τις βάσεις για επιχειρησιακή δικαστική συνεργασία μεταξύ των συμβαλλομένων κρατών. Την έχουν υπογράψει πολλά κράτη, συμπεριλαμβανομένων των ΗΠΑ και άλλων μη ευρωπαϊκών κρατών, καθώς επίσης και όλα τα κράτη μέλη. Ένας ορισμένος αριθμός κρατών μελών δεν έχουν ακόμα επικυρώσει αυτή τη σύμβαση ή το συμπληρωματικό πρωτόκολλό της που αφορά τις πράξεις ρατσιστικής και ξενοφοβικής φύσης οι οποίες διαπράττονται μέσω συστημάτων υπολογιστή. Δεδομένου ότι όλοι συμφωνούν για τη σημασία αυτής της Σύμβασης, η Επιτροπή θα ενθαρρύνει τα κράτη μέλη και τις οικείες τρίτες χώρες να επικυρώσουν τη Σύμβαση και εξετάζει τη δυνατότητα η Ευρωπαϊκή Κοινότητα να αποτελέσει συμβαλλόμενο μέρος της Σύμβασης.

3. Περαιτέρω διαμορφωση ειδικων μεσων για την καταπολεμηση του εγκληματοσ στον κυβερνοχωρο

3.1. Ενίσχυση της επιχειρησιακής συνεργασίας για την επιβολή του νόμου και των προσπαθειών κατάρτισης στο επίπεδο της ΕΕ

Η έλλειψη, ή η ανεπαρκής χρησιμοποίηση των άμεσων δομών για την επιχειρησιακή διασυνοριακή συνεργασία εξακολουθεί να αποτελεί αδυναμία μείζονος σημασίας στον τομέα της Δικαιοσύνης, της Ελευθερίας και της Ασφάλειας. Η παραδοσιακή αλληλοβοήθεια, όταν πρόκειται για επείγουσες υποθέσεις εγκλήματος στον κυβερνοχώρο, έχει αποδειχθεί ότι πάσχει από βραδύτητα και αναποτελεσματικότητα, ενώ δεν έχουν ακόμα αναπτυχθεί επαρκώς νέες δομές συνεργασίας. Παρόλο που οι εθνικές δικαστικές αρχές και οι αρχές επιβολής του νόμου συνεργάζονται στενά στην Ευρώπη μέσω της Ευρωπαϊκής Αστυνομικής Υπηρεσίας (Europol), της Eurojust και άλλων οργανισμών, παραμένει η προφανής ανάγκη ενίσχυσης και διευκρίνισης των αρμοδιοτήτων. Από διαβουλεύσεις που έχει αναλάβει η Επιτροπή, φαίνεται ότι αυτά τα κρίσιμης σημασίας μέσα δεν χρησιμοποιούνται κατά τον βέλτιστο δυνατό τρόπο. Μια περισσότερο συντονισμένη ευρωπαϊκή προσέγγιση πρέπει να είναι τόσο επιχειρησιακή όσο και στρατηγική και να καλύπτει επίσης την ανταλλαγή πληροφοριών και τις βέλτιστες πρακτικές.

Στο εγγύς μέλλον, η Επιτροπή θα δώσει ιδιαίτερη έμφαση στις ανάγκες κατάρτισης. Είναι αποδεδειγμένο ότι οι τεχνολογικές εξελίξεις δημιουργούν ανάγκη διαρκούς κατάρτισης των αρχών επιβολής του νόμου και των δικαστικών αρχών όσον αφορά ζητήματα σχετικά με το έγκλημα στον κυβερνοχώρο. Κατά συνέπεια, προβλέπεται ενισχυμένη και καλύτερα συντονισμένη χρηματική στήριξη από την ΕΕ σε πολυεθνικά προγράμματα κατάρτισης. Η Επιτροπή πρόκειται επίσης, σε στενή συνεργασία με τα κράτη μέλη και με άλλους αρμόδιους οργανισμούς όπως η Europol, η Eurojust, η Ευρωπαϊκή Αστυνομική Ακαδημία (CEPOL) και το Ευρωπαϊκό Δίκτυο Κατάρτισης Δικαστικών (EJNT), να εργαστεί για να επιτύχει συντονισμό και διασύνδεση όλων των οικείων προγραμμάτων κατάρτισης σε επίπεδο ΕΕ.

Η Επιτροπή θα διοργανώσει συνάντηση μεταξύ εμπειρογνωμόνων στον τομέα της επιβολής του νόμου, οι οποίοι θα προέρχονται από τα κράτη μέλη αλλά επίσης και από την Europol, το CEPOL και EJTN, για να συζητήσουν πώς θα βελτιωθεί η στρατηγική και επιχειρησιακή συνεργασία καθώς επίσης και η κατάρτιση σχετικά με το έγκλημα στον κυβερνοχώρο στην Ευρώπη το 2007. Μεταξύ άλλων, θα εξεταστεί η σκοπιμότητα της δημιουργίας μονίμου ευρωπαϊκού σημείου επαφής για ανταλλαγή πληροφοριών καθώς επίσης και ευρωπαϊκής πλατφόρμας κατάρτισης σχετικά με το έγκλημα στον κυβερνοχώρο. Αυτή η συνάντηση του 2007 θα είναι η πρώτη μιας σειράς συναντήσεων που έχουν προγραμματιστεί για το εγγύς μέλλον.

3.2. *Ενίσχυση του διαλόγου με τη βιομηχανία*

Τόσο ο ιδιωτικός όσο και ο δημόσιος τομέας έχουν συμφέρον να διαμορφώσουν από κοινού μεθόδους ανίχνευσης και πρόληψης των ζημιών που προξενούνται από τις αξιόποινες δραστηριότητες. Η κοινή συμμετοχή του ιδιωτικού και του δημόσιου τομέα, βασιζόμενη σε αμοιβαία εμπιστοσύνη και έχοντας κοινό στόχο τη μείωση των ζημιών, υπόσχεται να αποτελέσει αποτελεσματικό δρόμο για τη βελτίωση της ασφάλειας, όσον αφορά επίσης και την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η δημόσια και η ιδιωτική πτυχή της πολιτικής της Επιτροπής όσον αφορά το έγκλημα στον κυβερνοχώρο θα αποτελέσουν εν καιρώ μέρος προγραμματισμένης σφαιρικής ευρωπαϊκής πολιτικής για τον διάλογο μεταξύ του δημόσιου και του ιδιωτικού τομέα, καλύπτοντας ολόκληρο τον τομέα της ευρωπαϊκής ασφάλειας. Η πολιτική αυτή θα σημειώσει πρόοδο, ιδίως, χάρη στο ευρωπαϊκό φόρουμ για την ασφάλεια, την έρευνα και την καινοτομία, το οποίο η Επιτροπή σχεδιάζει να δημιουργήσει στο εγγύς μέλλον και στο οποίο θα συμμετέχουν τα ενδιαφερόμενα μέρη του δημόσιου και του ιδιωτικού τομέα.

Οι εξελίξεις σχετικά με τις σύγχρονες τεχνολογίες πληροφοριών και τα συστήματα ηλεκτρονικής επικοινωνίας ελέγχονται σε μεγάλο βαθμό από ιδιωτικές επιχειρήσεις. Ιδιωτικές εταιρίες πραγματοποιούν αξιολογήσεις κινδύνων, καταρτίζουν προγράμματα καταπολέμησης των αξιόποινων πράξεων και επινοούν τεχνικές λύσεις για την πρόληψη των αξιόποινων πράξεων. Η βιομηχανία έχει φανεί πολύ πρόθυμη να βοηθήσει τις δημόσιες αρχές για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, ιδίως όσον αφορά την καταπολέμηση της παιδοφιλικής πορνογραφίας[17] και άλλα είδη παράνομου περιεχομένου στο Διαδίκτυο.

Ένα άλλο ζήτημα αφορά την εμφανή έλλειψη ανταλλαγής πληροφοριών, εμπειρογνωμοσύνης και βέλτιστων πρακτικών μεταξύ του δημόσιου και του ιδιωτικού τομέα. Συχνά, για να προστατεύσουν τα εμπορικά τους πρότυπα και μυστικά, οι επιχειρήσεις του ιδιωτικού τομέα είναι απρόθυμες, ή δεν δεσμεύονται από τη νομοθεσία από καμία σαφή υποχρέωση ώστε να αναφέρουν ή να συμμερίζονται με τις αρχές επιβολής του νόμου χρήσιμες πληροφορίες σχετικά με αξιόποινες δραστηριότητες. Εντούτοις, οι πληροφορίες αυτές μπορεί να είναι απαραίτητες για να είναι σε θέση οι δημόσιες αρχές να διαμορφώνουν αποτελεσματική και κατάλληλη πολιτική καταπολέμησης των αξιόποινων πράξεων. Οι δυνατότητες βελτίωσης της διατομεακής ανταλλαγής πληροφοριών θα εξεταστούν επίσης υπό το πρίσμα των εν ισχύ κανόνων για την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η Επιτροπή διαδραματίζει ήδη σημαντικό ρόλο σε διάφορες δομές με συμμετοχή του δημοσίου και του ιδιωτικού τομέα οι οποίες καταπολεμούν το έγκλημα στον κυβερνοχώρο, όπως είναι η Ομάδα Εμπειρογνωμόνων για την πρόληψη της απάτης[18]. Η Επιτροπή είναι πεπεισμένη για το ότι μια αποτελεσματική γενική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο πρέπει επίσης να περιλαμβάνει στρατηγική συνεργασίας μεταξύ των επιχειρήσεων του δημόσιου και του ιδιωτικού τομέα, συμπεριλαμβανομένων των οργανώσεων της κοινωνίας των πολιτών.

Για να επιτύχει τη διεύρυνση της συνεργασίας μεταξύ του δημοσίου και του ιδιωτικού τομέα για τα ζητήματα αυτά, η Επιτροπή πρόκειται να διοργανώσει εντός του 2007 συνεδρίαση μεταξύ εμπειρογνωμόνων των αρχών επιβολής του νόμου και

εκπροσώπων του ιδιωτικού τομέα, ιδίως παρόχων υπηρεσιών Διαδικτύου, για να συζητήσουν το πώς θα βελτιώσουν την επιχειρησιακή συνεργασία στην Ευρώπη μεταξύ του δημόσιου και του ιδιωτικού τομέα[19]. Κατά τη διάρκεια αυτής της συνεδρίασης θα συζητηθούν όλα τα θέματα που θα κριθεί ότι μπορεί να προσθέσουν αξία σε αμφότερους τους τομείς, αλλά κυρίως τα ακόλουθα:

- Βελτίωση της επιχειρησιακής συνεργασίας κατά την καταπολέμηση αξιόποινων πράξεων και παράνομου περιεχομένου του Διαδικτύου, ειδικότερα στους τομείς της τρομοκρατίας, του υλικού σεξουαλικής κακοποίησης παιδιών και άλλων αξιόποινων δραστηριοτήτων ιδιαίτερα ευαίσθητων από τη σκοπιά της προστασίας των παιδιών

- Εγκαινίαση συμφωνιών μεταξύ του δημόσιου και του ιδιωτικού τομέα με σκοπό την παρεμπόδιση, σε όλα τα κράτη μέλη της ΕΕ, ιστοτόπων που περιλαμβάνουν παράνομο υλικό, ειδικότερα υλικό σεξουαλικής κακοποίησης παιδιών

- Διαμόρφωση προτύπου για την ανταλλαγή απαραίτητων και χρήσιμων πληροφοριών μεταξύ του ιδιωτικού και του δημόσιου τομέα· ένας από τους σχετικούς προβληματισμούς θα είναι η καλλιέργεια ατμόσφαιρας αμοιβαίας εμπιστοσύνης και λήψης υπόψη των συμφερόντων όλων των μερών

- Δημιουργία δικτύου σημείων επαφής για την επιβολή του νόμου, τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα

3.3. Η νομοθεσία

Η γενική εναρμόνιση των ορισμών των αξιόποινων πράξεων και των εθνικών ποινικών νομοθεσιών στον τομέα του εγκλήματος στον κυβερνοχώρο δεν είναι ακόμα σκόπιμη, λόγω της ποικιλομορφίας των ειδών αδικημάτων που καλύπτονται από την έννοια αυτή. Δεδομένου ότι η αποτελεσματική συνεργασία μεταξύ των αρχών επιβολής του νόμου εξαρτάται συχνά από το κατά πόσον έχουν τουλάχιστον εν μέρει εναρμονιστεί οι ορισμοί των αξιόποινων πράξεων, η εξακολούθηση της εναρμόνισης των νομοθεσιών των κρατών μελών συνεχίζει να αποτελεί στόχο μακροπρόθεσμο[20]. Όσον αφορά ορισμένους από τους ορισμούς των κυριότερων αξιόποινων πράξεων, έχει ήδη σημειωθεί ένα σημαντικό βήμα με την απόφαση πλαίσιο σχετικά με τις επιθέσεις εναντίον συστημάτων πληροφοριών. Όπως περιγράφεται ως άνω, έχουν εν τω μεταξύ εμφανιστεί νέες απειλές και η Επιτροπή παρακολουθεί προσεκτικά αυτές τις εξελίξεις, δεδομένης της σημασίας που έχει η διαρκής αξιολόγηση των αναγκών επιπρόσθετων νομοθετικών μέτρων. Η παρακολούθηση των εξελίξεων σχετικά με αυτές τις απειλές είναι στενά συντονισμένη με το Ευρωπαϊκό Πρόγραμμα Προστασίας των Υποδομών Ζωτικής Σημασίας.

Ωστόσο, θα πρέπει επίσης να προβλεφθεί η λήψη στοχοθετημένων νομοθετικών μέτρων για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Ένα ιδιαίτερο ζήτημα για το οποίο ενδέχεται να απαιτηθεί λήψη νομοθετικών μέτρων αφορά τις καταστάσεις στις οποίες το έγκλημα στον κυβερνοχώρο διαπράττεται σε συνδυασμό με κλοπή ταυτότητας. Κατά γενικό κανόνα, «κλοπή ταυτότητας» νοείται η χρησιμοποίηση προσωπικών στοιχείων ταυτοποίησης, π.χ. ενός αριθμού πιστωτικής κάρτας, ως μέσο για διάπραξη άλλων αξιόποινων πράξεων. Στα περισσότερα κράτη μέλη, ο κακοποιός που διαπράττει κλοπή ταυτότητας θα διωχθεί κατά πάσαν πιθανότητα για την απάτη, ή ενδεχομένως για κάποια άλλο αδίκημα, μάλλον αντί για την κλοπή ταυτότητας, δεδομένου ότι η απάτη θεωρείται ότι αποτελεί σοβαρότερο αδίκημα. Η κλοπή ταυτότητας αυτή καθεαυτή δεν συνιστά αξιόποινη πράξη σε όλα τα κράτη μέλη. Είναι συχνά ευκολότερο να αποδειχτεί το αδίκημα της κλοπής ταυτότητας από το αδίκημα της απάτης, έτσι ώστε η ευρωπαϊκή συνεργασία στον τομέα της επιβολής του νόμου θα επωφεληθεί αν η κλοπή ταυτότητας θεωρείται αξιόποινη πράξη σε όλα τα κράτη μέλη. Η Επιτροπή πρόκειται εντός του 2007 να εγκαινιάσει διαβουλεύσεις για να καθοριστεί κατά πόσον είναι σκόπιμη η λήψη νομοθετικών μέτρων.

3.4. Η κατάρτιση στατιστικών

Αποτελεί αντικείμενο γενικής συμφωνίας ότι είναι σε μεγάλο βαθμό ακατάλληλη η παρούσα κατάσταση της πληροφόρησης σχετικά με την επικράτηση της

εγκληματικότητας, και ιδίως ότι χρειάζεται να βελτιωθεί σε μεγάλο βαθμό για να καταστεί εφικτή η σύγκριση δεδομένων μεταξύ κρατών μελών. Ένα φιλόδοξο πενταετές πρόγραμμα για την αντιμετώπιση αυτού του προβλήματος εκτίθεται στην ανακοίνωση της Επιτροπής για χάραξη ολοκληρωμένης και συνεκτικής στρατηγικής της ΕΕ για την κατάρτιση στατιστικών σχετικά με την εγκληματικότητα και την ποινική δικαιοσύνη: Σχέδιο Δράσης της ΕΕ 2006 – 2010 της[21]. Η Ομάδα Εμπειρογνωμόνων που συγκροτήθηκε δυνάμει αυτού του σχεδίου δράσης αναμένεται ότι θα αποτελέσει κατάλληλο πλαίσιο για τη διαμόρφωση των απαιτούμενων δεικτών για τη μέτρηση της έκτασης του εγκλήματος στον κυβερνοχώρο.

4. Η ακολουθητέα οδος

Η Επιτροπή σκοπεύει εφεξής να προχωρήσει όσον αφορά τη γενική πολιτική καταπολέμησης του εγκλήματος στον κυβερνοχώρο. Λόγω των περιορισμένων εξουσιών της Επιτροπής στον τομέα του ποινικού δικαίου, η πολιτική αυτή μπορεί μόνο να αποτελέσει συμπλήρωμα των μέτρων που λαμβάνονται από τα κράτη μέλη και από άλλους φορείς. Τα σημαντικότερα μέτρα – έκαστο εκ των οποίων θα συνεπάγεται τη χρησιμοποίηση ενός, πολλών ή όλων των μέσων που παρουσιάζονται στο κεφάλαιο 3 – θα στηριχθούν επίσης μέσω του χρηματοδοτικού προγράμματος «Πρόληψη και Καταπολέμηση του Εγκλήματος».

4.1. Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο εν γένει

- Εξασφάλιση ενισχυμένης επιχειρησιακής συνεργασίας μεταξύ των αρχών επιβολής του νόμου και των δικαστικών αρχών των κρατών μελών, δράση η οποία θα αρχίσει με τη διοργάνωση ειδικής συνεδρίασης μεταξύ εμπειρογνωμόνων το 2007 και η οποία ενδέχεται να περιλαμβάνει τη δημιουργία ενός κεντρικού σημείου επαφής της ΕΕ όσον αφορά το έγκλημα στον κυβερνοχώρο

- Μεγέθυνση της χρηματοδοτικής στήριξης σε πρωτοβουλίες για βελτίωση της κατάρτισης των αρχών επιβολής του νόμου και των δικαστικών αρχών σχετικά με τους χειρισμούς που αφορούν υποθέσεις εγκλήματος στον κυβερνοχώρο και λήψη μέτρων για τον συντονισμό όλων των πολυεθνικών προσπαθειών κατάρτισης σ' αυτόν τον τομέα, χάρη στη δημιουργία πλατφόρμας κατάρτισης της ΕΕ

- Παρακίνηση των κρατών μελών και όλων των δημόσιων αρχών να δώσουν μεγαλύτερη έμφαση στη λήψη αποτελεσματικών μέτρων καταπολέμησης του εγκλήματος στον κυβερνοχώρο και στη χορήγηση επαρκών πόρων για την καταπολέμησή του

- Στήριξη των ερευνητικών δραστηριοτήτων που συμβάλλουν στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο

- Διοργάνωση τουλάχιστον ενός συνεδρίου μείζονος σημασίας (το 2007) με συμμετοχή των αρχών επιβολής του νόμου και φορέων του ιδιωτικού τομέα, ιδίως για την εγκαινίαση συνεργασίας για την καταπολέμηση των παρανόμων δραστηριοτήτων στο Διαδίκτυο, με χρήση ηλεκτρονικών δικτύων και εναντίον τους, καθώς επίσης και για την προώθηση αποτελεσματικότερων ανταλλαγών πληροφοριών μη προσωπικού χαρακτήρα, και για τη μεταπαρακολούθηση των πορισμάτων αυτού του συνεδρίου του 2007 με συγκεκριμένα σχέδια συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα

- Ανάληψη πρωτοβουλίας και συμμετοχή σε δράσεις με από κοινού συμμετοχή του δημόσιου και του ιδιωτικού τομέα οι οποίες αποσκοπούν στην ευαισθητοποίηση, ιδίως μεταξύ των καταναλωτών, του κόστους και των κινδύνων που αντιπροσωπεύει το έγκλημα στον κυβερνοχώρο, αποφεύγοντας εκ παραλλήλου την υπονόμευση της εμπιστοσύνης των καταναλωτών και των χρηστών την οποία θα συνεπάγετο η εστίαση στις αρνητικές μόνο πτυχές της ασφάλειας

- Ενεργός συμμετοχή και προώθηση της διεθνούς συνεργασίας παγκοσμίως για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

- Εγκαινίαση, συμβολή και παροχή στήριξης σε διεθνή σχέδια έργων που είναι σύμφωνα με την πολιτική της Επιτροπής σ' αυτόν τον τομέα, π.χ. έργα τα οποία

διαχειρίζεται το G 8 και έργα συμβατά με τα έγγραφα στρατηγικής ανά χώρα και ανά περιφέρεια (όσον αφορά τη συνεργασία με τις τρίτες χώρες)

- Λήψη συγκεκριμένων μέτρων για την ενθάρρυνση όλων των κρατών μελών και των οικείων τρίτων χωρών να επικυρώσουν τη Σύμβαση για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης και το συμπληρωματικό της πρωτόκολλο και εξέταση της δυνατότητας η Κοινότητα να καταστεί συμβαλλόμενο μέρος αυτής της Σύμβασης

- Εξέταση, μαζί με τα κράτη μέλη, του φαινομένου των συντονισμένων και ευρείας κλίμακας επιθέσεων κατά της υποδομής πληροφόρησης των κρατών μελών, αποσκοπώντας στην πρόληψη και την καταπολέμησή τους, συμπεριλαμβανομένων συντονισμένων απαντήσεων και ανταλλαγής πληροφοριών και βέλτιστων πρακτικών

4.2. Η καταπολέμηση των παραδοσιακών μορφών εγκληματικότητας στα ηλεκτρονικά δίκτυα

- Εγκαινίαση ανάλυσης εις βάθος, αποσκοπώντας στην εκπόνηση πρότασης για συγκεκριμένα νομοθετικά μέτρα της ΕΕ για την καταπολέμηση της κλοπής ταυτότητας

- Προώθηση της διαμόρφωσης τεχνικών μεθόδων και διαδικασιών για την καταπολέμηση της απάτης και του παράνομου εμπορίου στο Διαδίκτυο, συμπεριλαμβανομένων σχεδίων συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα

- Εξακολούθηση και εμβάθυνση των εργασιών που πραγματοποιούνται σε συγκεκριμένους στοχοθετημένους τομείς, όπως είναι οι εργασίες της Ομάδας Εμπειρογνωμόνων για την πρόληψη της απάτης οι οποίες αφορούν την καταπολέμηση της απάτης με μέσα πληρωμής άλλα εκτός από τα μετρητά σε ηλεκτρονικά δίκτυα

4.3. Παράνομα περιεχόμενα

- Εξακολούθηση εκπόνησης μέτρων για την καταπολέμηση συγκεκριμένων παράνομων περιεχομένων, ειδικά όσον αφορά το υλικό σεξουαλικής κακοποίησης παιδιών και προτροπής στην τρομοκρατία και ιδίως μέσω της μεταπαρακολούθησης της εφαρμογής της απόφασης πλαισίου για τη σεξουαλική εκμετάλλευση παιδιών

- Να κληθούν τα κράτη μέλη να διαθέσουν επαρκείς χρηματικούς πόρους για την ενίσχυση του έργου των αρχών επιβολής του νόμου, με ειδική έμφαση στην ταυτοποίηση των θυμάτων υλικού σεξουαλικής κακοποίησης το οποίο διανέμεται ηλεκτρονικά

- Εγκαινίαση και στήριξη δράσεων κατά των παρανόμων περιεχομένων που υπάρχει κίνδυνος να προτρέπουν ανηλίκους σε βίαιες και άλλου τύπου σοβαρές παράνομες συμπεριφορές, π.χ. ορισμένες μορφές ιδιαιτέρως βίαιων ηλεκτρονικών παιχνιδιών βίντεο

- Εγκαινίαση και προώθηση του διαλόγου μεταξύ κρατών μελών και με τρίτες χώρες σχετικά με τεχνικές μεθόδους για τη δράση κατά των παράνομων περιεχομένων καθώς επίσης και σχετικά με διαδικασίες για το κλείσιμο των παράνομων ιστοτόπων, αποσκοπώντας επίσης στη σύναψη επισήμων συμφωνιών με γειτονικές και άλλες χώρες σχετικά με το ζήτημα αυτό

- Σύναψη εθελούσιων συμφωνιών και συμβάσεων σε επίπεδο ΕΕ μεταξύ δημοσίων αρχών και ιδιωτικών επιχειρήσεων, ιδίως παρόχων υπηρεσιών Διαδικτύου, σχετικά με διαδικασίες για την παρεμπόδιση και το κλείσιμο των παράνομων ιστότοπων του Διαδικτύου

4.4. Μεταπαρακολούθηση

Στην παρούσα ανακοίνωση περιγράφεται ένας ορισμένος αριθμός δράσεων που αποσκοπούν στη βελτίωση των δομών συνεργασίας στην ΕΕ, ως επόμενα βήματα. Η Επιτροπή θα δώσει συνέχεια σ' αυτές τις δράσεις, θα αξιολογήσει την πρόοδο που θα έχει σημειωθεί κατά την υλοποίησή τους και θα απευθύνει εκθέσεις σχετικά στο Συμβούλιο και στο Κοινοβούλιο.

