Πάντειο Πανεπιστήμιο
Κοινωνικών και Πολιτικών Επιστημών
Τμήμα Κοινωνιολογίας
Τομέας Εγκληματολογίας

ΠΜΣ «Η ΣΥΓΧΡΟΝΗ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙ Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΗΣ»

Θέμα: Πλαστογραφία εγγράφων με τη χρήση νέων τεχνολογιών

Επιβλέπων Καθηγητής: Ιάκ. Φαρσεδάκης

Μεταπτυχιακή Φοιτήτρια: Βασιλική Θεοδ. Αθανασοπούλου

Μέλη της τριμελούς επιτροπής: Ιάκ. Φαρσεδάκης, Αντ. Μαγγανάς & Χριστ. Ζαραφωνίτου

Αθήνα, Δεκέμβριος 2007

Σελ.

Α΄ ΜΕΡΟΣ

Πλαστογραφία - Νέες Τεχνολογίες

Β΄ ΜΕΡΟΣ
Δίωξη - Νομοθεσία

Κεφάλαιο 3. Δίωξη

Κεφάλαιο 4. Νομοθεσία για το Ηλεκτρονικό Έγκλημα

Γ΄ ΜΕΡΟΣ
Προτάσεις - Μέτρα Πρόληψης

Κεφάλαιο 5.

ΕΙΣΑΓΩΓΗ

Νέες τεχνολογίες μας περιβάλλουν. Την ύπαρξή τους και την επίδρασή τους στην κοινωνική, την καθημερινή ζωή, την καταλαβαίνει όλος ο κόσμος. Όμως, όπως συνέβη και με όλες τις άλλες μεγάλες κοινωνικές ανατροπές κατά το παρελθόν, οι άνθρωποι βιώνουν τη διαρκούσα διαδικασία παραγωγής νέων τεχνολογιών, με διαφορετικούς τρόπους.

Σε μια προσπάθεια ευρύτερης αποσαφήνισης της έννοιας 'τεχνολογία', που ενυπάρχει με τη μορφή 'νέες τεχνολογίες' στον τίτλο της παρούσας μελέτης, επιλέξαμε μέσα από ένα πλήθος ορισμών, ως τον πλέον εύληπτο αυτόν που την ορίζει ως **την τρέχουσα κατάσταση της γνώσης μας για το πώς συνδυάζουμε πόρους ώστε να παράγουμε επιθυμητά προϊόντα, να λύσουμε προβλήματα, να εκπληρώσουμε τις ανάγκες μας, ή να ικανοποιήσουμε τη θέλησή μας**. Από την οπτική αυτή η τεχνολογία φαίνεται να περιλαμβάνει μεθόδους, δεξιότητες, διαδικασίες, τεχνικές, εργαλεία και πρώτες ύλες (και χρήσεις όπως την τεχνολογία υπολογιστών, την τεχνολογία κατασκευών, ή την ιατρική τεχνολογία).

Σύμφωνα με μια άλλη προσέγγιση θα λέγαμε ότι τεχνολογία ορίζεται [1]**η ικανότητα δραστικής επέμβασης του ανθρώπου με καταβολή διανοητικής και φυσικής προσπάθειας προκειμένου να δημιουργηθεί οποιαδήποτε υλική οντότητα**.

Δεν θα επιχειρήσουμε την παράθεση του συνόλου των ορισμών που έχουν κατά καιρούς διατυπωθεί σχετικά με την έννοια της τεχνολογίας και η αιτιολογική βάση είναι μάλλον απλή. Όπως συμβαίνει για τις περισσότερες έννοιες έτσι και για την έννοια της τεχνολογίας έχουν δοθεί πολλές και συχνά επαναλαμβανόμενες - αναμασημένες ερμηνείες. Οι ερμηνείες αυτές πέραν μιας πρώτης εννοιολογικής επαφής με τον κατά περίπτωση εξεταζόμενο όρο δεν φαίνεται να εκφράζουν και να γίνονται τελικά καθολικά αποδεκτές, αφού ο καθένας από εμάς συμβαίνει να αντιλαμβάνεται διαφορετικά, σύμφωνα με κριτήρια και βιώματα εντελώς υποκειμενικά, το τι τελικά σημαίνει η κάθε έννοια.

[1] http://el.wikipedia.org

Λαμβάνοντας υπόψη τα παραπάνω, κρίθηκε σκόπιμο να απεγκλωβίσουμε τον αναγνώστη από το χάος που δημιουργούν οι δοθέντες ορισμοί για την ‘τεχνολογία’ ων ουκ έστιν αριθμός, αλλά αφού δώσαμε -εισαγωγικά- μια αίσθηση, να παραμείνουμε πιστοί στη θεματική ενότητα της παρούσας μελέτης. Να προσεγγίσουμε δηλαδή την έννοια της τεχνολογία εστιάζοντας αποκλειστικά, αλλά όχι πάντα περιοριστικά στη σχέση της με το έγκλημα της πλαστογραφίας.

Πολύ γενικά λοιπόν θα λέγαμε, ότι όσο και αν σήμερα θεωρούμε δεδομένη αυτή την ικανότητα δραστικής επέμβασης στον κοινωνικό περίγυρο και στο φυσικό περιβάλλον (τεχνολογία), εντούτοις δεν ήταν πάντα αυτονόητη και χρειάστηκε μια μακρά πορεία πολλών δεκάδων χιλιάδων ή και εκατοντάδων χιλιάδων ετών ώστε να εξελιχθεί το ανθρώπινο ον, από ‘κατασκευαστή εργαλείων’ σε αποκωδικοποιητή των μυστικών της φύσης και σε διαμορφωτή του οικοσυστήματος. Η μελέτη της ιστορία της τεχνολογίας συμβάλλει στην απομυθοποίησή της, τη φέρνει στα ανθρώπινα μέτρα.

Κατά πόσο λοιπόν η τεχνολογία απομυθοποιημένη προκαλεί αποτελέσματα, τα οποία μεταξύ άλλων (λ.χ. οικονομικής, ενεργειακής άποψης), είναι χρήσιμα ή όχι και από κοινωνικής σκοπιάς, καλούμαστε -με τους περιορισμούς και τις προδιαγραφές που απαιτεί η διενεργούμενη μελέτη- να το διαπιστώσουμε μέσα από την αντιπαράθεση των δυνατοτήτων που παρέχει, αλλά αντίστοιχα και των προβλημάτων που γεννά η τεχνολογία αναφορικά με το έγκλημα της πλαστογραφίας. Είναι άλλωστε ανεδαφικό να νομίζει κανείς ότι μπορεί να δρέψει μόνο του ‘καλούς’ καρπούς της τεχνολογίας.

Προκειμένου να συμπεριλάβουμε όσα ακροθιγώς θίξαμε παραπάνω, διήλθαμε μέσα από την ακόλουθη ‘διαδρομή’ που ελπίζουμε τελικά να αποδειχθεί λειτουργική σαν σχήμα. Ειδικότερα:

Στο Κεφάλαιο Α΄ περιγράφεται από ποινική κυρίως άποψη το έγκλημα της πλαστογραφίας, στην παραδοσιακή του μορφή. Η εν λόγω ανάλυση βασίζεται στο σχετικό άρθρο 216 του Ποινικού Κώδικα. Στην αμέσως επόμενη ενότητα, αναπτύσσεται η έννοια του εγγράφου, με

ιδιαίτερη έμφαση στην ‘πρόσφατη’ διεύρυνσή της, αλλά αναφερόμαστε εξίσου και στις εξελίξεις που συντελέστηκαν στα συστατικά στοιχεία του ‘εγγράφου’. Επισημαίνεται ότι η περιορισμένη έκταση μιας διπλωματικής εργασίας είναι εκ των προτέρων αποτρεπτική στο να εξετάσει κανείς όλο το εύρος των διαγραφόμενων εξελίξεων.

Στο Κεφάλαιο Β΄ αναγνωρίζεται η ποσοτική και ποιοτική μετεξέλιξη της εγκληματικότητας και πιο συγκεκριμένα των νέων μορφών που έχει προσλάβει το έγκλημα της πλαστογραφίας με τη χρήση τεχνολογιών.

Διευκρινίζεται ότι όσον αφορά στα θέματα: ηλεκτρονικό έγκλημα, Διαδίκτυο κ.λ.π. που αναπτύσσονται στο παρόν Κεφάλαιο, η προσέγγιση που πραγματοποιήθηκε ενείχε την εξής δυσκολία. Η ανάλυση των εννοιών αυτών προτιμήθηκε να γίνει κατά πλάτος και όχι σε βάθος, καθώς είναι αρκετά δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του εγκλήματος στον κυβερνοχώρο (cyber crime), όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes), χωρίς την κατοχή όχι μόνο θεωρητικών αλλά και τεχνικών γνώσεων. Η επιλογή αυτή έγινε λαμβάνοντας ως δεδομένο ότι ο αναγνώστης της παρούσας μελέτης διαθέτει τις βασικές γνώσεις τόσο για τους ηλεκτρονικούς υπολογιστές όσο και για το Διαδίκτυο, καθώς και για τις υπηρεσίες που παρέχονται με αυτά.

Στο Β΄ Μέρος της εν λόγω μελέτης και συγκεκριμένα στο Κεφάλαιο Γ΄ γίνεται λόγος για τους εγχώριους μηχανισμούς δίωξης των παραδοσιακών και νέων μορφών πλαστογραφίας. Το κέντρο βάρους επικεντρώνεται στις αστυνομικές Υπηρεσίες: το Εργαστήριο Δικαστικής Γραφολογίας (Τομέας εξέτασης εγγράφων και γραφής - Τομέας εξέτασης ψηφιακών πειστηρίων) της Διεύθυνσης Εγκληματολογικών Ερευνών και το Τμήμα Δίωξης Ηλεκτρονικού εγκλήματος, αλλά και στη σχετικά νέα Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness & Response to Threats) του Υπουργείου Οικονομίας & Οικονομικών.

Το Κεφάλαιο Δ΄ είναι αφιερωμένο στη νομοθετική αντίδραση αναφορικά με το ψηφιακό έγκλημα. Παρά τις επισταμένες προσπάθειες συλλογής σχετικού βιβλιογραφικού υλικού, δια-

πιστώθηκε σαφής έλλειψη, η οποία είναι ευνόητο ότι οφείλεται στο γεγονός πως το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος.

Τέλος στο Κεφάλαιο Ε΄ της παρούσας μελέτης προτείνονται ορισμένα μέτρα πρόληψης και καταστολής, που αν και είναι επιλεγμένα ειδικά για την αντιμετώπιση των νέων μορφών πλαστογραφίας, εντούτοις θεωρούμε ότι βρίσκουν εφαρμογή γενικότερα στην αντιμετώπιση του ψηφιακού εγκλήματος.

Στόχος και επιθυμία μας είναι κατά τη διαπραγμάτευση της θεματικής ενότητας «Πλαστογραφία - Νέες Τεχνολογίες» να μείνουμε μακριά από ακραίες ‘τεχνο-φοβικές’ ή ‘τεχνο-φιλικές’ απολυτότητες. Να σταθούμε μπροστά στη γνώση και τη σωρευμένη πληροφορία που την περιβάλλει, με τρόπο που δεν είναι εκστατικός και αποτρεπτικός, αλλά με τρόπο που είναι κριτικός και δημιουργικός.

..//..

Α΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 1. ΠΛΑΣΤΟΓΡΑΦΙΑ (ΠΑΡΑΔΟΣΙΑΚΗ ΜΟΡΦΗ) & ΕΓΓΡΑΦΟ

Ας ξεκινήσουμε την ανάλυσή μας με τις απαραίτητες συστάσεις που απαιτεί κάθε καινούργια συνάντηση γνώσης. Απ' τη μια λοιπόν ο αναγνώστης απ' την άλλη το έγκλημα της πλαστογραφίας (στην παραδοσιακή του μορφή). Κι αν κάποιος θέλει να μάθει περισσότερα γι αυτή τη νέα γνωριμία, φυσικά και θα ανατρέξει στη σχετική διατύπωση του άρθρου 216 του Ποινικού Κώδικα (Π.Κ).

1.1 Το έγκλημα της πλαστογραφίας στον Ποινικό Κώδικα

Το δέκατο κεφάλαιο του Ειδικού Μέρους του Ποινικού Κώδικα αναφέρεται στα "Εγκλήματα σχετικά με τα Υπομνήματα". Ο τίτλος του κάθε κεφαλαίου, συνήθως, ενσωματώνει και συνάμα φανερώνει στον αναγνώστη το [2]έννομο αγαθό που προστατεύουν οι διατάξεις του νόμου, οι οποίες ακολουθούν.

[3]Σύμφωνα με τη γαλλική θεωρία το έννομο αγαθό που προσβάλλεται τόσο με τα εγκλήματα περί το νόμισμα όσο και με τα εγκλήματα περί τα υπομνήματα είναι η δημόσια πίστη, ενώ σύμφωνα με τη γερμανική θεωρία η οποία και έχει επικρατήσει στην Ελλάδα προστατευόμενο έννομο αγαθό είναι η ασφάλεια και εμπιστοσύνη των έγγραφων συναλλαγών.

Παρά τις όποιες θεωρίες, οι οποίες δεν χρήζουν περαιτέρω ανάλυσης, τουλάχιστον στο πλαίσιο της παρούσης μελέτης, βασικό έγκλημα του δέκατου κεφαλαίου είναι η πλαστογραφία, η οποία και αποτελεί τον πυρήνα των τριών πρώτων άρθρων. Ακολουθεί η υφαρπαγή ψευδούς βεβαίωσης (άρθρο 220β), οι ψευδείς ιατρικές πιστοποιήσεις (άρθρο 221γ), η υπεξαγωγή εγγράφων (άρθρο 222δ) και τέλος η μετακίνηση ορόσημων (άρθρο 223ε).

---

[2] Η πρόσληψη της εννοίας του εννόμου αγαθού ως αντικειμένου προστασίας του ποινικού δικαίου, συνδέεται όπως είναι γνωστό με τη γερμανική παράδοση και συνιστά μία από τις πιο σημαντικές παρακαταθήκες της γερμανικής ποινικής επιστήμης στον ευρωπαϊκό τουλάχιστον νομικό πολιτισμό. [Καιάφα-Γκμπάντι Μ. (2000) «*Το ποινικό δίκαιο στην καμπή του 2000: Με το βλέμμα προς το μέλλον χωρίς αποτίμηση του παρελθόντος;*», Υπεράσπιση, σελ. 49-50].

[3] Κωνσταντινίδης Α. (2000) «*Η έννοια και λειτουργία του εγγράφου στο Ουσιαστικό & Δικονομικό Ποινικό Δίκαιο*», Εκδόσεις Δίκαιο & Οικονομία Π.Ν. Σάκκουλας, σελ. 87, 91.

Παρατηρούμε ότι η πλαστογραφία στα άρθρα 216, 217 και 218 Π.Κ οριοθετεί τις πράξεις εκείνες οι οποίες έγκεινται στην πλαστότητα ή νόθευση των εγγράφων, το άρθρο 220β επισημαίνει την επίτευξη ψευδούς περιεχομένου σε γνήσιο έγγραφο, το άρθρο 221γ συγκεκριμενοποιεί το ψευδές περιεχόμενο στα ιατρικά πιστοποιητικά, το άρθρο 222δ καλύπτει την παράνομη καταστροφή διαφόρων εγγράφων και τέλος το άρθρο 223ε αναφέρεται στην αφαίρεση, επέμβαση, μετατόπιση ή και ψευδή τοποθέτηση σημείων που καθορίζουν κάποια όρια. Κοινό στοιχείο που μπορεί να εντοπίσει κανείς στις ανωτέρω διατάξεις είναι η προστασία εγγράφων ή σημείων, τα οποία μπορούν να επιφέρουν σημαντικές συνέπειες.

Άρθρο 216 (Πλαστογραφία)

«1. Όποιος καταρτίζει πλαστό ή νοθεύει έγγραφο με σκοπό να παραπλανήσει με τη χρήση του άλλον σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Η χρήση του εγγράφου από αυτόν θεωρείται επιβαρυντική περίπτωση.

2. Με την ίδια ποινή τιμωρείται όποιος για τον παραπάνω σκοπό εν γνώσει χρησιμοποιεί πλαστό ή νοθευμένο έγγραφο.

3. Αν ο υπαίτιος αυτών των πράξεων (παράγραφοι 1-2) σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον τιμωρείται με κάθειρξη μέχρι δέκα ετών, εάν το όφελος ή η βλάβη υπερβαίνουν το ποσόν των είκοσι πέντε εκατομμυρίων (25.000.000) δραχμών».

[4]Δράστης του εγκλήματος της παραγράφου 1 μπορεί να είναι οποιοσδήποτε. Αντικείμενο του εγκλήματος είναι το έγγραφο που πρέπει να φέρει για τη νόμιμη υπόστασή του τους απαιτούμενους εξωτερικούς τύπους. Ο δράστης πρέπει να καταρτίσει από την αρχή πλαστό ή να νοθεύσει έγγραφο ή σημείο.

Το έγγραφο μπορεί να είναι δημόσιο ή ιδιωτικό ή αλλοδαπό. Το έγγραφο αποτελεί δήλωση της βούλησης (θέλησης) του ανθρώπου. Η δήλωση βούλησης που περιέχεται στο έγγραφο πρέπει να είναι νοητή και να προκύπτει απ' αυτή το πρόσωπο που τη δηλώνει. Επομένως, έγγραφο χωρίς υπογραφή δεν είναι κατά την έννοια του νόμου έγγραφο, εκτός αν από το περιεχόμενό του είναι εμφανής ο εκδότης. Η δήλωση βούλησης πρέπει να συνδέεται στερεά προς ένα αντικείμενο που μπορεί να υπάρχει για ένα ορισμένο χρονικό διάστημα, όπως είναι π.χ. ο

[4] Ραφτόπουλος Π. (1996) «*Ποινικό Δίκαιο*», (χεο), Αθήνα, σελ. 445επ.

χάρτης, το ξύλο, ο λίθος, κλπ. Το έγγραφο πρέπει να προορίζεται ή να είναι πρόσφορο, κατάλληλο, να αποδείξει γεγονός που έχει έννομη συνέπεια.

Ως τέτοιο πρέπει να θεωρηθεί εκείνο που είναι σημαντικό για την παραγωγή, τη διατήρηση, τη μεταβολή ή την απόσβεση ενός δικαιώματος ή μιας έννομης σχέσης, δημόσιας ή ιδιωτικής φύσης. Επομένως, έγγραφα που αποδεικνύουν νομικώς αδιάφορα γεγονότα είναι και αδιάφορα για το δίκαιο.

1.1.1 Αντικειμενική υπόσταση - μορφολογικά στοιχεία - χρήση πλαστού εγγράφου

Η πλαστογραφία, στη βασική της μορφή, αποτυπώνεται στη διάταξη του άρθρου 216α παρ.1 Π.Κ. Ως έγκλημα χαρακτηρίζεται τυπικό[5], με βάση το αποτέλεσμα, αφού είναι αναπόσπαστα δεμένη η μεταβολή που επιφέρει στον εξωτερικό κόσμο με την ανθρώπινη ενέργεια. Βλάβης, επιφέροντας αποτέλεσμα ως μεταβολή στον εξωτερικό, υλικό κόσμο που έγκειται στη βλάβη ενός εννόμου αγαθού. Κίνησης, σχετικά με τον τρόπο τέλεσης, επειδή απαιτείται αυτοκυβερνούμενη μυϊκή κίνηση, που προκαλεί το αποτέλεσμα με πραγμάτωση της αντικειμενικής υπόστασης. Στιγμιαίο, ως προς το χρόνο τέλεσης, αφού η χρονική στιγμή της τυπικής περάτωσης είναι μοναδική και δε μπορεί να παραταθεί κατά τη βούληση του δράστη. Γνήσιο, προσβάλλοντας υπάρχον έννομο αγαθό και αποτελώντας έτσι τυποποίηση του ποινικού φαινομένου.

Τέλος, με βάση τον τρόπο τέλεσης η πλαστογραφία χαρακτηρίζεται ως έγκλημα πολύτροπο, δηλαδή στην αντικειμενική της υπόσταση προβλέπονται περισσότεροι από ένας γενικοί τρόποι τέλεσης, και συγκεκριμένα μη γνήσιο πολύτροπο ή [6]σωρευτικά μικτό, αφού οι διάφοροι αυτοί τρόποι δε μπορούν να εναλλαχθούν ή να σωρρευθούν πάνω στο ίδιο υλικό αντικείμενο, επειδή με τη μία προσβολή εξαντλείται η μία μονάδα του εννόμου αγαθού. Αν πραγματωθούν σωρευτικά, πρόκειται για συρροή εγκλημάτων.

---

[5] Θεοδωράκης Γ. (1990) «*Ποινικό δίκαιο: ειδικό μέρος: η πλαστογραφία (άρθρο 216 ΠΚ)*», Εκδόσεις Α. Σάκκουλας, Αθήνα - Κομοτηνή, σελ. 20.

[6] Μαγκάκης Γ. (1984) «*Ποινικό Δίκαιο Διάγραμμα γενικού μέρους*», Έκδοση Γ΄, Εκδόσεις Παπαζήση, Αθήνα, σελ. 141

Αντικειμενική υπόσταση - μορφολογικά στοιχεία

Αυτός ο τελευταίος χαρακτηρισμός της πλαστογραφίας, ως μη γνήσιο πολύτροπο ή σωρευτικά μικτό, επιβεβαιώνεται πλήρως με την αναζήτηση των στοιχείων της αντικειμενικής υπόστασης του εγκλήματος. Η πλαστογραφία τελείται με δύο διαφορετικούς τρόπους:

α) την κατάρτιση, δηλ. τη δημιουργία από την αρχή, πλαστού εγγράφου ή

β) τη νόθευση γνησίου που έγκειται στη αλλοίωση της έννοιας αυτού με μεταβολή του περιεχομένου του που επιτυγχάνεται με προσθήκη ή εξάλειψη λέξεων, αριθμών ή σημείων.

Οι δύο αυτοί τρόποι τέλεσης τυγχάνουν και ξεχωριστής αναλύσεως, λόγω της διαφορετικότητας των στοιχείων που τους συνθέτουν.

Ο πρώτος τρόπος τέλεσης της πλαστογραφίας (κατάρτιση) απασχόλησε και συνεχίζει να απασχολεί νομολογία και θεωρία. Η απόφαση του ακυρωτικού ΑΠ 1108/1986 επισήμανε ότι κατάρτιση πλαστού εγγράφου υπάρχει όταν το έγγραφο καταρτίστηκε από το δράστη επ' ονόματι άλλου σαν να εκδόθηκε από αυτόν, όχι όμως και όταν στο έγγραφο που υπογράφεται από τον εκδότη του και με το όνομά του βεβαιώνονται αναληθή πράγματα.

Τίθεται έτσι το ερώτημα αν μπορεί να χαρακτηριστεί κατάρτιση η περίπτωση όπου εκδότης και διανοητικό περιεχόμενο φαίνεται να συμπίπτουν, στο έγγραφο όμως εμπεριέχονται ψευδή περιστατικά. Η ανωτέρω απόφαση του Αρείου Πάγου, ξεκάθαρα, αποκλείει την περίπτωση αυτή. Στη θεωρία όμως, υποστηρίζεται και ιδιαίτερα από τον Ανδρούλακη η δυνατότητα ύπαρξης πλαστογραφίας, όταν κάποιος υπογράφει με το όνομά του. Τίθεται απλώς η προϋπόθεση στη συγκεκριμένη περίπτωση εκδότης του εγγράφου να μην είναι κατ' ουσίαν ο υπογράφων αλλά μία Αρχή, Υπηρεσία ή ένα νομικό πρόσωπο και ο υπογράφων να μην έχει το δικαίωμα να υπογράψει για λογαριασμό τους.

Για να θεωρηθεί τώρα ότι εκδότης είναι πράγματι το νομικό πρόσωπο λαμβάνεται υπόψη το περιεχόμενο του εγγράφου και συγκεκριμένα διάφορες εκφράσεις όπως: η Υπηρεσία μας, η εταιρία μας και γενικότερα ο απρόσωπος υπηρεσιακός πληθυντικός. Σημαντικό ρόλο παίζει το χαρτί στο οποίο αποτυπώνεται το διανοητικό περιεχόμενο του εγγράφου, αν είναι το επίσημο

της Υπηρεσίας, η σφραγίδα, ο αριθμός πρωτοκόλλου κά. Σε περίπτωση τώρα που ο υπογράφων εκπροσωπεί αυτή την Αρχή, Υπηρεσία ή νομικό πρόσωπο καθ' οιονδήποτε τρόπο τότε υπάρχει έγγραφο αναληθές κατά το περιεχόμενό του, όχι όμως κατάρτιση πλαστού.

Η κατάρτιση πλαστού εγγράφου, η εμφάνιση δηλαδή ότι εκδόθηκε από πρόσωπο άλλο από αυτό που πραγματικά το εξέδωσε, υπάρχει και στην περίπτωση που αποσπάται η υπογραφή κάποιου με εξαπάτηση. Η κατάρτιση πλαστού εγγράφου δεν περιορίζεται στην υπογραφή με ξένο όνομα, αλλά σε κάθε περίπτωση εξαπάτησης ως προς το πρόσωπο του αληθινού εκδότη. Έτσι, όταν αποσπάται παρά τη θέλησή του και εν αγνοία του η υπογραφή κάποιου και έπειτα προστίθεται σε άλλο έγγραφο, υπάρχει κατάρτιση. Ομοίως, **όταν 'επικολλάται' μία υπογραφή σε ένα έγγραφο (βλ. πιο αναλυτικά Κεφάλαιο 2.2.2 της παρούσης)**.

Ο Τσεβάς επισημαίνει ότι κατάρτιση πλαστού εγγράφου υπάρχει και όταν ο υπογράφων με το όνομά του οδηγείται στην υπογραφή υπό την επιρροή παραπλανήσεως. Και αυτό, γιατί στην περίπτωση αυτή δεν μπορεί να υποστηριχθεί ότι το περιεχόμενο του εγγράφου προέρχεται πνευματικά από τον εκδότη του. Επομένως, αυτό που πρέπει να διερευνηθεί είναι η διάσταση που υφίσταται ανάμεσα στην πατρότητα του διανοήματος του εγγράφου και σε εκείνη της υπογραφής, ιδίως στην περίπτωση που λαμβάνεται υπογραφή του εκδότη με εξαπάτηση και στην κατάχρηση της εν λευκώ υπογραφής.

Πρέπει βέβαια να διευκρινιστεί ότι στην περίπτωση που υπαγορεύεται κείμενο σε τρίτον με εξουσιοδότηση να υπογράψει αυτός για λογαριασμό του εκδότη, καθώς και στην περίπτωση εντολής σε τρίτον για διαμόρφωση κατά τη δική του σκέψη του περιεχομένου του εγγράφου και θέση της υπογραφής του εντολέα, με πιστή όμως απόδοση της θέλησης του εντολέα, δεν τίθεται θέμα κατάρτισης πλαστού εγγράφου.

Ο δεύτερος τρόπος τέλεσης της πλαστογραφίας έγκειται στη νόθευση γνησίου εγγράφου αλλοιώνοντας την έννοιά του με μεταβολή του περιεχομένου του. Η μεταβολή αυτή επιτυγχάνεται με **προσθήκη ή εξάλειψη λέξεων, αριθμών ή σημείων (βλ. πιο αναλυτικά Κεφάλαιο 2.2.2 της παρούσης)**.

Συζήτηση δημιούργησε το αν η δυνατότητα παραγωγής εννόμων συνεπειών είναι στοιχείο της αντικειμενικής υπόστασης του άρθρου 216 Π.Κ και ιδιαίτερα της νόθευσης γνησίου εγγράφου. Σε αυτό συνετέλεσε και η ΑΠ 1072/1988, η οποία ριζοσπαστικά υποστήριξε ότι, για να είναι πλήρης αιτιολογικά μια καταδικαστική απόφαση για νόθευση εγγράφου, πρέπει η αλλοίωση του περιεχομένου του εγγράφου να μπορούσε αντικειμενικά να έχει έννομες συνέπειες. Ερωτάται επομένως αν απαιτείται η νόθευση να μπορεί να προκαλέσει έννομες συνέπειες. Ο Μυλωνόπουλος διευκρινίζει ότι η νόθευση απαιτείται να αλλοιώνει το περιεχόμενο του εγγράφου και να το καθιστά πρόσφορο και δυνατό να παραπλανήσει κάποιον.

Η στοιχειοθέτηση της νόθευσης απαιτεί επομένως ικανότητα αυτής να προκαλεί παραπλάνηση τόσο για τη γνησιότητα του εγγράφου, αλλά και για ορισμένο γεγονός. Το γεγονός αυτό, που προκύπτει από τη νόθευση, πρέπει να μπορεί να προκαλέσει έννομες συνέπειες. Έτσι, η νόθευση μόνο έμμεσα δια του γεγονότος αυτού μπορεί να συνδεθεί με τις έννομες συνέπειες. Επομένως, δεν μπορούμε να δεχθούμε ότι η δυνατότητα παραγωγής εννόμων συνεπειών είναι στοιχείο της αντικειμενικής υπόστασης της νόθευσης εγγράφου. Το γεγονός όμως που αναφέραμε αποτελεί άγραφο στοιχείο της νόθευσης και για να προκαλεί έννομες συνέπειες πρέπει να είναι σημαντικό για την παραγωγή, διατήρηση, μεταβολή ή απόσβεση δικαιώματος ή έννομης σχέσης ιδιωτικής ή δημόσιας φύσης. Έννομες συνέπειες της νόθευσης είναι η απειλή ποινής. Το γεγονός, ως προς το οποίο σκοπείται η παραπλάνηση, είναι που θα πρέπει να προκαλεί έννομες συνέπειες.

Χρήση πλαστού εγγράφου

Το τελευταίο εδάφιο της παρ.1 του άρθρου 216 αναφέρεται στη χρήση του καταρτισθέντος ή νοθευθέντος εγγράφου από τον ίδιο τον πλαστογράφο, ανάγοντας την πράξη αυτή σε ιδιαίτερα επιβαρυντική περίπτωση. Από την άλλη, η παρ.2 του ίδιου άρθρου ποινικοποιεί με την απειλή της ίδιας ποινής τη χρήση του εγγράφου αυτού από κάποιον άλλον. Η συμπεριφορά αυτή βέβαια, τόσο της παρ.1 όσο και της παρ.2, πρέπει να συνοδεύεται από την απαιτούμενη υποκειμενική υπόσταση, που αναλύεται παρακάτω. Έτσι, στο τελευταίο εδάφιο της παρ.1, η

χρήση απαιτεί να προηγείται μια κατάρτιση ή νόθευση από τον ίδιο τον δράστη και αποτελεί απλώς επιβαρυντική περίπτωση, ενώ στην παρ.2 έχουμε ένα ξεχωριστό έγκλημα ο δράστης του οποίου χρησιμοποιεί συνειδητά πλαστό ή νοθευμένο έγγραφο, που κατάρτισε ή νόθευσε κάποιος άλλος.

Πρόβλημα δημιουργείται με τη διατύπωση αυτή του νόμου στην περίπτωση που ο πλαστογράφος χρησιμοποιήσει το έγγραφο μετά την παραγραφή της πράξης του. Η ΟλομΑΠ 414/57 υποστήριξε ότι, εάν η χρήση του πλαστού από τον πλαστογράφο γίνει πριν από την παραγραφή της πλαστογραφίας, αποτελεί ύστερη συντιμωρητή πράξη που απορροφάται στην προηγούμενή της πλαστογραφία και συμπαραγράφεται με εκείνη. Αν η χρήση γίνεται μετά την παραγραφή της πλαστογραφίας, τότε αποτελεί αυτοτελές έγκλημα και εμπίπτει στην παρ2. Η παραπάνω απόφαση αφήνει βέβαια ένα λογικό κενό αφού, εάν η χρήση γίνει λ.χ. μία μέρα πριν την παραγραφή της πλαστογραφίας, παραγράφεται και η χρήση πλαστού, αν και δεν αποτελεί αυτοτελές έγκλημα, μία μέρα μετά την τέλεσή της. Η ΑΠ 824/79 διευκρίνισε πως η παραπάνω άποψη πρέπει να εγκαταλειφθεί, αφού η διάκριση ανάμεσα στη χρήση πριν και μετά την παραγραφή δεν προκύπτει από το γράμμα του νόμου. Η ίδια απόφαση υποστήριξε ότι στο άρθρο 216 Π.Κ τυποποιούνται δύο αυτοτελή εγκλήματα, η κατάρτιση-νόθευση εγγράφου και η χρήση αυτού.

Όταν αυτά τελούνται από το ίδιο πρόσωπο, το δεύτερο χάνει την αυτοτέλεια του και γίνεται επιβαρυντική περίπτωση της πλαστογραφίας, εφόσον αυτή μπορεί να τιμωρηθεί. Εάν έχει όμως παραγραφεί, η χρήση του εγγράφου, οποτεδήποτε και αν έγινε, είτε πριν είτε μετά την παραγραφή της πλαστογραφίας, τιμωρείται ως ξεχωριστό έγκλημα κατά το άρθρο 216 παρ.2 και έχει αυτοτελή χρόνο παραγραφής από τη στιγμή της τέλεσής του. Ακολούθησε η ΑΠ 1130/91 που κατά πλειοψηφία επανατοποθετήθηκε σύμφωνα με την παλαιότερη εκ των προαναφερθέντων θέσεων της νομολογίας.