[1] Οι περισσότερες από τις παρατηρήσεις που περιλαμβάνονται στην παρούσα ανακοίνωση σχετικά με τις σημερινές τάσεις βασίζονται στην μελέτη για την εκτίμηση του αντικτύπου που είχε μια ανακοίνωση για το έγκλημα στον τομέα της πληροφορικής, την οποία είχε παραγγείλει η Επιτροπή το 2006 (Σύμβαση αριθ. JLS/2006/A1/003).

[2] Ως "ψάρεμα" (Phishing) χαρακτηρίζονται οι απόπειρες παράνομης πρόσβασης σε ευαίσθητες πληροφορίες, όπως είναι οι κωδικοί διέλευσης και τα στοιχεία πιστωτικών καρτών· προς αυτόν τον σκοπό, ο απατεώνας συμπεριφέρεται ως αξιόπιστο πρόσωπο στο πλαίσιο μιας ηλεκτρονικής επικοινωνίας.

[3] Δίκτυο προγραμμάτων ρομπότ ονομάζεται μια ομάδα προσβεβλημένων υπολογιστών που εκτελούν προγράμματα υπό κεντρικό έλεγχο.

[4] Οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην Εσωτερική Αγορά (ΕΕ L 178, 17.7.2000, σ. 1).

[5] COM(2000) 890, 26.1.2001.

[6] ΕΕ L 69, 16.3.2005, σ. 67.

[7] ΕΕ L 149, 2.6.2001, σ. 1.

[8] ΕΕ L 13, 20.1.2004, σ. 44.

[9] COM(2001) 298.

[10] COM(2006) 251.

[11] COM(2006) 688.

[12] Κανονισμός αριθ. 460/2004 για τη δημιουργία του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών, (ΕΕ L 77,13.3.2004, σ. 1).

[13] Η Ευρωπαϊκή Ένωση έχει ήδη, δυνάμει του 6ου προγράμματος πλαισίου για την έρευνα και την τεχνολογική ανάπτυξη, υποστηρίξει έναν ορισμένο αριθμό ενδιαφερόντων, και επιτυχημένων, ερευνητικών σχεδίων έργων.

[14] COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

[15] Βλέπε άρθρο 35 της Σύμβασης για το έγκλημα στον κυβερνοχώρο του Συμβουλίου της Ευρώπης

[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[17] Ένα πρόσφατο παράδειγμα είναι η συνεργασία σ' αυτόν τον τομέα μεταξύ των υπηρεσιών καταστολής και των εταιριών τραπεζικών καρτών, στο πλαίσιο της οποίας οι εταιρίες τραπεζικών καρτών βοήθησαν την αστυνομία να εντοπίσει αγοραστές παιδοφιλικού πορνογραφικού υλικού σε ηλεκτρονική μορφή.

[18] Βλέπε http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

[19] Η συνεδρίαση αυτή θα μπορούσε να θεωρηθεί ότι αποτελεί συνέχεια του φόρουμ της ΕΕ που παρουσιάζεται στο τμήμα 6.4 της ανακοίνωσης σχετικά με το ηλεκτρονικό έγκλημα.

[20] Αυτός ο πιο μακροπρόθεσμος στόχος έχει ήδη αναφερθεί στη σελίδα 3 της Ανακοίνωσης 2001.

[21] COM(2006) 437, 7.8.2006.

[redacted]

52006DC0688

Ανακοίνωση της Επιτροπής προς το Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική επιτροπή και την επιτροπή των Περιφερειών - Σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού /* COM/2006/0688 τελικό */

[pic] | ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ |

Βρυξέλλες, 15.11.2006

COM(2006)688 τελικό.

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΣΤΟ ΣΥΜΒΟΥΛΙΟ , ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού

ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΣΤΟ ΣΥΜΒΟΥΛΙΟ , ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ

Σχετικά με την καταπολέμηση των ανεπίκλητων ηλεκτρονικών μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού (Κείμενο που ενδιαφέρει τον ΕΟΧ)

1. Σκοπός της ανακοίνωσης

Η κοινωνία αποκτά διαρκώς μεγαλύτερη επίγνωση της ουσιαστικής σημασίας που έχουν τα σύγχρονα δίκτυα και οι υπηρεσίες ηλεκτρονικών επικοινωνιών στην καθημερινή ζωή, στις επιχειρήσεις ή στο σπίτι. Η ευρύτερη αφομοίωση των υπηρεσιών εξαρτάται από την ύπαρξη αξιόπιστων, ασφαλών και βάσιμων τεχνολογιών. Η ανακοίνωση της Επιτροπής σχετικά με τη στρατηγική για την ασφαλή κοινωνία της πληροφορίας[1] στοχεύει στη βελτίωση της ασφάλειας των εν γένει δικτύων και πληροφοριών και καλεί τον ιδιωτικό τομέα να αντιμετωπίσει τις αδυναμίες στα δίκτυα και τα συστήματα πληροφοριών που θα μπορούσαν να αποτελέσουν αντικείμενο εκμετάλλευσης με στόχο τη διάδοση ανεπίκλητων ηλεκτρονικών μηνυμάτων και κακόβουλου λογισμικού. Στην ανακοίνωση της Επιτροπής σχετικά με την ανασκόπηση του κοινοτικού πλαισίου κανονιστικών ρυθμίσεων προτείνονται νέοι κανόνες για την ενίσχυση της ασφάλειας και της προστασίας της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[2].

Η παρούσα ανακοίνωση πραγματεύεται την εξέλιξη των ανεπίκλητων ηλεκτρονικών μηνυμάτων εμπορικού χαρακτήρα (spam)[3], καθώς και απειλών όπως το κατασκοπευτικό και το κακόβουλο λογισμικό. Στηρίζεται σε προσπάθειες που έχουν καταβληθεί μέχρι στιγμής για την αντιμετώπιση των απειλών αυτών και προσδιορίζει περαιτέρω δράσεις που μπορούν να να αναληφθούν, συμπεριλαμβανομένων των ακόλουθων:

- ενίσχυση της κοινοτικής νομοθεσίας
- επιβολή του νόμου
- συνεργασία στο εσωτερικό των κρατών μελών καθώς και μεταξύ τους
- πολιτικός και οικονομικός διάλογος με τρίτες χώρες
- πρωτοβουλίες του κλάδου

- δραστηριότητες Ε&Α.

2. Το πρόβλημα - ο εξελίσσομενός χαρακτήρας των απείλων

Τα ανεπίκλητα ηλεκτρονικά μηνύματα[4] παρουσίασαν σημαντική ανάπτυξη την τελευταία πενταετία[5]. Όπως αναφέρουν πηγές του κλάδου, τα μηνύματα αυτά ανέρχονται πλέον σε ποσοστό περίπου 50-80% του συνόλου των μηνυμάτων που απευθύνονται σε τελικούς χρήστες.[6]. Μολονότι το μεγαλύτερο μερίδιο προέρχεται εκτός ΕΕ, στις ευρωπαϊκές χώρες οφείλεται πλέον το 25% των αναμεταδιδόμενων ανεπίκλητων μηνυμάτων[7]. Το παγκόσμιο κόστος των μηνυμάτων αυτών εκτιμάται σε 39 δις ευρώ το 2005. Το κόστος τους στις μεγαλύτερες ευρωπαϊκές εθνικές οικονομίες έχει εκτιμηθεί ότι ανέρχεται αντίστοιχα σε 3,5 δις για τη Γερμανία, 1,9 δις για το Ηνωμένο Βασίλειο και 1,4 δις για τη Γαλλία[8]. Η αποστολή αυτών των μηνυμάτων θεωρείται, αυτή καθαυτή, «επιχειρηματική δραστηριότητα». Οι αποστολείς ενοικιάζουν ή πωλούν τους καταλόγους διευθύνσεων ηλε-ταχυδρομείου που έχουν συγκεντρώσει σε εταιρείες για σκοπούς μάρκετινγκ. Η αποστολή ανεπίκλητων μηνυμάτων μέσω του Ίντερνετ είναι ιδιαίτερα προσοδοφόρα. Τούτο οφείλεται στο βελτηνεκές του μέσου, καθώς και στο χαμηλό κόστος που συνεπάγεται η μαζική αποστολή μηνυμάτων. Ταυτόχρονα όμως, μικρής έκτασης επενδύσεις για την καταπολέμηση των μηνυμάτων αυτών μπορούν επίσης να επιφέρουν σημαντικά αποτελέσματα. Ένα παράδειγμα αποτελεί η περίπτωση των Κάτω Χωρών, όπου επετεύχθη μείωση των εν λόγω μηνυμάτων σε ποσοστό 85% με επένδυση ύψους 570.000 ευρώ σε εξοπλισμό αντιμετώπισης.

Από απλή ενόχληση αρχικά, τα ανεπιθύμητα ηλεκτρονικά μηνύματα αποκτούν διαρκώς περισσότερο δόλιο και αξιόποινο χαρακτήρα. Εξέχον παράδειγμα αποτελεί η χρήση ηλε-μηνυμάτων «ψαρέματος» που παρασύρουν τους τελικούς χρήστες να αποκαλύψουν ευαίσθητα δεδομένα τους, μιμούμενα δικτυακούς τόπους υποτιθέμενων γνήσιων εταιριών, γεγονός που δημιουργεί ανησυχίες σχετικά με τις δυνατότητες διάπραξης απάτης και πρόκλησης ζημίας στη φήμη των εταιριών. Η διάδοση κατασκοπευτικού λογισμικού μέσω ηλε-ταχυδρομείου ή μέσω λογισμικού ιχνηλάτησης και αναφοράς της επιγραμμικής συμπεριφοράς των χρηστών συνεχίζει να αυξάνεται. Κατασκοπευτικό λογισμικό δύναται επίσης να συλλέγει πληροφορίες προσωπικού χαρακτήρα, όπως είναι οι κωδικοί πρόσβασης και οι αριθμοί των πιστωτικών καρτών.

Η μαζική αποστολή ανεπίκλητων ηλε-μηνυμάτων διευκολύνεται σε μεγάλο βαθμό από την διάχυση κακόβουλων κωδικών, όπως είναι τα «σκουλήκια» και οι «ιοί». Μόλις εγκατασταθούν, παρέχουν στον επιτιθέμενο τη δυνατότητα να αναλάβει τον έλεγχο ενός προσβεβλημένου υπολογιστικού συστήματος, μετατρέποντάς το σε «δίκτυο προγραμμάτων ρομπότ» (botnet),[9] αποκρύπτοντας την ταυτότητα του πραγματικού αποστολέα. Τα δίκτυα αυτά ενοικιάζονται από αποστολείς ανεπίκλητων μηνυμάτων, δράστες ηλεκτρονικού «ψαρέματος» και πωλητές κατασκοπευτικού λογισμικού για δόλιους και αξιόποινους σκοπούς. Εμπειρογνώμονες του κλάδου εκτιμούν ότι μέσω δικτύων προγραμμάτων ρομπότ αναμεταδίδεται άνω του από 50% των δόλιων ηλε-μηνυμάτων[10]. Η διάχυση κατασκοπευτικού λογισμικού και άλλων τύπων κακόβουλων κωδίκων για επιθέσεις σε καταναλωτές και εταιρείες έχει σημαντικό οικονομικό αντίκτυπο. Το παγκόσμιο οικονομικό κόστος από κακόβουλο λογισμικό εκτιμάται, για το 2005, σε ύψος 11 δις ευρώ[11].

3. το έως τώρα έργο - δράσεις που έχουν αναληφθεί από το 2004

Η ΕΕ θέσπισε, το 2002, οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες , με την οποία επιβάλλεται απαγόρευση στα αυτόκλητα μηνύματα[12], θεσπίζοντας την αρχή της συγκατάθεσης σε περίπτωση μάρκετινγκ σε φυσικά πρόσωπα . Τον Ιανουάριο του 2004, η Επιτροπή παρουσίασε ανακοίνωση σχετικά με τα αυτόκλητα μηνύματα, όπου προσδιορίζονται συμπληρωματικές δράσεις στην οδηγία[13]. Η Επιτροπή υπογράμμισε την ανάγκη ανάληψης δράσης εκ μέρους διαφόρων συντελεστών στα πεδία της ευαισθητοποίησης, της αυτορρύθμισης/των τεχνικών δράσεων, της συνεργασίας και της επιβολής του νόμου. Η Επιτροπή άρχισε να περιλαμβάνει το θέμα της καταπολέμησης των

αυτόκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού στον διάλογό της με τρίτες χώρες. Επιπλέον, η οδηγία για τις αθέμιτες εμπορικές πρακτικές[14] προστατεύει τους καταναλωτές έναντι επιθετικών εμπορικών πρακτικών· η διασυνοριακή συνεργασία για την καταπολέμηση των εν λόγω πρακτικών εντάσσεται στον κανονισμό για τη συνεργασία στην προστασία των καταναλωτών[15].

. 3.1. Δράσεις ευαισθητοποίησης

Η ανακοίνωση της Επιτροπής συνέβαλε στην αύξηση της ευαισθητοποίησης απέναντι στα αυτόκλητα μηνύματα, σε εθνικό και διεθνές επίπεδο, σε ολόκληρο τον πλανήτη. Σε επίπεδο ΕΕ, το πρόγραμμα Safer Internet plus programme προωθεί την ασφαλέστερη χρήση του Ίντερνετ και των νέων επιγραμμικών τεχνολογιών, ιδίως για τα παιδιά, ως μέρους μιας συνεκτικής προσέγγισης που προτείνει η Ευρωπαϊκή Ένωση.

Τα κράτη μέλη δρομολόγησαν ή υποστήριξαν εκστρατείες ευαισθητοποίησης των χρηστών σχετικά με το πρόβλημα των αυτόκλητων μηνυμάτων και τους τρόπους αντιμετώπισής του. Οι πάροχοι υπηρεσιών Ίντερνετ ανέλαβαν, γενικά, την ευθύνη συμβουλευτικών υπηρεσιών και τεχνικής βοήθειας στους πελάτες τους σχετικά με τρόπους προστασίας απέναντι σε κατασκοπευτικό λογισμικό και σε ιούς. Τον Φεβρουάριο του 2004, η Επιτροπή φιλοξένησε ημερίδα του ΟΟΣΑ σχετικά με τα αυτόκλητα μηνύματα. Η Επιτροπή συνέβαλε επίσης ενεργά στη σύσταση ' εργαλειοθήκης' του ΟΟΣΑ κατά των αυτόκλητων μηνυμάτων , η οποία περιλαμβάνει περιεκτική δέσμη κανονιστικών μεθόδων, τεχνικών λύσεων και πρωτοβουλιών του κλάδου για την αντιμετώπιση του φαινομένου.

Η παγκόσμια σύνοδος των Ηνωμένων Εθνών[16] για την κοινωνία της πληροφορίας (WSIS) αναγνώρισε ότι τα αυτόκλητα μηνύματα θα πρέπει να αντιμετωπίζονται στο εκάστοτε κατάλληλο εθνικό και διεθνές επίπεδο. Το 2004 και 2005 πραγματοποιήθηκαν θεματικές διασκέψεις της συνόδου, με διοργάνωση της ITU. Στο θεματολόγιο της διάσκεψης της Τύνιδας, που εγκρίθηκε τον Νοέμβριο του 2005 ζητείται αποτελεσματική αντιμετώπιση του σημαντικού και αυξανόμενου προβλήματος που συνιστούν τα αυτόκλητα μηνύματα[17].

3.2. Διεθνής συνεργασία

Τα αυτόκλητα μηνύματα έχουν διασυνοριακό χαρακτήρα· έχουν συγκροτηθεί διάφορες πρωτοβουλίες συνεργασίας και διασυνοριακοί μηχανισμοί επιβολής. Η Επιτροπή συγκρότησε δίκτυο επαφής των αρμόδιων αρχών για τα αυτόκλητα μηνύματα (CNSA), το οποίο συνέρχεται σε τακτικά διαστήματα, πραγματοποιεί ανταλλαγές βέλτιστων πρακτικών και συνεργάζεται διασυνοριακά σε θέματα επιβολής. Το CNSA έχει καταρτίσει διαδικασία συνεργασίας[18] για τη διασυνοριακή διεκπεραίωση των καταγγελιών που αφορούν αυτόκλητα μηνύματα. Οι υπηρεσίες της Επιτροπής υποστηρίζουν και συμμετέχουν ως παρατηρητές στο σχέδιο δράσης του Λονδίνου (LAP), το οποίο περιλαμβάνει αρχές επιβολής του νόμου από 20 χώρες, έχοντας, επίσης, θεσπίσει διαδικασία διασυνοριακής συνεργασίας. Το Νοέμβριο του 2005, πραγματοποιήθηκε κοινή συνάντηση εργασίας ΕΕ - CNSA – LAP. Ο ΟΟΣΑ ενέκρινε σύσταση για διασυνοριακή συνεργασία στην επιβολή νομοθεσίας κατά των αυτόκλητων μηνυμάτων, η οποία εγκρίθηκε τον Απρίλιο του 2006, όπου καλούνται οι αρχές επιβολής του νόμου να ανταλλάσσουν πληροφορίες και να συνεργάζονται[19].

Η Επιτροπή προτείνει περαιτέρω πρωτοβουλίες διεθνούς συνεργασίας . Οι ΗΠΑ και η ΕΕ συμφώνησαν «να συνεργαστούν για την αντιμετώπιση των αυτόκλητων μηνυμάτων μέσω κοινών πρωτοβουλιών επιβολής του νόμου, καθώς και να διερευνήσουν τρόπους αντιμετώπισης του παράνομου κατασκοπευτικού και κακόβουλου λογισμικού . Η Επιτροπή συμμετέχει επίσης στην ομάδα εργασίας της Καναδικής διεθνούς συνεργασίας σε θέματα αυτόκλητων μηνυμάτων. Πραγματοποιούνται συζητήσεις με μείζονες διεθνείς εταίρους, όπως η Κίνα και η Ιαπωνία. Όσον αφορά την Ασία, η Επιτροπή εισηγήθηκε κοινή δήλωση σχετικά με τη διεθνή συνεργασία για την αντιμετώπιση των αυτόκλητων μηνυμάτων, η οποία

εγκρίθηκε στη διάσκεψη ASEM για το ηλεκτρονικό εμπόριο, το Φεβρουάριο του 2005[20].

Στο θεματολόγιο της Τύνιδας, που εγκρίθηκε κατά την παγκόσμια διάσκεψη για την κοινωνία της πληροφορίας, το Νοέμβριο του 2005 , υπογραμμίζεται ότι η ασφάλεια του Ίντερνετ αποτελεί πεδίο όπου είναι απαραίτητη η βελτίωση της διεθνούς συνεργασίας και ότι το θέμα αυτό θα πρέπει να αντιμετωπιστεί στο πλαίσιο του μοντέλου βελτιωμένης συνεργασίας για τη διοίκηση του Ίντερνετ, που θα υλοποιηθεί στο πλαίσιο του μέτρου στη συνέχεια της Συνόδου.[21].

3.3. Έρευνα και τεχνολογική ανάπτυξη

Στο πλαίσιο του 6ου προγράμματος πλαισίου ΕΤΑ, η Επιτροπή δρομολόγησε έργα που θα συμβάλουν ώστε οι ενδιαφερόμενοι να αντιμετωπίσουν τα αυτόκλητα μηνύματα και άλλες μορφές κακόβουλου λογισμικού. Τα εν λόγω έργα[22] αρχίζουν από τη γενική παρακολούθηση δικτύου και ανίχνευση επιθέσεων έως συγκεκριμένη ανάπτυξη τεχνολογιών για την κατασκευή φίλτρων ανίχνευσης των αυτόκλητων μηνυμάτων, του ηλεκτρονικού «ψαρέματος» και του κακόβουλου λογισμικού. Στα επιτεύγματα συμπεριλαμβάνεται η συγκρότηση ερευνητικής κοινότητας με αντικείμενο τον περιορισμό του κακόβουλου λογισμικού και την ανάπτυξη ευρωπαϊκής υποδομής για την παρακολούθηση της κίνησης στο Ίντερνετ. Οι δραστηριότητες που εγκαινιάστηκαν πρόσφατα αφορούν προσαρμοστικά φίλτρα ηλεκτρονικού «ψαρέματος», που είναι σε θέση να ανιχνεύουν άγνωστες επιβουλές, και επιθέσεις στον κυβερνοχώρο. Η χρηματοοικονομική συμβολή στις δραστηριότητες αυτές ανέρχεται σε 13,5 εκατ. ευρώ.

3.4. Δράσεις του κλάδου

Η Επιτροπή χαιρετίζει την ανάληψη προδραστικού ρόλου εκ μέρους του κλάδου όσον αφορά τα αυτόκλητα μηνύματα. Οι πάροχοι υπηρεσιών έχουν, εν γένει, λάβει τεχνικά μέτρα για την αντιμετώπιση του φαινομένου, συμπεριλαμβανομένων των βελτιωμένων φίλτρων. Οι πάροχοι υπηρεσιών Ίντερνετ συγκρότησαν γραφείο τεχνικής αρωγής και παρέχουν στους χρήστες λογισμικό για την αντιμετώπιση των κακόβουλων μηνυμάτων, του κατασκοπευτικού και τουο κακόβουλου λογισμικού. Πολλοί πάροχοι έχουν θεσπίσει συμβατικές ρήτρες που απαγορεύουν επιγραμμικές αθέμιτες πρακτικές και παρατυπίες. Σε πρόσφατη υπόθεση αστικού δικαίου στο Ηνωμένο Βασίλειο, το δικαστήριο επέβαλε πρόστιμο ύψους 68.800 ευρώ σε αποστολέα αυτόκλητων μηνυμάτων για παραβίαση συμβατικής υποχρέωσης. Ομάδες του κλάδου έχουν θεσπίσει βέλτιστες πρακτικές για την αποτροπή επιγραμμικού «ψαρέματος», καθώς και για τη βελτίωση των μεθόδων "φιλτραρίσματος"[23].

Οι κινητοί φορείς εκμετάλλευσης έχουν ενεργοποιήσει κλαδικούς κώδικες δεοντολογίας που προβλέπουν την ανάληψη δράσης εναντίον των αυτόκλητων μηνυμάτων. Η ένωση GSM δημοσίευσε, το 2006, κώδικα ορθής πρακτικής για τα αυτόκλητα μηνύματα στις κινητές επικοινωνίες. Η Επιτροπή συγχρηματοδοτεί την πρωτοβουλία Spotspam - μια κοινοπραξία μεταξύ ιδιωτικών και δημόσιων φορέων με σκοπό τη δημιουργία βάσης δεδομένων για τη διευκόλυνση της διασυνοριακής διερεύνησης και επιβολής του νόμου σε περιπτώσεις αποστολής αυτόκλητων μηνυμάτων[24].

3.5. Δράσεις επιβολής

Είναι σαφές ότι η ανάληψη δράσης για καταπολέμηση των ανεπίκλητων μηνυμάτων έχει αποτελέσματα. Τα μέτρα "φιλτραρίσματος" που επιβλήθηκαν στη Φιλανδία περιόρισαν την αναλογία των ανεπίκλητων μηνυμάτων στο σύνολο της διαβιβαζόμενης ηλεκτρονικής αλληλογραφίας από ποσοστό 80% σε περίπου 30%. Μεγάλος αριθμός αρχών έχουν αναλάβει προσπάθειες επιβολής του νόμου για την ανάσχεση της αποστολής ανεπίκλητων μηνυμάτων[25].

Παρατηρούνται, ωστόσο, σημαντικές διαφορές μεταξύ των κρατών μελών όσον αφορά τον αριθμό των ενεργειών που διώκονται. Ορισμένες αρχές έχουν δρομολογήσει 100 ή περισσότερες διαδικασίες έρευνας, με επιτυχή κατάληξη και ποινική δίωξη των δραστηριοτήτων αποστολής ανεπίκλητων μηνυμάτων. Σε άλλα

κράτη μέλη, ο αριθμός των περιπτώσεων που διερευνήθηκαν είναι μόλις μονοψήφιος, ενίοτε δε και μηδενικός.

Οι περισσότερες δράσεις στοχεύουν «παραδοσιακές» μορφές ανεπίκλητων μηνυμάτων · άλλες περιπτώσεις, μολονότι έχουν επισημανθεί, αλλά δεν έχουν αποτελέσει αντικείμενο δίωξης , μολονότι συνιστούν μείζονα κίνδυνο.

4. η ακολουθητέα πορεία : Εργο προς εκτέλεση

4.1. Δράσεις σε επίπεδο κρατών μελών

Το τμήμα αυτό αφορά δράσεις κυβερνήσεων και εθνικών αρχών που σχετίζονται ιδιαίτερα με την επιβολή του νόμου και τη συνεργασία.

4.1.1. Καθοριστικοί παράγοντες επιτυχίας

Ο επίμονος και διογκούμενος χαρακτήρας του προβλήματος απαιτεί μεγαλύτερη ανάμειξη των κρατών μελών και παραχώρηση προτεραιότητας. Οι δράσεις θα πρέπει, ιδιαίτερα, να αντιμετωπίσουν τους «επαγγελματίες» αποστολής ανεπίκλητων μηνυμάτων, τους φορείς ηλεκτρονικού «ψαρέματος» και τη διάδοση κατασκοπευτικού και κακόβουλου λογισμικού. Καθοριστικοί παράγοντες επιτυχίας είναι:

- η αποφασιστική ανάληψη δέσμευσης εκ μέρους της κεντρικής κυβέρνησης για την καταπολέμηση επιγραμμικών αθέμιτων πρακτικών και παρατυπιών·

- η ανάληψη σαφούς οργανωτικής ευθύνης όσον αφορά τις δραστηριότητες επιβολής του νόμου·

- η διάθεση επαρκών πόρων στην αρχή επιβολής του νόμου·

Οι παράγοντες αυτοί δεν είναι δεδομένοι σε όλα τα κράτη μέλη.

4.1.2. Συντονισμός και ολοκλήρωση σε εθνικό επίπεδο

Στο πλαίσιο της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες και της γενικής οδηγίας για την προστασία των δεδομένων[26], οι εθνικές αρχές διαθέτουν εξουσίες που τους επιτρέπουν να αναλάβουν δράση έναντι των ακόλουθων παράνομων πρακτικών:

- αποστολή ανεπίκλητων ηλεκτρονικών μηνυμάτων (spam)[27]·

- αθέμιτη πρόσβαση σε τερματικό εξοπλισμό· είτε για την αποθήκευση πληροφοριών - όπως προγράμματα διαφημίσεων (adware) και κατασκοπευτικού λογισμικού (spyware) - είτε για την πρόσβαση σε πληροφορίες που είναι αποθηκευμένες στον εν λόγω εξοπλισμό[28]·

- προσβολή τερματικού εξοπλισμού με την εισαγωγή κακόβουλου λογισμικού (malware) , όπως «σκουλήκια» και «ιοί» και μεταβολή των προσωπικών υπολογιστών σε δίκτυα προγραμμάτων ρομπότ (botnets) ή χρήση τους για άλλους σκοπούς[29] ·

- παραπλάνηση των χρηστών για να αποκαλύψουν ευαίσθητες πληροφορίες[30], όπως κωδικοί πρόσβασης και στοιχεία από πιστωτικές κάρτες, μέσω των αποκαλούμενων μηνυμάτων ηλεκτρονικού «ψαρέματος».

Ορισμένες από τις πρακτικές αυτές εμπίπτουν επίσης στις διατάξεις του ποινικού δικαίου, συμπεριλαμβανομένης της απόφασης - πλαίσιο για τις επιθέσεις εναντίον συστημάτων πληροφοριών[31] . Σύμφωνα με αυτήν, τα κράτη μέλη πρέπει να προβλέπουν μέγιστη ποινή τουλάχιστον τριών ετών φυλάκισης ή και πέντε ετών, εφόσον τα αδικήματα έχουν διαπραχθεί στο πλαίσιο οργανωμένης εγκληματικής δραστηριότητας.

Σε εθνικό επίπεδο, οι εν λόγω διατάξεις δύναται να επιβληθούν από διοικητικούς φορείς ή/και αρχές αρμόδιες για την επιβολή του ποινικού δικαίου. Στις περιπτώσεις αυτές, πρέπει να διακρίνονται σαφώς οι αρμοδιότητες των διάφορων αρχών, καθώς και οι διαδικασίες συνεργασίας. Προς τούτο ενδέχεται να απαιτηθεί η λήψη αποφάσεων σε ανώτερο επίπεδο στο πλαίσιο των εθνικών κυβερνήσεων.

Η εντεινόμενη διαπλοκή ποινικών και διοικητικών πτυχών από τα ανεπίκλητα μηνύματα και άλλες επιβουλές δεν έχουν, μέχρι στιγμής, αποτελέσει αντικείμενο

προβληματισμού και ανάπτυξης των αντίστοιχων διαδικασιών συνεργασίας στα κράτη μέλη, η οποία να οδηγήσει σε προσέγγιση τις τεχνικές και διερευνητικές ικανότητες των διαφόρων φορέων. Απαιτείται κατάρτιση πρωτοκόλλων συνεργασίας για την κάλυψη πεδίων όπως η ανταλλαγή πληροφοριών και ερευνών, στοιχείων επαφών, τεχνική αρωγή και αλληλοπαραπομπή υποθέσεων .

Η στενή συνεργασία μεταξύ αρχών επιβολής του νόμου, των φορέων εκμετάλλευσης δικτύων και των παρόχων υπηρεσιών Ίντερνετ σε εθνικό επίπεδο είναι επίσης επωφελής όσον αφορά την ανταλλαγή πληροφοριών, τεχνικής εμπειρογνωμοσύνης, καθώς και για τη δίωξη επιγραμμικών αθέμιτων πρακτικών. Αρχές από τη Νορβηγία και τις Κάτω Χώρες έχουν αναφερθεί στη χρησιμότητα ανάλογης εταιρικής συνεργασίας μεταξύ δημόσιων και ιδιωτικών φορέων.

4.1.3. Πόροι

Απαιτείται διάθεση πόρων για την πρόσκτηση τεκμηρίων, την πραγματοποίηση ερευνών και την προετοιμασία κατηγορητηρίου. Οι αρχές έχουν ανάγκη από τεχνικούς και νομικούς πόρους, ενώ πρέπει και να εξοικειωθούν με τον τρόπο λειτουργίας των παραβατών, ώστε να μπορούν με επιτυχία να θέτουν τέρμα στις πρακτικές τους.

Σημαντικό εργαλείο μπορούν να αποτελέσουν οι επιγραμμικοί μηχανισμοί καταγγελιών, με συνεργαζόμενα συστήματα υποβολής και ανάλυσης αθέμιτων πρακτικών και παρατυπιών που έχουν αναφερθεί . Η πείρα έχει αποδείξει ότι περιορισμένες επενδύσεις μπορούν να έχουν σημαντικά αποτελέσματα . Ο περιορισμός των ανεπίκλητων μηνυμάτων στην Ολλανδία επιτεύχθηκε από ομάδα πέντε αφοσιωμένων υπαλλήλων πλήρους απασχόλησης στην OPTA, την αρμόδια εθνική αρχή, με εξοπλισμό καταπολέμησης ύψους 570.000 ευρώ. Με βάση αυτή την επένδυση, η πείρα που αποκτήθηκε από την καταπολέμηση του φαινομένου χρησιμοποιείται πλέον σε άλλα προβληματικά πεδία.

4.1.4. Διασυνοριακή συνεργασία

Το φαινόμενο των αυτόκλητων μηνυμάτων έχει παγκόσμιες διαστάσεις. Οι εθνικές αρχές είναι συχνά υποχρεωμένες να βασίζονται σε αρχές άλλων χωρών για τη νομική δίωξη όσων τα αποστέλλουν και, αφετέρου, ενδέχεται να ζητηθεί από αυτές η συνέχιση ερευνών που έχουν αρχίσει σε άλλες χώρες. .

Με δεδομένη την ενδεχόμενη επιφύλαξη της δέσμευσης περιορισμένων εθνικών πόρων για τη διερεύνηση προβλημάτων τρίτων, είναι ωστόσο σημαντικό να αναγνωρίσουν τα κράτη μέλη ότι η αποτελεσματική διασυνοριακή συνεργασία συνιστά ουσιώδη παράγοντα στην αντιμετώπιση των αυτόκλητων μηνυμάτων. Πρόσφατα, οι σχετικές αυστραλιανές και ολλανδικές αρχές αντιμετώπισης, συνεργάστηκαν, στο πλαίσιο μιας μεγάλης ανάλογης υπόθεσης.

Μέχρι στιγμής, 21 ευρωπαϊκές αρχές έχουν εγκρίνει τη διαδικασία συνεργασίας του CNSA[32] όσον αφορά τη διεκπεραίωση διασυνοριακών καταγγελιών· καλούνται και οι υπόλοιπες αρχές να πράξουν το ίδιο εντός των αμέσως επόμενων μηνών. Καλούνται ιδιαίτερα τα κράτη μέλη και οι αρμόδιες αρχές να προωθήσουν ενεργά τη χρήση:

- των κοινών εγγράφων pro forma CNSA-LAP

- της σύστασης του ΟΟΣΑ και της 'εργαλειοθήκης' για την επιβολή του νόμου όσον αφορά τα αυτόκλητα μηνύματα.

4.1.5 Προτεινόμενες δράσεις

Τα κράτη μέλη και οι αρμόδιες αρχές καλούνται:

- να καθορίσουν σαφείς αρμοδιότητες για τους εθνικούς φορείς που εμπλέκονται στην αντιμετώπιση των αυτόκλητων μηνυμάτων

- να εξασφαλίσουν αποτελεσματικό συντονισμό μεταξύ των αρμόδιων αρχών

- να εμπλέξουν τους συντελεστές της αγοράς σε εθνικό επίπεδο, αξιοποιώντας την τεχνογνωσία τους και τις πληροφορίες τους

- να εξασφαλίσουν τη διάθεση επαρκών πόρων για τις προσπάθειες επιβολής του νόμου

- να συμμετάσχουν στις διαδικασίες διεθνούς συνεργασίας και να αποδέχονται αιτήματα για διασυνοριακή αρωγή

4.2. Δράσεις του κλάδου

Το τμήμα αυτό αφορά δράσεις που μπορούν να αναληφθούν από τον κλάδο για την προαγωγή της εμπιστοσύνης των καταναλωτών και την περιστολή της καταχρηστικής αποστολής ηλε-μηνυμάτων.

4.2.1. Παράδοση και εγκατάσταση λογισμικού

Το κατασκοπευτικό λογισμικό συνιστά σοβαρή απειλή για την ιδιωτική ζωή των χρηστών. Οι προσφορές επιγραμμικής εγκατάστασης λογισμικού έχουν υιοθετηθεί πλειστάκις για τη διανομή και εγκατάσταση κατασκοπευτικού λογισμικού στον τερματικό εξοπλισμό των χρηστών. Το κατασκοπευτικό λογισμικό μπορεί επίσης να κρύβεται σε λογισμικό που διανέμεται με άλλα μέσα, όπως οι CD-ROM, για την εγκατάσταση σε υπολογιστή. Ανεπιθύμητα κατασκοπευτικά προγράμματα είναι δυνατόν να εγκατασταθούν μαζί με το λογισμικό που αγοράζει ο καταναλωτής.

Στη συνέχεια προσδιορίζονται συγκεκριμένες δράσεις για να αποφευχθεί να φτάσει το κατασκοπευτικό λογισμικό στο επίπεδο των τελικών χρηστών.

4.2.2. Ενημέρωση των καταναλωτών

Στις προσφορές λογισμικού ενδέχεται να περιλαμβάνεται η εγκατάσταση πρόσθετων προγραμμάτων. Σε περιπτώσεις όπου το πρόσθετο αυτό λογισμικό λειτουργεί ως κατασκοπευτικό λογισμικό, παρακολουθώντας τη συμπεριφορά των τελικών χρηστών (π.χ. για σκοπούς μάρκετινγκ), τούτο συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα και είναι παράνομο χωρίς την ενημέρωση και συγκατάθεση του χρήστη. Σε πολλές περιπτώσεις, η συγκατάθεση του χρήστη για την εγκατάσταση του εν λόγω λογισμικού είτε δεν λαμβάνεται είτε κρύβεται 'στα ψιλά γράμματα' μιας μακροσκελούς συμφωνίας αδειοδότησης.

Ενθαρρύνονται οι εταιρείες που προσφέρουν προϊόντα λογισμικού να περιγράφουν σαφώς και εμφανώς όλους τους όρους και προϋποθέσεις της προσφοράς, ιδίως εάν πρόκειται για επεξεργασία δεδομένων προσωπικού χαρακτήρα από οποιεσδήποτε διατάξεις παρακολούθησης που περιλαμβάνονται σε πακέτα λογισμικού.

Η αυτορρύθμιση καθώς και η χρήση κάποιου είδους 'σφραγίδας έγκρισης' θα μπορούσαν να αποτελέσουν μέσα για τη διάκριση των αξιόπιστων εταιριών από τις μη αξιόπιστες. Δεοντολογικοί κώδικες που αποβλέπουν στην ενημέρωση του καταναλωτή σχετικά με τους όρους που συνεπάγεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορούν να υποβάλλονται προς έγκριση στην ομάδα εργασίας για την προστασία των δεδομένων του άρθρου 29.

4.2.3 Συμβατικοί όροι στην αλυσίδα εφοδιασμού

Συχνά οι εταιρείες δεν έχουν επίγνωση του τρόπου με τον οποίο οι διαφημίσεις των προϊόντων και υπηρεσιών τους διανέμονται στο κοινό. Νόμιμο λογισμικό ενδέχεται να συσκευάζεται μαζί με κατασκοπευτικό λογισμικό που χρησιμοποιείται για πρόσβαση σε ευαίσθητα δεδομένα, συμπεριλαμβανομένων δεδομένων πιστωτικών καρτών, εμπιστευτικών εγγράφων κ.λπ.

Οι εταιρίες που διαφημίζουν ή/και πωλούν προϊόντα πρέπει να εξασφαλίζουν ότι οι δραστηριότητες των συμβαλλόμενων με αυτές μερών είναι νόμιμες και θεμιτές. Μια εταιρεία πρέπει να έχει αντίληψη των σχέσεων μέσα στη συμβατική αλυσίδα, να παρακολουθεί τη συμμόρφωση με το νόμο και να καταγγέλει τη συμβατική σχέση σε περίπτωση αθέμιτων πρακτικών σε οποιοδήποτε σημείο της αλυσίδας, τερματίζοντας την περαιτέρω σχέση με εταιρείες που στηρίζουν ανάλογες πρακτικές.

4.2.4 . Μέτρα ασφάλειας από τους παρόχους υπηρεσιών

Σύμφωνα με έρευνα του ENISA που διεξήχθη το 2006[33], επιβεβαιώνεται ότι οι πάροχοι υπηρεσιών έχουν εν γένει λάβει μέτρα για την αντιμετώπιση των αυτόκλητων μηνυμάτων. Αναφέρεται, ωστόσο, ότι οι πάροχοι υπηρεσιών θα

μπορούσαν να συμβάλουν περαιτέρω στην εν γένει ασφάλεια του δικτύου, ενώ απευθύνεται η σύσταση να δοθεί μεγαλύτερη έμφαση στο "φιλτράρισμα" των ηλεμηνυμάτων που εξέρχονται από το δίκτυο παρόχου υπηρεσιών (φιλτράρισμα εξερχόμενης κίνησης) . Η Επιτροπή ενθαρρύνει τους παρόχους υπηρεσιών να εφαρμόζουν την εν λόγω σύσταση.

Η ομάδα εργασίας για την προστασία των δεδομένων του άρθρου 29 ενέκρινε γνωμοδότηση για θέματα προστασίας της ιδιωτικής ζωής που σχετίζονται με την παροχή υπηρεσιών ελέγχου των ηλεκτρονικών μηνυμάτων[34], βάσει της οποίας παρέχονται κατευθύνσεις στο ζήτημα του απορρήτου των επικοινωνιών με ηλεμηνύματα και, ειδικότερα, στο "φιλτράρισμα" επιγραμμικών επικοινωνιών έναντι ιών, αυτόκλητων μηνυμάτων και παράνομου περιεχομένου.

4.2.5. Προτεινόμενες δράσεις

Η Επιτροπή καλεί:

- τις εταιρείες να εξασφαλίσουν ότι το επίπεδο των πληροφοριών για την αγορά εφαρμογών λογισμικού είναι σύμφωνο με τη νομοθεσία για την προστασία των δεδομένων.

- τις εταιρείες να απαγορεύουν, με συμβατικούς όρους, την παράνομη χρήση του λογισμικού σε διαφημίσεις, να παρακολουθούν τον τρόπο με τον οποίο οι διαφημίσεις φτάνουν στους καταναλωτές, καθώς και τις αθέμιτες πρακτικές.

- τους παρόχους υπηρεσιών ηλεκτρονικού ταχυδρομείου να εφαρμόσουν πολιτική "φιλτραρίσματος" που εξασφαλίζει τη συμμόρφωση με τη σύσταση και τις κατευθύνσεις σχετικά με το "φιλτράρισμα" των ηλε-μηνυμάτων.

4.3. Ανάληψη δράσης σε ευρωπαϊκό επίπεδο

Η Επιτροπή θα συνεχίσει να ασχολείται με θέματα γύρω από τα αυτόκλητα μηνύματα, το κατασκοπευτικό και το κακόβουλο λογισμικό σε διεθνή φόρουμ, διμερείς συναντήσεις καθώς και όπου αλλού ενδείκνυται στις συμφωνίες με τρίτες χώρες, και θα συνεχίσει να ενισχύει τη συνεργασία μεταξύ των ενδιαφερόμενων, συμπεριλαμβανομένων των κρατών μελών, των αρμόδιων αρχών και του κλάδου. Πρόκειται επίσης να αναλάβει νέες πρωτοβουλίες στο πεδίο της νομοθεσίας και της έρευνας που θα αποβλέπουν στο να δοθεί νέα ώθηση στην καταπολέμηση των αθέμιτων πρακτικών που υπονομεύουν την κοινωνία της πληροφορίας. Η Επιτροπή εργάζεται για την περαιτέρω ανάπτυξη συνεκτικής πολιτικής για την καταπολέμηση των αξιοποίνων πράξεων στον κυβερνοχώρο. Η πολιτική αυτή θα παρουσιαστεί στο πλαίσιο ανακοίνωσης που αναμένεται να εγκριθεί στις αρχές του 2007.

4.3.1. Ανασκόπηση του πλαισίου των κανονιστικών ρυθμίσεων

Στην ανακοίνωση της Επιτροπής[35] σχετικά με το κανονιστικό πλαίσιο για τις ηλεκτρονικές επικοινωνίες, προτείνονται αυστηρότεροι κανόνες στο πεδίο της προστασίας της ιδιωτικής ζωής και της ασφάλειας. Βάσει της πρότασης, οι φορείς εκμετάλλευσης δικτύων και οι πάροχοι υπηρεσιών θα υποχρεωθούν:

- να κοινοποιούν στην αρμόδια αρχή κράτους μέλους οποιαδήποτε συμβάν παραβίασης της ασφάλειας που έχει ως αποτέλεσμα την απώλεια δεδομένων προσωπικού χαρακτήρα ή/και διακοπή στη συνέχεια παροχής της υπηρεσίας.

- να κοινοποιούν στους πελάτες τους οποιοδήποτε συμβάν παραβίασης της ασφάλειας με συνέπεια την απώλεια, τροποποίηση, πρόσβαση ή καταστροφή προσωπικών δεδομένων των πελατών.

Οι εθνικές ρυθμιστικές αρχές θα διαθέτουν την ευχέρεια να εξασφαλίζουν ότι οι φορείς εκμετάλλευσης υλοποιούν καταλλήλως τις πολιτικές ασφάλειας, ενώ μπορούν να θεσπιστούν νέοι κανόνες που θα προβλέπουν συγκεκριμένα επανορθωτικά μέτρα ή θα περιλαμβάνουν ένδειξη σχετικά με το επίπεδο των αναμενόμενων ποινών σε περιπτώσεις παραβάσεων.

4.3.2. Ο ρόλος του ENISA

Στις προτάσεις περιλαμβάνεται επίσης η διάταξη όπου αναγνωρίζεται ο συμβουλευτικός ρόλος του ENISA σε θέματα ασφαλείας. Άλλα που καθήκοντα που

προβλέπονται για τον ENISA περιγράφονται στην ανακοίνωση της Επιτροπής σχετικά με την στρατηγική στην ασφάλεια[36] και περιλαμβάνουν:

.

- την οικοδόμηση, με τα κράτη μέλη και τους ενδιαφερόμενους, εταιρικής σχέσης εμπιστοσύνης για την ανάπτυξη ενδεδειγμένου πλαισίου συλλογής δεδομένων σχετικά με συμβάντα ασφάλειας και τα επίπεδα εμπιστοσύνης καταναλωτή.

.

Ο ENISA θα αναλάβει το συντονισμό του πλαισίου αυτού με την Eurostat, ενόψει των κοινοτικών στατιστικών αναφορικά με την κοινωνία της πληροφορίας και το πλαίσιο συγκριτικής αξιολόγησης της πρωτοβουλίας i2010[37].

.

- εξέταση της σκοπιμότητας/εφικτότητας ενός ευρωπαϊκού συστήματος συναγερμού και κοινοποίησης πληροφοριών για τη διευκόλυνση της αποτελεσματικής απόκρισης σε υφιστάμενες και νέες επιβουλές κατά των ηλεκτρονικών δικτύων.

4.3.3. Έρευνα και ανάπτυξη

Τ ο επόμενο, 7ο ΠΠ, έχει ως στόχο τη συνεχιζόμενη ανάπτυξη της γνώσης και των τεχνολογιών για ασφαλείς υπηρεσίες και συστήματα πληροφοριών, σε στενό συντονισμό με πρωτοβουλίες πολιτικής. Στα θέματα εργασίας που αναφέρονται σε κακόβουλο λογισμικό αναμένεται να συμπεριληφθούν τα κρυφά δίκτυα προγραμμάτων ρομπότ (botnets) και οι ιοί, καθώς και οι επιθέσεις σε κινητές και φωνητικές υπηρεσίες.