Ανακεφαλαιώνοντας θα λέγαμε ότι η κάθε περίπτωση πρέπει να κρίνεται από το δικαστήριο in concreto, έχοντας πάντα υπόψη ότι η παραγραφή ενός εγκλήματος έχει ως γενεσι-

ουργούς λόγους την εξασθένιση των αποδείξεων, αλλά και την αποδυνάμωση της ποινής ενόψει των σκοπών που έχει να επιτελέσει.

1.1.2 Υποκειμενική υπόσταση - Καταλογισμός

Η πλαστογραφία είναι πλημμέλημα. Περίπτωση πλαστογραφίας από αμέλεια στον Ποινικό Κώδικα δεν υπάρχει τυποποιημένη. Σύμφωνα με το άρθρο 26 παρ.1 Π.Κ, η υπαιτιότητα που απαιτείται για τον αρχικό καταλογισμό του δράστη είναι **δόλος**. Ο βαθμός του δόλου όμως που ζητούμε περιορίζεται στον άμεσο δόλο α΄ βαθμού. Έτσι απαιτείται γνώση και θέληση των περιστατικών της πλαστογραφίας, κάτι που γίνεται αντιληπτό με τη χρησιμοποίηση της λέξης «με σκοπό». Για το έγκλημα της παρ.2 όμως, χρήση του πλαστού από άλλον, αρκεί και άμεσος δόλος β΄ βαθμού (εν γνώσει).

Η πλαστογραφία ανήκει στα εγκλήματα υπερχειλούς υπόστασης. Επομένως, η υποκειμενική της υπόσταση δεν καλύπτει απλώς αλλά υπερκαλύπτει την αντικειμενική. Ο σκοπός να παραπλανήσει με τη χρήση του εγγράφου άλλον είναι μέρος της υποκειμενικής υπόστασης της πλαστογραφίας. Το έγκλημα ολοκληρώνεται τυπικά με την πραγμάτωση της αντικειμενικής υπόστασης, δηλαδή την κατάρτιση ή νόθευση εγγράφου. Αν ο δράστης επιτύχει την παραπλάνηση άλλου, τότε έχουμε ουσιαστική αποπεράτωση του εγκλήματος, δηλαδή εξισορρόπηση των δύο υποστάσεων. Έτσι, για την υποκειμενική υπόσταση της πλαστογραφίας καταλήγουμε ότι απαιτείται άμεσος δόλος α΄ βαθμού και σκοπός για παραπλάνηση άλλου με τη χρήση του εγγράφου, χωρίς απαραίτητα η παραπλάνηση να επέλθει (αρκεί δηλ να υπάρχει απλώς τέτοιος σκοπός).

Το στοιχείο αυτό, ο σκοπός δηλ για παραπλάνηση, παίζει τον πιο σημαντικό ρόλο για τον αρχικό καταλογισμό της πράξης σε κάποιον, που τελεί τα στοιχεία της αντικειμενικής υπόστασης της πλαστογραφίας. Έτσι, αν κανείς καταρτίζει ένα πλαστό έγγραφο ή νοθεύει τέτοιο, χωρίς να έχει σκοπό να παραπλανήσει κάποιον αλλά π.χ προκειμένου να επιδείξει ότι έχει τις δυνατότητες να το κάνει, τότε ελλείψει κάλυψης της αντικειμενικής υπόστασης από απαραίτητο

στοιχείο της υποκειμενικής, όπως είναι ο σκοπός για παραπλάνηση στο 216 Π.Κ, η αρχικά και τελικά άδικη αυτή πράξη δεν καταλογίζεται στο ‘δράστη’.

1.1.3 Απόπειρα - Συρροή - Συμμετοχή

Απόπειρα

Η πλαστογραφία, όπως είδαμε, θεωρείται έγκλημα τυπικό. Η ΑΠ 580/1979 διευκρίνισε ότι η δυνατότητα για παραπλάνηση περί γεγονότος δυναμένου να έχει έννομες συνέπειες είναι απαραίτητο στοιχείο της αντικειμενικής υπόστασης. Αυτό σημαίνει ότι για τη στοιχειοθέτηση του εγκλήματος δεν αρκεί η αλλοίωση του εγγράφου, αλλά πρέπει αυτό να διατηρεί τις ιδιότητες του εγγράφου κατά το άρθρο 13γ Π.Κ.

Η αποδεικτική προσφορότητα απαιτείται να συντρέχει τόσο πριν όσο και μετά την τέλεση της πράξης. Έτσι, η προσφορότητα παραπλάνησης ενός πλαστού εγγράφου ανάγεται σε άγραφο συστατικό της αντικειμενικής υπόστασης του άρθρου 216 Π.Κ.

Αυτό όμως σημαίνει ότι, αν το νοθευμένο έγγραφο είναι αδύνατον να παραπλανήσει άλλον για γεγονός που έχει έννομες συνέπειες, δεν υπάρχει τετελεσμένη πράξη. Υπάρχει όμως απόπειρα, αφού η νόθευση του εγγράφου συνιστά αρχή εκτέλεσης και το μόνο στοιχείο που απολείπεται είναι η προσφορότητα της νόθευσης για παραπλάνηση. Ο βαθμός υλοποίησης της αντικειμενικής υπόστασης αποτελεί, στα τυπικά εγκλήματα, αποφασιστικό κριτήριο για την αντιδιαστολή μεταξύ απόπειρας και τετελεσμένου εγκλήματος.

Η απροσφορότητα παραπλανήσεως στο άρθρο 216 Π.Κ ακρωτηριάζει την αντικειμενική υπόσταση. Έτσι, δεν υπάρχει τετελεσμένο έγκλημα, παραμένει όμως στο επίπεδο της πρόσφορης απόπειρας, αφού υλοποιείται μέρος της αντικειμενικής υπόστασης. Εξάλλου, για την ολοκλήρωση της πλαστογραφίας δεν απαιτείται περιουσιακή ζημία, με αποτέλεσμα να στενεύουν τα όρια της απόπειρας.

Συρροή

Η πλαστογραφία συρρέει συχνά με τα άρθρα 220 & 258γ Π.Κ, 100 παρ.1ι του Τελωνειακού Κώδικα, ενώ ιδιαίτερο ενδιαφέρον παρουσιάζει η συρροή της με το έγκλημα της απάτης 386 Π.Κ (σχετική αναφορά ακολουθεί στο Κεφάλαιο 2.2 της παρούσης). Ειδικότερα:

i) Μεταξύ της βασικής (πλημμελληματικής) πλαστογραφίας (άρθρο 216 παρ.1 εδαφ.α΄ Π.Κ) και της **απάτης**, η συρροή θεωρείται αληθινή πραγματική λόγω της ετερότητας των προβαλλομένων εννόμων αγαθών. Πράγματι, το έγκλημα της πλαστογραφίας στη βασική του μορφή προσβάλλει τη γνησιότητα του εγγράφου υπό την έννοια της αδυναμίας εξασφάλισης πλέον της δι' εγγράφων απόδειξης έναντι των μη γνησίων και μη ανταποκρινόμενων στην αρχική τους μορφή εγγράφων, ενώ το έγκλημα της απάτης θίγει το έννομο αγαθό της περιουσίας. Η θέση αυτή περί αληθινής συρροής πρέπει να ισχύσει γενικά, ανεξάρτητα δηλαδή από το αν η πλημμελληματική πλαστογραφία συνοδεύεται ή όχι με χρήση του πλαστού εγγράφου, και τούτο γιατί ούτε με τη χρήση, ούτε πολύ περισσότερο με μόνη την κατάρτιση ή τη νόθευση, εκφράζεται η περιουσιακή βλάβη που προκαλείται με την τελειωμένη απάτη. Πρέπει ωστόσο να σημειωθεί ότι στην περίπτωση αυτή συρροή μεταξύ απάτης και της χρήσης πλαστού, είτε ως επιβαρυντικής περίστασης (άρθρο 216 παρ.1 εδαφ.β΄ Π.Κ), είτε ως αυτοτελούς εγκλήματος (άρθρο 216 παρ.2 Π.Κ), είναι κατ' ιδέαν αληθινή, καθώς συμπίπτει ένα τμήμα των δύο εγκλημάτων, δηλαδή η χρήση του πλαστού με την πράξη εξαπάτησης, κατά κανόνα τουλάχιστον.

ii) Η απόπειρα απάτης συνιστά διακινδύνευση και όχι βλάβη της περιουσίας. Κατά συνέπεια συρρέει αληθινά με την (πλημμελληματική) πλαστογραφία χωρίς χρήση του πλαστού, αφού στην τελευταία δεν αντιμετωπίζεται απαξιολογικά η διακινδύνευση της περιουσίας. Η συρροή αντίθετα είναι φαινομενική, όταν την (πλημμελληματική) πλαστογραφία συνοδεύει η χρήση του πλαστού και η χρήση αυτή ταυτίζεται κατά τα πραγματικά περιστατικά με τα πραγματικά περιστατικά που συγκροτούν την απόπειρα απάτης. Εδώ η χρήση του πλαστού εγγράφου -είτε υπό τη μορφή αυτοτελούς εγκλήματος, είτε ως επιβαρυντική περίσταση της απλής πλαστο-

γραφίας- απορροφά την απόπειρα απάτης, στο μέτρο που απαξιολογικά ενέχει μέσα της τη διακινδύνευση της περιουσίας που η απόπειρα απάτης εκφράζει.

iii) Πρόβλημα υπάρχει με την αξιολόγηση της σχέσης της απόπειρας απάτης από τη μια και της κακουργηματικής πλαστογραφίας (άρθρο 216 παρ.3 Π.Κ) από την άλλη. Εφόσον η φύση του αδίκου που σχετίζεται με τη διάταξη του άρθρου 386 Π.Κ εμφανίζεται απολύτως διευκρινισμένη, είναι φανερό ότι η απάντηση στο ερώτημα, αν και στην περίπτωση αυτή πρέπει να υιοθετηθεί η λύση της αληθινής συρροής, εξαρτάται από τα προστατευόμενα έννομα αγαθά της διάταξης του άρθρου 216 παρ.3 Π.Κ. Η διευρυμένη απαξία της διακεκριμένης σε βαθμό κακουργήματος πλαστογραφίας αντλεί το περιεχόμενό της τόσο από τη βλάβη του εννόμου αγαθού της γνησιότητας του εγγράφου, όσο και από τη συνδεδεμένη με τις επιδιώξεις του δράστη βλάβη του εννόμου αγαθού της περιουσίας. Στο μέτρο λοιπόν που η απόπειρα απάτης συνιστά -όπως έγινε δεκτό ανωτέρω- διακινδύνευση του εννόμου αγαθού της περιουσίας, μπορεί να υποστηριχθεί ότι αντιμετωπίζεται απαξιολογικά πλήρως από την ευρύτερη διάταξη του άρθρου 216 παρ.3 Π.Κ που καταλαμβάνει και την περιουσιακή βλάβη, έτσι ώστε να παρέλκει αυτοτελής τιμώρησή της. Διαφορετική λύση θα οδηγούσε σε διπλή αξιολόγηση του ίδιου στοιχείου σε βάρος του κατηγορουμένου, πράγμα ανεπίτρεπτο. Υπό το πρίσμα των σκέψεων αυτών θα πρέπει να γίνει δεκτό ότι η απόπειρα απάτης συρρέει φαινομενικά και όχι αληθινά με την κακουργηματική πλαστογραφία, από την οποία και απορροφάται.

iv) Όσον αφορά στη συρροή ολοκληρωμένης απάτης και κακουργηματικής πλαστογραφίας μπορούν να γίνουν οι ακόλουθες παρατηρήσεις: Η επέλευση της περιουσιακής βλάβης στην κατ' άρθρο 216 παρ.3 εδαφ.α΄ Π.Κ πλαστογραφία αποτελεί την ουσιαστική αποπεράτωσή της. Παραλλήλως έχουν πληρωθεί και όλοι οι όροι της τελειωμένης απάτης, η οποία αποτελεί έτσι συντιμωρητή μεταγενέστερη πράξη. Εφαρμόζεται επομένως μόνο η διάταξη του άρθρου 216 παρ.3 εδαφ.α΄ Π.Κ, η διατύπωση του οποίου, ιδίως μετά την τροποποίησή του με τα άρθρα 1 παρ.7 του Ν. 2408/1996 και 14 παρ.3 του Ν. 2721/1999, φαίνεται να ευνοεί την υποστήριξη

της άποψης ότι ο αριθμητικός προσδιορισμός της βλάβης σημαίνει και επελθούσα βλάβη και επομένως τελειωμένη απάτη. Υπό αυτή την ερμηνευτική εκδοχή, η κατ' άρθρον 216 παρ.3 εδαφ.α΄ Π.Κ πλαστογραφία εμπεριέχει και όλα τα στοιχεία της απάτης.

Για το λόγο αυτό εγκαταλείπεται η υπό το προηγούμενο νομοθετικό καθεστώς λύση της αληθινής συρροής και προκρίνεται ως ορθότερη η φαινομενική συρροή των δύο εγκλημάτων, οπότε και εφαρμόζεται η διάταξη του άρθρου 216 παρ.3 εδαφ.α΄ Π.Κ, η οποία απορροφά την τετελεσμένη απάτη, καθώς σε αντίθετη περίπτωση θα επρόκειτο για διπλή αξιολόγηση του αυτού στοιχείου της αντικειμενικής υπόστασης, ήτοι της περιουσιακής βλάβης.

Συμμετοχή

Το έγκλημα της πλαστογραφίας αντιμετώπισε ένα σοβαρό πρόβλημα μετά τον ορισμό που έδωσε η ΑΠ 144/1992 για τη συναυτουργία: απαραίτητος όρος για την κατά συναυτουργία τέλεση του εγκλήματος είναι η γνώση της πρόθεσης του άλλου να τελέσει μία πράξη και η θέληση σύμπραξης με αυτόν, ενώ η σύμπραξη μπορεί να περιορίζεται και στην ενέργεια μερικότερων πράξεων κατά την τέλεση του εγκλήματος, χωρίς να είναι απαραίτητη η αναφορά των επιμέρους ενεργειών κάθε συναυτουργού για την από κοινού πραγμάτωση της αντικειμενικής υπόστασης.

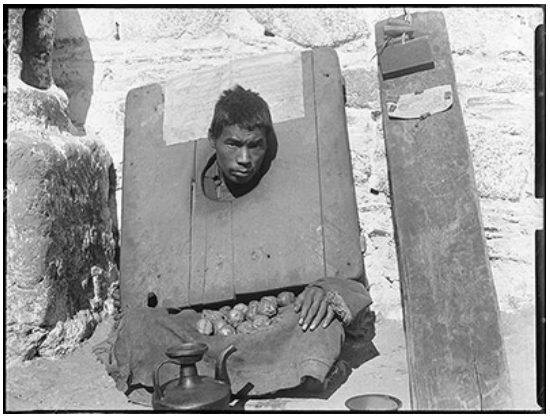
Τίθεται, επομένως το ερώτημα "Ποιες μπορεί να είναι οι μερικότερες αυτές πράξεις για την κατά συναυτουργία τέλεση του 216 Π.Κ;" Θεωρείται λίγο δύσκολο πρακτικά δύο άτομα μαζί, κρατώντας για παράδειγμα το μολύβι, να νοθεύουν ή να καταρτίζουν ένα έγγραφο.

Στο ελληνικό ποινικό δίκαιο συναυτουργός είναι αυτός που τελεί πράξη τυποποιημένη, πράξη δηλαδή της αντικειμενικής υπόστασης, όχι όμως οποιαδήποτε μερικότερη πράξη για την ολοκλήρωση του εγκλήματος. Με αυτόν τον τρόπο διαχωρίζεται και η συναυτουργία από τις υπόλοιπες περιπτώσεις συμμετοχικής δράσης των άρθρων 46 & 47 Π.Κ. Εξάλλου, γίνεται δεκτό ότι στα σύνθετα και πολύπρακτα εγκλήματα, συναυτουργός θεωρείται αυτός που πραγματώνει ένα συνθετικό μέρος της πράξης. Έτσι, η κατάφαση συναυτουργίας κατά την ΑΠ144/92 χρήζει διευκρίνισης των μερικότερων πράξεων που αναφέρει και αναγωγής αυτών

σε μέρος της αντικειμενικής υπόστασης ενός εγκλήματος. Οι επιμέρους πράξεις των συμμετόχων αθροιζόμενες πρέπει να οδηγούν, συμπληρώνοντας η μία την άλλη, στο αποτέλεσμα. Αν απλώς η κάθε ενέργεια εκθέτει το έννομο αγαθό στη διάθεση του άλλου συμμετόχου, τότε πρέπει να αντιμετωπιστεί σύμφωνα με τις περιπτώσεις της συνέργειας.

Τέλος, ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση της ηθικής αυτουργίας σε πλαστογραφία. Όταν κάποιος παροτρύνεται να καταρτίσει πλαστό ή να νοθεύσει, χωρίς όμως ο φυσικός αυτουργός να έχει σκοπό να παραπλανήσει με την πράξη του αυτή κάποιον, ενώ ο ηθικός αυτουργός έχει τέτοιο σκοπό και συνάμα κατευθύνει με πρόθεση το φυσικό αυτουργό στην τέλεση της πράξης, υπάρχει ηθική αυτουργία σε πλαστογραφία, μολονότι στο φυσικό δράστη είναι μη τελικά καταλογιστή η πράξη του, ελλείψει μέρους της υποκειμενικής υπόστασης. Και αυτό, γιατί στην ηθική αυτουργία απαιτείται απλώς τελικά άδικη πράξη από την πλευρά του φυσικού αυτουργού (άρθρο 46 παρ.1α Π.Κ).

1.1.4 Ποινική κύρωση



Μοναχός στην περιοχή Lhasa καταδικασμένος για πλαστογραφία 1920, χαρακτηριστική λεπτομέρεια το 'καρφιτσωμένο' πλαστογραφημένο έγγραφο στο επάνω δεξιό τμήμα της φωτογραφίας (από τη συλλογή του Sir Charles Bell)

Κατά το άρθρο 216 παρ.1 Π.Κ «*όποιος καταρτίζει πλαστό ή νοθεύει έγγραφο…. τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών*». Επομένως, απειλείται ένα φάσμα ποινής μεταξύ τριών μηνών και πέντε ετών για την τέλεση της πλαστογραφίας. Με την ίδια ποινή τιμωρείται

και όποιος εν γνώσει του χρησιμοποιεί πλαστό ή νοθευμένο έγγραφο. Η πλαστογραφία του άρθρου αυτού είναι έγκλημα που διώκεται αυτεπάγγελτα.

Υπάρχει και η διακεκριμένη περίπτωση πλαστογραφίας της παρ.3, που αναγάγει την πράξη αυτή σε κακούργημα. Η ποινή πάντως που αντιστοιχεί στη βασική μορφή του εγκλήματος μπορεί, αν πληρωθούν οι όροι του άρθρου 84 Π.Κ, να μειωθεί ως προς το κατώτατό της όριο και να λάβει τη μορφή της απειλούμενης ποινής μιας φυλάκισης, δηλ. από δέκα ημέρες έως πέντε έτη. Η πλαστογραφία στη βασική της μορφή παραγράφεται μετά τα πέντε έτη.

1.2 Η έννοια του 'εγγράφου'

Κατά τη μελέτη των στοιχείων που συνθέτουν το έγκλημα της πλαστογραφίας, κρίθηκε σκόπιμο να σταθούμε σε μια βασική έννοια που εμπεριέχεται σε αυτήν, την έννοια του 'εγγράφου'. [7]Υπό το προϊσχύσαν λοιπόν δίκαιο, ορισμό της έννοιας του εγγράφου περιείχε το άρθρο 384 Κ.Πολ.Δ, σύμφωνα με το οποίο: *«Έγγραφα είναι χειρόγραφοι ή τυπωμέναι διατριβαί ή υπομνήματα»*.

Ως υπομνήματα (instrumenta) θεωρούνταν τα ανθρώπινα έργα, που ήταν προορισμένα για την απομνημόνευση γεγονότων ή πράξεων, ενώ ως έγγραφα (documenta) ορίζονταν «*τα επί χάρτου ή άλλης παραπλήσιας ύλης κατασκευασμένα διά γραφής ή άλλου παραπλησίου τρόπου υπομνήματα*». Τα έγγραφα, ως υποδιαίρεση των υπομνημάτων, αποτελούσαν την δια της γραφής απομνημόνευση. Οι συντάκτες του Κ.Πολ.Δ απέφυγαν να προσδιορίσουν την έννοια του εγγράφου, από τις σχετικές συζητήσεις διαφαίνεται πάντως η πρόθεσή τους να θέσουν ως εννοιολογική αφετηρία τα διδασκόμενα στο πλαίσιο της Πολ.Δ/1834.

Σύμφωνα με το ισχύον δίκαιο η έννοια του εγγράφου περιγράφεται στο άρθρο 13 Π.Κ εδαφ.γ΄, όπως τροποποιήθηκε (το εδαφ.β΄) με το άρθρο 2 του Ν. 1805/1988. Πιο συγκεκριμένα έγγραφο ορίζεται: *«...κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός·*

[7] Ένωση Ελλήνων Δικονομολόγων «*Τα έγγραφα στην πολιτική δίκη*» Πρακτικά του 17ου Πανελλήνιου Συνεδρίου (Χανιά 3-6 Οκτωβρίου 1991), Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα-Κομοτηνή 1994 σελ.97.

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 δε 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, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία».

Με βάση τον παραπάνω ορισμό που δίνεται άμεσα από το νόμο, η θεωρία και η νομολογία κινήθηκαν, ώστε να περιορίσουν ή να επεκτείνουν τη σημασία του εγγράφου, σχετικά με διάφορα αντικείμενα με τα οποία έγινε προσπάθεια να συνδεθεί. Έτσι η ΑΠ 1992/1984 (Ποιν. Χρον. 1985, σελ. 600) αναφέρει ότι έγγραφο είναι: «*κάθε ανθρώπινη ενέργεια μνημείο, το οποίο περιέχει γραφή ή άλλο σημείο παράστασης εννοιών για γεγονότα που έχουν έννομη σημασία και συνεπώς για την έννοια του εγγράφου σημασία έχει ο προορισμός (ή) η προσφορότητα του να αποδείξει τέτοια γεγονότα».*

Χρησιμοποιώντας τα στοιχεία αυτά ο Μανωλεδάκης θεωρεί έγγραφο: «*κάθε γραπτό ή σημείο το οποίο: α) περιέχει αποτυπωμένα - ενσωματωμένα γεγονότα, σημαντικά για το δίκαιο, το οποίο είναι προορισμένο, αν πρόκειται για σημείο, ή και απλώς πρόσφορο, αν πρόκειται για γραπτό, να αποδείξει τα γεγονότα β) η αποτύπωση - ενσωμάτωση να έχει γίνει κατά τέτοιο τρόπο, ώστε να αντέξει με το πέρασμα του χρόνου και γ) το περιεχόμενο της αποτύπωσης και η πηγή προέλευσης να είναι κατανοητά».* Συνοπτικά απαιτείται απόδειξη, διάρκεια και εγγύηση, όπως χαρακτηριστικά αναφέρει. Επισημαίνεται επίσης ότι, επειδή έγγραφα δεν είναι μόνο τα γραπτά αλλά και τα σημεία, σύμφωνα με το άρθρο 13γ Π.Κ, δεν είναι απαραίτητο ένα έγγραφο να είναι αντιληπτό με τις ανθρώπινες αισθήσεις.

Στην ίδια γραμμή πλεύσης βρίσκονται και οι απόψεις του Ανδρουλάκη, ο οποίος επικεντρώνεται σε δύο προϋποθέσεις για την κήρυξη ενός αντικειμένου ως εγγράφου. Απαιτείται καταρχήν μια σταθερή ενσωμάτωση σε μια ύλη ενός διανοητικού περιεχομένου, στοιχείο που διαφοροποιεί το έγγραφο από τα απλά αντικείμενα αυτοψίας, αφού αυτό λέει κάτι, ξεπερνώ-

ντας την υλική του ύπαρξη, και συγκεντρώνεται στην ενσωμάτωση και μετάδοση ενός νοήματος (πληροφοριακή λειτουργία)

Κατά δεύτερον, πρέπει να προκύπτει ο εκδότης - εκφραστής του διανοητικού αυτού περιεχομένου, αφού στο έγγραφο αυτό που ενδιαφέρει είναι η καθήλωση των απόψεων ενός προσώπου σε μία ύλη, έτσι ώστε να το διαθέτουμε με ασφάλεια κάθε στιγμή, απαλλαγμένο από τις μοιραίες κυμάνσεις, αθέλητες ή ηθελημένες, της κάθε φορά ζωντανής αναπαραγωγής του. Έτσι, προστατεύεται η αποδεικτική λειτουργία του εγγράφου που βασίζεται στη διαιωνιστική του λειτουργία (scripta manent) και στο προσωπικό εγγυητικό γνώρισμα του εκδότη. Κατά τον Ανδρουλάκη, το να αναφέρεται το έγγραφο σε γεγονός με έννομη σημασία, δεν προσθέτει τίποτα παραπάνω στα ανωτέρω στοιχεία και κατά το συγγραφέα αυτό είναι ένα απλό χαρακτηριστικό του εγκλήματος της πλαστογραφίας.

Παρά τις οποίες προσπάθειες καθορισμού των στοιχείων του εγγράφου, θα πρέπει να παραδεχτούμε ότι οι κοινωνικές αλλαγές και η τεχνολογική πρόοδος έχουν μεταβάλλει το ρόλο του εγγράφου, με αποτέλεσμα στην πράξη να παρουσιάζονται περιπτώσεις εγγράφων που χρήζουν ιδιαίτερης μελέτης και ανάλυσης, όπως: η [8]φωτοτυπία, ο αριθμός πλαισίου αυτοκινήτου (85, 89, 90 Ν. 2094/1992 «Κύρωση του Κώδικα Οδικής κυκλοφορίας»), οι μαγνητοταινίες (βλ. ενδεικτικά Συμβλ. Α.Π. 631/1990, Ποιν. Χρον. 1991, σελ. 71 «Οι μαγνητοταινίες και οι βιντεοκασέττες ως έγγραφα»), το TELEX (Α.Π. 1246/1990, Ποιν. Χρον. 1991, σελ. 538 με παρατ. Κωνσταντινίδη Α. στη σελ. 940), τα προγράμματα Η/Υ κ.λ.π.

1.2.1 'Πρόσφατες' αλλαγές στην έννοια του 'κλασικού εγγράφου'

Λαμβάνοντας υπόψη τα παραπάνω, που δίνουν κατά τη γνώμη μας μια γεύση της ευρύτητας που χαρακτηρίζει την έννοια του εγγράφου, επιλέξαμε να αναφερθούμε στην ευρύτητα που παρουσιάζει ακόμα και το καλούμενο ως 'κλασικό έγγραφο'. Δηλαδή ένα συνηθισμένο φύλλο χάρτου, με ορισμένες επ' αυτού χειρόγραφες ενδείξεις γραφής, ενδεχομένως και κάποια

[8] βλ. περαιτέρω Κωνσταντινίδης Α. (2000) όπ. παρ., σελ. 37επ.

υπογραφή. Η δυναμική ενός ‘κλασικού εγγράφου’ άπτεται στις αδιάκοπες αλλαγές που συμβαίνουν στη χειρόγραφη γραφή και τη διαφαινόμενη μετεξέλιξή της σε μηχανική, στις επιπτώσεις που επιφέρει η αλλαγή αυτή στον τύπο του χάρτου, αλλά και την τελική μετάλλαξη κατά μία έννοια του ‘κλασικού εγγράφου’ στην έννοια του ‘ηλεκτρονικού’.

Αναδεύοντας στην ανάλυση που ακολουθεί ορισμένα ιστορικά στοιχεία, δεν επιθυμούμε να κουράσουμε τον αναγνώστη, το αντίθετο μάλιστα, θέλουμε να αντιληφθεί πόσες ανακατατάξεις έχουν συμβεί τα τελευταία χρόνια στη βασική έννοια του εγκλήματος της πλαστογραφίας, το έγγραφο (με την κλασική του μορφή), ευαισθητοποιώντας τον ταυτόχρονα για τις μελλοντικές που δεν φαίνεται να είναι και τόσο μακριά.

1.2.1α Χειρόγραφη γραφή (Γραφικά Μέσα - Μελάνη)

Παρακάτω θα παρουσιάσουμε τις ‘πρόσφατες’ εξελίξεις στον τομέα των γραφικών μέσων και της χρησιμοποιηθείσας μελάνης, με ιδιαίτερη έμφαση στο στυλογράφο σφαιριδίου (BIC) ελαιώδους βάσης, που πραγματικά έφερε επανάσταση στη χειρόγραφη γραφή, επικρατώντας των προηγούμενων αυτού γραφικών μέσων. Η επιλογή αυτή δεν έγινε αυθαίρετα αλλά αποτελεί στοχευμένη ενέργεια, αφού κατά την περιήγησή μας στη βιβλιογραφία[9] που αφορά στις γραφολογικές εξετάσεις σε περιπτώσεις πλαστογραφίας, το θέμα του στυλογράφου και δη του στυλογράφου σφαιριδίου προβάλλει μείζον για πολλούς λόγους, που δεν είναι της παρούσης. Κατόπιν τούτου έχουμε τα ακόλουθα:

[10]Ο Ουγγρικής καταγωγής δημοσιογράφος Laszlo Biro εφηύρε τον πρώτο στυλογράφο σφαιριδίου (ballpoint pen) το 1938. Ο Biro είχε παρατηρήσει ότι ο τύπος μελανιού που χρησιμοποιείται στην εκτύπωση εφημερίδων στέγνωνε γρήγορα, αφήνοντας το έγγραφο στεγνό. Αποφάσισε να δημιουργήσει ένα γραφικό μέσο χρησιμοποιώντας τον ίδιο τύπο μελανιού. Έτσι πρόσθεσε στην άκρη του νέου γραφικού μέσου μία μικροσκοπική μπίλια (βλ. κατωτέρω φωτο-

[9] βλ. ενδεικτικά Stewart L. (1985) «Ballpoint Ink Age Determination by Volatile Componet Comparison - A Preliminary Study», Journal of Forensic Sciences, JFSCA, Vol.30, No.2, σσ.405-411.
[10] http://inventors.about.com/library/weekly/aa101697.htm.

γραφία), η οποία κατά την περιστροφή της έπαιρνε μελάνι από τη σχετική θήκη και την εναπόθετε στο χαρτί.

Αυτή η πατέντα φαίνεται αρχικά να είχε κατοχυρωθεί με δίπλωμα ευρεσιτεχνίας το 1888 από τον John J. Loud για να χρησιμεύσει στο μαρκάρισμα δέρματος. Εντούτοις, αυτό το δίπλωμα ευρεσιτεχνίας έμεινε εμπορικά ανεκμετάλλευτο. Ο Biro κατοχύρωσε την ευρεσιτεχνία του το 1938 και υπέβαλε εκ νέου το 1943, αίτηση για δίπλωμα ευρεσιτεχνίας στην Αργεντινή, όπου είχε μεταναστεύσει.

Η βρετανική κυβέρνηση αγόρασε τα δικαιώματα χορήγησης αδειών σε αυτό το δίπλωμα ευρεσιτεχνίας, με τη σκέψη ότι ίσως φαινόταν χρήσιμο στην Πολεμική Αεροπορία κατά τη διάρκεια του πολέμου, προκειμένου η μελάνη του νέου αυτού γραφικού μέσου να μην διαρρέει όταν τα μαχητικά αεροπλάνα κινούνται σε μεγάλα υψόμετρα. Η επιτυχής απόδοσή των νέων γραφικών μέσων τα έφερε στο προσκήνιο.

Ο Biro όμως είχε παραμελήσει να πάρει ένα αμερικανικό δίπλωμα ευρεσιτεχνίας για το στυλογράφο σφαιριδίου. Έτσι η νεοσύστατη επιχείρηση ‘Eterpen’ στην Αργεντινή εμπορευματοποίησε του στυλογράφους Biro και ο τύπος χαιρέτησε την επιτυχία αυτού του στυλογράφου, καθώς μπορούσε κάποιος να γράψει για ένα ολόκληρο έτος χωρίς να χρειάζεται να ξαναγεμίσει μελάνη. Το Μάιο του 1945 η επιχείρηση ‘Eversharp’ συνεργάζεται με την ‘Eberhard-Faber’ για να αποκτήσουν τα αποκλειστικά δικαιώματα των στυλογράφων Biro.

Ένα μήνα αργότερα ο Milton Reynolds επιχειρηματίας από το Σικάγο, σε επίσκεψή του στο Μπουένος Άιρες είδε σε ένα κατάστημα τους στυλογράφους Biro και αναγνώρισε τη δυνατότητα πωλήσεών τους, γι’ αυτό και αγόρασε μερικούς ως δείγματα. Ο Reynolds κατά την επιστροφή του στην Αμερική ίδρυσε την εταιρεία Reynolds International Pen Company α-

γνοώντας τα δικαιώματα των διπλωμάτων ευρεσιτεχνίας της Eversharp. Σε τέσσερις μήνες ο Reynolds αντιγράφει το προϊόν και το πωλεί με την επωνυμία ‘Reynold's Rocket’ σε τμήμα του καταστήματος Gimbel στην πόλη της Νέας Υόρκης. Η απομίμηση αυτή του Reynolds κτυπά την Eversharp στην αγορά.