4.3.4. Διεθνής συνεργασία

Καθώς το Ίντερνετ είναι παγκόσμιο δίκτυο, πρέπει η ανάληψη δέσμευσης για την καταπολέμηση των αυτόκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού να είναι κοινή σε ολόκληρο τον κόσμο. Η Επιτροπή προτίθεται, κατά συνέπεια, να ενισχύσει τον διάλογο και τη συνεργασία με τρίτες χώρες σε θέματα αντιμετώπισης των εν λόγω επιβουλών και των αξιόποινων δραστηριοτήτων που συνδέονται με αυτές. Για το σκοπό αυτό, η Επιτροπή θα κινηθεί για να εξασφαλίσει ότι τα θέματα των ανεπίκλητων μηνυμάτων, του κατασκοπευτικού και κακόβουλου λογισμικού θα αντιμετωπιστούν στο πλαίσιο συμφωνιών μεταξύ της ΕΕ και τρίτων χωρών, θα επιδιώξει σαφή δέσμευση εκ μέρους των πλέον θιγομένων τρίτων χωρών, ώστε να συνεργαστούν αποτελεσματικότερα με κράτη μέλη της ΕΕ για την αντιμετώπιση των εν λόγω επιβουλών και θα παρακολουθήσει από κοντά την πορεία της επιβολής στόχων για τους οποίους υπάρχει κοινή ανάληψη δέσμευσης.

4.3.5. Προτεινόμενες δράσεις

Η Επιτροπή:

- θα συνεχίσει να καταβάλει προσπάθειες περαιτέρω ευαισθητοποίησης και ενίσχυσης της συνεργασίας μεταξύ των ενδιαφερόμενων

- θα συνεχίσει την ανάπτυξη συμφωνιών με τρίτες χώρες όπου θα συμπεριλαμβάνεται το θέμα της καταπολέμησης των ανεπίκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού

- θα αποβλέψει στην υιοθέτηση νέων νομοθετικών προτάσεων, στις αρχές του 2007, που θα ενισχύουν τους κανόνες στο πεδίο της προστασίας της ιδιωτικής ζωής και της ασφάλειας στον τομέα των επικοινωνιών και θα εισηγηθεί πολιτική σχετικά με τις αξιόποινες πράξεις στον κυβερνοχώρο

- θα εμπλέξει την τεχνογνωσία του ENISA σε θέματα που αφορούν την ασφάλεια

- θα υποστηρίξει την έρευνα και ανάπτυξη στο 7ο ΠΠ.

5. Συμπέρασμα

Απειλές όπως τα ανεπίκλητα ηλεκτρονικά μηνύματα, το κατασκοπευτικό και το κακόβουλο λογισμικό υπονομεύουν την εμπιστοσύνη και την ασφάλεια της κοινωνίας

της πληροφορίας, με συνεπαγόμενα παράλληλα σημαντικό οικονομικό αντίκτυπο. Μολονότι ορισμένα κράτη μέλη έχουν αναλάβει πρωτοβουλίες, στην ΕΕ, ως σύνολο, είναι ανεπαρκής η δραστηριότητα που στοχεύει στην αντιμετώπιση της εξέλιξης αυτής . Η Επιτροπή αξιοποιεί το ρόλο της ως μεσάζοντα για την επίτευξη μεγαλύτερης ευαισθητοποίησης σχετικά με την ανάγκη ανάληψης ευρύτερης πολιτικής δέσμευσης για την αντιμετώπιση των εν λόγω απειλών.

Πρέπει να αναβαθμιστούν οι προσπάθειες επιβολής της νομοθεσίας για την αναχαίτιση όσων εσκεμμένα την παραβαίνουν. Ο κλάδος θα πρέπει να αναλάβει περαιτέρω δράση, συμπληρωματική προς τις δραστηριότητες επιβολής του νόμου. Απαιτείται συνεργασία σε εθνικό επίπεδο, τόσο στο εσωτερικό των κυβερνήσεων όσο και μεταξύ κυβερνήσεων και του κλάδου. Η Επιτροπή θα ενισχύσει τον διάλογο και τη συνεργασία με τρίτες χώρες, ενώ θα εξετάσει επίσης τη δυνατότητα υποβολής νέων νομοθετικών προτάσεων, και θα αναλάβει δράσεις έρευνας για την περαιτέρω ενίσχυση της προστασίας της ιδιωτικής ζωής και της ασφάλειας στον τομέα των ηλεκτρονικών επικοινωνιών.

Η ολοκληρωμένη και κατά το δυνατόν παράλληλη υλοποίηση των δράσεων που προσδιορίζονται στην την στην παρούσα ανακοίνωση μπορεί να συμβάλει στον περιορισμό των απειλών που υποσκάπτουν επί του παρόντος τα οφέλη από την κοινωνία της πληροφορίας και την οικονομία.Η Επιτροπή θα παρακολουθεί την υλοποίηση των εν λόγω δράσεων και, το 2008, θα εκτιμήσει την ενδεχόμενη ανάγκη ανάληψης περαιτέρω δράσης.

[1] COM(2006)251. τελικό

[2] COM(2006)334 τελικό.

[3] COM(2004)28. τελικό

[4] Το spam αναφέρεται στην αποστολή ανεπίκλητων επικοινωνιών (μηνυμάτων), π.χ. μέσω ηλε-ταχυδρομείου, για εμπορικούς σκοπούς. Τα ανεπίκλητα ηλε-μηνύματα μπορούν, ωστόσο, να περιέχουν επίσης κακόβουλο και κατασκοπευτικό λογισμικό.

[5] Το 2001τα ανεπίκλητα μηνύματα ανέρχονταν στο 7% της παγκόσμιας κίνησης ηλε-ταχυδρομείου.

[6] Symantec 54%; Messagelabs 68,6 MAAWG 80-85.

[7] Q1 2006 (Sophos) Ασία 42,8%, Β.Αμερική 25,6, Ευρώπη 25,0, Ν.Αμερική 5,1, Αυστραλασία 0,8 Αφρική 0,6, λοιπά 0,1.

[8] Ferris research, 2005.

[9] Τα botnet είναι υπονομευμένοι υπολογιστές που χρησιμοποιούνται από τους αποστολείς spam για μαζική αποστολή ηλε-μηνυμάτων μέσω εγκατάστασης κρυμμένου λογισμικού που μετατρέπει τους υπολογιστές σε εξυπηρετητές ταχυδρομείου εν αγνοία των χρηστών.

[10] Κυριότερες χώρες που πλήττονται από botnet, σύμφωνα με τη μελέτη Symantec, (Q 3-4 2005) : ΗΠΑ 26 %, ΗΒ 22%, Κίνα 9%, Γαλλία, Ν.Κορέα, Καναδάς 4%, Ταϊβάν, Ισπανία, Γερμανία 3%,Ιαπωνία 2%.

[11] Computer Economics: the 2005 Malware Report.

[12] Άρθρο 13 της οδηγίας 2002/58.

[13] Ό.π. υποσημείωση 3.

[14] Παράρτημα 1, σημείο 26, της οδηγίας 2005/29/ΕΚ

[15] Κανονισμός (ΕΚ) αριθ. 2006/2004

[16] WSIS, Γενεύη, Δεκέμβριος 2003

[17] Θεματολόγιο της Τύνιδας, παράγραφος 41.

[18] http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf

[19] http://www.oecd-antispam.org/

[20] http://www.asemec-london.org/

[21] Θεματολόγιο της Τύνιδας, παράγραφοι 39-47. http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

[22] www.diadem http://cordis.europa.eu/fp6/projects.htm#search

[23] http://www.maawg.org/home/

[24] http://www.spotspam.net

[25] Από έρευνα του CNSA προκύπτει ότι 15 από τα 18 μέλη που απάντησαν, άσκησαν ποινικές διώξεις κατά τη χρονική περίοδο 2003-2006.

[26] Οδηγία 95/46/ΕΚ.

[27] Άρθρο 13 της οδηγίας για την προστασία της ιδιωτικής ζωής.

[28] Άρθρο 5 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής.

[29] Βλ. υποσημείωση 28.

[30] Άρθρο 6 (α) της γενικής οδηγίας για τημ προστασία των δεδομένων.

[31] Απόφαση πλαίσιο 2005/222/JHA του Συμβουλίου.

[32] Ό.π., υποσημείωση 18.

[33] http://www.enisa.eu.int/doc/pdf/deliverables/enisa_security_spam.pdf

[34] Γνώμη 2/2006, WP 118.

[35] http://europa.eu.int/information_society/policy/ecomm/tomorrow/index_en.htm

[36] Ό.π., υποσημείωση 1.

[37] Πλαίσιο συγκριτικής αξιολόγησης της ομάδας ανωτέρου επιπέδου i2010 της 20ης Απριλίου 2006.

[redacted]

32005F0222

Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου, της 24ης Φεβρουαρίου 2005, για τις επιθέσεις κατά των συστημάτων πληροφοριών

Επίσημη Εφημερίδα αριθ. L 069 της 16/03/2005 σ. 0067 - 0071

Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου

της 24ης Φεβρουαρίου 2005

για τις επιθέσεις κατά των συστημάτων πληροφοριών

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

τη συνθήκη για την Ευρωπαϊκή Ένωση, και ιδίως το άρθρο 29, το άρθρο 30 παράγραφος 1 στοιχείο α), το άρθρο 31 παράγραφος 1 στοιχείο ε) και το άρθρο 34 παράγραφος 2 στοιχείο β),

την πρόταση της Επιτροπής,

τη γνώμη του Ευρωπαϊκού Κοινοβουλίου [1],

Εκτιμώντας τα ακόλουθα:

(1) Ο στόχος της παρούσας απόφασης-πλαίσιο είναι η βελτίωση της συνεργασίας μεταξύ των δικαστικών και άλλων αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, μέσω της προσέγγισης των κανόνων του ποινικού

δικαίου των κρατών μελών που αφορούν επιθέσεις κατά των συστημάτων πληροφοριών.

(2) Έχουν διαπιστωθεί επιθέσεις κατά των συστημάτων πληροφοριών, οφειλόμενες ιδίως στην απειλή που αντιπροσωπεύει το οργανωμένο έγκλημα, και υπάρχει αυξημένη ανησυχία ενώπιον του ενδεχόμενου τρομοκρατικών επιθέσεων κατά των συστημάτων πληροφοριών που αποτελούν μέρος της ζωτικής σημασίας υποδομής των κρατών μελών. Αυτή η κατάσταση αποτελεί απειλή για την επίτευξη μιας ασφαλέστερης κοινωνίας της πληροφορίας και ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, και χρειάζεται, ως εκ τούτου, να αντιμετωπισθεί στο επίπεδο της Ευρωπαϊκής Ένωσης.

(3) Η αποτελεσματική αντιμετώπιση αυτών των απειλών προϋποθέτει ευρεία προσέγγιση όσον αφορά την ασφάλεια των δικτύων και των πληροφοριών, όπως τονίσθηκε στο πρόγραμμα δράσης eEurope, στην ανακοίνωση της Επιτροπής με τον τίτλο "Ασφάλεια των δικτύων και πληροφοριών: Πρόταση ευρωπαϊκής πολιτικής" και στο ψήφισμα του Συμβουλίου της 28ης Ιανουαρίου 2002 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων [2].

(4) Η ανάγκη για ακόμα μεγαλύτερη συνειδητοποίηση των προβλημάτων που αφορούν την ασφάλεια των πληροφοριών και για την παροχή πρακτικής βοήθειας τονίσθηκε επίσης στο ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 5ης Σεπτεμβρίου 2001.

(5) Τα σημαντικά νομικά κενά και οι διαφορές των νομοθεσιών των κρατών μελών στο συγκεκριμένο τομέα μπορεί να παρεμποδίσουν την καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας και μπορεί να περιπλέξουν την αποτελεσματική συνεργασία των αστυνομικών και δικαστικών υπηρεσιών σε περίπτωση επιθέσεων κατά των συστημάτων πληροφοριών. Ο υπερεθνικός και χωρίς σύνορα χαρακτήρας των σύγχρονων συστημάτων πληροφοριών συνεπάγεται ότι οι επιθέσεις κατά των συστημάτων αυτών έχουν συχνά διασυνοριακή διάσταση, υπογραμμίζοντας, κατ' αυτόν τον τρόπο, την επείγουσα ανάγκη να υπάρξει προσέγγιση των ποινικών δικαίων στο συγκεκριμένο τομέα.

(6) Το πρόγραμμα δράσης του Συμβουλίου και της Επιτροπής όσον αφορά την άριστη δυνατή εφαρμογή των διατάξεων της συνθήκης του Άμστερνταμ για τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης [3], το Ευρωπαϊκό Συμβούλιο του Τάμπερε της 15ης και 16ης Οκτωβρίου 1999, το Ευρωπαϊκό Συμβούλιο της Σάντα Μαρία ντα Φέιρα της 19ης και 20ής Ιουνίου 2000, η Επιτροπή στον "Πίνακα αποτελεσμάτων" και το Ευρωπαϊκό Κοινοβούλιο στο ψήφισμά του της 19ης Μαΐου 2000 αναφέρουν ή απευθύνουν έκκληση για νομοθετική δράση κατά του εγκλήματος που χρησιμοποιεί τις προηγμένες τεχνολογίες, συμπεριλαμβάνοντας κοινούς ορισμούς, ποινικούς χαρακτηρισμούς και κυρώσεις.

(7) Είναι ανάγκη να συμπληρωθούν οι εργασίες που έχουν πραγματοποιηθεί από τους διεθνείς οργανισμούς, ειδικότερα οι εργασίες του Συμβουλίου της Ευρώπης για την προσέγγιση του ποινικού δικαίου και οι εργασίες της ομάδας G8 για τη διακρατική συνεργασία στον τομέα του εγκλήματος υψηλής τεχνολογίας, προτείνοντας κοινή προσέγγιση στο επίπεδο της Ευρωπαϊκής Ένωσης στο συγκεκριμένο τομέα. Αυτή η ανάγκη αναπτύχθηκε ευρύτερα στην ανακοίνωση την οποία απηύθυνε η Επιτροπή στο Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο, την Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών, με τον τίτλο "Για μια ασφαλέστερη κοινωνία της πληροφορίας με τη βελτίωση της ασφάλειας των υποδομών πληροφόρησης και την καταπολέμηση του εγκλήματος πληροφορικής".

(8) Θα πρέπει να υπάρξει προσέγγιση του ποινικού δικαίου όσον αφορά τις επιθέσεις κατά των συστημάτων πληροφοριών για να διασφαλισθεί η μέγιστη δυνατή δικαστική και αστυνομική συνεργασία όσον αφορά τα ποινικά αδικήματα που έχουν σχέση με επιθέσεις κατά των συστημάτων πληροφοριών και συμμετοχή στην καταπολέμηση του οργανωμένου εγκλήματος και της τρομοκρατίας.

(9) Όλα τα κράτη μέλη έχουν επικυρώσει τη σύμβαση του Συμβουλίου της Ευρώπης, της 28ης Ιανουαρίου 1981, για την προστασία του ατόμου από την

αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Οι πληροφορίες προσωπικού χαρακτήρα που αποτελούν αντικείμενο επεξεργασίας στο πλαίσιο της εφαρμογής της παρούσας απόφασης-πλαίσιο θα πρέπει να προστατεύονται σύμφωνα με τις αρχές της εν λόγω σύμβασης.

(10) Οι κοινοί ορισμοί στο συγκεκριμένο τομέα, ειδικότερα για τα συστήματα πληροφοριών και τα ηλεκτρονικά δεδομένα, έχουν σημασία προκειμένου να εξασφαλισθεί η συνεκτική προσέγγιση στα κράτη μέλη κατά την εφαρμογή της παρούσας απόφασης-πλαίσιο.

(11) Είναι ανάγκη να επιτευχθεί κοινή προσέγγιση για τα στοιχεία αντικειμενικής υπόστασης των ποινικών αδικημάτων, προβλέποντας κοινά αδικήματα παράνομης πρόσβασης σε σύστημα πληροφοριών, παράνομης παρεμβολής σε σύστημα και παράνομης παρεμβολής σε δεδομένα.

(12) Για το σκοπό της καταπολέμησης του εγκλήματος σε σχέση με ηλεκτρονικούς υπολογιστές, κάθε κράτος μέλος θα πρέπει να εξασφαλίζει ουσιαστική δικαστική συνεργασία όσον αφορά τα αδικήματα που βασίζονται στους τύπους των πράξεων που αναφέρονται στα άρθρα 2, 3, 4 και 5.

(13) Είναι ανάγκη να αποφευχθεί η υπερβολική ποινικοποίηση, κυρίως υποθέσεων ήσσονος σημασίας, καθώς και η ενοχοποίηση κατόχων δικαιωμάτων και εξουσιοδοτημένων ατόμων.

(14) Είναι ανάγκη να προβλεφθούν από τα κράτη μέλη κυρώσεις των επιθέσεων κατά των συστημάτων πληροφοριών. Οι προβλεπόμενες κυρώσεις πρέπει να είναι αποτελεσματικές, ανάλογες και αποτρεπτικές.

(15) Είναι σκόπιμο να προβλεφθούν πιο αυστηρές κυρώσεις όταν μια επίθεση κατά συστήματος πληροφοριών διαπράττεται στο πλαίσιο εγκληματικής οργάνωσης, όπως ορίζεται στην κοινή δράση 98/733/ΔΕΥ, της 21ης Δεκεμβρίου 1998, σχετικά με το αξιόποινο της συμμετοχής σε εγκληματική οργάνωση, στα κράτη μέλη της Ευρωπαϊκής Ένωσης [4]. Επίσης είναι σκόπιμο να προβλέπονται αυστηρότερες κυρώσεις, όταν μια τέτοια επίθεση έχει προκαλέσει σοβαρές ζημίες ή έχει θίξει θεμελιώδη συμφέροντα.

(16) Θα πρέπει επίσης να προβλεφθούν μέτρα συνεργασίας μεταξύ των κρατών μελών, προκειμένου να εξασφαλίζεται η αποτελεσματική δράση κατά των επιθέσεων που αφορούν τα συστήματα πληροφοριών. Ως εκ τούτου, τα κράτη μέλη θα πρέπει να χρησιμοποιούν, για την ανταλλαγή πληροφοριών, το υφιστάμενο δίκτυο λειτουργικών σημείων επαφής που αναφέρεται στη σύσταση του Συμβουλίου της 25ης Ιουνίου 2001 για σημεία επαφής τα οποία λειτουργούν 24 ώρες το εικοσιτετράωρο για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας [5].

(17) Δεδομένου ότι οι στόχοι της παρούσας απόφασης-πλαίσιο, που συνίστανται στο να κατοχυρωθεί ότι οι επιθέσεις κατά των συστημάτων πληροφοριών θα τιμωρούνται σε όλα τα κράτη μέλη με αποτελεσματικές, ανάλογες και αποτρεπτικές ποινικές κυρώσεις και να βελτιωθεί και ενθαρρυνθεί η δικαστική συνεργασία με την άρση των ενδεχόμενων επιπλοκών, δε μπορούν να επιτευχθούν επαρκώς από τα κράτη μέλη, επειδή οι κανόνες πρέπει να είναι κοινοί και συμβιβάσιμοι, και μπορούν, ως εκ τούτου, να επιτευχθούν καλύτερα στο επίπεδο της Ένωσης, η Ένωση μπορεί να θεσπίσει μέτρα, σύμφωνα με την αρχή της επικουρικότητας η οποία αναφέρεται στο άρθρο 5 της συνθήκης. Σύμφωνα με την αρχή της αναλογικότητας, η οποία αναφέρεται στο εν λόγω άρθρο, η παρούσα απόφαση-πλαίσιο δεν υπερβαίνει τα αναγκαία όρια για την επίτευξη αυτών των στόχων.

(18) Η παρούσα απόφαση-πλαίσιο σέβεται τα θεμελιώδη δικαιώματα και τηρεί τις αρχές που αναγνωρίζονται από το άρθρο 6 της συνθήκης για την Ευρωπαϊκή Ένωση και αντικατοπτρίζονται στο Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, και κυρίως στα κεφάλαια II και VI,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ-ΠΛΑΙΣΙΟ:

Άρθρο 1

Ορισμοί

Για τους σκοπούς της παρούσας απόφασης-πλαίσιο, νοείται ως:

α) "Σύστημα πληροφοριών": οποιαδήποτε συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από τους υπολογιστές με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους.

β) "Ηλεκτρονικά δεδομένα": οποιαδήποτε παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από σύστημα πληροφοριών, συμπεριλαμβανομένου ενός προγράμματος που παρέχει τη δυνατότητα στο σύστημα πληροφοριών να εκτελέσει μια λειτουργία.

γ) "Νομικό πρόσωπο": κάθε οντότητα που έχει αυτό το καθεστώς βάσει του ισχύοντος δικαίου, εκτός των κρατών ή άλλων δημόσιων οργάνων κατά την άσκηση κρατικής εξουσίας και των δημόσιων διεθνών οργανισμών.

δ) "Χωρίς δικαίωμα": πρόσβαση ή παρεμβολή μη εξουσιοδοτημένη από τον ιδιοκτήτη ή άλλο δικαιούχο του συστήματος ή μέρους του, ή μη επιτρεπόμενη δυνάμει της εθνικής νομοθεσίας.

Άρθρο 2

Παράνομη πρόσβαση σε σύστημα πληροφοριών

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως πρόσβαση, χωρίς δικαίωμα, στο σύνολο ή σε μέρος συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

2. Κάθε κράτος μέλος μπορεί να αποφασίσει ότι η αναφερόμενη στην παράγραφο 1 πράξη ποινικοποιείται μόνον όταν το αδίκημα διαπράττεται κατά παράβαση μέτρου ασφαλείας.

Άρθρο 3

Παράνομη παρεμβολή σε σύστημα

Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή, μετάδοση, ζημία, διαγραφή, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Άρθρο 4

Παράνομη παρεμβολή σε δεδομένα

Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι η εκ προθέσεως διαγραφή, ζημία, φθορά, αλλοίωση, απόκρυψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά, τιμωρείται ως ποινικό αδίκημα όταν διαπράττεται χωρίς δικαίωμα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις.

Άρθρο 5

Ηθική αυτουργία, υποβοήθηση και συνέργεια και απόπειρα

1. Κάθε κράτος μέλος εξασφαλίζει ότι η ηθική αυτουργία, η υποβοήθηση και συνέργεια σε αδίκημα που αναφέρεται στα άρθρα 2, 3 και 4, τιμωρείται ως ποινικό αδίκημα.

2. Κάθε κράτος μέλος εξασφαλίζει ότι η απόπειρα διάπραξης των αδικημάτων που αναφέρονται στα άρθρα 2, 3 και 4, τιμωρείται ως ποινικό αδίκημα.

3. Κάθε κράτος μέλος μπορεί να αποφασίσει να μην εφαρμόζει την παράγραφο 2, για τα αδικήματα που αναφέρονται στο άρθρο 2.

Άρθρο 6

Κυρώσεις

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, τιμωρούνται με αποτελεσματικές, ανάλογες και αποτρεπτικές ποινικές κυρώσεις.

2. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι τα αδικήματα που αναφέρονται στα άρθρα 3 και 4, τιμωρούνται με ποινικές κυρώσεις μεγίστης διάρκειας ενός έως τριών ετών φυλακίσεως τουλάχιστον.

Άρθρο 7

Επιβαρυντικές περιστάσεις

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα για να εξασφαλίσει ότι το αδίκημα που αναφέρεται στο άρθρο 2 παράγραφος 2 και το αδίκημα που αναφέρεται στα άρθρα 3 και 4 τιμωρούνται με ποινικές κυρώσεις μέγιστης διάρκειας δύο έως πέντε ετών φυλάκισης τουλάχιστον, όταν διαπράττονται στα πλαίσια εγκληματικής οργάνωσης, όπως ορίζεται στην κοινή δράση 98/733/ΔΕΥ, εκτός από το επίπεδο κυρώσεων που αναφέρεται στην κοινή αυτή δράση.

2. Ένα κράτος μέλος μπορεί επίσης να λαμβάνει τα μέτρα που αναφέρονται στην παράγραφο 1, όταν το αδίκημα έχει προκαλέσει σοβαρές ζημίες ή έχει θίξει ζωτικά συμφέροντα.

Άρθρο 8

Ευθύνη νομικών προσώπων

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα προκειμένου να εξασφαλίσει ότι τα νομικά πρόσωπα είναι δυνατό να υπέχουν ευθύνη για τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, που έχουν τελεσθεί προς όφελός τους από οιοδήποτε πρόσωπο, ενεργώντας είτε ατομικά είτε ως μέλος οργάνου του νομικού προσώπου, το οποίο κατέχει ιθύνουσα θέση εντός του νομικού προσώπου, βασιζόμενη σε:

α) εξουσία εκπροσώπησης του νομικού προσώπου, ή

β) εξουσία λήψης αποφάσεων για λογαριασμό του νομικού προσώπου, ή

γ) εξουσία άσκησης ελέγχου εντός του νομικού προσώπου.

2. Πέραν των περιπτώσεων που προβλέπονται στην παράγραφο 1, τα κράτη μέλη εξασφαλίζουν ότι ένα νομικό πρόσωπο μπορεί να θεωρηθεί υπεύθυνο όταν η απουσία εποπτείας ή ελέγχου εκ μέρους ενός από τα πρόσωπα που αναφέρονται στην παράγραφο 1 κατέστησε δυνατή την τέλεση των αδικημάτων που αναφέρονται στα άρθρα 2, 3, 4 και 5 προς όφελος του εν λόγω νομικού προσώπου από πρόσωπο που τελεί υπό την εξουσία του.

3. Η ευθύνη του νομικού προσώπου δυνάμει των παραγράφων 1 και 2 δεν αποκλείει την ποινική δίωξη κατά φυσικών προσώπων που συμμετέχουν ως αυτουργοί, ηθικοί αυτουργοί ή συνεργοί στην τέλεση αδικημάτων που αναφέρονται στα άρθρα 2, 3, 4 και 5.

Άρθρο 9

Κυρώσεις κατά νομικών προσώπων

1. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα προκειμένου να εξασφαλίσει ότι σε νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 8 παράγραφος 1, επιβάλλονται αποτελεσματικές, ανάλογες και αποτρεπτικές κυρώσεις, στις οποίες περιλαμβάνονται χρηματικές ποινές ή πρόστιμα και, ενδεχομένως, άλλες κυρώσεις, όπως:

α) αποκλεισμός από δημόσιες παροχές ή ενισχύσεις·

β) μέτρα προσωρινής ή οριστικής απαγόρευσης της άσκησης εμπορικής δραστηριότητας·

γ) θέση υπό δικαστική εποπτεία, ή

δ) δικαστική εκκαθάριση.

2. Κάθε κράτος μέλος λαμβάνει τα αναγκαία μέτρα προκειμένου να εξασφαλίσει ότι σε νομικό πρόσωπο το οποίο υπέχει ευθύνη δυνάμει του άρθρου 8 παράγραφος 2, επιβάλλονται αποτελεσματικές, ανάλογες και αποτρεπτικές κυρώσεις ή μέτρα.

Άρθρο 10

Δικαιοδοσία

1. Κάθε κράτος μέλος θεμελιώνει τη δικαιοδοσία του για τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, όταν το αδίκημα διαπράττεται:

α) εν όλω ή εν μέρει στην επικράτειά του, ή

β) από υπήκοό του, ή

γ) προς όφελος νομικού προσώπου που εδρεύει στην επικράτειά του εν λόγω κράτους μέλους.

2. Για να θεμελιώσει τη δικαιοδοσία του σύμφωνα με την παράγραφο 1 στοιχείο α), κάθε κράτος μέλος εξασφαλίζει ότι στη δικαιοδοσία αυτή εμπίπτουν περιπτώσεις κατά τις οποίες:

α) ο δράστης διέπραξε το αδίκημα ευρισκόμενος στην επικράτειά του, ανεξάρτητα από το αν το αδίκημα στρέφεται κατά συστήματος πληροφοριών στην επικράτειά του, ή

β) το αδίκημα στρέφεται κατά συστήματος πληροφοριών στην επικράτειά του, ανεξάρτητα από το αν ο δράστης διαπράττει το αδίκημα ευρισκόμενος στην επικράτειά του.

3. Κράτος μέλος το οποίο, δυνάμει του εθνικού του δικαίου, δεν εκδίδει ή δεν παραδίδει μέχρι στιγμής τους υπηκόους του, λαμβάνει τα αναγκαία μέτρα προκειμένου να θεμελιώσει τη δικαιοδοσία του και, όταν απαιτείται, προκειμένου να ασκήσει δίωξη όσον αφορά τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5, εφόσον διαπράττονται από υπήκοο του εκτός της επικράτειάς του.

4. Όταν αδίκημα υπάγεται στη δικαιοδοσία περισσοτέρων του ενός κρατών μελών και οποιοδήποτε εκ των συγκεκριμένων κρατών μπορεί εγκύρως να ασκήσει δίωξη βάσει των ίδιων πραγματικών περιστατικών, τα συγκεκριμένα κράτη μέλη συνεργάζονται προκειμένου να αποφασίσουν ποιο εξ αυτών θα προβεί στη δίωξη των δραστών με σκοπό, εφόσον είναι δυνατό, να συγκεντρωθεί η διαδικασία σε ένα μόνο κράτος μέλος. Προς το σκοπό αυτό, τα κράτη μέλη μπορούν να προσφεύγουν σε οποιοδήποτε όργανο ή μηχανισμό εγκαθιδρυμένο στο εσωτερικό της Ευρωπαϊκής Ένωσης για να διευκολύνουν τη συνεργασία μεταξύ των δικαστικών τους αρχών καθώς και το συντονισμό των ενεργειών τους. Λαμβάνονται υπόψη διαδοχικά τα ακόλουθα στοιχεία:

- κράτος μέλος είναι εκείνο στην επικράτεια του οποίου ετελέσθησαν τα αδικήματα σύμφωνα με την παράγραφο 1 στοιχείο α) και την παράγραφο 2,

- κράτος μέλος είναι εκείνο του οποίου είναι υπήκοος ο δράστης,

- κράτος μέλος είναι εκείνο στο οποίο ανακαλύφθηκε ο δράστης.

5. Κράτος μέλος μπορεί να αποφασίσει να μην εφαρμόζει, ή να εφαρμόζει μόνο σε ειδικές περιπτώσεις ή συνθήκες, τους κανόνες δικαιοδοσίας που ορίζονται στην παράγραφο 1 στοιχεία β) και γ).

6. Τα κράτη μέλη ενημερώνουν τη γενική γραμματεία του Συμβουλίου και την Επιτροπή όταν αποφασίζουν να εφαρμόσουν την παράγραφο 5, προσδιορίζοντας, εφόσον χρειάζεται, τις ειδικές περιπτώσεις ή συνθήκες στις οποίες εφαρμόζεται η απόφαση.

Άρθρο 11

Ανταλλαγή πληροφοριών

1. Με σκοπό την ανταλλαγή πληροφοριών σχετικά με τα αδικήματα που αναφέρονται στα άρθρα 2, 3, 4 και 5 και σύμφωνα με τους κανόνες προστασίας δεδομένων, τα κράτη μέλη διασφαλίζουν τη χρήση του υφιστάμενου δικτύου

λειτουργικών σημείων επαφής που είναι διαθέσιμο σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας.

2. Κάθε κράτος μέλος ενημερώνει τη γενική γραμματεία του Συμβουλίου και την Επιτροπή για το σημείο επαφής που έχει ορίσει με σκοπό την ανταλλαγή πληροφοριών για τα αδικήματα που αφορούν επιθέσεις κατά των συστημάτων πληροφοριών. Η γενική γραμματεία διαβιβάζει αυτές τις πληροφορίες στα άλλα κράτη μέλη.

Άρθρο 12

Εφαρμογή

1. Τα κράτη μέλη λαμβάνουν τα απαραίτητα μέτρα για να συμμορφωθούν με τις διατάξεις της παρούσας απόφασης-πλαίσιο έως τις 16 Μαρτίου 2007.

2. Έως τις 16 Μαρτίου 2007, τα κράτη μέλη διαβιβάζουν στη γενική γραμματεία του Συμβουλίου και στην Επιτροπή το κείμενο των διατάξεων με τις οποίες μεταφέρουν στο εθνικό τους δίκαιο τις υποχρεώσεις που υπέχουν δυνάμει της παρούσας απόφασης-πλαίσιο. Έως τις 16 Σεπτεμβρίου 2007, το Συμβούλιο αξιολογεί, βάσει έκθεσης που εκπονείται με βάση τις πληροφορίες αυτές καθώς και βάσει γραπτής έκθεσης της Επιτροπής, το βαθμό στον οποίο τα κράτη μέλη έχουν συμμορφωθεί με τις διατάξεις της παρούσας απόφασης-πλαίσιο.

Άρθρο 13

Έναρξη ισχύος

Η παρούσα απόφαση-πλαίσιο αρχίζει να ισχύει την ημερομηνία της δημοσίευσής της στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Βρυξέλλες, 24 Φεβρουαρίου 2005.

Για το Συμβούλιο

Ο Πρόεδρος

N. Schmit

[1] ΕΕ C 300 E της 11.12.2003, σ. 26.

[2] ΕΕ C 43 της 16.2.2002, σ. 2.

[3] ΕΕ C 19 της 23.1.1999, σ. 1.

[4] ΕΕ L 351 της 29.12.1998, σ. 1.

[5] ΕΕ C 187 της 3.7.2001, σ.

Β.Ξένη νομοθεσία στην Αγγλική Γλώσσα

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)
(A)
(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [1]
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;
shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided

in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is—
(1)
(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)
(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)
(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)
(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)
(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
(d)
(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section—
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer—
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means—
(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) [2] of the Federal Reserve Act;
(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

[1] So in original. Probably should be followed by "or".

[2] See References in Text note below.

Canada

Canada is in the middle of making cybercrime related amendments in 2003.
Canadian Criminal Code Sections:
342.1 (1) Every one who, fraudulently and without color of right,
(a) obtains, directly or indirectly, any computer service,
(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system.
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.
342.2 (1) Every person who, without laful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
(b) is guilty of an offence punishable on summary conviction.
430. (1.1) Every one commits mischief who wilfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, intercepts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

United Kingdom

The Police and Justice Act 2006 Chapter 48 (November 2006) amend the Computer Misuse act, see Part 5 sections 35-38. The new amendments reads as follows:
35 Unauthorised access to computer material

(1) In the Computer Misuse Act 1990 (c. 18) ("the 1990 Act"), section 1 (offence of unauthorised access to computer material) is amended as follows.

(2) In subsection (1)-

(a) in paragraph (a), after "any computer" there is inserted ", or to enable any such access to be secured";

(b) in paragraph (b), after "secure" there is inserted ", or to enable to be secured,".
(3) For subsection (3) there is substituted-

"(3) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

36 Unauthorised acts with intent to impair operation of computer, etc

For section 3 of the 1990 Act (unauthorised modification of computer material) there is substituted-

"3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if-

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act-

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section-

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both."

37 Making, supplying or obtaining articles for use in computer misuse offences

After section 3 of the 1990 Act there is inserted-

"3A Making, supplying or obtaining articles for use in offence under section 1 or 3

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section "article" includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

38 Transitional and saving provision

(1) The amendments made by-

(a) subsection (2) of section 35, and

(b) paragraphs 19(2), 25(2) and 29(2) of Schedule 14,
apply only where every act or other event proof of which is required for conviction of an offence under section 1 of the 1990 Act takes place after that subsection comes into force.

(2) The amendments made by-

(a) subsection (3) of section 35, and

(b) paragraphs 23, 24, 25(4) and (5), 26, 27(2) and (7) and 28 of Schedule 14,
do not apply in relation to an offence committed before that subsection comes into force.

(3) An offence is not committed under the new section 3 unless every act or other event proof of which is required for conviction of the offence takes place after section 36 above comes into force.

(4) In relation to a case where, by reason of subsection (3), an offence is not committed under the new section 3-

(a) section 3 of the 1990 Act has effect in the form in which it was enacted;

(b) paragraphs 19(3), 25(3) to (5), 27(4) and (5) and 29(3) and (4) of Schedule 14 do not apply.
(5) An offence is not committed under the new section 3A unless every act or other event proof of which is required for conviction of the offence takes place after section 37 above comes into force.

(6) In the case of an offence committed before section 154(1) of the Criminal Justice Act 2003 (c. 44) comes into force, the following provisions have effect as if for "12 months" there were substituted "six months"-

(a) paragraph (a) of the new section 1(3);

(b) paragraph (a) of the new section 2(5);

(c) subsection (6)(a) of the new section 3;

(d) subsection (5)(a) of the new section 3A.
(7) In this section-

(a) "the new section 1(3)" means the subsection (3) substituted in section 1 of the 1990 Act by section 35 above;

(b) "the new section 2(5)" means the subsection (5) substituted in section 2 of the 1990 Act by paragraph 17 of Schedule 14 to this Act;

(c) "the new section 3" means the section 3 substituted in the 1990 Act by section 36 above;

(d) "the new section 3A" means the section 3A inserted in the 1990 Act by section 37 above.

Computer Misuse Act 1990
Chapter 18

1. Unauthorized access to computer material:
(1) A person is guilty of an offense if-
(a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer, or to enable any such access to be secured,
(b) the access he intends to secure, or to enable to be secured, is unauthorized, and
(c) he knows at the time when he causes the computer to perform the function that that is the case.
(2) The intent a person has to have to commit an offense under this section need not to be directed at:
(a) any particular program or data,
(b) a program or data of any particular kind, or
(c) a program or data held in any particular computer.
(3) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

2. Unauthorized access with intent to commit or facilitate commission for further offences.
(1) A person is guilty of an offense under this section if he commits an offense under section 1 above (" the unauthorized access offence") with intent
(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.
(2) This section applies to offences
(a) for which the sentence is fixed by law; or
(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates Courts Act 1980).
(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorized access offence or on any future occasion.
(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.
(5) A person guilty of an offence under this section shall be liable
(a) on summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.
3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if-

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.
(2) This subsection applies if the person intends by doing the act-

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer;

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to-

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.
(5) In this section-

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.
(6) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

3A Making, supplying or obtaining articles for use in offence under section 1 or 3

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.

(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.

(4) In this section "article" includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable-

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a

fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

See: **http://www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm**

Germany

The government of Germany *has on September 20 2006* proposed a new draft law *on cybercrime aiming to close any remaining loopholes.*

Current Penal Code
Section 202a. Data Espionage:
(1) Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine .
(2) Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.
Section 303a. Alteration of Data
(1) Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.
(2) The attempt shall be punishable.
Section 303b. Computer Sabotage
(1) Imprisonment not exceeding five years or a fine shall be imposed on any person who interferes with data processing which is of essential importance to another business, another's enterprise or an administrative authority by:
1. committing an offence under section 300a(1) or
2. destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier.
(2) The attempt shall be punishable.
See www.gesetze-im-internet.de/bundesrecht/stgb/

Section 263a Computer Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorized use of data or other unauthorized influence on the order of events, shall be punished with imprisonment for not more than five years or a fine.

(2) Section 263 subsections (2) to (7), shall apply accordingly.

Italy

Penal Code Article 615 ter: Unauthorized access into a computer or telecommunication systems:
Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.
The imprisonment is from one until five years:
1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even

without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator.
2) if to commit the crime the culprit uses violence upon things or people, or if he is manifestedly armed.
3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or damage of the data, the information or the programs contained in it.
Should the deeds of the 1st and 2nd paragraphs concern computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or whatsoever public interest, the penalty is - respectively- one to five years or three to eight years' imprisonment. In the case provided for in the 1st paragraph, the crime is liable to punishment only after an action by the plaintiff; the other cases are prosecutioned "ex-officio".
-615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:
Whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits or deliver codes, key-words or other means for the access to a computer or telecommunication system protected by safety measures, or however provides information or instructions fit to the above purpose, is punished with the imprisonment not exceeding one year and a fine not exceeding 10 million liras.
The penalty is imprisonment from one until two years and a fine from 10 until 20 million liras in the case of one of the circumstances numbered in 1 and 2 in the 4th paragraph of article 617-quater.
-615 quinquies: Diffusion of Programs Aimed to Damage or to Interrupt a Computer System:
Whoever propagates, transmits or delivers a computer program - edited by himself or by another - with the aim and the effect to damage a computer or telecommunication system, the data or the programs contained or pertinent to it, or rather the partial or total interuption or an alteration in its working, is punished with imprisonment not exceeding two years and fined not exceeding 20 million liras.

France

Penal Code
Amended as Law no.2004-575 of June 21, 2004, entered into force on June 23, 2004. See the explanatory report.
Ratification of the Council of Europe Convention on Cybercrime was made on January 10, 2006.
Article 323-1:
Fraudulent accessing or remaining within all or part of an automated data processing system is punished by a sentence not exceeding two years' imprisonment and a fine of 30.000 euro.
Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is not exceeding three years' imprisonment and a fine of 45.000 euro.
Article 323-2
Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine of 75.000 euro.
Article 323-3
The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine of 75.000 euro.
Article 323-3-1
Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty.

Switzerland

Penal Code:
Article 143bis: Unauthorized access to data processing system.
Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.
Article 144bis: Damage to data
1. Anyone, who without authorisation alters, erases, or renders useless data which is stored or transferred by

electronic or similar means, shall be punished by imprisonment for a term of up to three years or a fine of up to forty thousand Swiss francs if a complaint is made.
If the offender has caused serious damage, a sentence of five years penal servitude can be imposed. The offence shall be prosecuted ex officio.
2. Any person who produces, imports, circulates, promotes, offers or otherwise makes available programs, which he/she knows, or ought to assume, are to be used for purposes of committing an offence mentioned in paragraph 1 above, or gives instructions for the production of such programs, shall be punished by imprisonment for a term of up to three years or a fine of up to forty thousand Swiss francs.
If the offender commits the offence on a habitual basis for profit, a sentence of up to five years penal servitude can be imposed.

Spain

The Ministerio del Interior has prepared a proposal for cybercrime laws, amending several articles in the Penal Code.
Excerpts from the Spanish Penal Code:
CHAPTER I
On the discovery and revealing of secrets
Article 197.
1. Any individual who, for the purpose of discovering the secrets or violating the privacy of another and without the consent of the latter, takes possession of that individual's papers, letters, electronic mail messages or any other personal documents or belongings or intercepts his or her telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or images or any other communications signal, will be punished by imprisonment from between one and four years and a fine of between twelve and twenty-four months [sic].
2. The same punishment will be applicable to any individual who, without authorization, seizes, uses or modifies, to the detriment of a third party, such private personal or family data of another individual as may be recorded on computer, electronic or telematic files or media, or in any other type of file or record, whether public or private. The same punishment will be imposed on any individual who, without authority, accesses such data by any means or alters or uses such data to the detriment of the owner of the data or of a third party.
3. Punishment consisting of imprisonment from between two and five years will be imposed if the data or facts discovered or the images captured, as indicated in the proceeding paragraphs, are divulged, revealed or transferred to third parties.
Punishment consisting of imprisonment from between one and three years and a fine of between twelve and twenty-four months [sic] will be imposed on any individual who, with prior knowledge of the illicit origin of [such facts or data] [but] without having taken part in their discovery, commits the acts described in the preceding paragraph.
4. If the acts described in paragraphs 1 and 2 of this article are committed by the persons in charge of or responsible for the computer, electronic or telematic files and media or files or records, punishment consisting of imprisonment from between three and five years will be imposed, and if such private data are disseminated, transferred or made public, the upper half [sic] of the punishment will be imposed.
5. In addition, when the acts described in the above sections involve personal data revealing the ideology, religion, beliefs, health, racial origin or sexual orientation, or if the victim is a minor or incapacitated, the upper half [sic] of the punishments stipulated will be imposed.
6. If such acts are committed with intent to profit, the upper half [sic] of the punishments set forth respectively in paragraphs 1 through 4 of this article will be imposed. If in addition they involve the data mentioned in paragraph 5, the punishment will consist of imprisonment from between four and seven years.
SECTION 1. ON FRAUD
Article 248.
1. Any individual will be guilty of fraud who, with intent to profit, uses sufficient deceit to cause another individual to err, inducing him or her to commit an act of disposition to the detriment of him or herself or a third party.

2. Also guilty of fraud will be any individual who, with intent to profit and using computer manipulation or any similar contrivance, causes the unauthorized transfer of any personal asset to the detriment of a third party.

Article 264.

1. Punishment consisting of imprisonment from between one and three years and a fine of between twelve and twenty-four months [sic] will be imposed on any individual who causes the injury identified in the preceding article in any of the following circumstances:

1. The acts are committed for the purpose of preventing the free exercise of authority or in vengeance therefor, whether the crime is committed against public authorities or against private citizens who, whether acting as witnesses or in any other capacity, have contributed, or might in the future contribute, to the execution or application of the Law or General Provisions.

2. Infection or contagion of cattle is caused by any means.

3. Poisonous or corrosive substances are used.

4. Assets in the public or community domain or assets designated for public or community use are involved.

5. The acts lead to the bankruptcy of the individual affected or place him or her in a grave economic situation.

2. The same punishment will be imposed on any individual who, in any way, destroys, modifies, misuses or otherwise damages such electronic data, programs or documents of others as may be contained in computer networks, media or systems.

Article 256.

Any individual who makes use of any telecommunications terminal equipment without the consent of the owner thereof, causing damage to the latter in excess of fifty thousand pesetas, will be subject to punishment consisting of a fine of between three and twelve months [sic].

Article 270.

Punishment consisting of imprisonment from between six months and two years or a fine of between six and twenty-four months [sic] will be imposed on any individual who, with intent to profit and to the detriment of a third party, reproduces, plagiarizes, distributes or publicly communicates, either wholly or in part, a literary, artistic or scientific work or the transformation, interpretation or artistic execution thereof contained in any medium or communicated by any means, without the authorization of the holders of the corresponding intellectual property rights or successors thereof.

The same punishment will be imposed on any individual who intentionally imports, exports or stores copies of such works or productions or executions without the authorization specified above.

The same punishment will be imposed in the event of the manufacture, circulation and possession of any medium specifically designed to facilitate the unauthorized suppression and neutralization of any technical device used to protect computer programs.

SECTION 2. ON CRIMES INVOLVING INDUSTRIAL PROPERTY

Article 273.

1. Punishment consisting of imprisonment from between six months and two years and a fine of between six and twenty-four months [sic] will be imposed on any individual who, for industrial or commercial purposes, without the consent of the owner of a patent or utility model, and with prior knowledge of its registration, manufactures, imports, possesses, utilizes, offers or introduces into the market items covered by such rights.

2. The same punishment will be imposed on any individual who, in the same fashion and for the above-indicated purposes, uses or offers the use of a procedure covered by a patent, or who possesses, offers, introduces into the market or uses the product directly obtained by the patented procedure.

3. The same punishment will be imposed on any individual who commits any of the acts characterized in the first paragraph of this article, under identical circumstances, with regard to objects covered in favor of a third party by an industrial or artistic model or drawing or topography of a semiconductor product.

11. Νομολογία

ΣΤΟΙΧΕΙΑ ΑΠΟΦΑΣΗΣ

Δικαστήριο: ΑΡΕΙΟΣ ΠΑΓΟΣ ΤΜΗΜΑ ΣΤ'
Τόπος: ΑΘΗΝΑ
Αριθ. Απόφασης: 1059
Έτος: 1995

Περίληψη Απάτη με ηλεκτρονικό υπολογιστή - Αποδοχές - Αποδοχή προϊόντων εγκλήματος -. Συνιστά το έγκλημα του άρθρ. 386Α ΠΚ η καταχώρηση στον ηλεκτρονικό υπολογιστή αποδοχών μεγαλυτέρων εκείνων που αναγράφονται στα αντίστοιχα παραστατικά. Η είσπραξη των μεγαλυτέρων αυτών αποδοχών συνιστά αποδοχή προϊόντων εγκλήματος.