Η Μ.Βρετανία δεν έμεινε πίσω στις πωλήσεις ballpoint pens που διετέθησαν προς πώληση στο κοινό τα Χριστούγεννα του 1945 από την επιχείρηση ‘Miles-Martin Pen Company’.

Η Eversharp μήνυσε το Reynolds για την αντιγραφή του σχεδίου που είχε αποκτήσει νόμιμα. Το προηγούμενο δίπλωμα ευρεσιτεχνίας (1888) από τον John Loud θα είχε ακυρώσει τις αξιώσεις και των δύο πλευρών,.εντούτοις, κανένας δεν το ήξερε αυτό τότε.

Οι συχνοί πόλεμοι τιμών, τα προϊόντα κακής ποιότητας κ.λ.π. έριξαν περί το έτος 1948 τις τιμές των στυλογράφων από την αρχική τιμή των $12.50 σε λιγότερο από 50 σεντ ανά μονάδα. Ακολούθησε μια περίοδο κάμψης με αξιοσημείωτη την αλλαγή που έκανε το 1950 ο Γάλλος Βαρόνος επ’ ονόματι Bich στην ονομασία των στυλογράφων και τους μετονόμασε σε **BIC**.

Τον Ιανουάριο του 1954 η επιχείρηση ‘Parker’ εισήγαγε με κάποιες αλλαγές ένα παρόμοιο προϊόν το Jotter, που διαρκούσε πέντε φορές περισσότερο από τους αντίστοιχους στυλογράφους της Eversharp και του Reynolds. Παράλληλα παρέχοταν ποικίλα σε μεγέθη γραφίδας κ.λ.π. ενώ το καλύτερο από όλα ήταν ότι σε διάστημα ενός έτους η Parker πώλησε 3,5 εκατομμύρια Jotters με τιμές από $2.95 έως $8.75.

Η Eversharp πώλησε το μερίδιό της στην Parker. Την πρόσφατη δεκαετία του '50 η BIC® κρατούσε το 70% της ευρωπαϊκής αγοράς, ενώ γύρω στο 1958 η BIC αγόρασε το 60% της επιχείρησης ‘Waterman’ που είχε έδρα στη Νέα Υόρκη και γύρω στο 1960 η BIC απέκτησε το 100% της επιχείρησης. Η BIC πωλεί ballpoint στις ΗΠΑ για 29 - 69 σεντς.

Σήμερα η ιδιαίτερα δημοφιλής σύγχρονη έκδοση των στυλογράφων του Biro, έχει έναν καθημερινό παγκόσμιο αριθμό πωλήσεων 14.000.000 κομματιών και έχει αφήσει κατά πολύ πίσω τα παλιότερα γραφικά μέσα.

Ανακεφαλαιώνοντας όλα όσα διατυπώθηκαν παραπάνω σχετικά με την επανάσταση που έφεραν οι στυλογράφοι σφαιριδίου, αλλά και τη συνεχή εξέλιξη των χρησιμοποιούμενων γραφικών μέσων - μελανιών (όπως λ.χ. roller ball pens υγρής μελάνης), θα πρέπει μολαταύτα να παραδεχτούμε ότι σταδιακά φαίνεται να υποχωρεί η χειρόγραφη γραφή έναντι της λεγόμενης 'μηχανικής' γραφής.

Κάτι ανάλογο ισχύει και για τον τομέα των χειρόγραφων υπογραφών όπου όσον αφορά κυρίως άτομα με πλήθος καθημερινών συναλλαγών, διαπιστώνεται η 'αυτοματοποίηση' των υπογραφών τους[11] π.χ. με την εντυπωματική αποτύπωση των υπογραφών τους σε σώμα σφραγίδας.

1.2.1β Μηχανική γραφή (Γραφομηχανές - Εκτυπωτές)

Μηχανική γραφή καλείται η δια μηχανής (γραφομηχανής, συστήματος Η/Υ & εκτυπωτή κ.λ.π.) παραγόμενη γραφή. Από τα μηχανικά μέσα θα σταθούμε στα πλέον χαρακτηριστικά:

Γραφομηχανή

Η ιστορία της γραφομηχανής[12] αρχίζει από το 18ο αιώνα, όταν ο Άγγλος **Henry Mill** το 1714 κατασκεύασε μια συσκευή που μπορούσε να δίνει γράμματα τυπογραφικού περίπου χαρακτήρα. Η βασίλισσα της Αγγλίας μάλιστα του έδωσε και ειδικό δίπλωμα ευρεσιτεχνίας. Αν και αυτή ήταν η πρώτη προσπάθεια, η πρώτη μηχανή που πραγματικά λειτούργησε ήταν αυτή που κατασκεύασε ο Ιταλός Pellegrino Turri το 1808 για την τυφλή φίλη του Κοντέσα Carolina Fantoni da Fivizzono.

Ακολούθησαν πολλές δοκιμές για την τελειοποίηση της συσκευής αυτής, ειδικότερα το 1828 ο Ώστιν Μπαρτ από το Ντετρόιτ κατασκεύασε μια γραφομηχανή που την ονόμασε 'τυπογράφο'. Ήταν όμως αρκετά αργή στο γράψιμο. Από τότε πέρασαν αρκετά χρόνια αναζητήσεων και πειραματισμών μέχρι που το 1867 ο Αμερικανός Christopher Latham Sholes μαζί με

[11] πρβλ. Gencavage J. (1986) «*Facsimile Signatures Produced by Gelatin transfer Duplicator - Recognition and Identification*», Journal of Forensic Sciences, JFSCA, Vol. 31, No1, σσ.106-116.

[12] Οι συσκευές με τις οποίες μπορούμε να γράψουμε ένα κείμενο με στοιχεία τυπογραφικά» (http://www.livepedia.gr).

τους συνεργάτες του S. W. Soule και G. Glidden, φτιάχνουν μια αρκετά πρακτική μηχανή. Ο Sholes όμως μη έχοντας υπομονή να εμπορευτεί το νέο προϊόν αποφάσισε να πουλήσει τα δικαιώματα της γραφομηχανής στον James Densmore.

Το 1873 η γραφομηχανή γίνεται πλέον βιομηχανικό προϊόν. Πιο συγκεκριμένα [13]το εργοστάσιο του Remington & Sons, το οποίο έως το 1870 κατασκεύαζε όπλα για τον αμερικανικό Εμφύλιο δεν ήξερε τι να κάνει με το περισσευούμενο σίδερο στις αποθήκες του και αποφάσισε να καταπιαστεί με τις γραφομηχανές. Οι γραφομηχανές αυτές υπάρχουν και σήμερα, βελτιωμένες βέβαια κατά πολύ. Στη συνέχεια άρχισαν να φτιάχνουν γραφομηχανές και οι εταιρείες Underwood, Royal κ.ά. που φρόντισαν για την καλυτέρευσή τους.

Remington No 2 (περί το 1878)

Το 1914 ο Τζαίημς Σμάθερ παρουσίασε την πρώτη γραφομηχανή που κινούνταν με ηλεκτρισμό. Η μαζική παραγωγή της ηλεκτροκίνητης γραφομηχανής άρχισε το 1930.

IBM Electromatic (1934)

[13] Μιχαλοπούλου Α. (2007) «*Αντηχήσεις Οι παλαιοί των ημερών*», Εφημερίδα 'Καθημερινή'.

Το θέμα είναι ότι παρά το χαμηλό κόστος και την τελειοποίηση στη λειτουργία τους, οι γραφομηχανές στις μέρες μας έχουν πλέον αντικατασταθεί από τους Η/Υ και τους εκτυπωτές, ενώ όσοι συνεχίζουν να γράφουν στη γραφομηχανή ή να παραδίδουν χειρόγραφα θεωρούνται στην καλύτερη περίπτωση 'ρομαντικοί'. Αυτή η μετάβαση βέβαια δεν έγινε απ' τη μια μέρα στην άλλη, αλλά χρειάστηκαν αρκετά χρόνια ας δούμε περιληπτικά ορισμένα ιστορικά στοιχεία.

Εκτυπωτές

Κατά τις μεταπολεμικές δεκαετίες η παγκοσμιοποίηση, κατά ένα σημαντικό μέρος της, περιγράφεται και βιώνεται ως εξάπλωση των τεχνολογιών και αύξηση των χρηστών και των χρήσεων. Είναι η εποχή που η τεχνολογία αρχίζει να επηρεάζει εντονότατα τη συγκέντρωση της πληροφορίας και συνακόλουθα τη διαμόρφωση της Κοινωνίας της Γνώσης.

Η λήξη του Β΄ Παγκοσμίου Πολέμου, συνοδεύεται από δύο μεγάλης σημασίας γεγονότα. Το 1945 είναι η πρώτη φορά που κάποιος 'απαιτεί' την υποβοήθηση του ανθρώπινου νου, ώστε να μπορεί να σκέφτεται όχι ευθύγραμμα και σε συνέχεια, αλλά σύνθετα και συνδυαστικά. Ένα χρόνο αργότερα, το 1946, θα τεθεί σε λειτουργία ο πρώτος ηλεκτρονικός υπολογιστής και θα εγκαινιασθεί έτσι η ψηφιακή εποχή (digital age).

Όσον αφορά τους εκτυπωτές [14]η αρχή έγινε το 1938, όταν ο Chester Carlson εφηύρε μια διαδικασία ξηράς εκτύπωσης αποκαλούμενη ηλεκτροφωτογραφία (Xerox), η οποία και απετέλεσε τη βάση για τους εκτυπωτές laser που θα ακολουθούσαν. Για εννέα ολόκληρα χρόνια ο Carlson προσπαθούσε να πουλήσει την τεχνολογία σε επιχειρήσεις όπως: RCA, Remington, Rand, General Electric, Eastman Kodak, IBM χωρίς όμως αποτέλεσμα.

Το 1953, όταν η 'Remington-Rand' θέλοντας να υποστηρίξει τον υπολογιστή Univac παρουσίασε τον πρώτο μεγάλο εκτυπωτή, ενώ το 1959 παρουσιάστηκε στην Αμερική η πρώτη αυτόματη συσκευή τεχνολογίας Xerox (Xerox 914).

[14] http://inventors.about.com/library/inventors/blcomputer_printers.htm.

Στις αρχές του 1969 ξεκίνησαν προσπάθειες από το Ερευνητικό Κέντρο Xerox Palo Alto, οι οποίες και τελικώς ολοκληρώθηκαν το Νοέμβριο του 1971, ούτως ώστε να κατασκευασθεί ο πρώτος εκτυπωτής laser που ονομάσθηκε 'EARS'. Ο μηχανικός της Xerox, Gary Starkweather προσάρμοσε την τεχνολογία Xerox προσθέτοντας μια ακτίνα λέιζερ. Ο πρώτος εκτυπωτής laser 'Xerox 9700' δόθηκε στην κυκλοφορία το 1977. Λίγα χρόνια αργότερα το 1981 κυκλοφόρησε ο 'Xerox Star 8010' στη διόλου ευκαταφρόνητη τιμή των $17,000.

[15]Απ' την άλλη η επιχείρηση IBM, θέλοντας να υποστηρίξει τα υπολογιστικά θηρία της που άκουγαν στο όνομα mainframe (υπερ-υπολογιστές), παρουσίασε για πρώτη φορά εκτυπωτή laser το **1975** τον ονόμασε 'IBM 3800' και τον εγκατέστησε την επόμενη χρονιά σε κεντρικό λογιστικό γραφείο στο Milwaukee, Wisconsin.

Το υψηλό κόστος όμως και η έλλειψη αξιοπιστίας των συσκευών δεν επέτρεψαν την εξάπλωσή τους, όμως η ιδέα παρέμεινε και ανανεώθηκε από τη Hewlett Packard (HP) και η πραγματική επανάσταση δεν άργησε να γίνει. Άρχισε το 1984, όταν η HP ήλθε να ταράξει τα νερά με τον πρώτο προσιτό, ταχύ και αξιόπιστο LaserJet. Βασισμένη σε τεχνολογικές λύσεις που αναπτύχθηκαν από την Canon, δημιούργησε ένα κατεστημένο που είχε ως αποτέλεσμα να τελειώσει η δεκαετία του '80 με σχεδόν απόλυτη κυριαρχία των laser αλλά και των κρουστικών εκτυπωτών.

Όσον αφορά τους εκτυπωτές τεχνολογίας inkjet αυτοί κατασκευάστηκαν το 1976, αλλά μόλις το 1988 κατόρθωσαν τελικά να αποτελέσουν εκτυπωτές οικιακής χρήσης στην τιμή των 1.000$.

Σήμερα η πρόσβαση και η χρήση συστημάτων Η/Υ με εκτυπωτές (ανεξαρτήτου τεχνολογίας) είναι πλέον πολύ εύκολή και προσιτή στους περισσότερους από εμάς, είτε βρισκόμαστε στο σπίτι, είτε στο χώρο εργασίας/διασκέδασης, με αποτέλεσμα πολλές φορές να προτιμούμε (ως προς τη σύνταξη), αλλά και να συναλλασσόμαστε με μηχανογραφημένα έγγραφα. Η πραγματικότητα αυτή ενισχύει την άποψη που διατυπώθηκε παραπάνω και αφορά στη σταδια-

[15] http://www.in.gr.

κή μείωση χειρόγραφων εγγράφων στις καθημερινές μας συναλλαγές και κατ' επέκταση ως πειστήρια εγκλημάτων πλαστογραφίας.

1.2.1γ Χαρτί

Από τις αλλαγές που προκύπτουν κατά το πέρασμα από τη χειρόγραφη γραφή στη μηχανική, δεν θα μπορούσαμε να παραλείψουμε αυτές που αφορούν το στοιχείο του 'χάρτου'. Ας δούμε όμως κατ' αρχήν ορισμένα ιστορικά στοιχεία: [16]Ο πάπυρος, η μεμβράνη και το χαρτί είναι οι ύλες με τη μεγαλύτερη διάδοση από τα πρώτα χρόνια μ.Χ. Τον πάπυρο τον χρησιμοποιούσαν κυρίως στην αρχαιότητα, τη μεμβράνη στο Μεσαίωνα και το χαρτί, που έχει την καταγωγή του από τους Κινέζους, πέρασε στη Δύση με τους Άραβες από τον 11^{ο} αιώνα.

Η κατασκευή του πάπυρου ήταν μονοπώλιο της Αιγύπτου έως τον 7^{ο} αιώνα. Η τεχνική αυτής της κατασκευής περιγράφεται από τον Πλίνιο στη Φυσική Ιστορία του. Η πρώτη ύλη είναι το στέλεχος από το καλάμι που καλλιεργείται στην κοιλάδα του Νείλου. Λωρίδες επιμήκεις και εγκάρσιες, κολλημένες με το νερό του ποταμού, σχημάτιζαν φύλλα που πήγαιναν στο εμπόριο κομμένα σε ορισμένο σχήμα ή κυλινδρικά.

Η εφεύρεση της μεμβράνης αποδίδεται από το θρύλο στους κατοίκους της Περγάμου στη Μικρά Ασία. Η πρώτη ύλη της μεμβράνης είναι το δέρμα από πρόβατο, κατσίκα ή μικρό μοσχάρι. Είναι πολύ στερεή και λεία και ο Μεσαίωνας τη διατήρησε πολύ καιρό για τα βιβλία και τις επίσημες πράξεις παρά τον ανταγωνισμό του χαρτιού. Το αρχαιότερο δείγμα γραπτής μεμβράνης είναι ένα απόσπασμα που ανήκει ίσως στο τέλος του 1^{ου} αιώνα. Η χρήση της γίνεται κοινή τον 4^{ο} αιώνα. Από τον 9^{ο} έως τον 13^{ο} αιώνα είναι η μοναδική ύλη για τα βιβλία και σχεδόν μοναδική για τους χάρτες.

Το χαρτί [17]εφευρέθηκε στην Κίνα το 2^{ο} αιώνα μ.Χ. Οι Κινέζοι προσπάθησαν να το κατασκευάσουν με διάφορα υλικά, πριν χρησιμοποιήσουν τις ίνες λιναριού, που έδωσαν την πιο καλή ποιότητα. Τα στελέχη του λιναριού τα έβαζαν στο νερό για να ξεχωρίσουν οι ίνες, ύστε-

[16] Higounet C. «*Η Γραφή*», Εκδόσεις Δαίδαλος -Ι.Ζαχαρόπουλος Α.Ε., σελ. 10-11.
[17] http://www.tmth.edu.gr/el/kiosks/typography/technology/typo_t2.html.

ρα τις έπλεναν και τις κοπάνιζαν. Έτσι οι ίνες έδιναν έναν πολτό που, μαζί με νερό και άμυλο, οδηγούσαν στο χαρτί. Τα πιο παλιά γνωστά γραπτά τεκμήρια σε χαρτί είναι βουδιστικά κείμενα του 2ου αιώνα.

Από τους Κινέζους μετά από καιρό θα γνωστοποιηθεί η μέθοδος στους Γιαπωνέζους και στους Μογγόλους τον 8ο αιώνα, που θα τη μεταβιβάσουν στους Πέρσες της Σαμαρκάνδης[18], οι οποίοι με τη σειρά τους θα τη διδάξουν στους Άραβες εμπόρους. Οι τελευταίοι θα εισάγουν το χαρτί στην Ισπανία και τη Σικελία. Το 13ο αιώνα σημαντικά εργοστάσια χαρτιού ήταν εγκατεστημένα στην Ευρώπη, με την Ισπανία να είναι η πρώτη δυτική χώρα με εργοστάσια χαρτιού.

Τα χαρτιά μας σήμερα [19]έχουν ως βασική πρώτη ύλη τις φυτικές ίνες που περιλαμβάνουν: ίνες από κορμούς δέντρων (μαλακά ξύλα, σκληρά ξύλα), άλλες φυτικές ίνες όπως λινάρι, κάνναβη, γιούτα, άχυρο, βαμβάκι κ.λ.π. Από όλες αυτές στην κατασκευή του χαρτιού χρησιμοποιούνται περισσότερο οι ίνες των ξύλων.

Μπορούν να χρησιμοποιηθούν τρεις βασικές μέθοδοι για την κατασκευή πολτού από ίνες ξύλου: α) μηχανική, β) μηχανική/χημική και γ) χημική. Η μηχανική πολτοποίηση απομακρύνει τη λιγνίνη από τις ίνες με φυσικά μέσα. Η μηχανική/χημική τόσο με φυσικά όσο και με χημικά και η χημική εξ ολοκλήρου με χημικά.

Το επόμενο στάδιο στη διαδικασία κατασκευής του χαρτιού -και το τελικό στην πολτοποίηση- είναι η <u>λεύκανση.</u> Κατά την κατεργασία αυτή, ο πολτός λευκαίνεται, καθαρίζεται και σταθεροποιείται με την ελάχιστη δυνατή φθορά των ινών. Η κατεργασία μπορεί να είναι συνεχής ή κατά παρτίδες.

*

Σήμερα ανατέλλει μια νέα εποχή για το χαρτί, οι νέες τεχνολογιές επεξεργάζονται θέματα όπως η μείωση της κατανάλωσης χαρτιού. Πιο συγκεκριμένα: [20]Οι επιστήμονες της Xerox επινόησαν έναν τρόπο για τη δημιουργία εκτυπώσεων που να διαρκούν μόνο μία ημέρα, έτσι

[18] Η Σαμαρκάνδη ήταν ένα από τα μεγαλύτερα κέντρα κατασκευής χαρτιού στο τέλος του Μεσαίωνα.
[19] Bernard M., Peacock J. & Berrie C. (1997) «*Τεχνολογία παραγωγής εντύπου*», μτφρ. Γ. Χατήρης, Επιμέλεια ελληνικής έκδοσης Καραγιάννης Β., Εκδόσεις Ιων, σελ. 181.
[20] http://www.Computertriti.gr

ώστε το χαρτί να μπορεί να χρησιμοποιηθεί ξανά και ξανά. Αυτή η τεχνολογία, που βρίσκεται ακόμη σε προκαταρκτικό στάδιο, θολώνει τα όρια ανάμεσα στα εκτυπωμένα έγγραφα και την ψηφιακή απεικόνιση και θα μπορούσε τελικά να οδηγήσει σε σημαντική μείωση της κατανάλωσης χαρτιού.

Η πειραματική τεχνολογία εκτύπωσης, μια συνεργασία μεταξύ του Κέντρου Ερευνών της Xerox στον Καναδά και του Κέντρου Ερευνών του Palo Alto, θα μπορούσε να αντικαταστήσει τις εκτυπωμένες σελίδες που χρησιμοποιούνται για μικρό χρονικό διάστημα προτού πεταχτούν στα σκουπίδια. Η Xerox εκτιμά ότι δύο στις πέντε σελίδες που εκτυπώνονται στο γραφείο προορίζονται για αυτό που αποκαλείται 'καθημερινή χρήση', όπως για e-mail, ιστοσελίδες και υλικό αναφοράς που έχει εκτυπωθεί μόνο για μια απλή ανάγνωση.

Η Xerox έχει κατοχυρώσει την ευρεσιτεχνία της τεχνολογίας που αποκαλεί '**το χαρτί που σβήνει μόνο του'**. Αυτή τη στιγμή αποτελεί μέρος ενός εργαστηριακού σχεδίου που εστιάζει στην έννοια των μελλοντικών δυναμικών εγγράφων. Για να αναπτύξουν το χαρτί που σβήνει μόνο του, οι ερευνητές χρειάστηκε να βρουν τρόπους δημιουργίας προσωρινών εικόνων.

Η στιγμή της έμπνευσης ήρθε από την ανάπτυξη συνθέτων που αλλάζουν χρώμα όταν απορροφούν ένα συγκεκριμένο μήκος κύματος φωτός και μετά εξαφανίζονται βαθμιαία. Στην παρούσα εκδοχή του, το χαρτί σβήνει από μόνο του σε περίπου 16-24 ώρες και μπορεί να χρησιμοποιηθεί πολλές φορές.

Η εγγεγραμμένη εικόνα εξαφανίζεται βαθμιαία με φυσικό τρόπο όσο περνάει η ώρα ή μπορεί να σβηστεί αμέσως αν εκτεθεί στη θερμότητα. Ενώ οι υποψήφιοι χρήστες έχουν δείξει ενδιαφέρον για τα προσωρινά έγγραφα, υπάρχουν ακόμα πολλά που πρέπει να γίνουν για να μπορέσει η εν λόγω τεχνολογία να κυκλοφορήσει στο εμπόριο. Τα προσωρινά έγγραφα είναι μέρος των διαρκών επενδύσεων της Xerox στην αειφόρο καινοτομία -ή στα λεγόμενα 'πράσινα προϊόντα'- που επιφέρουν μετρήσιμα οφέλη στο περιβάλλον.

Απ' την άλλη [21]η Fujitsu παρουσίασε το πρώτο '**ηλεκτρονικό χαρτί'**, το οποίο διαθέτει μάλιστα και μνήμη απεικόνισης, ακόμα και όταν δεν τροφοδοτείται με ρεύμα. Το νέο ηλεκτρονικό χαρτί μπορεί να απεικονίσει έγχρωμες εικόνες, οι οποίες παραμένουν ανεπηρέαστες ακόμα και αν αυτό τσαλακωθεί, διπλωθεί ή διακοπεί η τροφοδοσία του με ρεύμα. Ένα επιπλέον χαρακτηριστικό που κάνει το επίτευγμα της Fujitsu πολύ σημαντικό, είναι ότι το ηλεκτρονικό χαρτί που κατασκεύασε είναι χαμηλής κατανάλωσης (καταναλώνει ρεύμα μόνο όταν αλλάζουν τα απεικονιζόμενα στοιχεία) σε τέτοιο σημείο που να είναι δυνατή η τροφοδοσία του από πολύ μικρές μπαταρίες.

Για αυτούς τους λόγους το νέο ηλεκτρονικό χαρτί της Fujitsu θεωρείται ιδανικό για χρήση σε διαφημιστικά φυλλάδια, εφημερίδες, ακόμα και manual που θα ενημερώνονται μόνα τους και αυτόματα από την εταιρεία που τα έχει παραγάγει.

1.2.1δ Ηλεκτρονικό έγγραφο

Ερχόμαστε λοιπόν στη 'μετάλλαξη' του 'κλασικού εγγράφου' στο καλούμενο 'ηλεκτρονικό έγγραφο'. Το ηλεκτρονικό έγγραφο είναι η καρδιά της λεγόμενης κοινωνίας της πληροφορίας και των ολοένα αυξανόμενων κοινωνικοοικονομικών φαινομένων που την συναπαρτίζουν. Έτσι είναι αυτονόητο ειδοποιό χαρακτηριστικό της ηλεκτρονικής επιχείρησης (e-business), της ηλεκτρονικής επικοινωνίας, της ηλεκτρονικά καταρτιζόμενης σύμβασης, του ηλεκτρονικού εμπορίου (e-commerce). Ενίοτε δε καθιερώνεται ως αποκλειστικός νόμιμος τύπος εκτοπίζοντας το παραδοσιακό έγγραφο, όπως π.χ. στις χρηματιστηριακές συναλλαγές.

Ακόμη αποτελεί ολοένα δημοφιλέστερο -συχνά δε αποκλειστικό νόμιμο- μέσο καταχωρίσεων και δημοσιότητας: δικαιώματα επί ακινήτων (άρθρο 101 Ν. 2664/1998), δημοσίων ομολόγων (άρθρα 5, 6 Ν. 2198/1994), εισηγμένων στο χρηματιστήριο μετοχών (άρθρα 41-43, 49 Ν. 2396/ 96, Απόφαση ΔΣ Επιτροπής Κεφαλαιαγοράς 9820/154/16-3-1999, όπως ισχύουν μετά τις μέχρι σήμερα τροποποιήσεις τους), πρωτόκολλα δημοσίων υπηρεσιών τηρούνται υπο-

[21] http://www.e-pcmag.gr/modules/news/article.php?storyid=925

χρεωτικά σε ηλεκτρονικό αρχείο κ.λ.π. Ακόμη σε ηλεκτρονικά αρχεία καταχωρούνται ολοένα και περισσότερα προσωπικά δεδομένα π.χ. αρχεία νοσηλείας των νοσοκομείων, πελατολόγια διαφόρων επαγγελματιών κ.λπ.

Ως εκ τούτου το ηλεκτρονικό έγγραφο αποτελεί το βασικό αντικείμενο του ηλεκτρονικού δικαίου (βλ. αναλυτικότερα Κεφ.4). Τα παραπάνω σημαίνουν ότι **το ηλεκτρονικό έγγραφο δεν είναι αντικείμενο έρευνας μόνο για τον αστικολόγο, αλλά και για τους νομικούς τους ασχολούμενους με τους υπόλοιπους κλάδους του δικαίου**. Ακόμη από τα παραπάνω γίνεται εμφανές ότι για την κοινωνία της πληροφορίας το ηλεκτρονικό έγγραφο δεν αποτελεί μόνο τον εννοιολογικό πυρήνα της προβληματικής του τύπου των δικαιοπραξιών, αλλά και το ειδοποιό σώμα της ηλεκτρονικής δημοσιότητας. Στην περίπτωση που η ηλεκτρονική καταχώριση προβλέπεται ως όρος δημοσιότητας, ηλεκτρονικό έγγραφο, με την έννοια που μας απασχολεί εδώ, αποτελεί η τυχόν προηγούμενη ηλεκτρονική επικοινωνία του ενδιαφερόμενου με το φορέα της καταχώρισης, ενώ η ίδια η καταχώριση θα μπορεί να νοηθεί μόνο ως μορφή δημόσιου ή ιδιωτικού επαγγελματικού βιβλίου.

Στο νόμο δεν απαντάται ορισμός του ηλεκτρονικού εγγράφου. Έτσι ως τέτοιο θα μπορούσε, να νοηθεί με βάση και την κοινή πείρα: «*κάθε έγγραφο που έχει ως ειδοποιό χαρακτηριστικό το ότι δημιουργείται με τη βοήθεια της ηλεκτρονικής τεχνολογίας*».

Δεδομένου, λοιπόν, ότι είναι αδιάφορος ο τρόπος δημιουργίας του λοιπού περιεχομένου του εγγράφου, εκτός από την υπογραφή, είναι προφανές ότι η ειδοποιός διαφορά του ηλεκτρονικού εγγράφου έγκειται μόνο στο μέσο δημιουργίας της υπογραφής του. Γι' αυτό και ο ιστορικός νομοθέτης δεν ομιλεί για ηλεκτρονικό έγγραφο, αλλά για ηλεκτρονικές υπογραφές, ήτοι στο μέσο με το οποίο βεβαιώνεται η αυθεντικότητά του. Με την έννοια αυτή ηλεκτρονικό έγγραφο είναι κατά συνέπεια: «*κάθε έγγραφο του οποίου η υπογραφή παράγεται (εξ ολοκλήρου ή απλώς αποτυπώνεται) με τη βοήθεια της ηλεκτρονικής τεχνολογίας*».

Όπως είναι προφανές, στον ορισμό αυτό περιλαμβάνονται τόσο έγγραφα που έχουν εξ ολοκλήρου ηλεκτρονική υπόσταση όσο και έγγραφα που δεν έχουν μεν καθ' αυτά ηλεκτρονι-

κή, αλλά χάρτινη υπόσταση, όμως το περιεχόμενο και η υπογραφή τους αποτυπώνονται σ' αυτά με τη βοήθεια της ηλεκτρονικής τεχνολογίας. Με βάση το κριτήριο αυτό θα μπορούσε κανείς να διακρίνει ανάμεσα σε **γνήσια ηλεκτρονικά έγγραφα** (έγγραφα με στενή έννοια) και **μη γνήσια**. Η διάκριση δεν στερείται πρακτικής σημασίας, στο μέτρο που η κοινοτική οδηγία 1999/93 και η πράξη προσαρμογής σ' αυτή ρυθμίζουν μόνο το ηλεκτρονικό έγγραφο με στενή έννοια. Πιο συγκεκριμένα:

Γνήσια ηλεκτρονικά έγγραφα

Είναι έγγραφα με ολοκληρωτικά ηλεκτρονική υπόσταση, δηλ. καταχωρήσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό (π.χ. σκληρό δίσκο, δισκέτα, zip, cd κ.λ.π). Φυσικά ούτε του γνησίου ηλεκτρονικού εγγράφου απαντάται ευθέως ρητά ο ορισμός στο νόμο.
Μολαταύτα το άρθρο 2 αρ.1 Οδ.99/93, καθορίζει έμμεσα την έννοια και το περιεχόμενό του, όταν ορίζει τι υπογράφεται με την ηλεκτρονική υπογραφή, η οποία συνιστά το ειδοποιό χαρακτηριστικό του ηλεκτρονικού εγγράφου, σύμφωνα με όσα δείχθηκαν παραπάνω.

Πράγματι το παραπάνω άρθρο ορίζει ότι η ηλεκτρονική υπογραφή θα πρέπει να συνάπτεται με δεδομένα σε ηλεκτρονική μορφή, που θα αποτελούν, λοιπόν, το υπόλοιπο περιεχόμενο του ηλεκτρονικού εγγράφου. Έτσι ως ηλεκτρονικό έγγραφο θα μπορούσε να νοήσει κανείς, και πάλι σύμφωνα και με την κοινή πείρα: «*οποιοδήποτε (υλικό) φορέα καταχωρημένων ηλεκτρονικών δεδομένων*».

Τούτο, καθώς η διάταξη δεν διακρίνει -και ορθά- αν τα δεδομένα αυτά θα είναι καταχωρημένα σε σκληρό δίσκο, cd, zip, μικροτσίπ ή δισκέτα, άλλωστε αυτό δεν θα διαφοροποιούσε κατά τίποτε ούτε τη φύση του πράγματος, ούτε την ταυτότητα του σκοπού της ρύθμισης.

Παρεμφερής, αλλά κάπως στενότερος ο ορισμός που φαίνεται να υιοθετεί ο καθηγητής Νομικής του Πανεπιστημίου Αθηνών Κουσούλης Σ., που όμως συμπεριλαμβάνει στην έννοια του ηλεκτρονικού εγγράφου και το αποτέλεσμα της επεξεργασίας των καταχωρισμένων στο μαγνητικό υλικό ηλεκτρονικών δεδομένων, με αποτέλεσμα η έννοια του γνήσιου ηλεκτρονι-

κού εγγράφου να διολισθαίνει και πάλι στο -διακριτό και από τον ίδιο τον Κουσούλη παραδοσιακό χάρτινο έγγραφο.

Σήμερα ο ίδιος ταυτίζει το e-γγραφο με το print-out, που ισοδυναμεί όμως με computerfax. Ακόμη στενότερος ο ορισμός του ηλεκτρονικού εγγράφου που υιοθετεί η Μιχαηλίδου Χ., ο οποίος και μετυιοθετήθηκε τελικά σχεδόν αυτούσιος και από την (πρώτη ad hoc ελληνική δικαστική απόφαση) Μον. Πρωτ. Αθ 1327/2000, Δ 32, σελ. 445επ.:

«*Ως ηλεκτρονικό έγγραφο (σ.σ. προφανώς με στενή έννοια) θεωρείται το σύνολο των εγγραφών δεδομένων στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή, τα οποία, αφού γίνουν αντικείμενο επεξεργασίας, αποτυπώνονται με βάση τις εντολές του προγράμματος κατά τρόπον αναγνώσιμο από τον άνθρωπο στην οθόνη του μηχανήματος είτε στον προσαρτημένο εκτυπωτή του*».