Κείμενο Απόφασης

Κατά το άρθρο 386 Α του ΠΚ, όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του άρθρ. 386. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν παθόντες είναι ένα ή περισσότερα πρόσωπα. Εξ άλλου κατά το άρθρ. 394 παρ.1 ΠΚ όποιος με πρόθεση αποκρύπτει, αγοράζει, λαμβάνει ως ενέχυρο ή με άλλον τρόπο δέχεται στην κατοχή του πράγμα που προήλθε από αξιόποινη πράξη ή μεταβιβάζει σε άλλον την κατοχή τέτοιου πράγματος ή συνεργεί σε μεταβίβαση ή με οποιονδήποτε τρόπο ασφαλίζει την κατοχή του σε άλλον, τιμωρείται με φυλάκιση, ανεξάρτητα αν είναι τιμωρητέος ή όχι ο υπαίτιος του εγκλήματος από το οποίο προέρχεται το πράγμα. Τέλος η ειδική και εμπεριστατωμένη αιτιολογία των δικαστικών αποφάσεων που επιβάλλεται από τις διατάξεις των άρθρ. 93 παρ.3 του Σ και 139 του ΚΠΔ πρέπει να υπάρχει, όχι μόνον ως προς τα περιστατικά που απαρτίζουν την κατηγορία, αλλά και ως προς τους αυτοτελείς ισχυρισμούς, δηλαδή τους ισχυρισμούς εκείνους που προβάλλονται στο δικαστήριο της ουσίας, σύμφωνα με τα άρθρ. 170 παρ.2 και 333 παρ.2 ΚΠΔ, από τον κατηγορούμενο ή τον συνήγορό του και τείνουν στην άρση του άδικου χαρακτήρα της πράξης ή της ικανότητας προς καταλογισμό ή τη μείωση αυτής, καθώς και στην εξάλειψη του αξιοποίνου ή τη μείωση της ποινής. Ειδικότερα επί αυτοτελών ισχυρισμών του κατηγορουμένου το δικαστήριο υποχρεούται να διαλάβει στην απόφασή του την πιο πάνω αιτιολογία, μόνο όταν αυτοί προβάλλονται κατά τρόπο ορισμένο και σαφή, δηλαδή με την επίκληση όλων των πραγματικών περιστατικών που είναι αναγκαία για τη θεμελίωσή τους, όχι δε και επί αόριστης προβολής τους, η οποία υπάρχει και όταν γίνεται μόνο απλή επίκληση της νομικής διάταξης που τους προβλέπει ή του χαρακτηρισμού με τον οποίο είναι γνωστοί στη νομική ορολογία. Στην κρινόμενη υπόθεση, όπως προκύπτει από το αιτιολογικό σε συνδυασμό με το διατακτικό, τα οποία παραδεκτώς αλληλοσυμπληρώνονται, της προσβαλλόμενης υπ' αριθ. 2231 - 2231α/1994 απόφασης, το Τριμελές Εφετείο Πειραιά, που δίκασε κατ' έφεση, μετά από εκτίμηση και αξιολόγηση των αναφερομένων αποδεικτικών μέσων, δέχθηκε, κατά την ανέλεγκτη ουσιαστική κρίση του, τα ακόλουθα: Οι κατηγορούμενοι αναιρεσείοντες Σ.Κ.** και Δ.Γ.** με σκοπό να προσπορίσουν στον εαυτό τους και στον άλλο κατηγορούμενο αναιρεσείοντα Π.Α.** παράνομο περιουσιακό όφελος με αντίστοιχη βλάβη της περιουσίας του ΟΛΠ, ενώ όφειλαν ως εργαζόμενοι στο τμήμα ελέγχου στοιχείων Η/Υ του ΟΛΠ να ελέγχουν τις εισόδους και εξόδους των Η/Υ και στη συνέχεια να διορθώνουν τα τυχόν λάθη των πρωτογενών στοιχείων που αφορούσαν τη μισθοδοσία του

προσωπικού του ΟΛΠ, κατά το από Αυγούστου 1990 μέχρι Μαρτίου 1992 χρονικό διάστημα έθεσαν σε εφαρμογή το εξής εγκληματικό σχέδιο: Καταχωρούσαν στον ηλεκτρονικό υπολογιστή της υπηρεσίας τους ως ημερήσιες αποδοχές που αφορούσαν τους ίδιους και τον αναιρεσείοντα Π.Α.**, όχι τις πραγματικές, αλλά κατά πολύ μεγαλύτερες από εκείνες που αναγράφονται στα δελτία διαθέσεως εργατικής ομάδας, χωρίς να υπάρχουν τα αντίστοιχα περιστατικά που να δικαιολογούν τις μεταβολές (αλλοιώσεις) αυτές των πρωτογενών αυτών στοιχείων, με αποτέλεσμα ο Η/Υ να παρουσιάζει εντελώς εσφαλμένη εικόνα, ότι δηλαδή αυτοί έχουν αυξημένες αποδοχές κατά 836.496 δρχ. ο πρώτος, 732.321 δρχ. ο δεύτερος και 707.171 δρχ. ο τρίτος. Έτσι οι αναιρεσείοντες Σ.Κ.** και Δ.Γ.** εισέπραξαν παράνομα και σε βάρος της περιουσίας του ΟΛΠ τα παραπάνω χρηματικά ποσά. Ο δε αναιρεσείων Π.Α.** με πρόθεση δέχθηκε στην κατοχή του πράγματα που προήλθαν από αξιόποινη πράξη δηλαδή εισέπραξε ως αποδοχές του για την εργασία του στον ΟΛΠ το πιο πάνω χρηματικό ποσό των 707.171 δραχμών (72.215 δρχ. το 1990, 377.321 δρχ. το 1991 και 257.635 δρχ. το 1992) αν και γνώριζε ότι δεν το δικαιούται και ότι αυτό προέρχεται από αξιόποινη πράξη και ειδικότερα από την πιο πάνω απάτη με υπολογιστή που διέπραξαν οι Σ.Κ.** και Δ.Γ.** Με τις παραδοχές αυτές το δικαστήριο κήρυξε ένοχους τους δύο πρώτους αναιρεσείοντες απάτης με υπολογιστή κατ' εξακολούθηση και τον τρίτο αποδοχής προϊόντων εγκλήματος κατ' εξακολούθηση. Με αυτά που δέχτηκε το εφετείο διέλαβε στην απόφασή του την από τις διατάξεις των άρθρ. 93 παρ.3 του Σ και 139 ΚΠΔ απαιτούμενη ειδική και εμπεριστατωμένη αιτιολογία, αφού παραθέτει λεπτομερώς και τα αποδεικτικά στοιχεία, στα οποία θεμελίωσε την κρίση του, και τα πραγματικά περιστατικά που δέχτηκε ότι αποδείχτηκαν και τα οποία πληρούν την αντικειμενική και υποκειμενική υπόσταση των πιο πάνω εγκλημάτων για τα οποία καταδικάστηκαν οι αναιρεσείοντες, και τέλος τις σκέψεις και τους συλλογισμούς με τους οποίους υπήγαγε τα περιστατικά στις παραπάνω ουσιαστικές ποινικές διατάξεις που εφάρμοσε. Επομένως οι λόγοι αναιρέσεως των υπό κρίση από 27.2.1995 και 2.3.1995 αιτήσεων από το άρθρ. 510 παρ.1 στοιχ. Δ' του ΚΠΔ με τους οποίους υποστηρίζονται τα αντίθετα, πρέπει ν' απορριφθούν ως αβάσιμοι.

Πρόεδρος: Κ. Δαφέρμος

Εισηγητές: Ι. Μυγιάκης

Λήμματα: Απάτη με ηλεκτρονικό υπολογιστή ,Αποδοχές ,Αποδοχή προϊόντων εγκλήματος

ΣΤΟΙΧΕΙΑ ΑΠΟΦΑΣΗΣ

Δικαστήριο: ΑΡΕΙΟΣ ΠΑΓΟΣ
Τόπος: ΑΘΗΝΑ
Αριθ. Απόφασης: 1277
Ετος: 1998

Κείμενο Απόφασης

Αριθμός 1277/1998 Το Δικαστήριο του Αρείου Πάγου ΣΤ' Ποινικό Τμήμα _ _ _ _ Συγκροτήθηκε από τους δικαστές: Κωνσταντίνο Λυμπερόπουλο, Αντιπρόεδρο, Γεώργιο Αρβανίτη, Ανδρέα Κατράκη, Κωνσταντίνο Τζένο και Γεώργιο Νικολόπουλο-Εισηγητή, Αρεοπαγίτες.- Με την παρουσία και του Αντεισαγγελέα Βασιλείου Ξενικάκη (γιατί κωλύεται ο Εισαγγελέας) και της Γραμματέως Μηλιάς Αθανασοπούλου.- Συνεδρίασε δημόσια και στο

ακροατήριο του Καταστήματος αυτού στις 6 Οκτωβρίου 1998 για να δικάσει την αίτηση του αναιρεσείοντος-κατηγορουμένου: Γ. Π. του Δ., κατοίκου Αργοστολίου Κεφαλληνίας, που εκπροσωπήθηκε από τον πληρεξούσιο δικηγόρο του Κωνσταντίνο Φαγογένη, για αναίρεση της υπ' αριθμ.298-306/1998 αποφάσεως του Πενταμελούς Εφετείου Αθηνών. Με πολιτικώς ενάγουσα την Εμπορική Τράπεζα της Ελλάδος, νομίμως εκπροσωπούμενη, που δεν παραστάθηκε στο ακροατήριο.- Το Πενταμελές Εφετείο Αθηνών με την απόφασή του με αριθμό 298-306/1998 διέταξε όσα λεπτομερώς αναφέρονται σ' αυτήν.- Και ο αναιρεσείων-κατηγορούμενος ζητάει τώρα την αναίρεση της απόφασης αυτής, για τους λόγους που αναφέρονται στην από 18 Μαρτίου 1998 αίτησή του αναιρέσεως, που καταχωρίστηκε στο οικείο πινάκιο με τον αριθμό 579/1998 ως και τους από 18 Μαΐου 1998 πρόσθετους λόγους αναίρεσης.- Α κ ο υ σ ε Τον πληρεξούσιο δικηγόρο του αναιρεσείοντος που και με προφορική ανάπτυξη στο ακροατήριο, ζήτησε όσα αναφέρονται και στα σχετικά πρακτικά. Και Τον Αντεισαγγελέα.- ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ Από τις διατάξεις των άρθρων 111, 112 και 113 του ΠΚ, όπως το τελευταίο ισχύει, μετά την αντικατάστασή του με το άρθρο 33 του ν.2172/1993 και το άρθρο 1 παρ.6 του ν. 2408/1996, προκύπτει ότι το αξιόποινο εξαλείφεται με την παραγραφή, η οποία, προκειμένου για πλημμελήματα, είναι πενταετής και αρχίζει από την ημέρα που τελέστηκε η αξιόποινη πράξη, αναστέλλεται δε για όσο χρόνο διαρκεί η κύρια διαδικασία και ωσότου καταστεί αμετάκλητη η καταδικαστική απόφαση, όχι όμως πέρα των τριών ετών. Η κύρια διαδικασία, από την έναρξη της οποίας υπολογίζεται η τριετής αναστολή της παραγραφής, αρχίζει από την επίδοση στον κατηγορούμενο του κλητηρίου θεσπίσματος ή της κλήσεως προς εμφάνιση στο ακροατήριο. Από τις ίδιες αυτές διατάξεις, σε συνδυασμό με εκείνες των άρθρων 310 παρ.1β, 370 εδ. β' και 511 του ΚΠΔ, προκύπτει ότι η παραγραφή, ως θεσμός δημοσίας τάξεως, εξετάζεται αυτεπαγγέλτως από το δικαστήριο σε κάθε στάση της διαδικασίας, ακόμη και από τον Άρειο Πάγο, ο οποίος, διαπιστώνοντας τη συμπλήρωσή της, έστω και μετά την άσκηση της αναιρέσεως, οφείλει να αναιρέσει την προσβαλλόμενη απόφαση και να παύσει οριστικά την ποινική δίωξη, υπό την προϋπόθεση ότι η απόφαση δεν έχει καταστεί αμετάκλητη και ότι η αίτηση αναιρέσεως είναι παραδεκτή, ήτοι έχει ασκηθεί νομότυπα και εμπρόθεσμα και περιέχει , σύμφωνα με το άρθρ. 474 παρ.2 του ΚΠΔ, ένα τουλάχιστον παραδεκτό λόγο αναιρέσεως, χωρίς να απαιτείται να είναι αυτός και βάσιμος. Στην προκειμένη περίπτωση, όπως προκύπτει από την προσβαλλόμενη 298, 306/1998 απόφαση του Πενταμελούς Εφετείου Αθηνών, με αυτή ο αναιρεσείων κηρύχθηκε ένοχος και καταδικάστηκε σε συνολική ποινή φυλακίσεως 4 ετών και 10 μηνών για απάτη σε βαθμό κακουργήματος και για πλαστογραφία και υπεξαγωγή εγγράφων σε βαθμό πλημμελήματος. Όλες οι πράξεις αυτές, κατά την απόφαση, φέρονται ότι έχουν τελεσθεί στις 28 Φεβρουαρίου 1990. Ενόψει του χρόνου αυτού της τελέσεώς τους, οι δύο τελευταίες πράξεις, της πλαστογραφίας και της υπεξαγωγής εγγράφων, που είναι πλημμελήματα, έχουν υποκύψει στην παραγραφή και συνεπώς έχει εξαλειφθεί το αξιόποινο για τις πράξεις αυτές, λόγω συμπληρώσεως οκταετίας από την ημέρα τελέσεως μέχρι σήμερα, συνυπολογιζομένης και της τριετούς αναστολής. Επομένως, εφόσον η κρινόμενη αίτηση αναιρέσεως του κατηγορουμένου έχει ασκηθεί νομότυπα και εμπρόθεσμα και περιέχει παραδεκτούς λόγους , πρέπει αυτεπαγγέλτως αλλά και κατά παραδοχή του σχετικού λόγου, να αναιρεθεί η προσβαλλόμενη απόφαση ως προς τις διατάξεις της που αφορούν στις παραπάνω δύο πράξεις, καθώς και ως προς τη συνολική ποινή και να παύσει οριστικά η ποινική δίωξη ως προς τις πράξεις αυτές κατά του κατηγορουμένου.- Κατά τη διάταξη της παρ.1 του άρθρου 386 του ΠΚ, όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία, πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων ως αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η προξενηθείσα ζημία είναι ιδιαιτέρως μεγάλη, με φυλάκιση τουλάχιστον δύο ετών. Κατά δε τη διάταξη της παρ.3 του ίδιου άρθρου, επιβάλλεται κάθειρξη μέχρι δέκα ετών αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια. Περαιτέρω, κατά το εδάφ. στ' του άρθρου 13 του ΠΚ, που προστέθηκε με το άρθρο 1 παρ.1 του ν. 2408/1996, κατ' επάγγελμα τέλεση του εγκλήματος συντρέχει όταν από την επανειλημμένη τέλεση της πράξης ή από την υποδομή που έχει διαμορφώσει ο δράστης με πρόθεση επανειλημμένης τέλεσης της πράξης, προκύπτει σκοπός του δράστη για πορισμό εισοδήματος. Ήτοι συντρέχει κατ' επάγγελμα τέλεση και όταν μία φορά ετελέσθη η πράξη, όχι όμως ευκαιριακά αλλά βάσει οργανωμένου σχεδίου, που δείχνει ότι ο δράστης έχει διαμορφώσει υποδομή και οργανωμένη ετοιμότητα με πρόθεση επανειλημμένης τέλεσης, από την οποία προκύπτει σκοπός του για πορισμό εισοδήματος. Διαφέρει δε το έγκλημα της απάτης του άρθρου 386 ΠΚ από το ειδικό έγκλημα του άρθρου 386 Α ΠΚ, που προστέθηκε με το άρθρο 5 του ν. 1805/1988, κατά το οποίο τιμωρείται με τις ποινές του άρθρου 386, όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος

είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο. Το άρθρο 386 ΠΚ περιορίζει την απάτη μόνο στις περιπτώσεις που η ξένη περιουσία βλάπτεται με την παραπλάνηση κάποιου φυσικού προσώπου, ενώ στο άρθρο 386Α ΠΚ η ξένη περιουσία βλάπτεται, ασχέτως παραπλανήσεως, με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων του υπολογιστή. Το έγκλημα της κοινής απάτης του άρθρ. 386 ΠΚ μπορεί, βέβαια, να διαπραχθεί και με τη χρησιμοποίηση του υπολογιστή ως μέσου για την παραπλάνηση του τρίτου. Εξάλλου, η απαιτούμενη από τις διατάξεις των άρθρ. 93 παρ.3 του Συντ. και 139 του ΚΠΔ ειδική και εμπεριστατωμένη αιτιολογία της καταδικαστικής αποφάσεως, η έλλειψη της οποίας ιδρύει λόγο αναιρέσεως από το άρθρο 510 παρ.1 στοιχ. Δ' του ΚΠΔ, υπάρχει όταν περιέχονται σ' αυτή τα πραγματικά περιστατικά που προέκυψαν από την ακροαματική διαδικασία, στα οποία στηρίχθηκε η κρίση του δικαστηρίου για τη συνδρομή των στοιχείων του εγκλήματος, οι αποδείξεις που λήφθηκαν υπόψη και οι νομικές σκέψεις υπαγωγής των περιστατικών αυτών στην ουσιαστική ποινική διάταξη που εφαρμόστηκε Για την πληρότητα της αιτιολογίας σε σχέση με το έγκλημα της απάτης πρέπει να εκτίθενται περιστατικά βλάβης της ξένης περιουσίας και να προσδιορίζεται ποια περιουσία υπέστη τη βλάβη και σε τι συνίσταται η βλάβη αυτή. Ακόμη, όταν το δικαστήριο δέχεται ότι η βλάβη ξένης περιουσίας επήλθε με την επέμβαση του δράστη στη μνήμη ηλεκτρονικού υπολογιστή με τη μετάδοση μη ορθών στοιχείων, ενώ παράλληλα δέχεται και ότι ο δράστης παρέστησε εν γνώσει ψευδή περιστατικά σε τρίτους συνεπεία των οποίων παραπλανήθηκαν και προέβησαν σε περιουσιακή διάθεση εκ της οποίας επήλθε βλάβη σε ξένη περιουσία, πρέπει να διευκρινίζεται τελικά στην απόφαση για ποια πράξη κηρύσσεται ένοχος ο κατηγορούμενος, της κοινής απάτης του άρθρου 386 ΠΚ ή της απάτης με ηλεκτρονικό υπολογιστή του άρθρου 386 Α, που είναι διαφορετικό έγκλημα. ΠΌταν ο κατηγορούμενος κηρύσσεται ένοχος απάτης σε βαθμό κακουργήματος, λόγω συνδρομής της επιβαρυντικής περιστάσεως της κατ' επάγγελμα τέλεσης, πρέπει να παρατίθενται στην απόφαση συγκεκριμένα περιστατικά που θεμελιώνουν κατά νόμο την έννοια της επιβαρυντικής αυτής περιστάσεως. Ειδικότερα, όταν το δικαστήριο δέχεται ότι η κατ' επάγγελμα τέλεση θεμελιώνεται στην υποδομή που έχει διαμορφώσει ο κατηγορούμενος με πρόθεση επανειλημμένης τέλεσης της πράξης από την οποία προκύπτει σκοπός για πορισμό εισοδήματος, πρέπει για την πληρότητα της αιτιολογίας ως προς την επιβαρυντική αυτή περίσταση να εκθέτει το δικαστήριο στην απόφασή του από ποια περιστατικά συνήγαγε την ύπαρξη της υποδομής και την πρόθεση για επανειλημμένη τέλεση της πράξης. Τέλος, εσφαλμένη εφαρμογή ουσιαστικής ποινικής διατάξεως, που ιδρύει λόγο αναιρέσεως από το άρθρο 510 παρ. 1 στοιχ. Ε του ΚΠΔ, υπάρχει και όταν η διάταξη αυτή παραβιάστηκε εκ πλαγίου για το λόγο ότι το πόρισμα της αποφάσεως, που περιλαμβάνεται στο συνδυασμό του αιτιολογικού με το διατακτικό, διαπιστώνονται κενά και ελλείψεις, που καθιστούν ανέφικτο τον έλεγχο από τον Αρειο Πάγο για την ορθή ή μη εφαρμογή του νόμου, οπότε η απόφαση στερείται νόμιμης βάσης. Έλλειψη αιτιολογίας και νόμιμης βάσης είναι δυνατόν να συρρέουν ως λόγοι αναιρέσεως. Στην προκειμένη περίπτωση, από το συνδυασμό του σκεπτικού προς το διατακτικό της προσβαλλόμενης απόφασης προκύπτει ότι το Πενταμελές Εφετείο Αθηνών που την εξέδωκε, ύστερα από αξιολόγηση των αναφερομένων σ' αυτή αποδεικτικών μέσων, δέχθηκε ανελέγκτως, σε σχέση με την πράξη της απάτης, ότι προέκυψαν τα ακόλουθα πραγματικά περιστατικά: Στις 28-2-1990, ο αναιρεσείων κατηγορούμενος Γ. Π., υπάλληλος της Εμπορικής Τράπεζας και χειριστής κατά την ημέρα εκείνη του τερματικού Ε του υποκαταστήματος της πλατείας Καραϊσκάκη, στην Αθήνα, έχοντας αφαιρέσει ένα ασυμπλήρωτο καρνέ επιταγών με αριθμούς 9023461 έως 9023480, από τις οποίες είχε συμπληρώσει επτά, με τους αριθμούς 9023467- 90234471, 9023478 και 9023480, με τα αντίστοιχα ποσά των δρχ. 2.640.000, 2.880.000, 3.450.000, 3.200.000, 3.150.000, 3.100.000 και 2.050.000, με την ημερομηνία έκδοσης 27-2-90 και 25-2-1990, τον τόπο έκδοσης, Αθήνα, το όνομα του φερόμενου ως κομιστή Γ. Κατεργιαννάκη και τα ονόματα των φερόμενων ως εκδοτών, εκπροσώπων του ΟΣΕ Φ. Κόκκοτου και Γερ. Τραγουλιά, με σκοπό να προσπορίσει στον εαυτό του παράνομο περιουσιακό όφελος, μετέδωσε από το παραπάνω Τερματικό Ε μήνυμα στη μνήμη του κεντρικού υπολογιστή της Εμπορικής Τράπεζας, με το οποίο συσχέτισε τους αριθμούς των πιο πάνω επτά επιταγών του καρνέ με το λογαριασμό καταθέσεων όψεως 81261105, που διατηρούσε στο ανωτέρω υποκατάστημα ο ΟΣΕ, ωσάν ο τελευταίος να είχε λάβει το καρνέ τούτο, καίτοι ουδέποτε το είχε λάβει. Στη συνέχεια, ο κατηγορούμενος, με την άμεση συνέργεια τρίτου άγνωστου προσώπου, στο οποίο παρέδωσε τις παραπάνω επτά πλαστογραφημένες επιταγές, παρέστησε εν γνώσει ψευδώς στους υπαλλήλους των Υποκαταστημάτων της Εμπορικής Τράπεζας, στα οποία στις 5-3-1990 εμφανίστηκαν οι επιταγές αυτές, ότι είχαν εκδοθεί πράγματι από τους εξουσιοδοτημένους εκπροσώπους του ΟΣΕ, σε χρέωση του λογαριασμού καταθέσεων όψεως του Υποκ/τος Καραϊσκάκη, με αποτέλεσμα να παραπλανηθούν οι εν λόγω αρμόδιοι υπάλληλοι και να εξοφλήσουν στον άγνωστο κομιστή τις επιταγές αυτές, σε χρέωση του λογαριασμού του ΟΣΕ με το συνολικό ποσό των 20.470.000 δρχ.,

βλάπτοντας, αντίστοιχα, την περιουσία του ΟΣΕ και της Τράπεζας, που μετά την αποκάλυψη της αλήθειας υποχρεώθηκε να καταβάλει το ποσό αυτόν στον ΟΣΕ, του οποίου απειλήθηκε η περιουσία. Με βάση τα περιστατικά αυτά το δικαστήριο κατέληξε στο σκεπτικό του ότι πρέπει να κηρυχθεί ένοχος ο αναιρεσείων απάτης κατ' επάγγελμα ενόψει της υποδομής που είχε διαμορφώσει με πρόθεση επανειλημμένης τέλεσης της πράξης, από την οποία προέκυπτε σκοπός για πορισμό εισοδήματος (επηρεασμός στοιχείων κεντρικού υπολογιστή και παραπλάνηση των αρμόδιων υπαλλήλων των υποκαταστημάτων με τις πλαστογραφημένες επιταγές). Στο διατακτικό κηρύσσεται ένοχος ο αναιρεσείων απάτης, ήτοι ότι με σκοπό ν' αποκομίσει παράνομο περιουσιακό όφελος έβλαψε την περιουσία του ΟΣΕ και της Εμπορικής Τράπεζας, πείθοντας άλλους σε πράξη με την εν γνώσει παράσταση ψευδών γεγονότων ως αληθινών, από την οποία η απειληθείσα και προσγενομένη ζημία στον ΟΣΕ και την Τράπεζα είναι ιδιαίτερα μεγάλη, προέβη δε στην πράξη του αυτή κατ' επάγγελμα, ήτοι με σκοπό τον βιοπορισμό και επί πλέον προέβη στην πράξη του αυτή επηρεάζοντας τη μνήμη του ηλεκτρονικού υπολογιστή με τη μετάδοση μη ορθών στοιχείων, όπως περιγράφεται ειδικότερα παραπάνω. Με τις παραδοχές αυτές η προσβαλλόμενη απόφαση δεν έχει την κατά τα άνω απαιτούμενη ειδική και εμπεριστατωμένη αιτιολογία, καθόσον δεν εκθέτει με σαφήνεια αν και ποια ζημία υπέστη στην περιουσία του ο ΟΣΕ, τον οποίο αναφέρει ως ζημιωθέντα η απόφαση, καίτοι δέχεται ότι του καταβλήθηκε αμέσως από την Τράπεζα το ποσό των 20.470.000 δρχ. Περαιτέρω, δεν γίνεται σαφές από την απόφαση ποια μορφή απάτης δέχεται το δικαστήριο ότι τέλεσε ο κατηγορούμενος. Την κοινή του άρθρου 386 ΠΚ ή την ειδική απάτη με υπολογιστή του άρθρου 386 Α, δοθέντος ότι δέχεται σωρευτικά τη συνδρομή περιστατικών και των δύο πράξεων, που είναι διαφορετικές και αναφέρει ότι η πράξη που τέλεσε ο κατηγορούμενος προβλέπεται και από τις δύο πιο πάνω διατάξεις, χωρίς να προκύπτει ποια ακριβώς μορφή απάτης δέχεται το δικαστήριο. Τέλος, για την επιβαρυντική περίσταση, που δίνει τον κακουργηματικό χαρακτήρα στην πράξη της απάτης που τέλεσε ο κατηγορούμενος, δέχεται η απόφαση ότι στην πράξη του αυτή προέβη κατ'επάγγελμα, ήτοι με σκοπό το βιοπορισμό, ενώ στο σκεπτικό θεμελιώνει την κατ' επάγγελμα τέλεση στην υποδομή που είχε διαμορφώσει ο κατηγορούμενος με πρόθεση επανειλημμένης τέλεσης της πράξης, χωρίς όμως να εκθέτει από ποια συγκεκριμένα περιστατικά συνήγαγε την κρίση του αυτή περί διαμορφωμένης υποδομής και πρόθεσης επανειλημμένης τέλεσης, παραθέτοντας μόνο σε παρένθεση την αόριστη φράση «επηρεασμός στοιχείων κεντρικού υπολογιστή». Επομένως, η προσβαλλόμενη απόφαση, εξαιτίας των παραπάνω ελλείψεων και ασαφειών στις κρίσιμες παραδοχές της, στερείται της απαιτούμενης αιτιολογίας, καθώς και νομίμου βάσεως, γιατί καθίσταται ανέφικτος ο αναιρετικός έλεγχος για την ορθή ή μη εφαρμογή των πιο πάνω ουσιαστικών ποινικών διατάξεων που προαναφέρθηκαν. Κατά συνέπεια και κατά παραδοχή ως κατ' ουσίαν βασίμων των σχετικών λόγων της κρινόμενης αιτήσεως, πρέπει να αναιρεθεί η προσβαλλόμενη απόφαση ως προς τον αναιρεσείοντα και κατά τη διάταξή της που αφορά στην πράξη της απάτης και ακολούθως να παραπεμφθεί η υπόθεση για νέα συζήτηση ενώπιον του ιδίου δικαστηρίου, που θα συγκροτηθεί από άλλους δικαστές εκτός εκείνων που δίκασαν, σύμφωνα με τη διάταξη του άρθρου 519 ΚΠΔ.- Για τους λόγους αυτούς - Αναιρεί την υπ'αριθ. 298, 306/1998 απόφαση του Πενταμελούς Εφετείου Αθηνών, ως προς όλες τις διατάξεις της και για όλες τις πράξεις που αφορούν στον αναιρεσείοντα κατηγορούμενο Γ. Π. - -Παύει οριστικά την ποινική δίωξη κατά του πιο πάνω κατηγορουμένου για τις πράξεις της πλαστογραφίας και υπεξαγωγής εγγράφων που φέρονται ότι τελέσθηκαν στην Αθήνα στις 28-2-1990.- -Παραπέμπει την υπόθεση, κατά τα λοιπά, ήτοι ως προς την πράξη της απάτης που φέρεται ότι τελέσθηκε από τον κατηγορούμενο αυτό για νέα συζήτηση ενώπιον του ίδιου δικαστηρίου, που θα συγκροτηθεί από άλλους δικαστές εκτός από εκείνους που δίκασαν προηγουμένως.- -Κρίθηκε και αποφασίστηκε στην Αθήνα στις 13 Οκτωβρίου 1998.- -Δημοσιεύθηκε στην Αθήνα σε δημόσια συνεδρίαση στο ακροατήριο στις 20 Οκτωβρίου 1998.- Ο ΑΝΤΙΠΡΟΕΔΡΟΣ Η ΓΡΑΜΜΑΤΕΑΣ

Δικαστήριο: ΑΡΕΙΟΣ ΠΑΓΟΣ
Τόπος: ΑΘΗΝΑ
Αριθ. Απόφασης: 201
Έτος: 2005

Περίληψη

Υπεξαίρεση - **Απάτη με υπολογιστή** - Συρροή -. Αν μετά την υπεξαίρεση ο δράστης προς συγκάλυψή της ή διατήρηση της κατοχής του υπεξαιρεθέντος τελέσει **απάτη με υπολογιστή** υπάρχει φαινομένη συρροή υπεξαιρέσεως και μη τιμωρητής μεταγενέστερης πράξης απάτης, εκτός αν η δεύτερη είναι βαρύτερη της πρώτης, οπότε απορροφά την υπεξαίρεση.

Κείμενο **Απόφασης**

(Α π ό σ π α σ μ α): Με το δεύτερο των αιτήσεων λόγο προβάλλει ο αναιρεσείων, με επίκληση του άρθρου 510 §1 στοιχ. Δ' ΚΠΔ, ότι προέβαλε και ανέπτυξε κατά τη διαδικασία τον αυτοτελή ισχυρισμό ότι η απάτη με ηλεκτρονικό υπολογιστή (άρθρο 386 Α' ΠΚ), δι' ην κατεδικάσθη με την προσβαλλομένη απόφαση, ευρίσκεται σε + φανομένη συρροή με την αξιόποινη πράξη της υπεξαιρέσεως (375 ΠΚ), διά την οποία με την πρωτοβάθμια απόφαση έπαυσε η κατ' αυτού ποινική δίωξη λόγω παραγραφής + αφού χαρακτηρίσθηκε ως πλημμέλημα υπό του πρωτοβαθμίου δικαστηρίου, και + ειδικότερα η πράξη της απάτης με ηλεκτρονικό υπολογιστή αποτελεί μη τιμωρητή + ύστερα πράξη, ως αποσκοπούσα τη συγκάλυψη της προηγηθείσης υπεξαιρέσεως, και + ότι το δικαστήριο απέρριψε τον ισχυρισμό του τούτον άνευ της απαιτουμένης + ειδικής και εμπεριστατωμένης αιτιολογίας. Ως, όμως, προκύπτει από την + προσβαλλομένη απόφαση, το δικαστήριο απέρριψε τον ισχυρισμόν αυτόν με την εξής αιτιολογία. « Ο κατηγορούμενος διατείνεται ότι το ως άνω έγκλημα, για το οποίο έχει καταδικασθεί, συνιστά ύστερη μη τιμωρητή πράξη σε σχέση προς το έγκλημα + της υπεξαίρεσης, για το οποίο με την προεκδοθείσα υπ' αριθ. 37/2002 απόφαση του Τριμελούς Εφετείου Δωδεκανήσου έπαυσε οριστικά η ποινική δίωξη λόγω + παραγραφής, μεταξύ των οποίων υφίσταται φαινόμενη συρροή και πρέπει να κηρυχθεί αθώος. Ο ισχυρισμός, όμως, αυτός του κατηγορουμένου πρέπει να απορριφθεί ως + αβάσιμος, καθόσον μεταξύ των εγκλημάτων της απάτης (με ηλεκτρονικό υπολογιστή) και της υπεξαίρεσης υπάρχει πραγματική συρροή, αφού πλήττουν διαφορετικά έννομα αγαθά, και στη συγκεκριμένη περίπτωση δεν βεβαιώθηκε από κανένα αποδεικτικό + μέσο και στοιχεί ότι οι επεμβάσεις του κατηγορουμένου στους ηλεκτρονικούς + υπολογιστές της εγκαλούσας εταιρίας έγιναν αποκλειστικώς προς τον σκοπό της + συγκάλυψης της υπεξαιρέσεως, αλλ' αντιθέτως αρκούντως βεβαιώθηκε ότι οι + επεμβάσεις αυτές αποτέλεσαν την αναγκαία προϋπόθεση για την πρόκληση της ζημίας της εγκαλούσας εταιρίας, στην οποία απέβλεψε ο κατηγορούμενος με αντίστοιχη + ωφέλεια αυτού». Με τις παραδοχές, όμως, αυτές το δικαστήριο της ουσίας διέλαβε στην προσβαλλομένη απόφασή του, ως προς την απόρριψη του εν λόγω ισχυρισμού του αναιρεσείοντος, την κατά τα άρθρα 93 §3 του Συντάγματος και 139 του ΚΠΔ ειδική και εμπεριστατωμένη αιτιολογία, δι' ο και ο περί του αντιθέτου προαναφερθής + λόγος αμφοτέρων των αιτήσεων είναι αβάσιμος. Περαιτέρω, και δεδομένου ότι ο + αυτός λόγος, όπως εκτίθεται αυτός, δύναται να εκτιμηθεί και ως εκ του στοιχ. Ε' του ανωτέρω άρθρου προβαλλόμενος, ειδικότερα δε ότι προβάλλεται με αυτόν η + αιτίαση της εσφαλμένης ερμηνείας και εφαρμογής του άρθρου 94 ΠΚ σε συνδυασμό + προς τα άρθρα 375 και 386 Α' ΠΚ, πρέπει να λεχθούν τα εξής: Από τις διατάξεις + των άρθρων 375 §1 και 386 Α' ΠΚ προκύπτει ότι εκάτεροι των πράξεων τούτων + απαρτίζεται από διαφορετικά στοιχεία και συνεπώς, αν ο δράστης τους είναι ένα + και το αυτό πρόσωπο, είναι δυνατή η πραγματική συρροή των δύο αυτών εγκλημάτων, εφόσον καθένα από αυτά στρέφεται κατά διαφορετικού αντικειμένου. Αν όμως και + τα δύο στρέφονται κατά του αυτού υλικού αντικειμένου, υφίσταται μεταξύ τους + φαινομένη συρροή, οπότε, αν μεν ο δράστης απέκτησε με απάτη το ιδιοποιούμενο + πράγμα δεν τιμωρείται η υπεξαίρεση, διότι απορροφάται από την απάτη, αν δε ο + δράστης υπεξαιρεί το ξένο κινητό πράγμα και ακολούθως επιχειρεί απατηλές + πράξεις προς συγκάλυψη της υπεξαιρέσεως ή διατήρηση της κατοχής του + υπεξαιρεθέντος, υπάρχει φαινομένη συρροή υπεξαιρέσεως και μη τιμωρητής + μεταγενεστέρας

πράξεως απάτης. Πάντως στην τελευταία αυτή περίπτωση + προϋποτίθεται ότι η απάτη προς εξασφάλιση του υπεξαιρεθέντος πράγματος είναι + ελαφροτέρα της υπεξαιρέσεως, ήτοι τιμωρείται ηπιώτερα της τελευταίας, διότι εάν η εξασφαλιστική απάτη είναι βαρυτέρα της υπεξαιρέσεως, ως όταν η απάτη + τιμωρείται εις βαθμόν κακουργήματος και η υπεξαίρεση εις βαθμόν πλημμελήματος, τότε η απάτη απορροφά την υπεξαίρεση διότι η απαξία της τελευταίας υπολείπεται της απαξίας της πρώτης. Στην προκειμένη περίπτωση, δέχεται το δικαστήριο, όπως προκύπτει από την προσβαλλομένη απόφαση, ότι με την προεκδοθείσα 37/2002 + απόφαση του Τριμελούς Εφετείου (κακουργημάτων) Δωδεκανήσου έπαυσε οριστικά η + ποινική δίωξη κατά του αναιρεσείοντος για υπεξαίρεση εις βαθμό πλημμελήματος + λόγω παραγραφής. Έτσι, όμως, το δι' ο κατεδικάσθη ο αναιρεσείων, εν συνεχεία, + με την προσβαλλομένη απόφαση έγκλημα της κακουργηματικής απάτης, και στην + περίπτωση που ήθελε γίνει δεκτόν ότι τούτο έγινε προς συγκάλυψη της + υπεξαιρέσεως, εν τούτοις, ως βαρύτερον, απορροφά την υπεξαίρεση. Επομένως, + εφόσον εκτιμηθεί ο αυτός δεύτερος λόγος των αιτήσεων, ως εκ των στοιχ. Ε' του + άρθρου 510 αριθ. 1 ΚΠΔ τοιούτος, είναι αβάσιμος, διότι το δικαστήριο ορθώς + ερμήνευσε και εφήρμοσε τις ανωτέρω διατάξεις και κατεδίκασε τον αναιρεσείοντα + διά κακουργηματικήν απάτη.

ΞΕΝΗ ΝΟΜΟΛΟΓΙΑ (ΙΤΑΛΙΑ)

La norma prevista e punita dall'art. 640 ter c.p. è posta a tutela sia della riservatezza e della regolarità dei sistemi informatici sia del patrimonio altrui e l'evento consiste nel conseguimento da parte del soggetto attivo di un ingiusto profitto con altrui danno. Accedere tramite Internet e operare immediati bonifici in favore del proprio c/c on-line non configura l'ipotesi di furto aggravato ed , in siffatte ipotesi, l'interprete deve spingersi sino a considerare se non vi sia stato un intervento non autorizzato (che è possibile effettuare con qualsiasi modalità) sui dati, informazioni e programmi ivi contenuti.

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

SEZIONE QUINTA PENALE

Composta dagli Ill.mi Sigg.ri Magistrati:

Dott. LATTANZI Giorgio - Presidente

1. Dott. PIZZUTI Giuseppe - Consigliere

2. Dott. MARINI Pier Francesco - Consigliere

3. Dott. FERRUA Giuliana - Consigliere

4. Dott. SICA Giuseppe - Consigliere

ha pronunciato la seguente:

SENTENZA

sul ricorso proposto da:

N. S. N. IL .....

avverso ORDINANZA del 09/05/2003 TRIB. LIBERTA' di CATANIA;

sentita la relazione fatta dal Consigliere Dr. SICA GIUSEPPE;

lette/sentite le conclusioni del P.G. Dr. Cosentino Francesco che ha

chiesto l'annullamento;

RITENUTO IN FATTO

Il tribunale di Catania, con il provvedimento impugnato del 9/5/2003, in sede di riesame, confermava l'ordinanza cautelare emessa dal G.I.P. di Siracusa, con la quale veniva disposta la misura cautelare in carcere nei confronti di N. S. indagato per furto aggravato ai sensi degli articoli 61, n. 7, 81 cpv, 624 e 625, n. 4 C.P., per avere sottratto dal C/C 33040, acceso presso la Banca Telematica Intesa "121", 30.000,00 euro, accedendo tramite

Internet e operando immediati bonifici in favore del proprio C/C.

Ricorre per Cassazione l'indagato prospettando erronea qualificazione del fatto reato contestato e l'erronea o falsa applicazione degli articoli 278 e 280 c.p.p.. Infatti, nel caso di specie, al piu', ricorreva l'ipotesi di cui all'art. 640 ter C.P., la c.d. frode informatica, che prevede una pena massima di anni tre di reclusione, non essendo applicabili le aggravanti speciali.

In ogni caso, anche se ricorresse l'ipotesi di furto, non sussisteva l'aggravante dell'art. 625, n. 4 C.P., atteso che essa richiede la destrezza e l'abilita' superiore a quella normale.

Con il secondo motivo deduce la violazione e la falsa applicazione dell'art. 275.2 bis c.p.p., potendo il N. godere della sospensione condizionale della pena, avendo il ricorrente riportato solo una condanna irrevocabile .....omissis.....

Lamenta ancora carenza di motivazione e violazione ed erronea applicazione dell'art. 273, nn. 1 e 1 bis c.p.p., non avendo motivato in ordine alla gravita' degli indizi, la cui ricorrenza era stata ritenuta scontata.

CONSIDERATO IN DIRITTO

Il ricorso merita accoglimento.

Il tribunale ha escluso che, nella specie, potesse ricorrere l'ipotesi affermata dal N., della violazione dell'art. 640 ter C.P., con conseguente inapplicabilita' della misura cautelare restrittiva, in quanto la norma era stata creata sul modello della truffa e tendeva a reprimere ogni fatto posto in essere mediante

alterazione di un funzionamento informatico o telematico che procuri a chi lo compie un ingiusto profitto con altrui danno, mentre nella fattispecie si era verificato l'impossessamento da parte dell'indagato di beni di altrui appartenenza.

E' evidente che, in tal modo, il tribunale ha limitato il suo esame solamente ad una delle ipotesi prese in considerazione dalla norma invocata.

Infatti - fermo restando che la norma e' posta a tutela sia della riservatezza e della regolarita' dei sistemi informatici che del patrimonio altrui e che l'evento consiste nel conseguimento da parte del soggetto attivo di un ingiusto profitto con altrui danno - trattasi di reato a forma libera che prevede, alternativamente una condotta consistente nell'alterazione del funzionamento del sistema informatico o telematico, ovvero in un intervento non autorizzato (che e' possibile effettuare con qualsiasi modalita') sui dati, informazioni e programmi ivi contenuti.

Tale ultima ipotesi, ai fini della ricorrenza o meno del reato di cui all'art. 640 ter C.P., perseguibile e querela, la cui ricorrenza -con riguardo alla pena edittale massima irrogabile - giustificherebbe l'accoglimento dell'impugnazione del N., pur avendo evidenziato che le operazioni erano state effettuate per via telematica attraverso l'utilizzazione di password, non

e' stata presa in considerazione dal tribunale.

Peraltro, per la giurisprudenza di questa Corte, il reato di frode informatica - che postula necessariamente la manipolazione del sistema - presenta la medesima struttura e gli stessi elementi costituivi della truffa, con l'unica differenza che non viene indotto in errore la persona del soggetto passivo, ma l'attivita' fraudolenta dell'agente investe il sistema informatico riferibile al suddetto (Cass. Sez. 6^, 14/12/1999, n. 3065, RV 214942).

La decisione impugnata va pertanto annullata con rinvio al tribunale di Catania per nuovo esame.

Restano assorbiti gli ulteriori motivi di ricorso.

P.Q.M.

Annulla l'ordinanza impugnata con rinvio al tribunale di Catania per nuovo esame.

Manda alla Cancelleria per gli adempimenti di cui all'art. 94 disp.

att. c.p.p..

Cosi' deciso in Roma, il 24 novembre 2003

Depositato in Cancelleria il 5 febbraio 2004

L'utilizzazione di carte di credito contraffatte per tramite del terminale Pos intestato ad uno degli indagati ed operante su conto corrente bancario nella sua titolarita' configura, secondo questa Corte di Cassazione, i reati di accesso abusivo (art. 615 ter cp), frode informatica (art.640 ter cp) e intercettazione fraudolenta di comunicazioni informatiche o telematiche (art. 617 quater cp).

CORTE SUPREMA DI CASSAZIONE

SEZIONE QUINTA PENALE

ud 1 ottobre2004 (dep. 27 gennaio 2004), n. 2672

Dott. FOSCARINI Bruno - Presidente

Dott. FERRUA Giuliana - Relatore

Consiglieri.....

ha pronunciato la seguente:

SENTENZA

sul ricorso proposto da:

Procuratore della Repubblica presso il Tribunale di Vibo Valentia;

avverso l'ordinanza emessa il 21-2-03 dal Tribunale di Catanzaro nei confronti di C. , nato il XXXX ;

visti gli atti, il provvedimento denunciato ed il ricorso;

sentita la relazione fatta dal Consigliere Dott. Giuliana Ferrua;

udito il Pubblico Ministero in persona del Sostituto Procuratore

Generale Dott. D'Angelo Giovanni che ha concluso per l'annullamento con rinvio dell'ordinanza impugnata.

MOTIVI DI RICORSO E RAGIONI DELLA DECISIONE

Con ordinanza 27-12-02 il G.I.P. presso il Tribunale di Vibo Valentia

applicava la misura cautelare degli arresti domiciliari a C. indagato per i seguenti reati: partecipazione ad

associazione finalizzata alla commissione di vari reati nel campo dell'informatica, posti in essere a scopo di lucro e tramite attivita' di contraffazione di carte di credito ed uso abusivo delle stesse (art. 416, capo A); frode informatica per avere, quale compiacente titolare dell'esercizio commerciale "N.M.", consentito in detto esercizio e con appositi strumenti, l'uso di carte di credito palesemente contraffatte e quindi di transazioni fraudolente, agendo abusivamente sul sistema informatico o telematico atto alla gestione dei pagamenti, procurando a se' o ad altri ingiusto profitto pari alle somme indebitamente sottratte alle societa' di gestione dei servizi di pagamento per via informatica, (art. 640 ter, capo B); intercettazione fraudolenta di comunicazioni informatiche o telematiche relative alla concessione dell'autorizzazione, per via telematica, all'uso di una carta di credito, attivita' posta in essere nella citata qualita' e nel suddetto esercizio, tramite carte contraffatte ed a mezzo del terminale Pos a lui intestato ed operante su conto bancario nella sua titolarita' (art. 617 quater, capo C), di accesso abusivo ad un sistema informatico o telematico quale quello concernente la gestione dei pagamenti tramite carte di credito e quello concernente relativo alla gestione dei conti correnti bancari, direttamente coinvolto per i prelievi dai conti dei titolari delle carte donate ed il successivo versamento sui conti degli esercizi commerciali, attivita' posta in essere nella citata qualita' e nel suddetto esercizio, tramite carte contraffatte (capo D), di alterazione e uso delle carte di credito in questione (art. 615 ter, capo F).