Ο ορισμός αυτός είναι αδικαιολόγητα διττά στενότερος του υπαγορευόμενου από την Οδ.99/93: Πρώτον κατά το είδος του υλικού φορέα (αποκλειστικά σκληρός δίσκος) και δεύτερον, επειδή προαπαιτεί αδικαιολόγητα να έχει εκτυπωθεί το περιεχόμενο του ηλεκτρονικού εγγράφου ή να έχει προβληθεί σε οθόνη Η/Υ με τη μορφή κειμένου.

Κι όμως είναι πιθανόν να λάβει κάποιος ένα ηλεκτρονικό μήνυμα δήλωση, χωρίς να θελήσει ποτέ να το εμφανίσει στην οθόνη του. Στην περίπτωση αυτή η λογικά συνεπής εφαρμογή του εδώ αποκρουόμενου ορισμού θα σήμαινε ότι η μονομερής τυπική ηλεκτρονική έγγραφη δήλωση που περιήλθε στο λήπτη δεν υπήρξε ποτέ.

Φυσικά το παραπέρα ζήτημα, δηλαδή αν θα συμπεριλάβει κανείς στην έννοια του ηλεκτρονικού εγγράφου και την ηλεκτρονική υπογραφή του, εξαρτάται από τη θέση που θα λάβει στο γενικότερο δογματικό πρόβλημα αν η υπογραφή είναι στοιχείο της υπόστασης ή του κύρους ή του παραδεκτού του εγγράφου.

Μη γνήσια ηλεκτρονικά έγγραφα

Μη γνήσια ηλεκτρονικά έγγραφα ορίζονται ως: [22]«*τα χάρτινα έγγραφα με περιεχόμενο και υπογραφή ηλεκτρονικά αποτυπωμένα σ' αυτά»* όπως λ.χ. το τηλεομοιότυπο (fax) και το τηλέτυπο (telex).

Τα μειονεκτήματα όμως που παρουσιάζουν γενικά τα ηλεκτρονικά έγγραφα δεν είναι και λίγα λ.χ. **στερούνται της σταθερότητας κατά την ενσωμάτωσή τους και μπορεί να υποστούν μετατροπές, αλλοιώσεις ή διαγραφές** που είναι δύσκολο αν όχι αδύνατον να εντοπιστούν, αλλά και ότι δεν διαθέτουν την ιδιόχειρη υπογραφή που είναι απαραίτητη στα έγγραφα όπου ο τύπος είναι συστατικός. Επιπλέον, όταν διακινούνται μέσω ανοικτών δικτύων, κίνδυνος να υποκλαπούν από τρίτους και να αλλοιωθεί ή τροποποιηθεί το περιεχόμενό τους.

Απαιτείται, συνεπώς, η ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών και προς τούτο χρησιμοποιούνται μέθοδοι κρυπτογράφησης που εξασφαλίζουν την ασφαλή μεταφορά δεδομένων Η/Υ μέσω ανοιχτών δικτύων, αλλά και η τεχνολογία της ηλεκτρονικής υπογραφής για την εξασφάλιση της γνησιότητας των εγγράφων που διακινούνται ηλεκτρονικά.

1.2.2 Γενικές Παρατηρήσεις

Ανακεφαλαιώνοντας τα όσα διατυπώθηκαν σχετικά με το έγγραφο ως βασικό συστατικό στοιχείο του εγκλήματος της πλαστογραφίας, ήμαστε πλέον σε θέση να φωνάξουμε και να τρομάξουμε μπροστά στην ευρύτητα που παρουσιάζει η έννοια 'έγγραφο'. Παράμετροι όπως π.χ. οι πινακίδες αυτοκινήτων, οι μαγνητοταινίες κ.λ.π. έμειναν ανέγγιχτες, βάσει των περιορισμών που επιβάλλει η έκταση μιας μεταπτυχιακής εργασίας.

Ήταν σχεδόν αδύνατο να συμπεριλάβουμε αναλύσεις που να αφορούν τις τεχνολογικές αλλαγές που έχουν υποστεί οι άλλοι παράμετροι, πλέον του 'κλασικού εγγράφου'. Έπρεπε να περιορισθούμε, γι' αυτό και σταθήκαμε στο συχνότερα συναλλασσόμενο τύπο εγγράφου, το

[22] Χριστοδούλου Κ. (2001)«*Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία*», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, σελ. 5.

‘κλασικό έγγραφο’, μελετώντας τις αλλαγές που έχουν επισυμβεί σε αυτό και οδηγούν στην έννοια του ‘ηλεκτρονικού εγγράφου’.

Αυτή η εξέλιξη (είτε λογίζεται ως θετική είτε ως αρνητική) δεν αποτελεί ένα ανεξάρτητο φαινόμενο, σε σχέση με όσα συμβαίνουν στο χώρο του εγκλήματος. Τα εγκλήματα ‘μεταμορφώνονται’ -μεταξύ άλλων παραγόντων- γιατί αλλάζουν τα συστατικά στοιχεία αυτών. Έτσι και για το έγκλημα της πλαστογραφίας είναι φυσικό και αναπόφευκτο να δημιουργηθούν κάποιες νέες μορφές που θα επιχειρήσουμε να συγκεντρώσουμε παρακάτω, πλην όμως πρέπει να έχουμε προκαταβολικά υπόψιν ότι οι τεχνολογικές εξελίξεις τρέχουν με γοργούς ρυθμούς, ενώ ο δύσμοιρος ερευνητής, στην περίπτωσή μας η συντάκτρια, πρέπει τακτικά να ‘παγώνει’ το χρόνο, ούτως ώστε να μπορεί να καταγράφει τα περισσότερα ελπίζουμε από τα τεκταινόμενα.

Η συγκέντρωση των πληροφοριών και η καταγραφή αυτών σε σχέση με το υπό διαπραγμάτευση θέμα απαιτεί ένα συμβιβασμό, που αρχικά δεν ήταν ορατός, ότι δηλαδή δεν είναι εφικτό να συμπεριληφθεί το σύνολο των νέων μορφών που παρουσιάζει το ‘παραδοσιακό’ έγκλημα της πλαστογραφίας, με τη λογική ότι συνεχώς γεννιούνται νέες μορφές.

Σχετικά με το θέμα ‘παραδοσιακών’ **Vs** ‘νέων’ μορφών εγκληματικότητας (ήτοι ηλεκτρονικό έγκλημα), θα λέγαμε ότι γενικότερα έχουν αναπτυχθεί διάφορες απόψεις, όπως ότι: [23]α) Το ηλεκτρονικό έγκλημα δεν υπάρχει ως αυτόνομη κοινωνική πραγματικότητα. Ο Douglas Reimer τονίζει ότι τα πληροφορικά εγκλήματα δεν είναι νέα εγκλήματα, είναι τα ίδια παλιά εγκλήματα που διαπράττονται με νέους και εφευρετικούς τρόπους που η υψηλή τεχνολογία των σύγχρονων υπολογιστών και τηλεπικοινωνιών καθιστά δυνατούς,

β) Το ηλεκτρονικό έγκλημα είναι μια νέα μορφή εγκληματικότητας, με συγκεκριμένα ποιοτικά χαρακτηριστικά &

γ) Στο διαδίκτυο αντανακλούνται οι κοινωνικές παθολογίες άρα αναπαράγονται οι παραδοσιακές μορφές εγκληματικότητας (με άλλα μέσα) αλλά ταυτόχρονα διαμορφώνονται οι προϋπο-

[23] Αρτινοπούλου Β. «*Ηλεκτρονικό Έγκλημα και Θυματοποίηση*» Ict Forum, Αθήνα 29-10-2007.

θέσεις για νέες μορφές εγκληματικότητας με σαφή ποιοτικά χαρακτηριστικά, μορφές εγκλημάτων που διαπράττονται αποκλειστικά στον κυβερνοχώρο (συνθετική άποψη)

Δεν είναι κρίσιμο ο αναγνώστης να ασπασθεί μία από τις παραπάνω απόψεις, άλλωστε είναι πολύ νωρίς, αφού ακόμα δεν έχουν παρουσιαστεί οι έννοιες όπως ηλεκτρονικό, ψηφιακό, πληροφορικό έγκλημα, έγκλημα στον κυβερνοχώρο. Ο λόγος που παρατέθηκαν οι προαναφερόμενες απόψεις είναι προκειμένου να θέσουμε μι βάση προβληματισμού και κριτικής θεώρησης όσων θα ακολουθήσουν. Με κομμένη λοιπόν την ανάσα προχωρούμε.

..//..

ΚΕΦΑΛΑΙΟ 2.

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ - ΠΛΑΣΤΟΓΡΑΦΙΑ & ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

2.1 Νέες τεχνολογίες - Διαδίκτυο

Εισαγωγή

Όπως έχει υποστηριχθεί, η σημαντικότερη εξέλιξη στο δεύτερο ήμισυ του 20ου αιώνα, υπήρξε η ραγδαία και πολύπλευρη ανάπτυξη της τεχνολογίας. Η επανάσταση που έφεραν οι νέες τεχνολογίες στις μεταφορές και τις επικοινωνίες, οδήγησε στη σχετικοποίηση των χωροχρονικών αποστάσεων, στο μετασχηματισμό της καπιταλιστικής παραγωγής, και στην παγκοσμιοποίηση της πολιτικής και κοινωνικής ζωής. Ειδικότερα, η εξάπλωση των ΜΜΕ και του Διαδικτύου διαμόρφωσαν μία νέα σχέση ανάμεσα στο χρόνο και το χώρο. Καθώς ο χρόνος της επικοινωνίας καταρρέει και συρρικνώνεται στο μηδενικό μέγεθος του στιγμιαίου, τα σημάδια του χώρου και του χρόνου παύουν να έχουν σημασία.

Σε αυτό που ονομάζεται *ψηφιακή κοινωνία* η πληροφορία κυκλοφορεί εφεξής ανεξάρτητα από τους φορείς της. Οι έννοιες του 'τοπικού' και του 'παγκόσμιου' συνδυάζονται πλέον με τρόπους αδιανόητους όχι μόνο για τις παραδοσιακές μορφές κοινωνικής ζωής, αλλά και για την ίδια την νεωτερική κοινωνία. Η σχετικοποίηση του χώρου και του χρόνου μέσα από τις νέες τεχνολογίες έχει άμεση επίδραση στην οικονομική ζωή, καθώς επιτρέπει τη χωρική διάσπαση των διαδικασιών έρευνας, παραγωγής και διάθεσης αγαθών και υπηρεσιών, αλλάζει την οργάνωση. Παράλληλα η ανάπτυξη της πληροφορικής καθώς και το Διαδίκτυο έχουν επιφέρει πρωτόγνωρες αλλαγές στην παραγωγική διαδικασία, στις εργασιακές σχέσεις, στις συναλλαγές και σε κάθε εκδήλωση της καθημερινότητας.

Η βάση των νέων τεχνολογιών της κοινωνίας αυτής είναι αναμφισβήτητα, το **Διαδίκτυο**. Πως όμως φτάσαμε εδώ; Το 1965, ο Theodore Holme Nelson, ανέπτυξε ένα σύστημα που φύλασσε και συνδύαζε μεγάλο αριθμό δεδομένων, παρέχοντας γρήγορη πρόσβαση σε μία επιζη-

τούμενη κατηγορία από αυτά. Υλοποίησε έτσι μια πρώτη μορφή υπερκειμένου (hypertext), άλλωστε ήταν ο ίδιος ο Nelson που διατύπωσε τον όρο hypertext. Έκτοτε, οι κόμβοι (nodes) και οι σύνδεσμοι (links) που συνέλαβε ο Nelson πήραν πρόσθετες διαστάσεις με την διασύνδεση πολλών ακόμα κατηγοριών υλικού (φωτογραφιών, σχεδίων κ.λ.π.), μεταβάλλοντας την λογική του hypertext, σε hypermedia.

Το Διαδίκτυο αποτελεί πλέον την κύρια 'μηχανή' με την οποία τα άτομα επικοινωνούν μεταξύ τους ταχύτερα και πιο άνετα, από ποτέ. Τα πάντα μπορούν να γίνουν με το πάτημα ενός κουμπιού του πληκτρολογίου του προσωπικού υπολογιστή ή με το κλικ του ποντικιού του, η φυσική παρουσία δεν είναι απαραίτητη όταν κάποιος λ.χ. θέλει να ψωνίσει, να ψάξει για πληροφορίες, αλλά και να συνομιλήσει με κάποιον άλλο. Η ανάπτυξη του Παγκόσμιου Ιστού (World Wide Web) έχει κάνει τη διάδοση των πληροφοριών κτήμα του καθενός και μάλιστα, σε ελάχιστο, χρόνο.

Στις <u>θετικές πλευρές</u> του Διαδικτύου περιλαμβάνεται κυρίως η διαπίστωση ότι αυτό αποτελεί μια τεράστια πηγή χρήσιμων πληροφοριών. Η σωστή χρήση του μπορεί να ανεβάσει το μορφωτικό επίπεδο των χρηστών του προσφέροντάς τους επίκαιρα στοιχεία από όλους τους τομείς της σύγχρονης γνώσης.

Αναρωτιέται όμως κανείς για το αν υπάρχουν και <u>μειονεκτήματα</u>. Η απάντηση είναι απλή, ασφαλώς και υπάρχουν. Δυστυχώς οι νέες τεχνολογίες και κυρίως το Διαδίκτυο μεταξύ άλλων δημιουργεί [24]κοινωνικές διακρίσεις, χωρίζοντας και διαιρώντας τα μέλη των σημερινών ψηφιακών κοινωνιών σε **ψηφιακά εγγράμματα** μέλη και **ψηφιακά αγράμματα**, ενώ παράλληλα διαμορφώνει ιδανικές συνθήκες για την **καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας**.

Όσον αφορά την ανάπτυξη νέων μορφών εγκληματικότητας, ενδεικτικά θα λέγαμε ότι ένα κλασικό μειονέκτημα και συγχρόνως λειτουργικό πρόβλημα του Διαδικτύου είναι η **ασφάλεια των πληροφοριών του** δηλ. η προστασία του περιεχομένου τους από οποιεσδήποτε

[24] Τσουραμάνης Χ. «*Ψηφιακή κοινωνία, ψηφιακή εγκληματικότητα και θυματοποίηση*» (http://www.teimes.gr/spoudastirio/yifiaki_eglimatikotita.doc).

αλλοιώσεις και καταστροφές που προέρχονται από μη εξουσιοδοτημένη χρήση των πόρων του.

Ένα πληροφοριακό σύστημα για να είναι ασφαλές θα πρέπει να διαθέτει: α) εμπιστευτικότητα, β) ακεραιότητα & γ) διαθεσιμότητα. Η απουσία των παραπάνω ιδιοτήτων ενός πληροφοριακού συστήματος το καθιστά ανασφαλές και σχετίζεται με την εγκληματικότητα που αναπτύσσεται στους κόλπους του. Στην περίπτωση αυτή μπορούμε να κάνουμε λόγο για **ψηφιακή εγκληματικότητα**, λαμβάνοντας υπόψη το γεγονός ότι για την εκδήλωσή της, αλλά και για την αντιμετώπισή της είναι απαραίτητη η γνώση της ψηφιακής τεχνολογίας και ιδίως αυτής που σχετίζεται με το Διαδίκτυο.

2.1.1 Ηλεκτρονικό - Ψηφιακό έγκλημα

[25]Το **ηλεκτρονικό έγκλημα** συνιστά μια ειδικότερη μορφή του κοινού εγκλήματος, όπως αυτό προσδιορίζεται στο άρθρο 14 Π.Κ. Σαν όρος αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων, μεταξύ άλλων εμπίπτουν σε αυτό και τα **εγκλήματα στον κυβερνοχώρο** (Cyber Crimes).

Σε μια προσπάθεια εννοιολογικού προσδιορισμού, θα λέγαμε ότι ως ηλεκτρονικό έγκλημα μπορεί να οριστεί: «[26]*αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών*», ενώ ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί «[27]*κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων*». Σημειώνεται ότι ο ορισμός αυτός διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΟΣΑ, που συνεστήθη ειδικώς για να εξετάσει το θέμα της

[25] Αγγελής Ι. «*Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη*» (http://www.lawnet.gr/pages/eofn/2/cybercrime.asp).
[26] Γιαννόπουλος Θ. (1986) «*Όψεις και Προβλήματα Ηλεκτρονικής Εγκληματικότητος*», Νομική Βιβλιοθήκη, σελ. 170επ.
[27] Μυλωνόπουλος Χρ. «*Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο*», Σειρά ΠΟΙΝΙΚΑ, Νο 33, σελ. 14.

ηλεκτρονικής εγκληματικότητας. Ο ορισμός αυτός βέβαια είναι πολύ ευρύς και είναι ευνόητο ότι μόνο ως οδηγός μπορεί να χρησιμοποιηθεί. Η οριστικοποίησή του επαφίεται στον εθνικό νομοθέτη και στη νομολογία των δικαστηρίων.

Λαμβάνοντας υπόψη τα παραπάνω και σε μια εκ νέου διείσδυση στον ωκεανό των εννοιών, απομονώνουμε αυτή του **ψηφιακού εγκλήματος** (digital crime), που τελικά -εξαιτίας της ευρύτητας που φαίνεται να τη χαρακτηρίζει- εξυπηρετεί καλύτερα κάποιες φορές τις ανάγκες της παρούσας μελέτης. Ψηφιακό έγκλημα λοιπόν μπορεί να θεωρηθεί «*κάθε παράνομη πράξη για τη διάπραξη, αλλά και για την αντιμετώπιση της οποίας απαιτείται η γνώση της ψηφιακής τεχνολογίας».* Το σύνολο επομένως, των ψηφιακών εγκλημάτων που τελούνται στον κυβερνοχώρο (cyberspace) συνιστούν την **ψηφιακή εγκληματικότητα** (digital criminality).

Εύλογος προκύπτει ο προβληματισμός τι διαφοροποιεί τα ψηφιακά εγκλήματα από τα παραδοσιακά εγκλήματα και απαιτεί την 'απομόνωσή' τους σε ειδική κατηγορία; Καταρχήν για την τέλεσή τους απαιτούνται άριστες και εξειδικευμένες γνώσεις, ενώ θεωρούνται πιο προηγμένα (ανεβασμένα) και από τα εγκλήματα του λευκού περιλαιμίου[28]. Επιπλέον τα ψηφιακά εγκλήματα περιλαμβάνουν τα εξής χαρακτηριστικά:

- διαπράττονται συνήθως από μακρινή απόσταση,
- ο εντοπισμός του ψηφιακού εγκληματία είναι τεχνολογικά περίπλοκος,
- αποδίδουν μεγάλα κέρδη με μικρό κίνδυνο ανακάλυψης του δράστη τους, ενώ ο αριθμός των θυμάτων τους συγκρινόμενος με εκείνο των παραδοσιακών εγκλημάτων είναι κατά πολύ μεγαλύτερος,
- οι οικονομικές απώλειες που προξενούνται στα 'ψηφιακά θύματα' είναι πολύ μεγαλύτερες από εκείνες των θυμάτων των παραδοσιακών εγκλημάτων και
- στο μεγαλύτερο μέρος τους δεν καταγράφονται από καμία επίσημη αρχή δηλ. ο 'σκοτεινός αριθμός' τους είναι ιδιαίτερα σημαντικός.

[28] Για τη σχέση του εγκληματία του κυβερνοχώρου και του εγκληματία του λευκού περιλαιμίου βλ. Αγγελής Ι. (2000), «Διαδίκτυο και Ποινικό Δίκαιο», Ποιν. Χρον., σελ. 678

Τα τρία δε τελευταία από τα παραπάνω χαρακτηριστικά πιστεύουμε ότι κατατάσσουν τα ψηφιακά εγκλήματα στο χώρο των **οικονομικών εγκλημάτων**. **'**Τόπος' τέλεσης τώρα των εν λόγω εγκλημάτων είναι ο αποκαλούμενος **κυβερνοχώρος**, ο οποίος προσδιορίζεται ως «*το σύνολο των ηλεκτρονικών κόσμων, όπως το Διαδίκτυο, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών. Καθοριστικό χαρακτηριστικό του κυβερνοχώρου είναι ότι η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση».*

*****

Ποια είναι όμως ακριβώς τα ψηφιακά εγκλήματα, που καταστρέφουν την καλή εικόνα της *ψηφιακής κοινωνίας* και του Διαδικτύου; Πως κατηγοριοποιούνται; Που εντάσσεται το έγκλημα της πλαστογραφίας; Στα ερωτήματα αυτά θα προσπαθήσουμε να απαντήσουμε στη συνέχεια.

2.1.2 Κατηγοριοποίηση ψηφιακών εγκλημάτων

Στη σημερινή εποχή παρατηρείται μεγάλη αύξηση των ψηφιακών εγκλημάτων και γενικά της ψηφιακής εγκληματικότητας, η οποία είναι ανάλογη με την συνεχώς αυξανόμενη χρήση του Διαδικτύου. Ανάλογη είναι και η ποικιλία των μορφών των διαφόρων ψηφιακών εγκλημάτων.

Σχετικά με την κατηγοριοποίηση των ψηφιακών εγκλημάτων, θα πρέπει να σημειώσουμε πως δεν παρατηρείται ομοφωνία μεταξύ των διαφόρων συγγραφέων που ασχολούνται με τον προσδιορισμό τους.

Σύμφωνα με την άποψη του Διδάκτωρος της Νομικής Σχολής του Δημοκρίτειου Παν/μιου Θράκης στην Εγκληματολογία Τσουραμάνη Χρ., [29]τα ψηφιακά εγκλήματα, θα μπορούσαν να χωριστούν σε δύο μεγάλες κατηγορίες με κριτήριο **τα μέσα τέλεσης και εξιχνίασής τους**. Πιο συγκεκριμένα:

[29] Τσουραμάνης Χρ. όπ. παρ.

- Τα **γνήσια** ψηφιακά εγκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, αποκλειστικά και μόνο με τη χρήση της ψηφιακής τεχνολογίας. Στην κατηγορία αυτή μπορούν να υπαχθούν:

  α) Η χωρίς νόμιμη εξουσιοδότηση είσοδος σε Η/Υ (hacking), **β**) Η κλοπή, η παραποίηση και η καταστροφή αρχείων Η/Υ, **γ**) Η προσωρινή ή οριστική διακοπή της λειτουργίας συστήματος Η/Υ που αποτελεί συνέπεια της λεγόμενης 'επίθεσης άρνησης παροχής υπηρεσιών', **δ**) Η διασπορά κακόβουλων προγραμμάτων ιών (virus), σκουληκιών (worms), Δούρειων Ίππων (Trojans) κ.λ.π. & **ε**) Η πειρατεία λογισμικού δηλ. προγραμμάτων Η/Υ που αφορά την παράνομη αντιγραφή τους και τη στη συνέχεια διάθεσή τους στην αγορά -και μέσω του Διαδικτύου- σε πολύ χαμηλότερη τιμή από εκείνη του πρωτοτύπου.

- Τα **παραδοσιακά ε**γκλήματα τα οποία τελούνται αλλά και εξιχνιάζονται, τόσο με την υποστήριξη της ψηφιακής τεχνολογίας, όσο και χωρίς τη βοήθειά της. Στη δεύτερη αυτή κατηγορία μπορούν να υπαχθούν:

  α) Διάφορα κοινά εγκλήματα. Σαν τέτοια μπορούμε να θεωρήσουμε π.χ. την κλοπή ενός Η/Υ, τμημάτων του κ.λ.π., εγκλήματα που τελούνται με τη βοήθεια του ηλεκτρονικού ταχυδρομείου ή ιστοσελίδων, όπως απάτες, εξυβρίσεις, εκβιασμοί κ.λ.π. επίσης οι προσβολές της πνευματικής ιδιοκτησίας, οι ανταλλαγές πληροφοριών μέσω του ηλεκτρονικού ταχυδρομείου μεταξύ τρομοκρατικών οργανώσεων αλλά και συμμοριών του κοινού ποινικού δικαίου καθώς και το ηλεκτρονικό ξέπλυμα βρώμικου χρήματος**, β**) Η κατασκοπεία είτε αυτή χαρακτηρίζεται σαν βιομηχανική ή σαν κρατική ή σαν πολιτική, **γ**) Οι υποκλοπές τηλεφωνικών συνομιλιών που έχουν σαν συνέπεια την προσβολή του προσωπικού απορρήτου των συνομιλούντων, **δ**) [30]Η δημιουργία πλαστών εγγράφων & **ε**) Περιπτώσεις σεξουαλικής κακοποίησης όπου η γνωριμία έγινε μέσω Διαδικτύου κ.λ.π.

[30] Ομιλία με θέμα «*Το έγκλημα παραμένει έγκλημα ακόμα και όταν πραγματοποιείται ηλεκτρονικά*» των: Παπαντωνίου Αντωνίου και Σερκετζή Νικολάου, του Τμήματος Ηλεκτρονικού Εγκλήματος Θεσσαλονίκης (http://www.ekato.org/gr/Conference_Speeches/ANTONIS_PAPANTONIOY.pdf).

Σύμφωνα πάλι με την άποψη της καθηγήτριας του Παντείου Πανεπιστημίου Αρτινοπούλου Β., [31]τα εγκλήματα που διαπράττονται στο Διαδίκτυο, μπορούν να διακριθούν: σε εγκλήματα κατά των ατομικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον των περιουσιακών αγαθών.

Πέραν των όποιων κατηγοριοποιήσεων τα συνηθέστερα εγκλήματα που τελούνται μέσω Διαδικτύου είναι κυρίως:

- Απάτη - Πλαστογραφία
- Παραβίαση Δεδομένων Προσωπικού Χαρακτήρα (Ν. 2472/97). Περιλαμβάνει τις περιπτώσεις κατά τις οποίες προβάλλονται ή χρησιμοποιούνται μέσω του Διαδικτύου στοιχεία προσωπικών δεδομένων τρίτων προσώπων, χωρίς να υπάρχει η ρητή συγκατάθεσή τους.
- Παραβίαση Απορρήτων.
- Αφορά τις περιπτώσεις μη εξουσιοδοτημένης πρόσβασης σε λογαριασμούς ηλεκτρονικού ταχυδρομείου, ή σε ξένα υπολογιστικά συστήματα. Το γεγονός αυτό μπορεί να επιτευχθεί είτε με χρήση τεχνικών παραβίασης της ασφάλειας του υπολογιστικού συστήματος (Hacking - Cracking), είτε με οποιοδήποτε άλλο τρόπο απόκτησης των κωδικών πρόσβασης.
- Πνευματική Ιδιοκτησία (Ν. 2121/1993) Στη χώρα μας ο όρος Πνευματική Ιδιοκτησία είναι συνυφασμένος με τη μουσική και τις κινηματογραφικές ταινίες. Στην πραγματικότητα εκτός από τους παραπάνω τομείς, στο Διαδίκτυο υπάρχει έντονη πειρατεία στο λογισμικό Η/Υ (παιχνίδια και προγράμματα), στα παιχνίδια για κονσόλες (Playstation κτλ).
- Εγκλήματα κατά της τιμής και της αξιοπρέπειας. Αφορά την δημοσίευση δυσφημιστικού ή εξυβριστικού κειμένου ή φωτογραφιών. Οι περιπτώσεις αυτές πραγματοποιούνται ως πράξεις αντεκδίκησης κατά κύριο λόγο μέσω του Διαδικτύου, καθώς επίσης και μέσω κινητών τηλεφώνων.

[31] Αρτινοπούλου Β. (2007) όπ. παρ.

- Διακίνηση υλικού παιδικής πορνογραφίας, που αποτελεί μία από τις σημαντικότερες μορφές ψηφιακών εγκλημάτων.

Συγχρόνως υπάρχουν και άλλες μικρότερης συχνότητας περιπτώσεις ηλεκτρονικών εγκλημάτων, όπως: Παράνομος Τζόγος, Εμπορία Ανθρώπων, Εμπορία Ναρκωτικών, Εμπορία Ανθρωπίνων Οργάνων και Ιστών, Εμπορία Όπλων, Κυβερνοτρομοκρατία κ.λ.π.

[32]Δυστυχώς δεν υπάρχουν επαρκή στατιστικά στοιχεία ακόμη, όχι μόνο στον ελληνικό, αλλά και στο διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται, και αυτό για να μην πλήττεται το κύρος κυρίως των εταιρειών που τυγχάνουν θύματα τέτοιων επιθέσεων. Κατά συνέπεια, οι διαστάσεις της εγκληματικότητας στο χώρο του Διαδικτύου είναι πιο δύσκολο να καθοριστούν από ότι στον 'κοινό' εγκληματικό χώρο (θεωρία του παγόβουνου).

2.2 Ηλεκτρονική πλαστογραφία και χρήση νέων τεχνολογιών

Λαμβάνοντας υπόψη αφενός όλα όσα ειπώθηκαν στην προηγούμενη ενότητα, αφετέρου τον κύριο άξονα ανάπτυξης της παρούσας μελέτης που δεν είναι άλλος από το έγκλημα της πλαστογραφίας, η ενότητα αυτή θα διαρθρωθεί ως εξής:

Αρχικά θα αναπτυχθεί το έγκλημα της απάτης μέσω Διαδικτύου, διότι όπως κρίνουμε η συγκεκριμένη αναφορά θα φανεί ιδιαιτέρως χρήσιμη, με βάση και τα όσα έχουν διατυπωθεί στο Κεφάλαιο 1.1.3 για τη συχνή συρροή απάτης και πλαστογραφίας. Στόχος να γίνει αντιληπτή η διαχωριστική και άλλοτε γραμμή σύνδεσης των δύο αυτών εγκλημάτων, αλλά κυρίως να διαμορφωθεί κατά το δυνατό πλήρη εικόνα περί του εξεταζόμενου εγκλήματος της πλαστογραφίας.

Στη συνέχεια θα ασχοληθούμε αποκλειστικά με την πλαστογραφία και πιο συγκεκριμένα θα αναφερθούμε στη διάπραξη πλαστογραφίας μέσω του Διαδικτύου και ευρύτερα με τη χρήση-υποστήριξη της ψηφιακής τεχνολογίας.

[32] Ζάννη Αν. (2005) «*Το διαδικτυακό έγκλημα*», Αθήνα, Εκδόσεις Σάκκουλα, σελ. 63, 64.

2.2.1 Το έγκλημα της απάτης

Με το νόμο 1805/1988 προστέθηκε στον Π.Κ το άρθρο 386α[33], 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 ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίησης μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο τιμωρείται…*».

Η διάταξη αυτή διατυπώθηκε [34]σχεδόν κατ' αντιγραφή της αντίστοιχης παραγράφου 263a του γερμανικού ποινικού κώδικα, με σκοπό να καλύψει τα κενά εφαρμογής των διατάξεων της κλασικής απάτης, ενόψει των προσβολών της περιουσίας με τη χρήση Η/Υ, στις οποίες δεν παρεισφρύει παραπλάνηση ανθρώπου. Ας δούμε όμως ορισμένες από τις πλέον διαδεδομένες απάτες μέσω του Διαδικτύου:

- Η απάτη με τα Νιγηριανά μηνύματα του ηλεκτρονικού ταχυδρομείου (**Nigerian e-mail fraud**). Στην περίπτωση αυτή το υποψήφιο θύμα λαμβάνει ένα e-mail με το οποίο ο απατεώνας του υπόσχεται μεγάλη χρηματική αμοιβή αν τον βοηθήσει να μεταφέρει χρήματα από τον τραπεζικό του λογαριασμό στο λογαριασμό του θύματος. Οι λόγοι τους οποίους επικαλείται ο απατεώνας για τη μεταφορά αυτή ποικίλλουν, συνήθως όμως αφορούν γνωστούς διπλωμάτες, επιχειρηματίες ή γόνους πλουσίων οικογενειών που θα πρέπει να εγκαταλείψουν τη χώρα τους εξαιτίας πολιτικών συγκρούσεων. Προτού όμως το θύμα εισπράξει το χρηματικό ποσό που του υποσχέθηκε ο απατεώνας, θα πρέπει να καταβάλει ορισμένα χρήματα για τα έξοδα μεταφοράς ή να δώσει για το λόγο αυτό τα στοιχεία του τραπεζικού του λογαριασμού. Εννοείται ότι στην πρώτη περί-

[33] βλ. ΑΠ 1277/1998 Ποιν. 1999.113 η οποία δέχθηκε ότι η απάτη με ηλεκτρονικό υπολογιστή (άρθρο 386α Π.Κ.) είναι «διαφορετικό έγκλημα» από την απάτη (άρθρο 386 Π.Κ.). Στην εν λόγω απόφαση, ο Άρειος Πάγος διαχώρισε το άρθρο 386 Π.Κ. από το άρθρο 386 *Α* Π.Κ. 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 386 *Α* Π.Κ. η ξένη περιουσία βλάπτεται, ασχέτως παραπλανήσεως, με την αθέμιτη επέμβαση στην πορεία επεξεργασίας των δεδομένων υπολογιστή. Βλ. επίσης, ΑΠ 1152/1999 Ποιν. 2000.141, όπου τονίζεται ότι το έγκλημα του άρθρου 386α Π.Κ. τελείται αποκλειστικά και μόνο με το επηρεασμό των στοιχείων του υπολογιστή, δηλαδή με την επέμβαση του δράστη κατά τον προγραμματισμό του συστήματος και την επεξεργασία των δεδομένων, σε οποιαδήποτε φάση 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. Βλ. επίσης, Κουράκης, Ν. & Πατεράκης Ν. (2001) «*Το έγκλημα της απάτης»,* Νομική Βιβλιοθήκη, σελ. 209.