Con provvedimento 20-2-03 il Tribunale di Catanzaro, in sede di riesame, revocava la suddetta misura per il reati di cui ai capi A, C e D e sostituiva per gli altri la misura degli arresti domiciliari con quella dell'obbligo di presentazione ai CC.

Avverso tale ultimo provvedimento ha proposto ricorso per Cassazione il Procuratore della Repubblica presso il Tribunale di Vibo Valentia deducendo mancanza ed illogicita' della motivazione in ordine alla esclusa sussistenza di gravi indizi per i reati sub A, C, D.

La Corte osserva.

Per quanto concerne il reato associativo (capo A) il motivo va disatteso in quanto si risolve in apodittici e generici asserti sull'avere il Tribunale del riesame operato una

valutazione del quadro indiziario e cautelare in termini superficiali, frammentari ed incompleti, limitandosi il ricorrente ad enunciare una serie di principi in materia di reato associativo nonche' in tema di motivazione, senza specificare in quali parti del provvedimento impugnato essi sarebbero stati violati e senza prendere in considerazione le pur precise ragioni poste a base della decisione denunciata.

La censura risulta invece fondata con riferimento alla esclusa sussistenza di gravi indizi per gli altri reati e cioe' per l'accesso abusivo al sistema informatico o telematico previsto dall'art. 615 ter c.p. e per l'intercettazione fraudolenta di informazioni informatiche o telematiche di cui all'art. 617 quater c.p.. Nel provvedimento impugnato si e' evidenziato come sussistessero gravi indizi circa l'avere il C. consentito l'utilizzazione di carte di credito contraffatte per tramite del terminale Pos a lui intestato ed operante su conto corrente bancario nella sua titolarita': orbene l'avere ritenuto che un tale situazione valesse esclusivamente ai fini dell'addebito di frode telematica e non anche in ordine all'indebita introduzione in un sistema protetto da misure di sicurezza ex art. 615 ter c.p., si palesa contraddittorio, posto che in realta' la condotta individuata ed attribuita all'indagato ha comportato anche siffatta introduzione. Ne puo' dubitarsi che i reati di accesso abusivo ad un sistema informatico e la frode informatica possano concorrere: trattasi di delitti diversi, il secondo dei quali postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del primo; d'altro canto l'accesso abusivo puo' essere commesso solo con riferimento a sistemi protetti, requisito non postulato per la frode informatica (Cass. 14-12-99 n. 03067 RV. 214947). Cosi' pure il reato di accesso abusivo puo' concorrere con quello di cui all'art. 12 D.L. 143/91 perche' non ogni autorizzazione viene necessariamente ottenuta in via telematica e non ogni accesso abusivo si realizza tramite utilizzo di carta di credito falsificata.

Inoltre la condotta in ordine alla quale il Tribunale ha ravvisato i gravi indizi ha al contempo realizzato un'intercettazione fraudolenta - perche' ottenuta con carta contraffatta - di comunicazioni, in particolare relative alla concessione dell'autorizzazione all'uso della carta di credito ai sensi dell'art. 617 quater. Sussiste del resto possibilita' di concorso di tale reato con quello di cui all'art. 12 e con la frode informatica: infatti non ogni autorizzazione viene necessariamente ottenuta in via telematica e non ogni intercettazione telematica si realizza tramite utilizzo di carta falsificata; del pari non ogni frode informatica avviene mediante intercettazione di comunicazioni e del resto non ogni intercettazione realizza una manipolazione con alterazione del sistema ne' un ingiusto profitto ed altrui danno.

S'impone pertanto l'annullamento del provvedimento impugnato con rinvio al Tribunale di Catanzaro il quale dovra' rivedere il proprio giudizio negativo sul quadro indiziario con riguardo ai reati in questione attenendosi ai principi sopra enunciati e quindi verificare in relazione agli stessi la ricorrenza delle esigenze cautelari.

P.Q.M.

La Corte, annulla l'ordinanza impugnata limitatamente alla esclusa sussistenza di gravi indizi per i reati di cui ai capi C e D con rinvio per nuovo esame al Tribunale di

Catanzaro; rigetta nel resto il ricorso.

Cosi' deciso in Roma, il 1 ottobre 2003.

Depositato in Cancelleria il 27 gennaio 2004

Indebito utilizzo di carte di credito prepagate o di strumenti analoghi e insussistenza dei delitti di accesso abusivo a sistema informatico e detenzione di codici di accesso. Sussistenza di una condotta qualificata ai sensi dell'articolo 12 decreto legge 143/91.

Cassazione Sez. II Penale
10 luglio 2003 (dep. 31/07/03)
Sent. n.32440

Presidente Sirena

Relatore Fenu

Pg Galasso

Ricorrente Vodafone Omnitel

Premessa

D.L. è stato tratto a giudizio del Tribunale di Torino per rispondere di detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici, codici contenuti nelle carte di credito telefoniche della società Omnitel (articolo 615quater Cp) e di frode informatica (articolo 640ter Cp), commessi in due tempi, in data anteriore e prossima al 30 ottobre 1999, in concorso con tale A.M., e in data anteriore e prossima al 12 novembre 1999.

La società Vodafone Omnitel spa già Omnitel Pronto Italia spa - si costituiva parte civile. Era emerso dall'attività istruttoria che il L. aveva ricevuto da parte di persona a lui sconosciuta offerta di ricaricare il cellulare proprio e di altri dietro il versamento di somma inferiore a quella necessaria per l'acquisto della carta telefonica e, dopo aver acquisito e usato dei numeri di codice che gli erano stati segnalati, aveva fatto analogo favore a un suo collega di lavoro, tale A.M., di poi separatamente giudicato.

Con sentenza resa in data 30 settembre 2002 il Tribunale ha pronunciato l'assoluzione del L. dai reati ascritti perché il fatto non sussiste. Ha ritenuto non configurabile il reato di cui all'articolo 615quater Cp perché il codice segreto non doveva considerarsi mezzo idoneo per l'accesso al sistema, ma solo il numero identificativo di un credito; onde difettavano anche gli elementi obiettivi del reato di frode informatica, non essendosi prodotta alcuna arbitraria modificazione del sistema informatico.

Avverso tale provvedimento ha proposto ricorso immediato per cassazione il Procuratore della repubblica di Torino deducendo:

1) la manifesta illogicità della motivazione, dovendosi ritenere che l'imputato aveva inciso sul sistema informatico, costituito da registrazioni, memorizzazioni, attraverso un supporto informatico criptato, la cui utilizzazione era avvenuta abusivamente;
2) l'erronea applicazione della legge penale, segnatamente dell'articolo 640ter Cp, perché attraverso l'uso abusivo del codice il soggetto attivo si era collegato col programma, e in tal guisa aveva alterato il suo funzionamento, in quanto tale operare «sfasa l'abbinamento tra l'acquirente della scheda e l'accreditamento della ricarica».
3) l'erronea applicazione della legge penale, in relazione al delitto di cui all'articolo 615quater Cp, dal momento che l'imputato si era procurato abusivamente i codici idonei all'accesso ad un sistema informatico. Doveva pertanto tenersi conto della coincidenza tra il codice che consente l'accesso con il codice che consente la ricarica, e quindi l'esistenza di protezioni pur minimali idonee a evitare l'accesso abusivo al sistema.

Dal canto proprio, la parte civile ha proposto ricorso ai soli effetti della responsabilità civile, deducendo motivi pressoché sovrapponibili a quelli formulati dalla parte pubblica. Ha sostenuto infatti col primo motivo che la tutela apprestata dalla norma di cui all'articolo 615quater Cp riguardava i sistemi informativi protetti e tale doveva ritenersi quello gestito dalla società telefonica, perché il codice a 14 cifre era appunto condizione necessaria per accedere, nel senso di entrare in comunicazione col sistema, onde non era fondata l'interpretazione che il Tribunale aveva dato della fattispecie. Col secondo motivo la ricorrente ha censurato l'inosservanza e l'erronea applicazione della legge anche per quel che attiene l'articolo 640ter Cp, poiché dall'indebito utilizzo dei codici di ricarica conseguiva il diniego automatico della ricarica stessa, il che comportava l'alterazione del sistema, con l'impedimento agli utenti inconsapevoli di utilizzare positivamente la

scheda di cui pure avevano legittimamente acquistato la disponibilità.

Motivi della decisione

Ritiene la Corte che il ricorso è fondato nei termini di cui si tratterà con la conseguenza che la sentenza del Tribunale va annullata con rinvio degli atti alla Corte di appello competente.

1) Si desume dalla sentenza impugnata che D.L., intestatario di cellulare dell'Omnitel, si era avvalso, per la ricarica del proprio e di altri apparecchi appartenenti a parenti ed amici, dei numeri di codice che gli erano stati indicati, dietro un compenso pari alla metà di quello ufficiale, da una persona di nazionalità straniera, numeri che erano contenuti in un elenco in possesso di questa. Era risultato dalle indagini che numerosi codici provenivano da schede regolarmente acquistate e di poi utilizzate da un gruppo di immigrati di origine romena. In seguito alla utilizzazione della carta, i codici, composti di 14 numeri, erano stati ricoperti con smalto per unghie e la scheda era stata inserita in una confezione analoga a quella contenente la scheda nuova. La scheda così rimessa a nuovo veniva ceduta da un componente del gruppo, con un elementare raggiro, al rivenditore, scambiandola cioè con una nuova, che si era fatto consegnare e che fingeva di restituire, adducendo di non essersi avvisto di non avere danaro sufficiente per acquistarla, e consegnando appunto al suo posto quella già utilizzata. Tale operazione aveva interessato un notevole numero di schede, di guisa che la società telefonica era stata messa in allarme e aveva denunciato il fatto, a seguito di varie proteste di utenti, che, avendo ricevuto dai rivenditori le schede alterate, non avevano potuto ricaricare il telefonino. Il Tribunale si è diffuso nella ricostruzione del meccanismo per la ricarica della scheda contenuta nel cellulare, con utilizzazione della tessera che contiene, ricoperti con una vernice rimovibile, i numeri di codice, i quali, comunicati a un risponditore automatico, portano all'accreditamento della somma, purché i più volte menzionati numeri non siano stati già utilizzati o bloccati per altro motivo, onde attraverso l'acquisto della scheda si attua l'accreditamento alla società telefonica di somma di denaro che poi, attraverso l'operazione descritta, consentirà di usufruire di un corrispondente traffico telefonico. Quanto all'azione che aveva portato all'acquisizione delle schede, il Tribunale ha ritenuto che potesse al più configurare «un furto con mezzi fraudolenti (articoli 624-625 n. 2 Cp) della scheda nuova». Ad avviso del Tribunale, l'interesse tutelato dalla norma di cui all'articolo 615quater Cp ha per oggetto i sistemi informatici e telematici, poiché punisce condotte di accesso abusivo o di permanenza all'interno di detti sistemi, vale a dire condotte di danno, che nella specie non erano riscontrabili. E per la configurabilità del delitto di frode informatica di cui all'articolo 640ter Cp, era richiesta l'alterazione del funzionamento ovvero l'intervento su dati e programmi del sistema informatico, con conseguente arbitraria modificazione dello stesso allo scopo di profitto, e anche tali elementi non erano riscontrabili nel caso in esame. Né era, infine, ipotizzabile la ricettazione, o la contravvenzione di incauto acquisto per essere mancato l'oggetto materiale del reato, avendo l'imputato utilizzato dei numeri di codice, senza l'apprensione materiale delle carte telefoniche.

2) Ciò posto, ad avviso della Corte, tenuto conto delle argomentazioni svolte

dai ricorrenti, il problema è quello di stabilire quali reati siano stati commessi dall'imputato, atteso che la materia è resa complessa dall'introduzione di nuove norme, non sempre di agevole interpretazione, volte a contrastare la cosiddetta pirateria informatica.
Ma per compiere tale accertamento è, altresì, necessario individuare anche i reati commessi dagli altri protagonisti della vicenda, sia perché tali delitti, come si vedrà tra breve, rifluiscono sulla posizione del L., sia perché in ordine agli stessi si è pronunciato - sia pure incidentalmente - il Tribunale di Torino.

3). Ebbene, ritiene questo Collegio che l'azione svolta da colui il quale si è recato dal tabaccaio, e si è fatto consegnare la tessera Omnitel, sostituendola con una tessera già usata, integri gli estremi del delitto di truffa (articolo 640 Cp) e non del reato di furto aggravato dall'uso di un mezzo fraudolento (articoli 624 e 625, numero 2, Cp), come si afferma nel provvedimento impugnato.
Per il vero la fattispecie è ai confini tra le due ipotesi delittuose, ma si propende per la sussistenza del delitto previsto dall'articolo 640 Cp per le ragioni che seguono.
Come è noto, la linea di confine tra la truffa e il furto aggravato dall'uso di un mezzo fraudolento viene individuata dalla dottrina sottolineando che sussiste il primo reato solo in quanto l'usurpazione è operata con l'altrui consenso, che deve essere cosciente e volontario; mentre si configura il furto quando l'usurpazione del bene avviene senza la cooperazione della vittima.
E la giurisprudenza concorda con la dottrina, affermando che «il criterio distintivo tra il reato di furto, aggravato dall'uso del mezzo fraudolento, e il reato di truffa, va ravvisato nello impossessamento mediante sottrazione invito domino che caratterizza il primo e manca nel secondo, nel quale, invece, il trasferimento del possesso della cosa avviene con il consenso del soggetto passivo, consenso viziato da errore per effetto degli artifici e raggiri posti in essere dall'agente» (Cassazione penale, sezione seconda, 22 marzo 1983, Gozzo, Rv 161783).
In quest'ottica si è poi sviluppata una giurisprudenza (anch'essa ai limiti) secondo cui «la sottrazione di merci dai banchi di un supermercato cui faccia seguito l'esibizione alla cassa di uno scontrino relativo a merce pagata in precedenza, non costituisce truffa, ma furto aggravato dal mezzo fraudolento: e ciò in quanto lo stratagemma posto in essere dal soggetto è diretto non già a farsi dare dal venditore cose di cui non ha ancora possesso, ma soltanto a non pagare il prezzo di cose di cui si è già impossessato prelevandole dai banchi di esposizione» (Cassazione penale, sezione quarta, 24 gennaio 1996, Gullà, Rv 204994).
Tale giurisprudenza, che potrebbe avere fuorviato il Tribunale di Torino, tuttavia non è applicabile alla fattispecie, in quanto nel caso concreto è stato il tabaccaio a consegnare la carta telefonica al falso acquirente, il quale gli aveva fatto credere che intendeva acquistarla.
In altri termini, il raggiro posto in essere da chi si è recato dal tabaccaio consta di due parti: la prima consiste nell'avere simulato di volere acquistare il documento in questione e la seconda nel fare finta di non avere denaro liquido e nel restituire una carta telefonica diversa da quella ottenuta con il primo comportamento.
Comunque, il possesso di quell'oggetto da parte dell'agente non si è verificato invito domino, dal momento che è stato il tabaccaio a consegnarlo al finto acquirente. e quindi, per utilizzare una terminologia della dottrina, l'usurpazione è stata operata con il consenso cosciente e volontario della vittima, a costei carpito con l'inganno.

4). Comunque, quale che sia il reato commesso da chi ottiene, con le modalità prima descritte, la carta telefonica dal tabaccaio, è certo che qurst'ultima costituisce cosa proveniente da delitto e che perciò colui il quale l'acquista - avendo coscienza di tale circostanza -commette il reato di ricettazione.
Sennonché, nel caso concreto la carta in questione non è stata ceduta all'imputato da colui che l'aveva sottratta al legittimo detentore, essendosi l'originario truffatore limitato a digitare il numero di codice segreto, e ad accreditare in tal modo la somma portata da quel documento sul telefono del L..
Sembra, quindi, che nel caso concreto la ricettazione debba essere esclusa, dal momento che - per espresso disposto legislativo - tale reato ricorre quando il soggetto agente acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, e il digitare un numero di codice può semmai riportarsi al concetto di acquisto di una utilità, che è sicuramente. diverso da quello di cosa, non equivalendo quest'ultimo a quello più ampio di bene.
Del resto, il legislatore, proprio nel successivo articolo 648bis Cp, sul riciclaggio, ha espressamente ricompreso tra gli oggetti materiali del reato anche le utilità, che parrebbero quindi restare escluse dal delitto di ricettazione,(In tal senso, peraltro, la giurisprudenza di questa Corte: cfr. Cassazione penale, sezione seconda, 4 dicembre 1962, Sterlini, in Cassazione penale Mass., 1963, 518).

5) Tuttavia, pur non sussistendo il delitto di ricettazione, il fatto in questione integra - ad avviso di questo Collegio - gli estremi del reato previsto dall'articolo 12 del decreto legislativo 3 maggio 1991, numero 143, convertito in legge 197/91.
Tale norma stabilisce, infatti, che «Chiunque, alfine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire 600. 000 a lire 3.000.000».
Ebbene, non v'è dubbio alcuno che la tessera Omnitel in questione costituisca un «documento analogo alle carte di credito o di pagamento, che abilita alla prestazione dei servizi telefonici»,- mentre è altrettanto certo che l'originario truffatore e l'imputato (a titolo di concorso con il primo avendo accettato l'offerta di acquisto del servizio a metà prezzo) l'abbiano indebitamente utilizzata; tale utilizzazione, peraltro, è indebita in quanto la tessera in questione era stata fraudolentemente sottratta a chi la deteneva legittimamente (cfr. sul tema la orinai numerosa giurisprudenza sull'uso indebito della così detta Viacard sottratta al legittimo proprietario, tra cui: Cassazione penale, sezione prima, 20 novembre 1997, Fava, Rv 209579).

6) Resta, infine, da esaminare se l'attività posta in essere dal ricorrente, anche in concorso con colui il quale gli ha ceduto a metà prezzo il diritto di credito incorporato nella carta prima sottratta, integri gli estremi dei delitti di cui agli articoli 615quater (contestato), 615ter (non contestato, ma ipotizzato dallo stesso difensore del L.) e 640ter del Cp..
L'esame va iniziato dai primi due delitti, collocati entrambi tra quelli contro l'inviolabilità del domicilio perché si è ritenuto che i sistemi informatici

costituiscano «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dallo articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del Cp» (cfr.: relazione sul disegno di legge).
Ebbene, l'incriminazione dell'accesso abusivo al sistema informatico altrui (articolo 615ter Cp) è sostanzialmente finalizzato a contrastare il rilevante fenomeno degli hackers, e cioè di quei soggetti che, servendosi del proprio elaboratore, collegato con la rete telefonica, riescono a entrare in comunicazione con i diversi sistemi informatici che a quella stessa rete sono collegati, aggirando le misure di protezione predisposte dal titolare del sistema.
Mentre con l'articolo 615quater Cp il legislatore ha inteso rafforzare la tutela e la segretezza dei dati e dei programmi contenuti in un elaboratore, già assicurata dall'incriminazione dell'accesso e della permanenza in un sistema ~~informatico o telematico prevista dall'articolo 615ter prima citato.~~
Quanto sopra premesso, si osserva che - ad avviso di questo Collegio - è corretta la decisione del Tribunale di Torino, secondo il quale nessuno di tali due reati è stato commesso dall'imputato.
Questi, infatti, non si è introdotto abusivamente nel sistema, ma si è limitato a utilizzare il numero segreto riportato nella carta Omnitel, indebitamente ottenendo (in violazione dell'articolo 12 del decreto legislativo numero 143/91, citato) la prestazione di servizi telefonici ai quali non aveva diritto.
Né la condotta di chi ha rubato una carta telefonica e la utilizza è in qualche modo assimilabile a quella degli hackers, per contrastare i quali sono state introdotte le norme in esame: nella prima ipotesi, infatti, l'agente non si introduce abusivamente in un sistema informatico, sia perché - come ha ben evidenziato il Tribunale di Torino - si ferma ai margini dello stesso, sia perché utilizza proprio quel mezzo che il gestore del sistema informatico ha previsto per il compimento di quell'operazione.
Diversa sarebbe, invece, l'ipotesi in cui un soggetto, utilizzando un elaboratore, riuscisse a entrare nella memoria di quello del gestore del servizio telefonico e a rilevare i numeri segreti in esso contenuti: in tale ipotesi vi sarebbe, infatti, la evidente violazione dell'articolo 615ter Cp.

7). Analogo discorso può essere effettuato con riferimento all'ipotesi delittuosa prevista dall'articolo 640ter Cp: tale reato presuppone, infatti, che l'agente consegua il profitto alterando il funzionamento di un sistema informatico o «intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi» in qurst'ultimo contenuti.
E tale - ad avviso di questo Collegio - non è l'ipotesi di chi utilizza una carta telefonica illecitamente sottratta al legittimo detentore, bensì quella dell'hacker, da ultimo descritta.

8). D'altro canto, tale interpretazione non lascia la fattispecie per cui è processo priva di tutela penale, dal momento che l'ipotesi di reato individuata come corretta, e cioè quella del citato articolo 12 del decreto legge numero 143/91, punisce l'agente con la reclusione da uno a cinque anni e la multa da lire 600.000 a lire 3.000.000, e cioè con una pena più severa di quella prevista dalle norme che sono state contestate al L..

9) Non si ritiene, infine, di provvedere in ordine alle spese processuali sostenute dalla parte civile nel presente grado di giudizio, atteso che la

condanna alla loro rifusione è subordinata alla pronuncia di una sentenza di accoglimento della domanda di risarcimento del danno, allo stato ancora mancante (cfr. articolo 541, comma 1, Cpp), ciò non toglie ovviamente che nell'ipotesi di futuro accoglimento di siffatta domanda, conseguente all'accertamento della responsabilità penale del L., la Corte di appello di Torino dovrà provvedere anche in ordine a tali spese, nonché in ordine a quelle sostenute dalla parte civile nel giudizio di primo grado. In tal senso del resto la giurisprudenza di questa Corte, secondo cui «poiché nel processo penale l'obbligo della rifusione delle spese giudiziali sostenute dalla parte civile è collegato alla soccombenza, la quale, nel giudizio di impugnazione deve essere valutata con riferimento al gravame, nell'ipotesi di ricorso del Pm la parte civile, pur avendo il diritto di intervenire, non può ottenere la rifusione predetta all'esito del giudizio di legittimità che si è concluso con l'annullamento con rinvio, ferma restando la possibilità di far valere le proprie ragioni nel corso ulteriore del processo. (Nella specie, su ricorso per saltum del Pm, era stata annullata con rinvio la sentenza del pretore che aveva assolto l'imputato dal reato di insolvenza fraudolenta in danno della società Autostrade spa)» (Cassazione penale, sezione seconda, 27 febbraio 1997, Pm in proc. Maiolino, Rv 207559, ma cfr. anche: Cassazione penale, sezione quarta, 15 ottobre 1999, Barbisan, Rv 216462).

10) Alla stregua delle superiori considerazioni e - considerato che i fatti puniti dalla disposizione di legge da ultimo citata sono stati materialmente contestati con i capi di imputazione all'imputato, il quale su di essi è stato messo in grado di difendersi, (come risulta dalla ricostruzione operata dallo stesso imputato e di cui tratta la sentenza del Tribunale a fol. 9) - la sentenza impugnata deve essere annullata con rinvio, previa qualificazione del fatto come violazione dell'articolo 12 decreto legge 143/91.

Gli atti - ai sensi dell'articolo 560, comma 4, Cpp - vanno trasmessi alla Corte di appello di Torino, la quale si uniformerà ai principi di diritto innanzi esposti.

PQM

Qualificata la condotta contestata all'imputato come violazione dell'articolo 12 decreto legge 143/91, annulla la sentenza impugnata e dispone trasmettersi gli atti alla Corte di appello di Torino per il giudizio.