[34] Βασιλάκη Ειρ. (1993) «*Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών*», Εκδόσεις Αντ. Ν. Σάκκουλα, σελ. 201 επ.

πτωση αμέσως μετά την αποστολή των χρημάτων θα διακοπεί η επικοινωνία με τον απατεώνα, ενώ στη δεύτερη το θύμα είναι πολύ πιθανό να χάσει όλα τα χρήματα του τραπεζικού του λογαριασμού. Φυσικά υπάρχει και το ενδεχόμενο με τον τρόπο αυτό ο απατεώνας έχοντας στη διάθεσή του τα στοιχεία της ταυτότητας του θύματος να το χρεώσει στη συνέχεια, με μεγάλα χρηματικά ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης και '419' από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

- Η απάτη με το **phishing mail**[35]. Στην περίπτωση αυτή ο απατεώνας προσπαθεί μέσω των μηνυμάτων που στέλνει, να αποσπάσει από το θύμα προσωπικά του οικονομικά δεδομένα, όπως τα στοιχεία της πιστωτικής του κάρτας ή του τραπεζικού του λογαριασμού. Στην αρχή το υποψήφιο θύμα λαμβάνει ένα e-mail, αποστολέας του οποίου φαίνεται να είναι η τράπεζά του. Με αυτό του ζητείται να επιβεβαιώσει το username και το password του τραπεζικού του λογαριασμού που διακινεί μέσω του Διαδικτύου (Web banking). Η σχετική αιτιολογία αναφέρεται σε προβλήματα στους Η/Υ της τράπεζας ή σε υποψίες ότι ο συγκεκριμένος λογαριασμός έχει ήδη παραβιασθεί και αν δεν γίνει η επιβεβαίωση, θα κλειδωθεί. Το e-mail αυτό έχει σύνδεσμο προς το δικτυακό τόπο της τράπεζας, ο οποίος όμως δεν είναι πραγματικός και μιμείται απλά τον αυθεντικό και έτσι το θύμα στέλνει τα στοιχεία που του έχουν ζητηθεί κατευθείαν στον απατεώνα.
- Άλλος τρόπος ψηφιακής απάτης είναι εκείνος που αφορά τη λήψη από το υποψήφιο θύμα ενός e-mail ή ενός Pop-up window που του εμφανίζεται κατά τη διάρκεια της περιήγησής του στον Ιστό, με το οποίο του γίνεται γνωστό ότι **κέρδισε ένα μεγάλο χρηματικό ποσό σε κάποια κλήρωση**. Για να το πάρει δε, θα πρέπει να καταβάλει ορισμένα χρήματα σε συγκεκριμένο λογαριασμό. Εννοείται ότι μετά την καταβολή των χρημάτων αυτών ο απατεώνας εξαφανίζεται και τα θύματα δεν παραλαμβάνουν κανένα

[35] βλ. σχετ. '*Phishing: Η νέα μέθοδος εξαπάτησης στο Διαδίκτυο*', 3ο Πανελλήνιο Συνέδριο Ηλεκτρονικό Έγκλημα 2005 Δικτυοπειρατεία & Τηλεπικοινωνιακή Απάτη Πρόληψη - Αντιμετώπιση - Λύσεις - Εφαρμογές (http://www.marinos.com.gr/bbpdf/pdfs/msg50.pdf)

νέο e-mail με το οποίο να τους γνωστοποιείται το πώς θα εισπράξουν τα υποτιθέμενα ‘κέρδη’ τους.

- Η απάτη με τα **sites - ‘μαϊμούδες’**. Στην περίπτωση αυτή ο ψηφιακός απατεώνας προσπαθεί να οδηγήσει το υποψήφιο θύμα του - χρήστη του Διαδικτύου για να κάνει μια οικονομική συναλλαγή, στο πιστό αντίγραφο του δικτυακού τόπου της τράπεζάς του ή του ηλεκτρονικού καταστήματος που επισκέπτεται, το οποίο έχει δημιουργήσει και ελέγχει πλήρως ο ίδιος. Το ανυποψίαστο θύμα πιστεύοντας ότι βρίσκεται στο site της τράπεζάς του ή ενός υπεράνω πάσης υποψίας ηλεκτρονικού καταστήματος δίνει όλα τα απαιτούμενα για τη συναλλαγή του στοιχεία (αριθμούς πιστωτικής κάρτας, λογαριασμού, κωδικούς πρόσβασης κ.λ.π.), τα οποία ο απατεώνας μπορεί να τα χρησιμοποιήσει στη συνέχεια είτε για να αδειάσει τον τραπεζικό λογαριασμό του θύματός του είτε για να επιβαρύνει την πιστωτική του κάρτα με αγορές τις οποίες αυτό ουδέποτε έχει πραγματοποιήσει.
- Καταναλωτικής φύσεως απάτες:
    - Προσποίηση πώλησης προϊόντος που δεν υπάρχει λαμβάνοντας τα χρήματα εκ’ των προτέρων (Απάτη Προκαταβολικής Πληρωμής).
    - Παροχή αγαθών ή υπηρεσιών χαμηλότερης ποιότητας από αυτή που πληρώνει ο πελάτης.
    - Εξαπάτηση των πελατών να αγοράσουν κάτι που δεν θέλουν μέσω τεχνικών μάρκετινγκ.
    - Αγορά προϊόντων και υπηρεσιών με χρέωση πιστωτικών καρτών ή λογαριασμών τρίτων προσώπων.
- Υπερχρέωση τηλεφωνικών λογαριασμών των χρηστών, η οποία γίνεται εξαιτίας της εγκατάστασης μικρών στο μέγεθος προγραμμάτων που ονομάζονται ‘**Dialers’** και έχουν τη δυνατότητα να διακόπτουν την τηλεφωνική σύνδεση χαμηλής χρέωσης και να

καλούν αριθμούς του εξωτερικού και κυρίως νησιών του Ειρηνικού, με χρέωση περίπου 1€/λεπτό.

2.2.2 Το έγκλημα της πλαστογραφίας

Πλαστογραφία με τη χρήση Η/Υ ενίοτε με πρόσβαση στο Διαδίκτυο

Αποφεύγοντας τις οποίες εισαγωγικές αναφορές, εισερχόμεθα άμεσα σε μια όσο το δυνατόν ουσιαστική περιγραφή ορισμένων μορφών πλαστογραφίας, που σχετίζονται με τη χρήση Η/Υ (Computer related Forgery)[36], ειδικότερα:

- **Εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικών υπολογιστών**, με σκοπό τα δεδομένα αυτά να θεωρούνται ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά. Αποκτώντας πρόσβαση σε ένα δίκτυο ο ψηφιακός εγκληματίας έχει τη διακριτική ευχέρεια να κλέψει, να μεταβάλλει ή να καταστρέψει αρχεία πληροφοριών ή προγραμμάτων και γενικά να κάνει οποιαδήποτε άλλη ενέργεια θα τα αχρηστεύσει μόνιμα ή προσωρινά, επιφέροντας με τον τρόπο αυτό ανυπολόγιστες οικονομικές ζημιές. Αν μάλιστα τα αρχεία αυτά περιέχουν οικονομικές πληροφορίες τα πράγματα είναι ιδιαίτερα επικίνδυνα. Στην περίπτωση αυτή το θύμα είναι κατά κύριο λόγο χρηματοπιστωτικό ίδρυμα, συνήθως Τράπεζα.

  Βλέπουμε λοιπόν πως εναρμονίζεται η 'παραδοσιακή' πλαστογραφία, με αυτή (την πλαστογραφία) που διαπράττεται με ηλεκτρονικά μέσα. Το προστατευόμενο έννομο αγαθό είναι το ίδιο με αυτό του άρθρου 216 Π.Κ (σε συνδ. με το άρθρο 13 περ.γ΄, όπως αυτό προστέθηκε με το άρθρο 2 Ν. 1805/88), δηλαδή η ασφάλεια, αξιοπιστία, πίστη και εγκυρότητα των ηλεκτρονικών δεδομένων, των οποίων η χρήση έχει έννομες συνέπειες.

[36] Αναφορικά με τη σχέση Η/Υ και εγκλήματος, ο καθηγητής David Carter μίλησε για τρεις βασικές: τον Η/Υ σαν στόχο (κλοπή ή καταστροφή Η/Υ ή λογισμικού), σαν εργαλείο (κλοπή κωδικών πιστωτικών καρτών,Hacking), σαν μέσο (παραγωγή πλαστών εγγράφων, παιδική πορνογραφία, «πειρατεία» λογισμικού), (http://www.lectlaw.com/files/cri14.htm).

- [37]**Πλαστογραφία - Spoofing**. Πλαστογράφηση ενός μηνύματος ώστε να φαίνεται ότι προέρχεται από άλλον αποστολέα.
- **Αγοραπωλησία με πλαστές επιταγές**. [38]Στη συγκεκριμένη περίπτωση, ένας απατεώνας αγοραστής σε μια δικτυακή δημοπρασία είναι δυνατό να συμφωνήσει με τον πωλητή να πληρώσει με επιταγή. Το υποψήφιο θύμα καταθέτει την επιταγή και ο πωλητής στέλνει το εμπόρευμα, όμως στις περισσότερες περιπτώσεις οι τράπεζες εμφανίζουν τα χρήματα στο λογαριασμό του θύματος προτού να ελεγχθεί η γνησιότητα της επιταγής. Λίγες ημέρες μετά η τράπεζα διαπιστώνει ότι η επιταγή είναι ακάλυπτη ή πλαστή και αφαιρεί το αντίστοιχο χρηματικό ποσό από το λογαριασμό του θύματος.
- **Πλαστογράφηση μέσων πληρωμής (πιστωτικών καρτών κ.λ.π.)**

  [39]Ο ηλεκτρονικός πλαστογράφος με σύστημα υπολογισμού:

  - εισχωρεί: στο μαγνητικό πεδίο αναγνώρισης μιας πιστωτικής κάρτας (μαύρη ταινία) και σβήνει τα πραγματικά στοιχεία κατόχου και αναγράφει άλλα πλασματικά, οπότε η κάρτα χρεώνει σε άλλο όνομα από αυτό που αναγράφεται στην κάρτα.
  - καταρτίζει από την αρχή πιστωτικές κάρτες, έναν άλλο τρόπο πλαστογράφησης του πλαστικού χρήματος συνιστά το γεγονός, ότι με μηχανικά μέσα αποσπούν τους αριθμούς μιας πιστωτικής κάρτας ενός πελάτη από οποιοδήποτε μέρος του κόσμου, καταρτίζουν μια νέα κάρτα λευκή, την οποία δίνουν σε συνεργαζόμενα καταστήματα, και μέσω των ειδικών συσκευών χρέωσης καρτών, χρεώνουν όποιο ποσό θέλουν ερήμην του κατόχου του αριθμού.

Σύμφωνα με τον καθηγητή της Νομικής Μυλωνόπουλο Χ., η πλαστογράφηση μέσων πληρωμής, όπως οι πιστωτικές κάρτες είναι η συνηθέστερη μορφή ηλεκτρονικού εγκλήματος[40]

[37] http://www.pcproblems.gr/pcfaq/index.php?action=artikel&cat=4&id=8&artlang=el
[38] Τσουραμάνης Χρ. όπ. παρ.
[39] Κανελλόπουλος Δ. (2007) «*Ηλεκτρονικά εγκλήματα στον κυβερνοχώρο*», Περιοδικό 'Εκπαίδευση & Νέες Τεχνολογίες', τεύχος 5ο , σελ. 19-20(http://www.eeep.gr/5_teyxos_ekpaideysi_kai _nees_texnologies.pdf).
[40] Δύο ενδεικτικά παραδείγματα από την ελληνική νομολογία σχετικά με θέματα πληρωμής μέσω πιστωτικών καρτών αποτελούν οι αποφάσεις ΕφΑθ 2319/1999 και ΑΠ 589/2001.

και συνεχίζει «*…υπάρχουν, όμως, και καινούριες μορφές cyber crime όπως η υποκλοπή στοιχείων στον αέρα, δηλαδή ενώ τα δεδομένα μεταδίδονται ασυρμάτως από έναν τόπο σε άλλον. Υπάρχει και η περίπτωση της "κλοπής ταυτότητας", κατά την οποία ένα πρόσωπο, λόγω της υφαρπαγής ή της καταστροφής των ηλεκτρονικών του δεδομένων ή της καταστροφής, κατ' ουσίαν παύει να υπάρχει. Πρόκειται για μια επικίνδυνη μορφή εγκληματικότητας η οποία ακόμα δεν έχει εμφανιστεί στην Ελλάδα. Στη χώρα μας δεν έχει αντιμετωπιστεί επαρκώς ούτε η πλαστογραφία των μέσων πληρωμής, μολονότι υπάρχει σχετική οδηγία και το σχετικό νομοσχέδιο*».

Στην Ελλάδα, τα θέματα των συναλλαγών που γίνονται με πιστωτική κάρτα ρυθμίζει η Υπουργική Απόφαση Ζ1-178/2001 που εναρμόνισε τις διατάξεις της Σύστασης 97/489 στην ελληνική νομοθεσία. Στην Ευρώπη ισχύουν επίσης η Οδηγία 1997/7/ΕΚ και οι Οδηγίες 1987/102 και 1990/88 που ρυθμίζουν θέματα σχετικά με την καταναλωτική πίστη.

Δειγματοληπτικά από την ελληνική και διεθνή πραγματικότητα, παραθέτουμε την ακόλουθη περιπτωσιολογία: [41]Τριμελής σπείρα με ειδικό μηχάνημα από την Αμερική αποκρυπτογραφούσε τον κωδικό της μαγνητικής ταινίας που υπήρχε πάνω στην κάρτα, αλλά χωρίς κομπιούτερ δεν θα μπορούσαν να αναπαραγάγουν τον αριθμό. Από το χειριστήριο και τον υπολογιστή πληκτρολογούσαν τον αριθμό και τον περνούσαν στο μαγνητικό πεδίο της ταινίας των καρτών. Η Αστυνομία θεωρεί ότι διάμεσος της κομπίνας ήταν καταστηματάρχης ή κάποιος μέσα από την τράπεζα που τους έδινε στοιχεία των κατόχων καρτών.

Το 1996 εξαρθρώθηκε διεθνές κύκλωμα παραχαρακτών πιστωτικών καρτών που είχε διασυνδέσεις με επιχειρηματικούς κύκλους από όλο τον κόσμο με έδρα τη Μαλαισία. Κάτοχος πιστωτικής κάρτας στα Χανιά βρέθηκε χρεωμένος σε εστιατόρια και ξενοδοχεία του Χονγκ Κονγκ από τις 29-12-1995 ως τις 03-02-1996 με 1.300.000 δρχ., ενώ άλλοι 44 Έλληνες από διάφορους νομούς είχαν υποστεί το ίδιο. Οι απατεώνες προμηθεύονταν τους αριθμούς των καρτών από το ηλεκτρονικό αρχείο που διατηρούν οι επιχειρηματίες, οι οποίοι συναλλάσσο-

[41] Μπίτσικα Π. (1997) «*Πώς η τεχνολογία μπορεί να γίνει σύμμαχος της εγκληματικότητας Οι ηλεκτρονικοί «φαντομάδες*», Εφημερίδα 'Το Βήμα', σελ. Α42, κωδικός άρθρου: Β12414Α421, ID: 4675.

νται με τους κατόχους. Στη συνέχεια τους τύπωναν με στοιχεία μαλαισιανής τράπεζας και προχωρούσαν στη χρέωση.

Τους απατεώνες έλκουν περισσότερο οι κάτοχοι προνομιούχων πιστωτικών καρτών, οι οποίες επιτρέπουν απεριόριστο αριθμό αγορών. Πριν από μερικά χρόνια συνελήφθη ο 'φαντομας' των κομπιούτερ, ο 31χρονος τότε Κέβιν Μίτνικ, ο πιο 'διαβόητος κλέφτης της πληροφορικής στον κόσμο'. Έκλεβε στοιχεία και πληροφορίες από διάφορες τράπεζες δεδομένων και είχε καταφέρει να αποκωδικοποιήσει περισσότερους από 20.000 κωδικούς αριθμούς πιστωτικών καρτών και εμπορικών πληροφοριών, αξίας πολλών δισεκατομμυρίων δολαρίων. Όλα αυτά μέσω κομπιούτερ.

Πλαστογραφία με τη χρήση ευρύτερα ψηφιακής τεχνολογίας

Εκτός από τους Η/Υ που αποτελούν κλασικό μέσο τέλεσης ηλεκτρονικών εγκλημάτων, υπάρχει πλήθος συσκευών (περιφερειακών και μη) με τη βοήθεια των οποίων μπορούν να διαπραχθούν ψηφιακά εγκλήματα. Ενδεικτικά αναφέρονται:

- Συσκευές κινητής τηλεφωνίας
- Παιχνιδομηχανές
- Σαρωτές
- Φωτοτυπικά μηχανήματα κ.λ.π.

Εμείς θα ασχοληθούμε με τις συσκευές που φαίνεται να διευκολύνουν περισσότερο την τέλεση του αδικήματος της πλαστογραφίας. Πιο συγκεκριμένα, ιδιαιτέρως χρήσιμοι αποδεικνύονται οι σαρωτές (scanner), οι ψηφιακές φωτογραφικές μηχανές και τα φωτοτυπικά μηχανήματα, που σε συνδυασμό με προγράμματα όπως το 'Fine Reader', 'Adobe Photoshop' κ.λ.π. μπορούν να κατασκευάσουν στη βάση ενός γνήσιου εγγράφου ένα καινούργιο πανομοιότυπο μεν, πλαστό δε έγγραφο.

Για να γίνουμε πιο κατανοητοί αποφασίσαμε να παρουσιάσουμε επιγραμματικά, χωρίς πολλές λεπτομέρειες εσκεμμένα, τη δημιουργία ενός πλαστού 'πιστοποιητικού', με ενέργειες

που συνολικά διήρκεσαν μόλις 30΄και κόστισαν 0 ευρώ (λαμβάνοντας υπόψη ότι έχουμε πρόσβαση σε σύστημα Η/Υ και δεν χρειάζεται να αγορασθεί) .

Καταρχήν είχαμε στην κατοχή μας ένα γνήσιο 'πιστοποιητικό' το οποίο αφού σαρώσαμε με ειδικό πρόγραμμα, στη συνέχεια με τη βοήθεια του προγράμματος 'Adobe Photoshop' και των δυνατοτήτων που προσφέρει, επεξεργαστήκαμε κάνοντας τις επιθυμητές αλλαγές. Το νέο έγγραφο δεν φέρει πρωτότυπα εντυπώματα σφραγίδων και χειρόγραφες ενδείξεις γραφής-υπογραφής, αλλά με τη χρήση καλής ποιότητας έγχρωμου φωτοτυπικού μηχανήματος το αποτέλεσμα μπορεί αρκετά εύκολα να παραπλανήσει τον μη ειδικό.

Στην περίπτωση φυσικά που κάποιος διαθέτει περισσότερο χρόνο και διάθεση μπορεί να κατασκευάσει πλαστές σφραγίδες προκειμένου να έχει πρωτότυπες εντυπωματικές αποτυπώσεις και παράλληλα να 'ιχνηλατήσει' τα χειρόγραφα στοιχεία (γραφή-υπογραφή) προκειμένου να έχει πρωτότυπη απεικόνιση.

Η όλη διαδικασία μπορεί να εξαντλείται σε λίγες γραμμές και να φαίνεται μάλλον εύκολη υπόθεση με μεγάλες πιθανότητες επιτυχίας, αλλά η αλήθεια είναι ότι ο ειδικός εξεταστής εγγράφων και γραφής είναι εκπαιδευμένος στο να εντοπίζει τα λάθη που συχνά διαφεύγουν της προσοχής του επίδοξου πλαστογράφου.

Συμπερασματικά λοιπόν θα λέγαμε ότι καλό είναι κάποιος να έχει γνώση των δυνατοτήτων που προσφέρει η τεχνολογία και να είναι συνεχώς σε εγρήγορση ούτως ώστε να μην βρεθεί θύμα πλαστογραφίας, πλην όμως σε όσους, λίγους ελπίζουμε, η όλη διαδικασία πλαστογράφησης φαίνεται πρόκληση και σκέφτονται να προχωρήσουν στη διάπραξη, θα συνιστούσαμε απόλυτη αποχή, καθώς όπως σε όλα τα εγκλήματα κάποια στοιχεία εγκαταλείπονται στο χώρο του εγκλήματος (στο έγγραφο).

[Ακολουθούν ψηφιακές απεικονίσεις]

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ
Ε Π Ι Σ Τ Η Μ Ω Ν

ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ
Τομέας Εγκληματολογίας

Γνήσιο έγγραφο

ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΕΜΙΝΑΡΙΟ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΣΠΟΥΔΩΝ

ΠΙΣΤΟΠΟΙΗΤΙΚΟ

Η κυρία **Αθανασοπούλου Βασιλική** του Θεοδώρου περάτωσε επιτυχώς το διετούς διάρκειας Μεταπτυχιακό Σεμινάριο Εγκληματολογικών Σπουδών, κατά τα ακαδ. έτη 2001-2002 και 2002-2003.

Η επίδοσή της, μετά από την υποστήριξη ενώπιον τριμελούς επιτροπής των εργασιών της με τα ακόλουθα θέματα: «Βιασμός» και «Μέτρα Υποστήριξης Θυμάτων Σεξουαλικής Κακοποίησης», ήταν :

«ΑΡΙΣΤΗ»

Ο ΕΠΙΣΤΗΜΟΝΙΚΟΣ ΥΠΕΥΘΥΝΟΣ ΤΟΥ ΣΕΜΙΝΑΡΙΟΥ

ΚΑΘ. ΙΑΚ. ΦΑΡΣΕΔΑΚΗΣ

ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ
Το γνήσιο της υπογραφής
Φαρσεδάκη
20.04
Γραμματέας του Τμήματος
Κοινωνιολογίας
ΣΧΟΙΝΙΟΥ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ
Ε Π Ι Σ Τ Η Μ Ω Ν

ΤΜΗΜΑ ΚΟΙΝΩΝΙΟΛΟΓΙΑΣ

Τομέας Εγκληματολογίας

Πλαστό έγγραφο

ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΕΜΙΝΑΡΙΟ ΕΓΚΛΗΜΑΤΟΛΟΓΙΚΩΝ ΣΠΟΥΔΩΝ

ΠΙΣΤΟΠΟΙΗΤΙΚΟ

Η κυρία **Αθανασοπούλου Βασιλική** του Θεοδώρου περάτωσε επιτυχώς το διετούς διάρκειας Μεταπτυχιακό Σεμινάριο Εγκληματολογικών Σπουδών, κατά τα ακαδ. έτη 2005-2006 και 2006-2007.

Η επίδοση της, μετά από την υποστήριξη ενώπιον τριμελούς επιτροπής της εργασίας της με το ακόλουθο θέμα: «Πλαστογραφία εγγράφων με τη χρήση νέων τεχνολογιών», ήταν :

«ΑΡΙΣΤΗ»

Αλλαγή στα στοιχεία κατά το δοκούν

Φωτομεταφορά των εντυπωμάτων των σφραγίδων και της χειρόγραφης υπογραφής

Ο ΕΠΙΣΤΗΜΟΝΙΚΟΣ ΥΠΕΥΘΥΝΟΣ ΤΟΥ ΣΕΜΙΝΑΡΙΟΥ

Αλλαγή στην ημερο-χρονολογία με χρήση των χαρακτήρων του γράφοντα

2.3 Ο δράστης ηλεκτρονικών εγκλημάτων

Ο καθηγητής Εγκληματολογίας Πανούσης Ι. επισημαίνει: «[42]*Στο χώρο του εγκλήματος εμφανίζονται νέα μοντέλα τόσο ως προς τη μορφή όσο και ως προς τα μέσα και τις μεθόδους. Όσο υιοθετούμε το δυτικό πρότυπο ζωής τόσο μεταβάλλεται και το στερεότυπο του εγκληματία. Η παγκοσμιοποίηση των αγορών παγκοσμιοποιεί και το έγκλημα, η κατάργηση των ευρωπαϊκών συνόρων διευκολύνει και τη διακίνησή του*».

Πράγματι μετά το 1990 υπήρξε σαφής τάση επέκτασης της εγκληματικότητας, που συνεχίστηκε ως το 1998 για να σταθεροποιηθεί ή και να μειωθεί σε κάποιους τομείς όταν η αστυνόμευση απέκτησε επιστημονικά χαρακτηριστικά και έλαβε υλική υποστήριξη. Το θέμα είναι ότι αργούμε, ενώ διαπιστώνεται ποιοτική και ποσοτική αλλαγή της εγκληματικότητας, συνδυάζοντας πολυ-επίπεδη παρέμβαση σε τομείς επιστημονικής, κοινωνικής και πολιτικής ζωής.

Το έγκλημα εκσυγχρονίζεται ως προς την υποδομή και τις μεθόδους του. Οι σύγχρονοι εγκληματίες είναι εφοδιασμένοι με νέου τύπου μηχανήματα και εργαλεία διάρρηξης, ενώ στηρίζουν πολλά στην πληροφορική και στις εξελίξεις της τεχνολογίας σε ό,τι αφορά τα όπλα, την κατόπτευση των στόχων και τη διαφυγή.

Με βάση τη διάκριση των ψηφιακών εγκλημάτων, σε γνήσια και σε παραδοσιακά (βλ. προηγούμενο Κεφάλαιο 2.1.2), θα πρέπει να πούμε πως ξεχωριστή κατηγορία εγκληματικής συμπεριφοράς, που παρουσιάζει ιδιαίτερο ενδιαφέρον και χρήζει περαιτέρω ανάλυσης, αποτελεί εκείνη την οποία επιδεικνύει ο δράστης των γνήσιων ψηφιακών εγκλημάτων.

Τα από εγκληματολογικής άποψη χαρακτηριστικά των δραστών των παραδοσιακών εγκλημάτων (εκβιαστών, απατεώνων, τρομοκρατών κλπ.) είναι ήδη γνωστά και δεδομένα και δεν αλλάζουν από το γεγονός ότι αλλάζει ο τόπος -'Διαδίκτυο'- και το μέσο εκδήλωσης -'ψηφιακή τεχνολογία'- της εγκληματικής τους συμπεριφοράς. Με βάση τις παραπάνω σκέψεις

[42] Λακόπουλος Γ. (2001) «*Αφύλακτη Πολιτεία Φοβισμένοι και ανεκπαίδευτοι αστυνομικοί, αδίστακτοι και αποφασισμένοι οι κακοποιοί*», Εφημερίδα 'Το Βήμα', σελ. Α03, κωδικός άρθρου: Β13196Α031 ID: 232917.

μας θα θεωρήσουμε στο σημείο αυτό ως ψηφιακό εγκληματία εκείνον που διαπράττει τα γνήσια ψηφιακά εγκλήματα.

2.3.1 Οι έννοιες Hacker - Cracker

Ο ψηφιακός εγκληματίας είναι γνωστός τόσο στο ευρύ κοινό όσο και στη βιβλιογραφία αλλά και στα ΜΜΕ κυρίως ως **Hacker**. [43]Αντίστοιχο συνώνυμο δεν υπάρχει στην ελληνική γλώσσα (και αν υπάρχει δεν χρησιμοποιείται -με εξαίρεση ίσως τον όρο 'εισβολέας'). Όταν σε οποιαδήποτε ενέργεια που σχετίζεται με τους Η/Υ και τα δίκτυα, υπεισέρχεται το στοιχείο της εγκληματικής πρόθεσης ο επιτιθέμενος χαρακτηρίζεται **Cracker** (σπάστης). Οι Crackers είναι Hackers που χρησιμοποιούν τη γνώση τους για τους Η/Υ για να αποκομίσουν όφελος για τους ίδιους ή για τρίτους. Εκτός από τους όρους Cracker και Hacker έχουν κατά καιρούς χρησιμοποιηθεί και άλλοι όροι για να περιγράψουν τους εγκληματίες του Διαδικτύου, όπως: **Hacktivists, Vandals, Cyberterrorists, Cyberpunk**.

[44]Ιστορικά, οι πρώτοι πειρατές των καλωδίων ήταν νεαροί υπάλληλοι της τηλεφωνικής εταιρείας Bell, το 1878, που μπέρδευαν ή έκοβαν τα καλώδια των τηλεφωνικών συνδέσεων και απλώς διασκέδαζαν με τις τρελές συνομιλίες που προέκυπταν. «*Αυτός ο συνδυασμός εξουσίας, τεχνογνωσίας και εξασφαλισμένης ανωνυμίας επέδρασε σαν ακαταμάχητος πειρασμός στα νεαρά αγόρια*», έγραφε ο Μπρους Στέρλινγκ στο «*The hacker crackdown*». Και αν Hacker, πρωτογενώς, σημαίνει «αυτός που πελεκάει το ξύλο με τσεκούρι», τώρα η διάσταση που έχει λάβει ο ίδιος χαρακτηρισμός είναι σχεδόν μυθική. Ας δούμε όμως 'ιστορικά' την εξέλιξη των Hackers:

Η <u>πρώτη γενιά</u> των Hackers περιλαμβάνει τους επιστήμονες που είχαν συμμετοχή στην ανάπτυξη των πρώτων μεθόδων προγραμματισμού υπολογιστών. Οι πρώτοι Hackers χαρακτηρίζονταν από μια απόλυτη προσήλωση στο έργο τους. Ζούσαν για να προγραμματίζουν. Κλεισμένοι στα εργαστήρια, κυρίως του MIT (Massachusetts Institute of Technology), κατά τις δε-

[43] Βλαχόπουλος Κ. (2007) «*Ηλεκτρονικό Έγκλημα*», Νομική Βιβλιοθήκη, σελ. 21επ.
[44] Μαρνέλλος Γ. & Κυριακόπουλος Κ. (2001) «*Το Δίκτυο των παρανόμων*», Εφημερίδα 'Ελευθεροτυπία'.

καετίες του 1950 και του 1960, δεν είχαν κάποια συστηματική και μόνιμη επαφή με την ευρύτερη κοινωνική πραγματικότητα και τις εξελίξεις της. Ο Ψυχρός Πόλεμος τους ήταν κάτι μακρινό, και το γεγονός ότι εργάζονταν για λογαριασμό στρατιωτικοβιομηχανικών κύκλων και μυστικών υπηρεσιών δεν τους απασχολούσε ιδιαίτερα. Πάντως, οι ηθικές αρχές του hacking είχαν νόημα για τη μικρή ομάδα των πρώτων Hackers και μάλλον δεν προβλημάτιζαν τους εργοδότες τους.

Η δεύτερη γενιά περιλαμβάνει τους επιστήμονες και επιχειρηματικά προσανατολισμένους επιστήμονες που έθεσαν ως σκοπό τους τη μετάδοση της χρήσης της πληροφορικής τεχνολογίας στον ευρύτερο πληθυσμό. Πρόκειται για τους επιστήμονες που ανέπτυξαν τους πρώτους προσωπικούς υπολογιστές, συστήματα υπολογιστών που περιλάμβαναν όλες τις ουσιαστικές ιδιότητες της πληροφορικής τεχνολογίας, έστω και αν δεν διέθεταν παρά περιορισμένες δυνατότητες. Επιπλέον, η δεύτερη γενιά ασχολήθηκε συστηματικά με τη μελέτη και τον πειραματισμό πάνω στους τρόπους βελτίωσης της επικοινωνίας μεταξύ ανθρώπων και υπολογιστώ».

Η τρίτη γενιά αναφέρεται στους προγραμματιστές που σχεδίασαν τις πρώτες αρχιτεκτονικές, πάνω στις οποίες θα αναπτύσσονταν στο κοντινό μέλλον τα ηλεκτρονικά παιχνίδια. Είναι φανερό ότι η τρίτη αυτή γενιά είναι πλέον σαφώς προσανατολισμένη σε μια ήδη δημιουργημένη αγορά πληροφορικής τεχνολογίας γύρω από τον προσωπικό υπολογιστή και προσπαθεί να ανταποκριθεί στη ζήτηση ή να δημιουργήσει μια ζήτηση με βάση πιθανές δυναμικές ανάγκες.

Οι τρεις πρώτες γενιές των Hackers δεν έχουν ιδιαίτερη σχέση με το πληροφορικό έγκλημα, αν και έχουν κάποια ασταθή σχέση καταγωγής και έναν -αμφισβητούμενο ως προς το αν είναι ευρύς ή στενός- κοινό τόπο με την έννοια του Hacker, όπως επικράτησε και καθιερώθηκε στις αρχές της δεκαετίας του 1980.

Είναι η τέταρτη γενιά των Hackers που προσεγγίζει τους διάφορους νομικούς ορισμούς του hacking ως εγκληματικής συμπεριφοράς. Η γενιά αυτή αποδέχεται τις ηθικές αρχές των

προηγούμενων γενεών, συγχρόνως όμως είναι σαφώς πολυπληθέστερη, έχει γεννηθεί και κοινωνικοποιηθεί σε ένα ήδη υπάρχον πληροφορικό περιβάλλον και αποτελείται από άτομα που ζουν σε διαφορετικές συνθήκες και έχουν διαφορετικούς στόχους και σκοπούς από τις προηγούμενες.

Μεγάλο μέρος των δραστηριοτήτων, που στο πλαίσιο του εργαστηρίου πληροφορικής ή του Διαδικτύου μεταξύ ερευνητικών κέντρων και επιστημόνων θεωρούνταν ως αυτονόητες, αναπτύσσουν έναν ουσιαστικά διαφορετικό χαρακτήρα όταν μεταφέρονται στην ευρύτερη κοινωνία ή, ακριβέστερα, στον ευρύτερο κυβερνοχώρο. Στο νέο αυτό, ποιοτικά διαφορετικό, πλαίσιο, η πρόσβαση σε έναν υπολογιστή δεν θεωρείται πλέον αμέσως ελεύθερη. Απαιτεί ορισμένες ρυθμίσεις κοινωνικότητας, η κυριότερη από τις οποίες είναι η εξουσιοδότηση. Ευνόητο είναι ότι η χωρίς εξουσιοδότηση πρόσβαση σε έναν υπολογιστή αρχίζει να γίνεται αντιληπτή ως παραβίαση, μια παραβίαση που μπορεί να αξιολογείται ως ανήθικη ή ως ανήθικη και εγκληματική.

Ας έρθουμε τώρα σε ένα άλλο θέμα. Σύμφωνα με τους [45]**Kovacich** και **Boni** μια επιχείρηση ή ένας οργανισμός που είναι τα συνήθη θύματα των ψηφιακών εγκληματιών, μπορούν να αναζητήσουν τους Hackers που έχουν τη δυνατότητα να προσβάλλουν τα συστήματά τους, σε μία από τις ακόλουθες κατηγορίες:

α. στους φοιτητές Πανεπιστημίων, καθώς και στους μαθητές μέσης εκπαίδευσης,

β. ανάμεσα στους υπαλλήλους τους,

γ. σε εκείνους που κινούνται στον υπόκοσμο των Η/Υ,

δ. σε παλιούς εγκληματίες από τον κόσμο των ναρκωτικών και του οργανωμένου εγκλήματος και τέλος

ε. στους επαγγελματίες που έχουν ως αντικείμενό τους τη βιομηχανική κατασκοπεία και οι οποίοι εργάζονται για λογαριασμό των ανταγωνιστών τους.

[45] Kovacich L. & Boni W. (2000) «*High-Technology-Crime Investigator's Handbook*» {Τσουραμάνης Χρ. «*Ψηφιακή κοινωνία, ψηφιακή εγκληματικότητα και θυματοποίηση*» (http://www.teimes.gr/spoudastirio/yifiaki_eglimatikotita.doc)}.

2.3.2 Τα κίνητρα και ο τρόπος δράσης των 'εισβολέων'

Τα κίνητρα των επιθέσεων διαφέρουν ανάλογα με την περίπτωση και την προσωπικότητα του 'εισβολέα'. Σε γενικές γραμμές, μπορούμε να διακρίνουμε τις ακόλουθες κατηγορίες[46]:

- **Ερασιτέχνες**: Πρόκειται για ανθρώπους χωρίς ιδιαίτερες δεξιότητες στους υπολογιστές, που προσπαθούν να εντοπίσουν μια ευπάθεια σε ένα υπολογιστικό σύστημα και στη συνέχεια να την εκμεταλλευτούν. Τα κίνητρά τους είναι η περιέργεια και η απόκτηση γνώσης, χωρίς όμως να αποκλείεται και το γεγονός να αποσκοπούν σε οποιοδήποτε είδους όφελος.
- **Hackers**: Είναι άριστοι γνώστες προγραμματισμού, δικτύων Η/Υ και Διαδικτύου. Σκοπός των επιθέσεών τους είναι η ικανοποίηση της περιέργειάς τους και η επιβεβαίωση της ικανότητάς τους για εισβολή.
- **Crackers**: Έχουν ως σκοπό την πρόκληση ζημιάς ή την αποκόμιση οφέλους από τα συστήματα στα οποία επιτίθενται.
- **Επαγγελματίες εισβολείς**: Οι επιθέσεις των εγκληματιών της κατηγορίας αυτής σχετίζονται με τα σοβαρότερα εγκλήματα του κυβερνοχώρου, όπως η βιομηχανική κατασκοπεία. Κερδίζουν μέρος ή το σύνολο του εισοδήματός τους από επιθέσεις.

Θα πρέπει να σημειώσουμε ακόμη πως η **επικινδυνότητα** των Hackers εξαρτάται από τα **κίνητρά** τους. Αν τα κίνητρά τους είναι η διασκέδαση ή η επιθυμία τους να αναγνωριστούν στον κύκλο τους ως αυθεντίες στους Η/Υ ή να μάθουν τον τρόπο λειτουργίας του συστήματος μιας επιχείρησης ή ενός οργανισμού, η παράνομη πρόσβασή τους σε αυτό σταματάει μέχρις εκεί και εκείνο που έχει υποστεί βλάβη πραγματικά είναι το γόητρο του συστήματος ασφαλείας της συγκεκριμένης επιχείρησης ή οργανισμού.

Αν όμως το κίνητρό τους είναι το **προσωπικό οικονομικό όφελος**, το οποίο μπορούν να επιτύχουν βλάπτοντας με οποιοδήποτε τρόπο το σύστημα ή τα αρχεία δεδομένων των θυμάτων τους ή πουλώντας σε τρίτους τις πληροφορίες που απεκόμισαν από αυτά, τότε οι ζημιές αυτών

[46] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 24 {ενδεικτικά Anderson R. (2001) «*Security Engineering: A guide to building dependable distributed systems*», New York: John Wiley and Sons, Inc}.

των τελευταίων είναι ανυπολόγιστες. Η σύγχρονη πρακτική θέλει δυστυχώς ένα αρκετά μεγάλο αριθμό από τους σημερινούς Hackers να έχει οικονομικά κίνητρα, πράγμα που αυτόματα αυξάνει τον επικίνδυνο χαρακτήρα τους.

Βλέπουμε λοιπόν ότι [47]δεν παρατηρούνται διαφοροποιήσεις ως προς τα κίνητρα της εγκληματικής δραστηριότητας των 'εισβολέων' σε σχέση με αυτά των δραστών του κοινού Ποινικού Δικαίου, αλλά μόνο ως προς τα μέσα διάπραξης. Απ' την άλλη πολύ λίγες έρευνες έχουν πραγματοποιηθεί, με αρκετά μεθοδολογικά προβλήματα, όσον αφορά το προφίλ των δραστών ηλεκτρονικών εγκλημάτων.

Όσον αφορά τώρα τον τρόπο δράσης - πρόσβασης ενός hacker στο σύστημα του υποψήφιου θύματός χωρίζεται σε δύο στάδια: ένα **προπαρασκευαστικό** και ένα **κύριο**. Πιο συγκεκριμένα: Στο προπαρασκευαστικό στάδιο ο hacker, *συγκεντρώνει πληροφορίες* (information gathering) για το σύστημα που επιθυμεί να προσβάλλει και *προσπαθεί να αποκτήσει πρόσβαση σε αυτό* 'σπάζοντας' τους κωδικούς εισόδου (password cracking), αποκτώντας έτσι τα δικαιώματα (privileges) ενός νόμιμου χρήστη του συστήματος.

Στο κύριο στάδιο ο hacker, επιδιώκει την εκπλήρωση των σκοπών για τους οποίους μπήκε παράνομα στο συγκεκριμένο σύστημα και αποχωρεί προσπαθώντας να μην αφήσει ίχνη που θα μπορούν να οδηγήσουν στην ανακάλυψη της ταυτότητάς του, ενώ παράλληλα φροντίζει να διατηρήσει το δικαίωμα επανεισόδου του στο σύστημα, όποτε πάλι ο ίδιος το επιθυμήσει.

2.3.3 Η ηθική των 'εισβολέων'

Ανατρέχοντας στη διεθνή βιβλιογραφία που σχετίζεται με την ηθική των Hackers, στεκόμαστε στο Levy St.[48], ο οποίος θεωρεί ως βασική ηθική αρχή, την ακόλουθη: «*Η πρόσβαση στους υπολογιστές -και οτιδήποτε θα μπορούσε να σε διδάξει κάτι για τον τρόπο που ο κόσμος*

[47] Αρτινοπούλου Β. (2007) όπ. παρ.
[48] Λάζος Γ. (2001) «*Οι hackers και η φιλοσοφία τους - Ποιος ποινικοποιεί δράσεις στο Δίκτυο;*», Εφημερίδα 'Ελευθεροτυπία' {Levy St. (1984) «*Hackers: Heroes of the Computer Revolution*» 3rd ed., New York: Penguin Books}.

λειτουργεί- πρέπει να είναι απεριόριστη και απόλυτη. Να αποδέχεσαι πάντα την προσταγή 'πάνω τα χέρια'».

Η αρχή αυτή αναλύεται σε μια σειρά μερικότερων αρχών, με κυριότερες:

- Οι πληροφορίες πρέπει να είναι ελεύθερες στον καθένα.
- Έλλειψη εμπιστοσύνης στην εξουσία - προώθηση της αποκέντρωσης.
- Οι Hackers πρέπει να κρίνονται με βάση την ικανότητά τους να hack-ίζουν, και όχι με βάση κίβδηλα κριτήρια, όπως τα πτυχία, η ηλικία, η φυλή ή η θέση.
- Μπορεί να δημιουργηθεί τέχνη και ομορφιά στον υπολογιστή.
- Οι υπολογιστές μπορούν να αλλάξουν τη ζωή προς το καλύτερο.

..//..

Β΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 3. ΔΙΩΞΗ

Ορισμένα Δικονομικά θέματα

Η διερεύνηση μιας υπόθεσης ηλεκτρονικού εγκλήματος πρέπει να συμβαδίζει με τους ισχύοντες κατά περίπτωση νόμους και κανονισμούς. Νομικοί προβληματισμοί προκύπτουν σχετικά με την έρευνα και κατάσχεση των ψηφιακών αποδείξεων, κατά πόσο δηλαδή οι γνώσεις ενός ερευνητή είναι επαρκείς για τη διεκπεραίωση μιας έρευνας σε ένα Η/Υ και αν η ανάλυση και διατήρηση των αποδείξεων γίνεται σύμφωνα με τις προβλεπόμενες διαδικασίες.

Σε μια δίκη αρχικά τίθεται υπό αμφισβήτηση η έρευνα και η κατάσχεση πληροφοριών. Σύμφωνα με το άρθρο 253 Κ.Π.Δ μια έρευνα μπορεί να διενεργηθεί όταν διεξάγεται ανάκριση για κακούργημα ή πλημμέλημα και μόνο με το μέσο αυτό μπορεί να βεβαιωθεί ή να διευκολυνθεί η διάπραξη του εγκλήματος, η ανακάλυψη των δραστών κ.λ.π. [49]Επιπλέον κατά τη διεξαγωγή μιας έρευνας πρέπει να τηρούνται και οι βασικές αρχές της αναγκαίας αναλογίας, της αναγκαιότητας και της απαγορεύσεως του υπερμέτρου. Επειδή δεν υφίσταται συγκεκριμένο νομοθετικό πλαίσιο για τις έρευνες στον κυβερνοχώρο, οι ανωτέρω διατάξεις εφαρμόζονται αναλογικά και στις περιπτώσεις ηλεκτρονικών εγκλημάτων. Επομένως, μια έρευνα θα επηρεάσει την αποδεικτικότητα των στοιχείων που συλλέχτηκαν.

[50]Κατά τη διεξαγωγή μιας έρευνας, το βασικό αγαθό, που διακυβεύεται, είναι η ιδιωτικότητα του ατόμου. Το Αμερικανικό Σύνταγμα απαιτεί την ύπαρξη εντάλματος για τη διεξαγωγή έρευνας, το οποίο εκδίδεται αν υπάρχει πιθανή αιτία ότι διαπράχθηκε έγκλημα. Το ένταλμα θα πρέπει να καθορίζει, επακριβώς το μέρος και τα αντικείμενα που μπορούν να ερευνηθούν. Π.χ. εάν η πιθανή αιτία υποδεικνύει ότι τα αποδεικτικά στοιχεία είναι αποθηκευμένα σε ένα CD, η αστυνομία δεν έχει το δικαίωμα να ερευνήσει κάθε υπολογιστή που υπάρχει στο χώρο. Αν το πράξει, έστω κι αν βρει επιπρόσθετα αποδεικτικά στοιχεία, αυτά δεν θα έχουν αποδεικτική αξία στο δικαστήριο γιατί παραβιάστηκε το ένταλμα.

[49] Καρράς Α. (1998) «*Ποινικό Δικονομικό Δίκαιο*», β΄ έκδοση, Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή, σελ. 474.
[50] Βλαχόπουλος Κ. (2007) όπ. παρ. σελ. 182, 183.

Το δεύτερο νομικό ζήτημα, που σχετίζεται με υποθέσεις που εμπλέκονται αποδεικτικά στοιχεία σε ψηφιακή μορφή, είναι το κατά πόσο τα προσόντα ενός επιστημονικού ερευνητή επαρκούν για τη διεκπεραίωση μιας ηλεκτρονικής έρευνας. Ο μεγαλύτερος προβληματισμός έγκειται στα χρησιμοποιούμενα από τον ερευνητή εργαλεία λογισμικού. Ο ερευνητής, απλά γνωρίζει τη χρήση ενός εργαλείου λογισμικού. Δεν μπορεί να έχει πρόσβαση στον πηγαίο κώδικα και έτσι δεν γνωρίζει τι εργασίες επιτελεί το λογισμικό.

Πώς λοιπόν μπορεί να βεβαιώσει ότι τα ψηφιακά δεδομένα, που συλλέχθηκαν, αποδεικνύουν την ενοχή ή την αθωότητα του κατηγορούμένου; Έως σήμερα, δεν υπάρχει απόφαση δικαστηρίου που να απέρριψε την επιστημονική άποψη ενός ερευνητή, τέτοιο ενδεχόμενο, όμως δεν αποκλείεται να συμβεί στο μέλλον από τη στιγμή που τα εργαλεία λογισμικού εξελίσσονται και γίνονται όλο και πιο πολύπλοκα.

Το τρίτο και τελευταίο ζήτημα αφορά την ανάλυση και διατήρηση των αποδεικτικών στοιχείων. Είναι κοινή πρακτική των διωκτικών αρχών, η αντιγραφή του μέσου αποθήκευσης, που θα εξετασθεί (π.χ. ενός σκληρού δίσκου) δημιουργώντας ακριβές αντίγραφο. Τα δικαστήρια έχουν αποδεχθεί, ότι εφόσον το αντίγραφο είναι ακριβές, τότε θεωρείται γνήσιο. Ωστόσο, πρέπει να λαμβάνεται κάθε απαραίτητο μέτρο για την άρτια διατήρησή του.

Οι ψηφιακές πληροφορίες μπορούν να επηρεαστούν από μαγνητικά πεδία, καιρικές συνθήκες κ.ά. Για παράδειγμα, στη υπόθεση Ohio v. Cook, ο κατηγορούμενος προέβαλλε μια σειρά από ισχυρισμούς έναντι της μη ορθής συλλογής και διατήρησης των ψηφιακών αποδείξεων, που οδήγησαν στην αλλοίωσή τους, όπως η μη τοποθέτηση του σκληρού δίσκου που αφαιρέθηκε σε αντιστατική θέση. Το δικαστήριο λαμβάνοντας υπόψη τα παραπάνω, καθώς και μια σειρά από άλλες παραλήψεις των διωκτικών αρχών κατά τη διατήρηση των ψηφιακών στοιχείων, έκρινε τον κατηγορούμενο αθώο λόγω αμφιβολιών.

3.1 Διεύθυνση Εγκληματολογικών Ερευνών - Εργαστήριο Δικ. Γραφολογίας

Εισαγωγή

Σύμφωνα με τον τέως Διευθυντή της Διεύθυνσης Εγκληματολογικών Ερευνών της ΕΛ.ΑΣ, Κυριακάκη Ε.[51]η κατάργηση των συνόρων στη δεκαετία του '90, στο χώρο της Βαλκανικής και της Ανατολικής Ευρώπης και το ρεύμα μετανάστευσης που ακολούθησε από αυτές και από χώρες του Τρίτου Κόσμου προς τις περισσότερο ανεπτυγμένες χώρες, σε συνδυασμό με την παγκοσμιοποίηση της οικονομίας, την τεχνολογική επανάσταση και τα επιτεύγματα της βιοτεχνολογίας, δημιούργησαν νέα δεδομένα στο Χάρτη της Εγκληματικότητας διεθνώς.

Σήμερα, αναμφισβήτητα, η εξιχνίαση του εγκλήματος περνάει κατά ένα μεγάλο ποσοστό στην αρμοδιότητα των Εγκληματολογικών Εργαστηρίων και η συμβολή της επιστημονικής αστυνομίας στον τομέα αυτό, είναι πλέον καθοριστική και παραδεκτή από όλους.

Είναι γνωστό ότι, τα τελευταία χρόνια η έμφωνη μαρτυρία έχει καταστεί μαχητή, ρευστή και έχει υποστεί ισχυρό κλονισμό, τόσο από τις εξελίξεις που συντελούνται ιδιαίτερα στο Δικονομικό Σύστημα, όσο και από αυτή καθ΄ εαυτή τη φύση της, με τις ανθρώπινες αδυναμίες, καθώς και την εμπλοκή της στον κυκεώνα των σκοπιμοτήτων.

Κατά συνέπεια, οι μόνοι αδέκαστοι, αδιάψευστοι και αδιαμφισβήτητοι μάρτυρες παραμένουν τα ίχνη και τα πειστήρια, τα ‘επισκεπτήρια’ δηλαδή των εγκληματιών στον τόπο του εγκλήματος. Έτσι, τα ίχνη των χεριών, ποδιών ή υποδημάτων τους, τα ίχνη των όπλων, μέσων και εργαλείων που χρησιμοποίησαν, οι τρίχες του σώματός τους, οι οργανικές και βιολογικές τους ουσίες, αλλά και κάθε τι που άφησαν στη σκηνή του εγκλήματος, είναι αντικείμενο επιστημονικής έρευνας και περαιτέρω εκμετάλλευσης, αφού δεν μεταβάλλουν, δεν αλλοιώνουν και δεν διαστρεβλώνουν τα γεγονότα, εκ προθέσεως. Η τεχνολογία σε κάθε περίπτωση είναι συνοδοιπόρος και χρήσιμος συνεργάτης της αστυνομίας στην καταπολέμηση του εγκλήματος.

[51] Κυριακάκης Ε. «*Επιστημονικές - τεχνικές δυνατότητες της Δ-νσης Εγκληματολογικών Ερευνών (Δ.Ε.Ε) στην καταπολέμηση του εγκλήματος*», Περιοδικό ‘Προβληματισμοί’ της Ελληνικής Εταιρείας Στρατηγικών Μελετών [ΕΛ.Ε.Σ.ΜΕ], τεύχος 16.

Οργάνωση & Λειτουργία της Διεύθυνση Εγκληματολογικών Ερευνών

Η Διεύθυνση Εγκληματολογικών Ερευνών είναι η Εθνική Εγκληματολογική Υπηρεσία της χώρας μας, έχει διοικητική αυτοτέλεια και υπάγεται απευθείας στο Αρχηγείο της Ελληνικής Αστυνομίας.

Λειτουργεί σε κεντρικό επίπεδο (Δ.Ε.Ε) και περιφερειακό, με την Υποδιεύθυνση Εγκληματολογικών Ερευνών Βόρειας Ελλάδας (Υ.Ε.Ε.Β.Ε) στη Θεσσαλονίκη και 64 Γραφεία Εγκληματολογικών Ερευνών (Γ.Ε.Ε) στις έδρες των Πρωτοδικείων. Το νομικό πλαίσιο λειτουργίας της στηρίζεται στις διατάξεις του άρθρου 30 του Π.Δ. 14/2001 (ΦΕΚ Α-12), του Π.Δ. 198/1992 (ΦΕΚ Α-92) και του Π.Δ. 342/1977 (ΦΕΚ Α-109), το οποίο αποτελεί και τον Κανονισμό Λειτουργίας της.

Τα Εργαστήρια της Δ.Ε.Ε είναι θεσμοθετημένα, ως τα μοναδικά Κρατικά Εργαστήρια, εφαρμόζουν δε μεθόδους και τεχνικές που είναι επιστημονικοτεχνικά τεκμηριωμένες, διεθνώς αναγνωρισμένες και δικαστικώς παραδεκτές, παρέχοντας έτσι σημαντική υποστήριξη και βοήθεια στο έργο των Διωκτικών Αρχών της χώρας, που σχετίζεται με την εξιχνίαση του εγκλήματος, κοινού και οργανωμένου, καθώς και της τρομοκρατίας, συμβάλλοντας αποφασιστικά στην καταστολή της εγκληματικότητας.

Η Δ.Ε.Ε έχει ενταχθεί στο Ευρωπαϊκό Δίκτυο Εγκληματολογικών Ινστιτούτων (ENFSI), ανταλλάσσει πληροφορίες μεταξύ κρατών-μελών της Ε.Ε μέσω INTERPOL, EUROPOL, EURODAC, Συνθήκης SCHENGEN κ.λ.π. και εκπροσωπείται με εμπειρογνώμονες Αξιωματικούς σε Ομάδες Εργασίας της Ε.Ε για θέματα Επιστημονικοτεχνικού - Εγκληματολογικού ενδιαφέροντος.

3.1.1 Τομέας Εξέτασης Εγγράφων και Γραφής

Ένα από τα εγκληματολογικά εργαστήρια της Δ.Ε.Ε είναι και αυτό της Δικαστικής Γραφολογίας όπου και λειτουργεί μεταξύ άλλων ο Τομέας Εξέτασης Εγγράφων και Γραφής. Στον

τομέα αυτό εξετάζονται τα έγγραφα (με τη στενή τους έννοια) και ανάλογα με τα ερωτήματα, υπάρχουν δυνατότητες:

α) ταυτοποίησης της γραφής, υπογραφής, μηχανικής γραφής,

β) διαχωρισμού του γνήσιου από το πλαστό,

γ) ανάλυσης της μελάνης, του χάρτου και άλλων υποστρωμάτων που χρησιμοποιούνται στα έγγραφα,

δ) διαπίστωσης της προσθήκης, της αλλοίωσης των εγγράφων &

ε) επαναφοράς και αποκρυπτογράφησης σβησμένων ή απαλειφόμενων στοιχείων κ.λ.π.

Ως επί το πλείστον οι εξετάσεις των εγγράφων αφορούν στις εξετάσεις χειρόγραφης γραφής και υπογραφών, με μικρότερο -ακόμα- το ποσοστό εξέτασης μηχανικής γραφής[52]. Επίσης πραγματοποιούνται και άλλες 'ειδικές' εξετάσεις λ.χ. χρονολόγησης μελάνης[53], διασταυρώσεις γραμμών[54], μικρομετρήσεις ακριβείας, αναλύσεις μελάνης και χάρτου, με τη χρήση συσκευών όπως: VSC, RAMAN[55], TLC[56], εμφάνισης λανθανουσών ενδείξεων, με τη χρήση της ηλεκτροστατικής συσκευής ανίχνευσης ESDA[57], η οποία εκμεταλλεύεται τις αρχές της ηλεκτροστατικής και ηλεκτροδυναμικής για να δημιουργήσει μια απεικόνιση των διαταραχών στην επιφάνεια του εξεταζόμενου χαρτιού κ.λ.π. Συγχρόνως δε δοκιμάζονται και νέα προγράμματα όπως το 'Grapholog', 'Memex'[58] κ.λ.π. που θα μπορούσαν να φανούν χρήσιμα κατά τη γραφολογική διερεύνηση υποθέσεων πλαστογραφίας.

---

[52] Jess D. (1998) «*Document Examiner Textbook*», Pantex International Ltd, σελ. 361

[53] βλ. σχετ. Brunelle R. & Cantu A. (1987) «*A Critical evaluation of Current Ink Dating Techniques*». Journal of Forensic Sciences, JFSCA, Vol. 32, No.6, σσ.1522-1536.

[54] βλ. σχετ. Moore D. (1978) «*Determing the Sequence of Ball-Point Pen Writings - A New Method?*», Journal of Forensic Sciences, JFSCA, Vol.23, No.1, σσ.142-148.

[55] βλ. σχετ. '*Forensic Science International'* (2003), Proceedings of the 3rd European Academy of Forensic Scienece Meeting, Elsevier Ireland Ltd, Vol. 136 Suppl.1 σσ.70,71.

[56] βλ. σχετ. Kuranz R. (1986) «*Technique for transferring Ink from a Written Line to a Thin-Layer Chromatographic Sheet*», Journal of Forensic Sciences, JFSCA, Vol.31, No.2, σσ. 655-657.

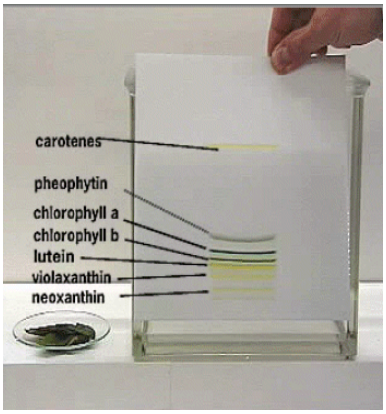
[57] βλ. σχετ. Moore D, (1988) «*The electrostatic Detection Apparatus (ESDA) and Its Effects on Latent Prints on Paper*», Journal of Forensic Sciences, JFSCA, Vol. 33, No.2, σσ. 357-377.

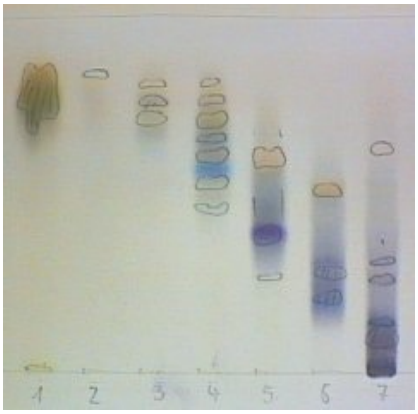
[58] Λαμπρόπουλος Γ. Β. (2001) «*Οι ψηφιακοί ντετέκτιβ της ΕΛ.ΑΣ. Πώς οι έλληνες και οι βρετανοί ειδικοί 'χαρτογραφούν' την οργάνωση '17 Νοέμβρη'*», Εφημερίδα 'Το Βήμα', σελ. Α32, κωδικός άρθρου: Β13245Α321, ID: 234759.

[Ψηφιακές απεικονίσεις ορισμένων εκ των ανωτέρω συσκευών]

VSC

RAMAN





TLC

ESDA

3.1.2 Τομέας Εξέτασης Ψηφιακών Πειστηρίων

Στο Εργαστήριο Δικαστικής Γραφολογίας λειτουργεί επίσης και ο Τομέας Εξέτασης Ψηφιακών πειστηρίων (Π.Δ. 223/16-7-2003). Ο τομέας δομήθηκε [59]πάνω στον πυρήνα δύο ειδικών που εξέταζαν τις προκηρύξεις διάφορων οργανώσεων, όταν αυτές άρχισαν να χρησιμοποιούν Η/Υ.

Αντικείμενα εργασίας του τομέα σήμερα είναι:

[59] Χρυσοχοΐδης Μ. (2001) «*Προετοιμαζόμαστε για τον κυβερνοπόλεμο*», Εφημερίδα 'Ελευθεροτυπία'.

- αναγνώσεις και συγκρίσεις ψηφιακών δεδομένων ή αρχείων ευρισκομένων σε ψηφιακούς χώρους Η/Υ ή σε περιφερειακά αυτών συστήματα,
- περί της γνησιότητας ψηφιακού υλικού-λογισμικού,
- επί κινητών τηλεφώνων ή άλλων ηλεκτρονικών συσκευών, οι οποίες περιέχουν ή αποθηκεύουν ψηφιακά δεδομένα,
- και αναγνώσεις δεδομένων επί μαγνητικών ταινιών πιστωτικών ή άλλων καρτών, καθώς και εξετάσεις επί άλλων σύγχρονων μέσων ψηφιακής αποθήκευσης δεδομένων σε ηλεκτρονικό κύκλωμα ή άλλης μορφής ψηφιακό χώρο.

Παράλληλα ο τομέας παρέχει τεχνική συνδρομή σε διαδικασίες κατάσχεσης, μεταφοράς, αποθήκευσης και αποστολής των ψηφιακών πειστηρίων, που σχετίζονται με εγκληματική δραστηριότητα. Επιπλέον τηρεί αρχείο διενεργούμενων εργαστηριακών εξετάσεων, καθώς και συλλογές ψηφιακών πειστηρίων, λογισμικών και συσκευών ψηφιακής αποθήκευσης, προς υποβοήθηση των συγκριτικών εν γένει εξετάσεων.

3.2 Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος

[60]Η ελληνική αστυνομία εδώ και χρόνια οργανώνεται και εξελίσσεται σύμφωνα με το πρότυπο του βρετανικού Computer Crime Unit και των τμημάτων των Cyber Crime στις αστυνομίες ολόκληρου του κόσμου.

Πιο συγκεκριμένα με το Π.Δ 100/2004 ιδρύθηκε το Τμήμα 5^{ο} Δίωξης Ηλεκτρονικού Εγκλήματος, υπαγόμενο στη Διεύθυνση Ασφάλειας Αττικής/ Υποδ-νση Δίωξης Οικονομικών Εγκλημάτων & Αρχαιοκαπηλίας & Ηθών και αντίστοιχα με το Π.Δ. 48/2004 ιδρύθηκε Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος, υπαγόμενο στην Υποδιεύθυνση Δίωξης Οικονομικών Εγκλημάτων της Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης.

Οι εν λόγω Υπηρεσίες έχουν ως αρμοδιότητες τη δίωξη εγκλημάτων που διαπράττονται στο Διαδίκτυο ή με τη χρήση αυτού, όπως επίσης και την επί 24ωρου έρευνα του Διαδικτύου

[60] http://www.yassas.com/Newsletter/1307/1307a.html

προς διαπίστωση εγκληματικών πράξεων που τελούνται στη Χώρα. Αποτελούνται από εξειδικευμένα στελέχη της Ελληνικής Αστυνομίας επιλαμβάνονται υποθέσεων σε όλη την επικράτεια, ενώ παράλληλα συνεργάζονται με αντίστοιχες Υπηρεσίες του εξωτερικού.

Πρόκειται για καθαρόαιμα επιχειρησιακά τμήματα που ασχολούνται με ευρεία γκάμα υποθέσεων, όπως:

- Παραχάραξη πιστωτικών καρτών.
- Παραποίηση ηλεκτρονικών σελίδων στο Διαδίκτυο.
- Διάπραξη εγκλημάτων, όπως πορνογραφία και παιδοφιλία, μέσω του Διαδικτύου.
- Παραβάσεις τηλεφωνικών δικτύων.
- Οικονομικές απάτες μέσω υπολογιστών, όπως παράνομη μεταφορά χρημάτων.
- Δυσφημήσεις προσώπων μέσω του Διαδικτύου.

Σύμφωνα με τα όσα αναφέρει σχετικά ο επικεφαλής της Δίωξης Ηλεκτρονικού Εγκλήματος Σφακιανάκης Ε., «[61]*κατά τη διάρκεια του 2006 δεχθήκαμε περίπου 400 καταγγελίες από πολίτες που αφορούσαν κυρίως περιπτώσεις απάτης μέσω Διαδικτύου με τη μέθοδο των απατηλών e-mail μηνυμάτων. Στο πρώτο εξάμηνο του 2007 οι καταγγελίες έχουν ήδη ξεπεράσει τις 400. Παράλληλα έχουν εξιχνιαστεί και αρκετές υποθέσεις όπως, οικονομικές απάτες, πλαστογραφήσεις πτυχίων, επιθέσεις ελλήνων χάκερ, υποθέσεις παιδεραστίας κ.λ.π*».

3.3 Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness & Response to Threats)

Το Υπουργείο Οικονομίας & Οικονομικών στο πλαίσιο της Ψηφιακής Στρατηγικής 2006-2013 προχώρησε στη σύσταση Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness & Response to Threats) ή D.A.R.T, όπως ανακοίνωσε στις 14-06-2007 ο ίδιος ο Υπουργός Οικονομίας και Οικονομικών. Βασικός σκοπός της Ομάδας είναι η πρόληψη και αντιμετώπιση των πάσης φύσεως ψηφιακών κινδύνων που μπορούν να απειλήσουν τους έλλη-

[61] http://www.euro2day.gr/articles/132106

νες πολίτες του κυβερνοχώρου. Στόχος η ενίσχυση της εμπιστοσύνης του κοινού των χρηστών στα νέα μέσα.

Η Ομάδα D.A.R.T συντονίζεται από τον ειδικό γραμματέα Ψηφιακού Σχεδιασμού του Υπουργείου Οικονομίας και Οικονομικών, ενώ συμμετέχουν, εκπρόσωποι της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ), της Αρχής Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε), της Δίωξης Ηλεκτρονικού Εγκλήματος του Υπουργείου Δημοσίας Τάξης κ.λ.π.

Ακόμη στην Ομάδα συμμετέχουν ειδικοί εμπειρογνώμονες της Ειδικής Γραμματείας Ψηφιακού Σχεδιασμού. Στους σκοπούς της Ομάδας περιλαμβάνονται επίσης η ενημέρωση, η πρόληψη, καθώς και η ανταλλαγή τεχνογνωσίας για την αντιμετώπιση κινδύνων.

Η Ομάδα δραστηριοποιείται σε τρεις πυλώνες. Ο πρώτος είναι αυτός της πρόληψης των ψηφιακών κινδύνων από πολίτες, επιχειρήσεις και δημόσιους φορείς. Στο επίπεδο της πρόληψης, η D.A.R.T προτείνει πρακτικά μέτρα για την αποφυγή ψηφιακών κινδύνων, αναπτύσσει τεχνικές αξιολόγησης και πρόβλεψης πιθανών ψηφιακών απειλών, παρακολουθεί την εξάπλωση ψηφιακών κινδύνων και τους τρόπους έγκαιρης αντιμετώπισής τους.

Στο πλαίσιο του δεύτερου πυλώνα, της ενημέρωσης δηλαδή για ψηφιακούς κινδύνους, η Ομάδα λειτουργεί ως κεντρικό σημείο για την ενημέρωση πολιτών και επιχειρήσεων, αναφορικά με ζητήματα αντιμετώπισης ψηφιακών κινδύνων και απειλών, αξιοποιώντας κάθε πρόσφορο μέσο. Ακόμη, ενημερώνει και παρέχει πληροφόρηση σχετικά με ζητήματα ψηφιακής ασφαλείας στο κοινό, σε δημόσιους, ιδιωτικούς και ανεξάρτητους φορείς που δραστηριοποιούνται σε θέματα τεχνολογιών πληροφορικής και επικοινωνιών, με στόχο την ευαισθητοποίηση και τη συνειδητοποίηση των ψηφιακών κινδύνων,και επιμελείται τη συλλογή και τη διάχυση πληροφοριών μέσα από πολλαπλά δίκτυα για την αύξηση της συνειδητοποίησης των ζητημάτων ψηφιακής ασφαλείας.

Στον τρίτο πυλώνα, αυτόν της ανταλλαγής τεχνογνωσίας, η Ομάδα συνεργάζεται με οργανώσεις και φορείς, διευκολύνει την επικοινωνία μεταξύ εμπειρογνωμόνων στους τομείς της

ασφαλείας συστημάτων, αναπτύσσει δεσμούς με ερευνητικούς οργανισμούς και συμμετέχει σε ερευνητικές δραστηριότητες, καθώς και σε εγχώρια και διεθνή forum, αναθέτει έρευνες και συντονίζει παρουσίαση μελετών αναφορικά με την ασφάλεια συστημάτων και την προστασία των πολιτών, επιχειρήσεων και του κράτους από ψηφιακούς κινδύνους ενώ συνεργάζεται με διεθνείς και εγχώριους φορείς του δημόσιου ή ιδιωτικού φορέα προκειμένου να εξασφαλιστεί η προστασία των δικαιωμάτων των πολιτών έναντι κακόβουλων απειλών.

Σύμφωνα με το portal που έχει δημιουργήσει η Ομάδα (www.dart.gov.gr), αρμόδιες αρχές για να προστατέψουν και να βοηθήσουν τον πολίτη είναι: α) η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, β) η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων και γ) το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος (βλ. προηγούμενο Κεφάλαιο).

Η Α.Δ.Α.Ε είναι ανεξάρτητη αρχή που έχει σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλον τρόπο, καθώς και την ασφάλεια των δικτύων και πληροφοριών. Η Ε.Ε.Τ.Τ είναι επίσης ανεξάρτητη αρχή η οποία αποτελεί τον εθνικό ρυθμιστή που ελέγχει και εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και Διαδικτύου, καθώς και την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

..//..

ΚΕΦΑΛΑΙΟ 4. ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Εισαγωγή

Ο λειτουργικός προορισμός του ποινικού δικαίου[62], όπως αυτό διαμορφώθηκε κατά τον 19ο αιώνα μέσα από τη διαδικασία θεμελίωσης του φιλελεύθερου αστικού κράτους και υπό την επίδραση των θεωρητικών του Διαφωτισμού, συλλαμβάνεται ως συνισταμένη δύο επιμέρους λειτουργιών: της προστατευτικής των εννόμων αγαθών και της εγγυητικής του ατόμου - πολίτη από την αυθαίρετη χρήση της ποινικής καταστολής εκ μέρους της κρατικής εξουσίας.

Στην παρούσα φάση κοινωνικής ανάπτυξης το ποινικό δίκαιο καλείται να διαδραματίσει έναν ηγεμονικό ρόλο στην αντιμετώπιση και επίλυση όχι μόνο των αυξημένης εντάσεως μορφών κινδύνων που προκαλεί ο τεχνολογικός εκσυγχρονισμός, αλλά και ευρύτερων συμπεριφορών, που δημιουργούν σοβαρούς κινδύνους για το κοινωνικό σύνολο, όπως η τρομοκρατία, το οργανωμένο έγκλημα κ.λ.π.

Παράλληλα, καλείται να ανταποκριθεί στην αύξηση της εγκληματικότητας, αλλά και στο διογκωμένο αίσθημα ανασφάλειας των πολιτών, που αλλάζει τα δεδομένα στις κοινωνικές σχέσεις, ανατρέπει τις ισορροπίες και δημιουργεί πιέσεις στους κρατούντες για λήψη ριζοσπαστικών αποφάσεων στο χώρο της αντεγκληματικής πολιτικής. [63]Η σχέση του δικαίου και των κοινωνικών μετασχηματισμών, δεν είναι μονομερής αλλά διαλεκτική, καθώς το δίκαιο όχι μόνο αντικατοπτρίζει τις διεργασίες του κοινωνικού χώρου, αλλά δημιουργεί και συνδιαμορφώνει με τη σειρά του, μέσω των επιταγών και απαγορεύσεων που υιοθετεί, την εκάστοτε κοινωνική πραγματικότητα.

Κατ' αυτόν τον τρόπο, τα τελευταία χρόνια σημειώνεται στις περισσότερες ευρωπαϊκές χώρες μια τάση επέκτασης και διεύρυνσης του πεδίου εφαρμογής του ποινικού δικαίου. [64]Οι

[62] Delmas - Marty M. (1998) «*Πρότυπα και Τάσεις Αντεγκληματικής Πολιτικής*», Νομική Βιβλιοθήκη, Αθήνα, σελ. 44επ.
[63] βλ. μεταξύ άλλων Πανούσης Γ. (1986) «*Ο ρόλος των ποινικών επιστημών στον κοινωνικό μετασχηματισμό*», σε Μνήμη Χωραφά Ν., Γάφου Η., Γαρδίκα Κ., τόμος Β΄, Εκδόσεις Α.Ν. Σάκκουλας, Αθήνα, σελ. 209-226.
[64] Ζαραφωνίτου Χ. (2002) «*Ο φόβος του εγκλήματος*», Εκδόσεις Α.Ν. Σάκκουλας, Αθήνα, σελ. 71επ.

πολίτες άλλωστε νιώθουν να απειλούνται άμεσα από την αύξηση της εγκληματικότητας και είναι πρόθυμοι να βοηθήσουν το κράτος και τους αρμόδιους φορείς στην αντιμετώπιση του εγκλήματος, να εκχωρήσουν μέρος των ατομικών τους ελευθεριών και δικαιωμάτων, χάριν της ασφάλειας.

Μπορεί όμως ο παγκόσμιος ιστός να ελεγχθεί από άποψη ποινικής συμπεριφοράς; Η απάντηση σύμφωνα με τον Εισαγγελέα Πρωτοδικών [65]Αγγελή Ι. είναι δύσκολη, κι 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.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικά τις καταστάσεις, πιεζόμενες από τα πράγματα. Κλασσικό παράδειγμα στον τομέα της τεχνολογίας, αποτελεί η εμφάνιση των εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές. Πριν από δυο δεκαετίες περίπου η συμβατική νομοθεσία δεν επαρκούσε για την αντιμετώπισή τους. Σήμερα όλες οι προηγμένες (τουλάχιστον) χώρες έχουν καταρτίσει σχετική νομοθεσία για την αντιμετώπιση των εγκλημάτων της πληροφορικής.

Ο επιστημονικός κλάδος που ασχολείται με τις ιδιαίτερες εκείνες έννομες σχέσεις που ανακύπτουν στην κοινωνία της πληροφορίας και τη χαρακτηρίζουν ονομάζεται [66]**ηλεκτρονικό δίκαιο**. Με αυτή την έννοια το ηλεκτρονικό δίκαιο δεν είναι παρά ένας μερικότερος τομέας του όλου δικαστικού οικοδομήματος, διακρινόμενος από αυτό όχι με γνώμονα κάποια δογματική του ιδιαιτερότητα, αλλά μόνο με βάση τον ειδικό πρακτικό του προσανατολισμό, δηλ. τη διερεύνηση των νομικών προβλημάτων της κοινωνίας της πληροφορίας.

Έτσι και το ηλεκτρονικό δίκαιο θα μπορούσε να υποδιαιρεθεί, όπως και το υπόλοιπο φυσικά, στις ενότητες που είναι ήδη γνωστές στην επιστήμη, το ηλεκτρονικό δημόσιο δίκαιο συ-

[65] Αγγελής Ι. όπ. παρ. (http://www.lawnet.gr/ pages/eofn/2/cybercrime.asp).
[66] Χριστοδούλου Κ. (2001) όπ. παρ., σελ. 1.

νταγματικό και διοικητικό, το ηλεκτρονικό ποινικό δίκαιο, το ηλεκτρονικό ιδιωτικό δικαιοουσιαστικό και δικονομικό υποδιαιρούμενο ενδεχομένως παραπέρα σε ηλεκτρονικό αστικό δίκαιο, με την έννοια του γενικού ηλεκτρονικού ιδιωτικού δικαίου, το ηλεκτρονικό εμπορικό δίκαιο στο μέτρο που ο χαρακτήρας του εγγράφου διαφοροποιείται από την εμπορικότητα της σχετικής επικοινωνίας κ.λπ.

Φυσικά η σημασία και η διακριτικότητα του κάθε υποκλάδου εξαρτάται από την πρακτική του χρησιμότητα, η οποία πάντως μοιραία θα διαφοροποιείται με την πάροδο του χρόνου και την πρόοδο της τεχνολογίας.

4.1 Παγκόσμια νομοθεσία

4.1.1 Ηνωμένες Πολιτείες Αμερικής

[67]Το πρώτο νομοθέτημα σχετικά με το ηλεκτρονικό έγκλημα θεσπίστηκε στις Ηνωμένες Πολιτείες της Αμερικής, το 1984. Ο νόμος 'Computer Fraud and Abuse Act', προσπάθησε, ανεπιτυχώς θα λέγαμε, να θέσει ένα βασικό νομικό πλαίσιο για τη νέα αυτή μορφή εγκλήματος. Η έλλειψη όρων σχετιζόμενων με τη νέα τεχνολογία των ηλεκτρονικών υπολογιστών, αλλά και η αποτυχία προσδιορισμού των ορίων δικαιοδοσίας των δικαστηρίων, ήταν από τα σημαντικότερα προβλήματα.

Επιπλέον, ο νόμος περιοριζόταν, στην προστασία κρατικών υπολογιστικών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, με σκοπό την απόκτηση απόρρητων πληροφοριών που θα μπορούσαν να βλάψουν τις Η.Π.Α.

Τα προβλήματα αυτά, οδήγησαν πολύ γρήγορα στην πρώτη αναθεώρηση[68], το 1986, στην οποία προστέθηκε μια ακόμη ενότητα, που προέβλεπε ότι *«όποιος σκόπιμα αποκτά πρόσβαση σε ομοσπονδιακό υπολογιστικό σύστημα χωρίς εξουσιοδότηση και συνέπεια της πρόσβασης αυτής τροποποιεί, προκαλεί ζημιά ή καταστρέφει πληροφορίες που είναι αποθηκευμένες σε έναν ηλεκτρονικό υπολογιστή κρατικού ενδιαφέροντος ή εμποδίζει την εξουσιοδοτημένη χρήση*

[67] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 129, 130.
[68] Συνολικά πραγματοποιήθηκαν 8 αναθεωρήσεις έως το 1996.

ενός υπολογιστή ή των πληροφοριών που είναι αποθηκευμένες σε αυτών τιμωρείται...». Στην τροποποίηση αυτή χρησιμοποιήθηκε πιο σαφής ορολογία, ενώ διαφαίνεται και η πρώτη προσπάθεια αντιμετώπισης περιπτώσεων άρνησης εξυπηρέτησης με τη φράση *«εμποδίζει την εξουσιοδοτημένη χρήση ενός υπολογιστή»*. Και πάλι, όμως, η συγκεκριμένη τροποποίηση αναφέρονταν μόνο σε κρατικά υπολογιστικά συστήματα.

Η πιο σημαντική τροποποίηση του νομοθετήματος αυτού έγινε το 1994, η οποία επέφερε αλλαγές σε τρία σημαντικά σημεία:

α) η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικού υπολογιστές, που χρησιμοποιούνται στο διαπολιτειακό εμπόριο

β) αφαιρέθηκε ο όρος, «μη εξουσιοδοτημένη πρόσβαση», που σημαίνει ότι οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες θα μπορούσαν να διωχθούν και

γ) συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών θεωρούνταν, πλέον, παράνομες, όπως η διασπορά κακόβουλου λογισμικού.

Τέλος, το 1996, συμπληρώθηκε ο νόμος αυτός με τη National Information Infrastructure Protection Act, η οποία αναφέρεται στους «προστατευμένους υπολογιστές». Η πιο σημαντική διάταξη του νομοθετήματος αυτού προβλέπει ότι κάθε μεμονωμένος χρήστης, που εισέρχεται σε ένα προστατευμένο υπολογιστή, είναι υπεύθυνος όχι μόνο για τις πράξεις του, αλλά και για τις συνέπειες αυτών, ενώ εάν η πρόσβασή του είναι εξουσιοδοτημένη, είναι ποινικά υπεύθυνος μόνο εάν έχει πρόθεση να προξενήσει ζημιά στο θύμα.

Οι διατάξεις αυτές, με μικρές τροποποιήσεις που έχουν επέλθει στη συνέχεια, ισχύουν και σήμερα, ενσωματωμένες στο κεφάλαιο 18, παράγραφος 1030 του Ποινικού Κώδικα των Η.Π.Α.

Εκτός των ανωτέρω, σε κάθε πολιτεία υπάρχουν σε ισχύ διάφορες διατάξεις, που αντιμετωπίζουν το ηλεκτρονικό έγκλημα με διαφορετικό τρόπο. Η απουσία ενιαίων διατάξεων σε όλα τα μήκη και πλάτη των Η.Π.Α, αποτελεί τη μεγαλύτερη πληγή του δικαϊκού συστήματος.

4.1.2 Αυστραλία

[69]Η Αυστραλία είναι η χώρα που έχει δώσει τη μεγαλύτερη, μετά τις Η.Π.Α, προσοχή στην αντιμετώπιση του ηλεκτρονικού εγκλήματος. Ο νόμος 'Crime Act 1914' προβλέπει τέσσερις βασικές μορφές ηλεκτρονικού εγκλήματος:

- Παράνομη πρόσβαση σε δεδομένα αποθηκευμένα σε κρατικό ηλεκτρονικό υπολογιστή.
- Καταστροφή δεδομένων αποθηκευμένων σε κρατικό ηλεκτρονικό υπολογιστή.
- Πρόσβαση σε δεδομένα αποθηκευμένα σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.
- Καταστροφή δεδομένων σε ηλεκτρονικό υπολογιστή χρησιμοποιώντας μέσα κρατικής διευκόλυνσης.

Ο νόμος, που σήμερα είναι σε ισχύ στην Αυστραλία, αναφέρεται ως 'The Cybercrime Act 2001'[70], ο οποίος προήλθε από την τροποποίηση του νόμου 'Crime Act' και του Ποινικού Κώδικα που ψηφίστηκε το 1995. Ο νόμος προβλέπει τρεις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων:

- Μη εξουσιοδοτημένη πρόσβαση, μετατροπή και φθορά δεδομένων, με σκοπό τη διάπραξη σοβαρού εγκλήματος. Στην περίπτωση αυτή, η ποινή είναι ισοδύναμη της αντίστοιχης που επιβάλλεται στο συμβατικό έγκλημα.
- Μη εξουσιοδοτημένη τροποποίηση δεδομένων, που οδηγεί σε φθορά δεδομένων.
- Μη εξουσιοδοτημένη φθορά ηλεκτρονικών επικοινωνιών, για την οποία προβλέπεται ποινή έως δέκα ετών.

Παράλληλα, ο νόμος δημιούργησε τέσσερις νέες μορφές εγκλημάτων:

- Μη εξουσιοδοτημένη πρόσβαση ή μετατροπή προστατευομένων δεδομένων.
- Παράνομη καταστροφή δεδομένων αποθηκευμένων σε δίσκους Η/Υ.
- Κατοχή ή έλεγχος δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικών αδικημάτων.

[69] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 130, 131.
[70] http://www.findlaw.com.au/article/1408.htm

- Παραγωγή, προμήθεια ή απόκτηση δεδομένων, με σκοπό τη διάπραξη ηλεκτρονικού εγκλήματος.

Στο νόμο περιλαμβάνονται ακόμη, διατάξεις για τον τρόπο έρευνας ηλεκτρονικών αδικημάτων από τις διωκτικές αρχές και τις μεθόδους εξέτασης δεδομένων, που είναι αποθηκευμένα σε ηλεκτρονικά μέσα.

4.1.3 Κίνα

[71]Η Κίνα, αντιμετωπίζει το ηλεκτρονικό έγκλημα με ειδική νομοθεσία που έχει θεσπιστεί για το σκοπό αυτό. Το άρθρο 23 του Νομοθετικού Διατάγματος 147, καθιστά παράνομη οποιαδήποτε δραστηριότητα σχετίζεται με τη διασπορά ιών ή άλλου είδους «κακόβουλου» λογισμικού, σε ηλεκτρονικούς υπολογιστές. Παράνομη, επίσης, είναι η πώληση συστημάτων προστασίας υπολογιστών χωρίς άδεια. Οι κυρώσεις που προβλέπονται για την παραβίαση των παραπάνω διατάξεων, περιλαμβάνουν χρηματικό πρόστιμο, που κυμαίνεται από 5.000 έως 15.000 γιεν, ανάλογα με τη σοβαρότητα του εγκλήματος.

Εξαιρετικό ενδιαφέρον παρουσιάζουν ορισμένες διατάξεις της νομοθεσίας στην Κίνα, τις οποίες δεν συναντάμε σε άλλες χώρες. Για παράδειγμα, θεωρείται παράνομη η δημιουργία, αναπαραγωγή, ανάκτηση και διάδοση πληροφοριών, που μπορούν να βλάψουν την εθνική ενότητα. Επίσης απαγορεύεται η παραποίηση της αλήθειας και η διάδοση φημών που μπορούν να βλάψουν τη συνοχή της κοινωνίας, η διάδοση προλήψεων, υλικού σχετικά με τη βία κ.ά., δημιουργώντας σαφή ερωτήματα για τα όρια της ελευθερίας του λόγου στο Διαδίκτυο.

4.1.4 Διεθνείς προσπάθειες

[72]Σε διεθνές επίπεδο, η Interpol προσέγγισε πρώτη το ζήτημα του ηλεκτρονικού εγκλήματος, στο Τρίτο Διεθνές Συμπόσιο για την Απάτη, στο Παρίσι, το 1979. Διάφορες άλλες προ-

[71] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 133.
[72] Βλαχόπουλος Κ. (2007) όπ. παρ. σελ. 133-135.

σεγγίσεις έλαβαν χώρα κατά τα χρόνια που ακολούθησαν, με πιο σημαντικές αυτές που αναπτύχθηκαν από τον OECD, τα Ηνωμένα Έθνη και την «Ομάδα των Οκτώ».

α) Organization for Economic Cooperation and Development (OECD)

Ο Οργανισμός για την Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α) διόρισε στο Παρίσι, το 1983, μια επιτροπή, για το ζήτημα του ηλεκτρονικού εγκλήματος και την ανάγκη, που αυτό δημιουργεί, για την τροποποίηση των ποινικών διατάξεων στα κράτη-μέλη του οργανισμού. Η επιτροπή, αφού εξέτασε τις ισχύουσες νομοθετικές διατάξεις των κρατών-μελών, κατέληξε σε ένα κείμενο για το ηλεκτρονικό έγκλημα, που λειτουργούσε ως κοινός παρονομαστής μεταξύ των διαφορετικών νομικών προσεγγίσεων, που εξετάστηκαν στα κράτη-μέλη. Οι διατάξεις του κειμένου αυτού απαγόρευαν την εισαγωγή, τροποποίηση, διαγραφή και απόκρυψη δεδομένων, με σκοπό την παράνομη μεταφορά κεφαλαίων, τη διάπραξη πλαστογραφίας και την παρεμπόδιση λειτουργίας ενός υπολογιστή ή δικτύου. Επίσης, απαγόρευαν την πρόσβαση σε σύστημα Η/Υ χωρίς άδεια, ενώ προστάτευαν και την παράνομη αντιγραφή και διάθεση πακέτων λογισμικού.

β) Οργανισμός Ηνωμένων Εθνών

Τα Ηνωμένα Έθνη παρουσίασαν ένα ψήφισμα, σχετικά με τη νομοθεσία για το ηλεκτρονικό έγκλημα, στο 8^{ο} Συνέδριο για την Πρόληψη του Εγκλήματος και την Μεταχείριση των Παραβατών. Το Εγχειρίδιο για την Πρόληψη και τον Έλεγχο του Ηλεκτρονικού Εγκλήματος εκδόθηκε το 1994. Το Εγχειρίδιο αυτό αντιμετωπίζει συνολικά το ζήτημα του ηλεκτρονικού εγκλήματος παρουσιάζοντας την έκταση του φαινομένου, τις μορφές του και την υπάρχουσα νομοθεσία σε διάφορες χώρες, και καταλήγει σε προτάσεις για την καλύτερη αντιμετώπισή του.

Το συγκεκριμένο κείμενο, πρέπει να αναθεωρηθεί, λόγω των τεχνολογικών εξελίξεων που συντελέστηκαν μετά την έκδοση του. Αποτελεί, όμως, την πρώτη συστηματική διεθνή

προσπάθεια νομοθετικής προσέγγισης του ηλεκτρονικού εγκλήματος. Για το λόγο αυτό, θεωρείται η βάση πάνω στην οποία μπορούν να στηριχθούν μελλοντικές προσπάθειες.

γ) Ομάδα των Οκτώ - Group of Eight (08)

Οι οκτώ ισχυρότερες χώρες του κόσμου, δημιούργησαν το 1997 μια Υποομάδα για το Έγκλημα Υψηλής Τεχνολογίας. Η Υποομάδα αυτή σε μια συνάντηση που πραγματοποιήθηκε τον ίδιο χρόνο στην Ουάσινγκτον, με τη συμμετοχή των υπουργών Εσωτερικών και Δικαιοσύνη των οκτώ χωρών, κατέληξε σε *«Δέκα Αρχές»* και *«Δέκα Τομείς Δράσης»* για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Οι αρχές αυτές είχαν ως σκοπό τη διασφάλιση της ενιαίας αντιμετώπισης του εγκληματικού φαινομένου, σε όλες τις χώρες του κόσμου.

4.2 Ευρώπη και ηλεκτρονικό έγκλημα

Η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος στον Ευρωπαϊκό χώρο, πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης, το 1976 στο Στρασβούργο, στις εργασίες του Συνεδρίου για τις Εγκληματολογικές Πλευρές του Οικονομικού Εγκλήματος. Ήταν η πρώτη φορά που παρουσιάστηκαν οι μορφές του ηλεκτρονικού εγκλήματος, συμπεριλαμβανόμενης και της απάτης.

Το 1986, συστήθηκε μια επιτροπή από το Ευρωπαϊκό Συμβούλιο, η οποία εξέτασε την ισχύουσα νομοθεσία στα κράτη-μέλη, τα δε συμπεράσματά της συμπεριλήφθησαν στη Σύσταση του 1989, η οποία όριζε εγκληματικές πράξεις, όπως απάτη και πλαστογραφία με ηλεκτρονικούς υπολογιστές, καταστροφή δεδομένων και λογισμικού, μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη αναπαραγωγή λογισμικού κ.ά. Επίσης, η Σύσταση αυτή περιελάμβανε και μια σειρά από Οδηγίες (μη υποχρεωτικές) προς τα κράτη-μέλη, σχετικά με τη μεθοδολογία θέσπισης νομοθετικών κειμένων για το ηλεκτρονικό έγκλημα.

Το Συμβούλιο της Ευρώπης αντιμετώπισε αποφασιστικότερα το ζήτημα της νομοθεσίας για το ηλεκτρονικό έγκλημα το 1996, εκδίδοντας δύο Συστάσεις: τη Σύσταση No R (89)9 σχε-

τικά με το έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικού υπολογιστή και τη Σύσταση No R (95)13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των Η/Υ. Οι συστάσεις αυτές αποτέλεσαν τη βάση για τη Σύμβαση για τον Κυβερνοχώρο του 2001.

Οι εργασίες για τη δημιουργία μιας Σύμβασης για τον Κυβερνοχώρο ξεκίνησαν το 1997, όταν συστήθηκε μια επιτροπή ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με σκοπό να εξετάσει τα νομοθετικά προβλήματα που προκύπτουν από την εγκληματική δραστηριότητα, που αναπτύσσεται και συνεχών διευρύνεται στον κυβερνοχώρο. Αν και αρχικά η περαίωση των εργασιών της επιτροπής, είχε προσδιοριστεί για το 1999, τα ιδιαίτερα προβλήματα που συνάντησαν τα μέλη της, έθεσαν νέα προθεσμία το έτος 2000.

Τελικά, το κείμενο της *«Σύμβασης για το Έγκλημα στον Κυβερνοχώρο»,* υπογράφηκε στις 23-11-2001, στη Βουδαπέστη, από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου[73]. Στη Σύμβαση, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα:

- για τα αδικήματα κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων και των συστημάτων Η/Υ, τέτοια αδικήματα είναι η παράνομη πρόσβαση, η παράνομη υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών,
- για τα αδικήματα που σχετίζονται με τους υπολογιστές, όπως η απάτη με Η/Υ και **πλαστογραφία**,

[73] Η Σύμβαση έχει υπογραφεί ως σήμερα από τις ακόλουθες χώρες:
2001: Αλβανία, Αρμενία, Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρο5, Εσθονία, Φιλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ισλανδία, Ιταλία, Μολδαβία, Ολλανδία, Νορβηγία, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία, Σουηδία, Ελβετία, Σκόπια, Ουκρανία, Αγγλία, Καναδά$, Ιαπωνία, Νότια Αφρική, Η.Π.Α.
2002: Ιρλανδία, Μάλτα, Σλοβενία.
2003: Δανία, Λιθουανία, Λουξεμβούργο.
2004: Λετονία.
2005: Βοσνία-Ερζεγοβίνη, Τσεχία, Σερβία, Σλοβακία, Μαυροβούνιο.
Ο αριθμός των χωρών που έχουν εναρμονίσει την εθνική τους νομοθεσία σύμφωνα με τις επιταγές της Σύμβασης και έχουν θέσει σε ισχύ τις νέες διατάξεις είναι πολύ μικρότερος: Αλβανία (2004), Βοσνία - Ερζεγοβίνη (2006), Βουλγαρία (2005), Κροατία (2004), Κύπρος (2005), Δανία (2005), Εσθονία (2004), Γαλλία (2006), Ουγγαρία (2004), Λιθουανία (2004), Νορβηγία (2006), Ρουμανία (2004), Σλοβενία (2005), Σκόπια (2005) και Ουκρανία (2006). **Στην Ελλάδα αναμένεται να τεθεί σε ισχύ.**

- για τα αδικήματα σχετικά με το περιεχόμενο όπως είναι το αδίκημα της παιδικής πορνογραφίας &
- για τα αδικήματα που σχετίζονται με καταπάτηση πνευματικής ιδιοκτησίας.

Επιπρόσθετα περιλαμβάνονται ρυθμίσεις για τη συνέργια, την απόπειρα και την υποκίνηση ηλεκτρονικών εγκλημάτων, καθώς και την ευθύνη των επιχειρήσεων. Ακόμα τονίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγεται το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά. Η εν λόγω Σύμβαση έχει χαρακτηρισθεί από πολλούς ως το πιο άρτιο κείμενο σχετικά με το ηλεκτρονικό κείμενο στην Ευρωπαϊκή Ένωση και έχει ήδη υπογραφεί από 33 κράτη συμπεριλαμβανομένων των ΗΠΑ, Καναδά, Ν. Αφρική και Ιαπωνία. Φυσικά δεν λείπουν οι επικριτές της[74].

Παράλληλα υπάρχουν και άλλα γενικά νομοθετήματα που βοηθούν **στην καταπολέμηση του ηλεκτρονικού εγκλήματος**. Ενδεικτικά αναφέρουμε τα ακόλουθα που ισχύουν στην Ευρωπαϊκή Ένωση:

1. Η Σύσταση του Συμβουλίου με αριθμό 9193/01, με την οποία καλούνται τα κράτη μέλη να συμμετάσχουν στο δίκτυο πληροφόρησης της Ομάδας των Οκτώ, το οποίο λειτουργεί 24 ώρες το εικοσιτετράωρο, για την καταπολέμηση του εγκλήματος υψηλής τεχνολογίας.
2. Η Σύσταση του Συμβουλίου No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer related crime).
3. Η Σύσταση του Συμβουλίου No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology). Η σπουδαιότητα της σύστασης αυτής είναι μεγάλη, διότι καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο, οι γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων.

[74] Βλαχόπουλος Κ. (2007) όπ. παρ., σελ. 142-144.

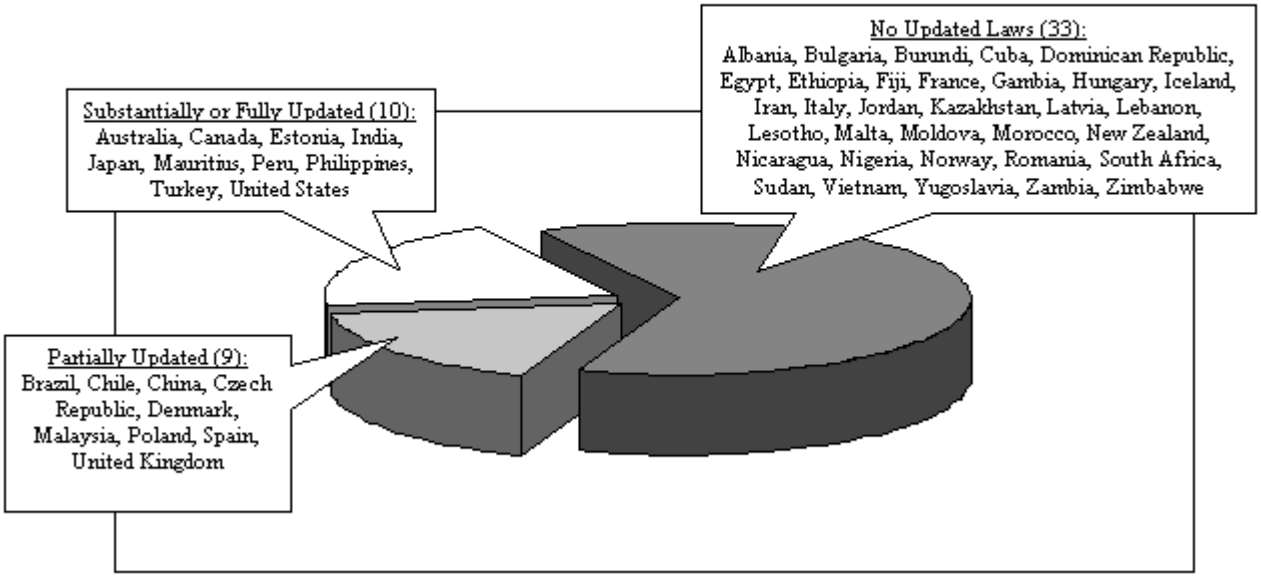
4. [75]Το Ψήφισμα του Συμβουλίου με αριθμό 2003/ C 48/01, για την ασφάλεια των δικτύων και των πληροφοριών.
5. Το Ψήφισμα 97/C70/01 του Συμβουλίου και το άρθρο 2 της Σύμβασης της Europol (ν. 2605/1998).
6. Η Σύσταση του Συμβουλίου με αριθμό 95/144/ΕΚ, όπου αναφέρονται οι προτροπές του Συμβουλίου σχετικά με την ασφάλεια των συστημάτων πληροφορικής.
7. Η Κοινή θέση της 27ης Μαΐου 1999 (1999/364/ΔΕΥ), όπου τα κράτη μέλη υποστηρίζουν την κατάρτιση του σχεδίου σύμβασης του Συμβουλίου της Ευρώπης σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και ότι φροντίζουν ώστε να περιληφθούν στη σύμβαση διατάξεις που θα διευκολύνουν την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων που άπτονται των ηλεκτρονικών συστημάτων και δεδομένων.
8. Το Ψήφισμα του Συμβουλίου με αριθμό 2002/C 43/02 για κοινή προσέγγιση και ειδικές δράσεις στον τομέα της ασφάλειας των πληροφοριών και των δικτύων.
9. Το έγγραφο με αριθμό 2000/C 124/01 σχετικά με τη στρατηγική της Ευρωπαϊκής Ένωσης για την πρόληψη και τον έλεγχο του οργανωμένου εγκλήματος. Στο έγγραφο αυτό αναλύονται διεξοδικά τα μέτρα που πρέπει να ληφθούν για την πρόληψη και την καταπολέμηση του οργανωμένου εγκλήματος όπου εντάσσονται και πολλές μορφές του ηλεκτρονικού εγκλήματος.
10. Το Σχέδιο Δράσης με αριθμό 97/C 251/01 για την καταπολέμηση του οργανωμένου εγκλήματος.

Διεθνώς επικρατεί ανάλογος αναβρασμός, σύμφωνα και με τα αποτελέσματα έρευνας που τιτλοφορείται «Cyber Crime... and Punishment?»[76] και διεξήχθη το Δεκέμβριο του 2000 από την εταιρεία 'McConnell International' σε 52 χώρες. Κατεδείχθη λοιπόν ότι 33 από τις 52 χώρες δεν έχουν ακόμη προβεί σε κανενός είδους τροποποίηση της νομοθεσίας τους, προκει-

[75] Αρτινοπούλου Β. (2007) όπ. παρ.
[76] http://www.mcconnellinternational.com/services/cybercrime.htm

μένου να διώκονται κάποια από τα αδικήματα που τελούνται στον κυβερνοχώρο (βλ. φωτοτεχνικό πίνακα).

Figure 1: Extent of Progress on Updating Cyber Crime Laws



Οι Φιλιππίνες είναι η μόνη χώρα της οποίας η νομοθεσία έχει τροποποιηθεί, έτσι ώστε να αντιμετωπίζει ως ποινικό αδίκημα και τους δέκα τύπους εγκλημάτων στον κυβερνοχώρο. Στις ΗΠΑ δεν διώκεται ποινικά η πλαστογραφία και στην Ιαπωνία από την τσιμπίδα του νόμου ξεφεύγει η διασπορά ιών. Αξίζει να σημειωθεί ότι, ακόμη και όταν η νομοθεσία προβλέπει νομική δίωξη των κυβερνοεγκλημάτων, οι ποινές που ορίζονται δεν είναι ικανές να αποτρέψουν τα αδικήματα αυτά.

4.3 Τι ισχύει στην Ελλάδα

Στην ελληνική έννομη τάξη, νομοθεσία ειδική για θέματα Διαδικτύου που να ρυθμίζει τη συμπεριφορά των χρηστών του δεν υπάρχει. Ο όρος 'ηλεκτρονικό έγκλημα' δεν αναφέρεται πουθενά στο ελληνικό δίκαιο. Οι παραβάσεις που διαπιστώνονται για αδικήματα που διαπράττονται μέσω Διαδικτύου τιμωρούνται σύμφωνα με τη νομοθεσία της κλασικής μορφής τέλεσης των αδικημάτων αυτών. Ισχύουν νόμοι για εγκλήματα που διαπράττονται με Η/Υ (**1805/1988**), για την προστασία προσωπικών δεδομένων από τη χρήση των τηλεπικοινωνιών (**2867/2000,** ο

οποίος αντικατέστησε τον **2246/1994**), την προστασία προσωπικών δεδομένων κατά τη χρήση του Διαδικτύου (**2774/1999,** σε συνδυασμό με **2472/1997**), την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας (**2225/1994**, σε συνδυασμό με **3115/2003**) κ.λ.π. Επιπρόσθετα ειδικότερες διατάξεις για θέματα που σχετίζονται με το ηλεκτρονικό έγκλημα περιλαμβάνονται στο Π.Δ. 131/2003, το οποίο θεσπίσθηκε σε εφαρμογή κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο και αναφέρεται στην 'ανεπιθύμητη αλληλογραφία' και στην ευθύνη των παρόχων υπηρεσιών Διαδικτύου για πράξεις των χρηστών τους.

Ειδικά ο **Ν. 1805/1988,** τροποποίησε - συμπλήρωσε τις σχετικές διατάξεις του Π.Κ, που αφορούν τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές. [77]Πιο συγκεκριμένα προστέθηκαν τέσσερα εμβόλιμα άρθρα: εδαφ.β΄ στο άρθρο 13 περ.γ΄ (που περιγράφεται η έννοια του εγγράφου), 370β, 370γ και 386α.

Αναφορικά με τις περιπτώσεις πλαστογραφίας με υπολογιστή εφαρμόζεται και ο Ν. 1608/50, όπως τροποποιήθηκε με το **Ν. 1738/87**. Ειδικότερα, η παράνομη αντιγραφή δεδομένων ή λογισμικού συνιστά πλαστογραφία, αν ο δράστης ενεργεί με το σκοπό να παραπλανήσει άλλον με τη χρήση του αντιγράφου για γεγονός που μπορεί να έχει έννομη σημασία, ενώ η χρήση του αντιγραμμένου λογισμικού συνιστά επιβαρυντική περίπτωση. Επιπλέον, η αλλοίωση των δεδομένων μπορεί να πληροί την ειδική υπόσταση της πλαστογραφίας με τη μορφή της νόθευσης.

Φυσικά όταν καταρτιζόταν ο νόμος αυτός, το Διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη κατάρτισης ειδικότερης νομοθεσίας. Ανεξάρτητα όμως από το εάν ο Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής, το βέβαιο είναι ότι δεν επαρκεί να καλύψει τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του Διαδικτύου.

Απ' την άλλη έχει υποστηριχθεί η άποψη [78]ότι δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομι-

[77] Ιγγλεζάκης Ι. (2006) «*Εισαγωγή στο δίκαιο της πληροφορικής*», Εκδόσεις Σάκκουλα, Αθήνα, σελ. 209, 221.
[78] της Εθνικής Επιτροπής Τηλεπικοινωνιών στο περιοδικό 'Ο κόσμος του internet', Νοέμβριος 1997, σελ. 45

κό κενό στο Διαδίκτυο, διότι αναλογικά το κοινό δίκαιο μπορεί να εφαρμοστεί και στο χώρο του Διαδικτύου. Η άποψη αυτή βέβαια είναι εμφανώς εσφαλμένη, καθότι στον ποινικό τουλάχιστο χώρο, δεν ισχύει η αρχή της αναλογίας.

Στο βαθμό, λοιπόν, που τα προβλεπόμενα εγκλήματα (άρθρα 370β, 370γ, 386α) διαπράττονται και σε περιβάλλον Διαδικτύου, τότε τα άρθρα αυτά εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

[79]Τα εγκλήματα του κυβερνοχώρου τελούνται με απαραίτητη προϋπόθεση τη χρήση τηλεπικοινωνιών, σταθερής ή κινητής τηλεφωνίας (Υπηρεσίες WAP). Ο **Ν. 2246/1994** ψηφίστηκε για την οργάνωση και εν γένει λειτουργία του τομέα τηλεπικοινωνιών και ρυθμίζει θέματα σχετικά με το Διαδίκτυο. Προσδιορίζει συγκεκριμένα ότι φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι τα φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού. Σύμφωνα με το άρθρο 2 παρ. 3 Ν. 2246/1994 συνιστάται η Εθνική Επιτροπή Τηλεπικοινωνιών, η οποία έχει τεχνικές, νομικές και προανακριτικές αρμοδιότητες, γνωμοδοτεί για την έκδοση των κωδίκων δεοντολογίας, επιβάλλει διοικητικά πρόστιμα, και ελέγχει γενικώς την ομαλή και ορθή λειτουργία του τομέα τηλεπικοινωνιών. Σύμφωνα με το **Ν. 2472/1997** (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) προβλέπονται ποινικές κυρώσεις για όποιον προβαίνει σε διασύνδεση αρχείων χωρίς να τη γνωστοποιήσει στην αρμόδια αρχή και για όποιον χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων αυτών, ή τα αφαιρεί, αλλοιώνει, βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο. Αυτή είναι μία γενική διάταξη, που αποσκοπεί πράγματι στην προστασία προσωπικών δεδομένων, αλλά δεν καλύπτει τα γνήσια εγκλήματα κυβερνοχώρου, αφού η διασύνδεση αρχείων ή η επέμβαση σε δεδομένα, ή η διάδοση δεδομένων, η επεξεργασία και ανα-

[79] Σόφος Θ. (2001) «*Η Θέμιδα τώρα 'βλέπει' προς την οθόνη*», Εφημερίδα 'Ελευθεροτυπία'.

κοίνωσή τους μπορεί να πραγματοποιηθεί και χωρίς τη βούληση και γνώση του κατόχου ηλεκτρονικού υπολογιστή ή του χρήστη του Διαδικτύου. Π.χ. ένας κατευθυνόμενος από το δράστη ηλεκτρονικός «ιός» (virus) προσβάλλει το σύστημα και χρησιμοποιεί όλες τις ηλεκτρονικές διευθύνσεις (e-mail) φίλων, γνωστών του κ.λπ., που έχει αποθηκεύσει ο ανυποψίαστος κάτοχος και χρήστης του Διαδικτύου, προκειμένου να αποστείλει ο δράστης σε αυτούς ευαίσθητα προσωπικά δεδομένα. Η χρήση συγκεκριμένων κωδίκων για τη μετατροπή δεδομένων με σκοπό την ανάγνωσή τους αποσκοπεί στην προστασία των δεδομένων αυτών. Με την κρυπτογραφία αποτρέπεται δηλαδή η πρόσβαση σε δεδομένα από μη εξουσιοδοτημένα πρόσωπα. Προς τούτο έχει διαμορφωθεί ένας ιδιαίτερος επιστημονικός κλάδος, η διαχείριση ασφάλειας δικτύων («security administration»).

Σύμφωνα με το άρθρο 1 του **Ν. 2225/1994** ιδρύεται η Εθνική Επιτροπή Προστασίας Απορρήτου των Επικοινωνιών, της οποίας αποστολή είναι και η προστασία του απορρήτου της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης. Υπό τις προϋποθέσεις του Ν. 2225/1994 είναι δυνατή η παρακολούθηση ανταλλαγής ηλεκτρονικής αλληλογραφίας (e-mail). Π.χ. ο Α εκβιάζει τον Β με την αποστολή e-mail, ο Β καταγγέλλει την εκβίαση στην αστυνομία και η αστυνομία ζητά από τον παροχέα (Internet Service Provider) να παρακολουθήσει την ανταλλαγή e-mail. Ο παροχέας δεν δικαιούται να επικαλεστεί το απόρρητο των επικοινωνιών.

[80]Πρόσφατα τέθηκε σε ισχύ το Π.Δ 47/2005,από την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε), που αφορά τις διαδικασίες, τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του

Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων Διεθνών Οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων. Και οι τρεις παραπάνω Διεθνείς Οργανισμοί έχουν ασχοληθεί με το έγκλημα στον Κυ-

[80] Αρτινοπούλου Β. (2007) όπ. παρ.

βερνοχώρο. Σχετική όμως Σύμβαση -όπως είδαμε παραπάνω- καταρτίσθηκε μόνο στα πλαίσια του Συμβουλίου της Ευρώπης.

Τι γίνεται όμως στην πράξη;

Στην πράξη [81]αστυνομικοί, εισαγγελείς, δικαστές και δικηγόροι αναζητούν ακόμα τις τεχνικές γνώσεις και το νομικό οπλοστάσιο που απαιτούνται για τη διαλεύκανση υποθέσεων που σχετίζονται με το Διαδίκτυο. Το πρόβλημα που υπάρχει από την έλλειψη εμπειρίας και τεχνογνωσίας είχε διατυπώσει πριν από λίγα χρόνια ο εισαγγελέας Αγγελής Ι., ο οποίος είχε επισημάνει ότι:

«*…όλοι όσοι ασχολούνται με τη διαλεύκανση τέτοιων υποθέσεων πρέπει να κατέχουν πολύ εξειδικευμένες γνώσεις περί τεχνολογίας (ηλεκτρονικών υπολογιστών και Διαδικτύου). Βέβαια, ακόμη και αν φτάσουμε σε αυτό το επίπεδο, η τεχνολογία θα συνεχίσει να εξελίσσεται με μεγάλη ταχύτητα και η νομική επιστήμη να ακολουθεί ασθμαίνουσα. Τουλάχιστον, όμως, τότε θα έχουν εκδικαστεί κάποιες υποθέσεις και θα έχει παραχθεί νομολογία*».

Στο μεταξύ, λόγω έλλειψης εμπειρίας, τόσο οι δικαστικές όσο και οι διωκτικές αρχές[82] αδυνατούν να συλλάβουν τις πραγματικές διαστάσεις και τις μορφές που μπορεί να λάβει το ηλεκτρονικό έγκλημα ώστε να το εξιχνιάσουν και να αποδώσουν δικαιοσύνη. Σχετική εκπαίδευση δεν προβλέπεται ούτε καν στο σημερινό πρόγραμμα σπουδών της Εθνικής Σχολής Δικαστών, ώστε οι μελλοντικοί εκπρόσωποι του κλάδου να είναι πιο καταρτισμένοι.

Αλλά και οι δικηγόροι στην πλειονότητά τους δεν είναι καθόλου εξοικειωμένοι ή αγνοούν πλήρως υποθέσεις ηλεκτρονικής εγκληματικότητας ώστε να υπερασπιστούν πολίτες που έχουν εξαπατηθεί ή προσβληθεί. Πάντως, υπάρχουν αρκετοί νεότεροι δικηγόροι που έχουν κάνει διδακτορικό σε ηλεκτρονικές εφαρμογές, μεταξύ των οποίων είναι και το Διαδίκτυο.

Όπως εξηγεί άλλωστε ο καθηγητής Ποινικών Επιστημών Μυλωνόπουλος Χ., «*Ως εμπειρογνώμονες υπάρχουν ειδικοί στην ασφάλεια δικτύων. Αλλά αυτό απαιτεί υψηλή εξειδίκευση, με συνέπεια να δυσχεραίνεται η επικοινωνία μεταξύ του νομικού και του ειδικού στην*

[81] Μπούμπουκα Α. (2006) «*Τυφλή η Θέμιδα στο Διαδίκτυο*», Εφημερίδα 'Κυριακάτικη Ελευθεροτυπία'.
[82] Η αστυνομική διερεύνηση γενικότερα, αλλά και η ανακριτική προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις. Εξειδικευμένες γνώσεις. Για τις δυσκολίες στον εντοπισμό και τη δίωξη του πληροφορικού εγκλήματος βλ. Λάζος Γ. (2001) «*Πληροφορική και έγκλημα*», Νομική Βιβλιοθήκη, Αθήνα, σελ. 211επ.

ασφάλεια δικτύου, πολλοί σίγουρα καταφεύγουν και σε ειδικούς στο εξωτερικό για τέτοιες περιπτώσεις».

Επιπρόσθετα [83]το πρόβλημα της **δικαιοδοσίας** στα εγκλήματα που τελούνται στο Διαδίκτυο δεν είναι απλό, καθώς το Διαδίκτυο λόγω της παγκοσμιότητάς[84] του επιτρέπει στον οποιοδήποτε να εισάγει και να καταστήσει προσβάσιμη από όλα τα σημεία του πλανήτη οποιαδήποτε πληροφορία θελήσει. Για την ανεύρεση της αρμοδιότητας του δικαστηρίου πρέπει να καθοριστεί ο τόπος τέλεσης του αδικήματος. Για τον καθορισμό του τόπου τελέσεως του αδικήματος υποστηρίζονται τέσσερις θεωρίες:

α) Η θεωρία του τόπου ενέργειας, σύμφωνα με την οποία ως τόπος τέλεσης θα πρέπει να θεωρηθεί ο τόπος όπου ετελέσθη η ενέργεια που έτεινε στο άδικο αποτέλεσμα και αν η ενέργεια έλαβε χώρα σε περισσότερα από ένα κράτη, καθώς και ο τόπος όπου ολοκληρώθηκε.

β) Η θεωρία του τόπου του αποτελέσματος, όπου ως τόπος τελέσεως θεωρείται ο τόπος όπου εκδηλώθηκε το ζημιογόνο αποτέλεσμα.

γ) Η μικτή θεωρία, όπου ως τόπος τελέσεως θεωρείται τόσο ο τόπος ενέργειας όσο και ο τόπος του αποτελέσματος με δικαίωμα επιλογής του αδικηθέντος.

δ) Η θεωρία του βαρύνοντος τόπου, σύμφωνα με την οποία ο τόπος του αδικήματος εντοπίζεται στο κράτος όπου το έγκλημα εκδηλώθηκε κατά την κύρια σημασία του. Βέβαια υπάρχουν δυσκολίες κατά την εφαρμογή της θεωρίας δεδομένου ότι είναι δύσκολο να καθοριστεί ο βαρύνων τόπος για την τέλεση της Διαδικτυακής αδικοπραξίας.

Κλείνοντας θα θέλαμε να τονίσουμε ότι στους όποιους ‘περιορισμούς’ αντιτίθεται το άρθρο 5α του Συντάγματος της Ελλάδας:

1. Καθένας έχει δικαίωμα στην πληροφόρηση, όπως νόμος ορίζει. Περιορισμοί στο δικαίωμα αυτό είναι δυνατόν να επιβληθούν με νόμο μόνο εφόσον είναι απολύτως αναγκαίοι και δικαιολογούνται για λόγους εθνικής ασφάλειας, καταπολέμησης του εγκλήματος ή προστασίας δικαιωμάτων και συμφερόντων τρίτων.
2. Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλ-

[83] Ομιλία με θέμα «*Το έγκλημα παραμένει έγκλημα ακόμα και όταν πραγματοποιείται ηλεκτρονικά*» των: Παπαντωνίου Αντωνίου και Σερκετζή Νικολάου, του Τμήματος Ηλεκτρονικού Εγκλήματος Θεσσαλονίκης (http://www.ekato.org/gr/Conference_Speeches/ANTONIS_PAPANTONIOY.pdf)
[84] Τα κύρια χαρακτηριστικά του εγκλήματος: παγκοσμιότητα, διαχρονικότητα, αλληλεξάρτηση των στοιχείων του εγκληματικού φαινομένου, και η αμφισβήτηση και η δυσχέρεια ορισμού των στοιχείων του βλ. Φαρσεδάκης Ι. (1996) «*Στοιχεία εγκληματολογίας*», Αθήνα, Νομική Βιβλιοθήκη, σελ 72-74.

λαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9α και 19.

Γ΄ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 5. ΠΡΟΤΑΣΕΙΣ - ΜΕΤΡΑ ΠΡΟΛΗΨΗΣ

Εισαγωγή

Αφού επεξεργαστήκαμε αρκετές εκδοχές για το ξεκίνημα του Κεφαλαίου αυτού, κρίθηκε βέλτιστο να ξεκινήσουμε με την εξής παραδοχή. Το ηλεκτρονικό έγκλημα με όποια μορφή και αν υιοθετεί εξαπλώνεται και μάλιστα με γοργούς ρυθμούς. Οι λόγοι αυτής της ταχύτατης εξέλιξης συνοψίζονται στους ακόλουθους.

Καταρχήν το Διαδίκτυο σαν χωροχρόνος είναι αχανές, ο χρόνος της επικοινωνίας καταρρέει και συρρικνώνεται στο μηδενικό μέγεθος του στιγμιαίου, τα σημάδια του χώρου και του χρόνου παύουν να έχουν σημασία[85]. Πάνω στο θέμα αυτό θα παραθέσουμε ορισμένα στοιχεία που κατορθώσαμε να συγκεντρώσουμε. Πρόσφατα λοιπόν, μόλις [86]την τελευταία δεκαετία του 20ου αιώνα η παγκόσμια επιστημονική κοινότητα ανακάλυψε το καταθετήριο και διακινητήριο πληροφοριών που λέγεται Διαδίκτυο. Ήταν ό,τι καλύτερο μπορούσε να συμβεί σε μια εποχή που η συσσωρευμένη γνώση είχε γεμίσει κάθε αστικό αποθηκευτικό χώρο με άπειρα αρχεία. Έτσι τη δεκαετία που ακολούθησε όλοι βάλθηκαν να μεταφέρουν τα πάντα στο γνωστό μας Internet. Δίκτυα, υποδίκτυα και υπερδίκτυα κάθε είδους στήθηκαν, άλλα ανοιχτά σε όλους (ο γνωστός μας Παγκόσμιος Ιστός - το Web) και άλλα προσβάσιμα μόνον στους πεφωτισμένους. Η 'νέα γραφή' που είχε ανακαλύψει ο άνθρωπος, η 'υπερκειμενική' του Internet, του επέτρεπε πλέον να καταγράφει οτιδήποτε ψηφιακά, σε υπερσυμπιεσμένη μορφή.

Όπως έδειξε αυτή η πρώτη δεκαετία διαδικτύωσης, το Internet και οι κόμβοι του **δεν είναι απλά μία ακόμη υποδομή καταχώρισης στοιχείων και ενημέρωσης, αλλά και ένας πολλαπλασιαστής των εξελίξεων**. Η πολυδιασταύρωση στοιχείων και ιδεών, όπως και η δυνατότητα επεξεργασίας προβλημάτων από δικτυωμένους υπολογιστές ανά τον κόσμο, έφεραν τις επί μέρους επιστήμες και τεχνολογίες πολλά βήματα μπροστά. Οι εξελίξεις είναι πλέον τό-

[85] Bauman Z. (2004) «*Παγκοσμιοποίηση. Οι συνέπειες για τον άνθρωπο*», Εκδόσεις Πολύτροπον, Αθήνα, σελ. 26.
[86] Καφαντάρης Τ. (2004) «*Η κιβωτός της γνώσης*», Εφημερίδα 'Βήμα Science', σελ. Η01, κωδικός άρθρου: Β14188Η011, ID: 263464.

σες πολλές, ώστε τα εξειδικευμένα ενημερωτικά δελτία να μοιάζουν με τα δελτία ειδήσεων της τηλεόρασης: τα νέα του πρωινού ‘μπαγιατεύουν’ ως το απόγευμα.

Παράλληλα γιγαντώνεται το ποιοτικό πρόβλημα αξιολόγησης και κατάταξης των επιστημονικών εξελίξεων. **Ποιος μπορεί να κρατήσει αξιόπιστο λογαριασμό σε αυτόν τον κυκεώνα ανακοινώσεων, δημοσιεύσεων, σχολιασμών και αντιπαραθέσεων**; Τέλος, η ‘ακράτεια παραγωγής πληροφοριών’, που ευνοεί το Διαδίκτυο, επαναφέρει το πρόβλημα της καταχώρισης και αποθήκευσης, με νέα οξύτητα και σε νέα διάσταση.

Η ‘ψηφιακή χαρτούρα’, που αντικατέστησε την κλασική, είναι πλέον επιφορτισμένη με πολλαπλάσιο όγκο πληροφοριών, καθώς σε κάθε σελίδα χαρτιού αντιστοιχεί τώρα ένα αρχείο πολυμέσων (multimedia), όπου το κείμενο διανθίζεται με γραφήματα, γραφικά, ήχους και βιντεοσκοπημένες παρουσιάσεις, συν μια τεράστια πλέον βιβλιογραφία, που με τη σειρά της παραπέμπει σε αντίστοιχα φορτωμένες πολυμεσικές σελίδες. Όλα αυτά απαιτούν όχι μόνον αποθηκευτικούς χώρους και διαδικασίες ξεδιαλέγματος, αλλά και δικτύωση ακόμη μεγαλύτερης χωρητικότητας για τη διακίνησή τους.

Όπως είχε μετρηθεί το Νοέμβριο του 2002, ο κόσμος μας παράγει ετησίως 2.000.000.000 γιγαμπάιτ νέων πληροφοριών, από τις οποίες εκτυπώνεται σε χαρτί μόλις το 0,003%. Μόνο στο Διαδίκτυο παράγονται καθημερινά 7.300.000 νέες σελίδες.

Όλη αυτή η έκταση του Διαδικτύου διευκολύνει κατά κάποιον τρόπο τη διάπραξη εγκλημάτων, καθώς δημιουργεί την εντύπωση περί ύπαρξης ανωνυμίας. Απ’ την άλλη ο εντοπισμός των κατά περίπτωση δραστών δυσχεραίνει, γεγονός που οφείλεται στη δυσκολία εντοπισμού και ανάλυσης των ψηφιακών ιχνών που αφήνουν οι δράστες.

Ένα πρόσθετο πρόβλήμα στο διαφαινόμενο χάος αποτελεί η μη εναρμονισμένη νομοθεσία μεταξύ των κρατών, ούτως ώστε να υπάρχει μια κοινή ασπίδα άμυνας και ευρύτερης επικοινωνίας. Παράλληλα τα διαλαμβανόμενα μέτρα ασφάλειας θα λέγαμε ότι παρουσιάζουν αρκετές ελλείψεις και είναι αλήθεια ότι στο σημείο αυτό υπάρχουν πολλά που θα μπορούσαν να γίνουν.

Με βάση όλα τα παραπάνω, θα αναπτύξουμε ορισμένες προτάσεις - μέτρα πρόληψης, που περιλαμβάνουν όλους εκείνους τους [87]παρεμβατικούς, αμυντικούς, τιμωρητικούς μηχανισμούς που αποβλέπουν στην αποτροπή από το έγκλημα και γενικά στον περιορισμό της εγκληματικότητας.

5.1 Προτάσεις - Μηχανισμοί Δίωξης

5.1.1 Αναβάθμιση και μετεξέλιξη των μηχανισμών δίωξης

Η παγκοσμιοποίηση του εγκλήματος, σε συνδυασμό με τις συντελούμενες ευρύτερες κοινωνικοπολιτικές, οικονομικές και τεχνολογικές ανακατατάξεις, απαιτούν ριζικές αλλαγές στο υφιστάμενο Διεθνές Νομικό Πλαίσιο, καθώς και στα Εθνικά, Αστυνομικά και Δικαστικά συστήματα. [88]Οι δυνάμεις καταστολής άλλωστε οφείλουν να ενεργοποιούνται σ' ένα πρώιμο του εγκλήματος στάδιο, καταδιώκοντας ό,τι εκφεύγει από τα αφηρημένα όρια της κοινωνικής κανονικότητας και ό,τι προκαλεί τη συλλογική ηθική, [89]καθώς κάθε ρωγμή στο σύστημα τάξης μπορεί να οδηγήσει στον εκφυλισμό των νόμων και στο έγκλημα.

Στο πλαίσιο αυτό, καθίσταται επιτακτική η ανάγκη εκσυγχρονισμού των διωκτικών μεθόδων και διαδικασιών, που εφαρμόζουν οι Διωκτικές Αρχές στη δίωξη του εγκλήματος, η αποτελεσματικότητα των οποίων θα εξαρτηθεί σύμφωνα με τον τέως Διευθυντή της Διεύθυνσης Εγκληματολογικών Ερευνών της ΕΛ.ΑΣ Κυριακάκη Ε.[90], σε μεγάλο βαθμό από την εκμετάλλευση των δυνατοτήτων των Εγκληματολογικών Εργαστηρίων.

Ειδικότερα προκειμένου η Διεύθυνση Εγκληματολογικών Ερευνών να είναι αυτοτελής, διεπιστημονική, έχοντας εθνική και όχι μόνο εμβέλεια και να παραμείνει εφάμιλλη των Εγκληματολογικών Υπηρεσιών των τεχνολογικά προηγμένων Χωρών, ώστε να ανταποκριθεί

[87] Σπινέλλη Κ. (1982) «*Η Γενική Πρόληψη των εγκλημάτων. Θεωρητική και εμπειρική διερεύνηση μορφών κοινωνικού ελέγχου*», Εκδόσεις Α.Ν. Σάκκουλας, σειρά Ποινικά, Αθήνα, σελ. 56.
[88] Παπαθεοδώρου Θ. (2002) «*Δημόσια ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση*», Νομική Βιβλιοθήκη, Αθήνα, σελ.233.
[89] Βιδάλη Σ. (2001) «*Η ελληνική αστυνομία του 21ου αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής*», στο Πανούσης Γ. - Βιδάλη Σ. (2001) «*Κείμενα για την αστυνομία και την αστυνόμευση*», Εκδόσεις Α.Ν. Σάκκουλας, σειρά Εγκληματο-Λογικά, Αθήνα, σελ.15-26, σελ.17.
[90] Κυριακάκης Ε. όπ. παρ.

κατά τον καλύτερο δυνατό τρόπο στη σημαντική αποστολή της, είναι ανάγκη να αναβαθμισθεί και να μετεξελιχθεί σε '**Εθνικό Κέντρο Αστυνομικών και Εγκληματολογικών Ερευνών**'.

Προς το σκοπό αυτό, απαιτείται να γίνει οργανωτικός και λειτουργικός ανασχεδιασμός της Δ.Ε.Ε, ο οποίος να περιλαμβάνει, μεταξύ των άλλων, την ίδρυση Σχολής Εγκληματολογικών Σπουδών και τη δημιουργία Κέντρου Περιφερειακής Συνεργασίας στην Υ.Ε.Ε.Β.Ε (Θεσσαλονίκη), για παροχή τεχνογνωσίας σε θέματα εγκληματολογικής έρευνας, στις Βαλκανικές και πρώην Ανατολικές χώρες.

Απ' την άλλη σύμφωνα με μια πρόταση που είχε διατυπωθεί αρχικώς από τον τέως υπουργό Δημόσιας Τάξης Παπαθεμελή Στ., η [91]ανάγκη αποτελεσματικής αντιμετώπισης των νέων μορφών εγκληματικότητας πρέπει να περνάει μέσα από την αναζήτηση νέων μορφών αστυνομικής δράσης. Έτσι, λοιπόν, δεν θα πρέπει να αποκλείεται ακόμη και η σύσταση ειδικού σώματος αστυνομικών ερευνητών (detectives). Η ηγεσία του Υπουργείου έχει επεξεργασθεί και ολόκληρο σχέδιο για τη στελέχωση του νέου Σώματος. Κατ' αρχήν προβλέπεται η δημιουργία 22 θέσεων ειδικού επιστημονικού προσωπικού, με σχέση εργασίας ιδιωτικού δικαίου αορίστου χρόνου, που θα κατανέμονται ως εξής: 3 θέσεις σε θέματα εγκληματολογίας, 2 θέσεις σε θέματα ψυχιατρικής, 7 θέσεις σε θέματα Ποινικού Δικαίου, 2 θέσεις σε θέματα ιατροδικαστικής, 3 θέσεις σε θέματα οικονομικών επιστημών, 2 θέσεις σε θέματα αρχαιολογίας και 3 θέσεις σε θέματα αιρέσεων και θρησκειολογίας.

Αποστολή των ειδικών επιστημονικών ερευνητών θα είναι: *«η συμβολή τους στη συστηματικότερη, μεθοδικότερη και αποτελεσματικότερη καταπολέμηση του οργανωμένου εγκλήματος και άλλων σοβαρών μορφών εγκληματικότητας καθώς και στη διαλεύκανση συμβάντων ιδιαίτερου αστυνομικού ενδιαφέροντος, με την παροχή υπηρεσιών ερευνητικής, επιστημονικής και τεχνικής υποστήριξης στο επιτελικό, διερευνητικό, προανακριτικό και ανιχνευτικό έργο των αστυνομικών αρχών»*.

[91] Νικολακόπουλος Δ. (1997) «*Οι κομμουνιστοφάγοι έγιναν detectives Οι κοινωνικές και πολιτικές εξελίξεις μετά τη μεταπολίτευση άλλαξαν και τον έλληνα αστυνομικό*», Εφημερίδα 'Το Βήμα', σελ. Α24, κωδικός άρθρου: Β12429Α241 ID: 11530.

Προϋπόθεση για τη δημιουργία του νέου τύπου αστυνομικού θεωρείται και η αποσαφήνιση των διατάξεων που θίγουν τα ατομικά δικαιώματα των πολιτών. Ήδη υπόψη της πολιτικής ηγεσίας του Υπουργείου έχουν τεθεί εκθέσεις των υπηρεσιών της ΕΛ.ΑΣ, όπου επισημαίνονται τα εξής: *«Από την μέχρι τώρα εμπειρία προκύπτει η ανάγκη αλλά κρίνεται και υπηρεσιακώς σκόπιμη και επωφελής για πληρέστερη ενημέρωση και καθοδήγηση των αστυνομικών αρχών και του προσωπικού επί ορισμένων σημαντικών τομέων δράσης που άπτονται των ατομικών δικαιωμάτων των πολιτών»*. Οι τομείς αυτοί εντοπίζονται στις έρευνες, στις προσαγωγές ατόμων, στην προστατευτική φύλαξη ατόμων και στη χρήση των υπηρεσιακών όπλων. *«Η αποσαφήνιση των συναφών διατάξεων»*, αναφέρεται χαρακτηριστικά, *«συνεπάγεται μεγαλύτερη ασφάλεια χειρισμών και βελτίωση της αποτελεσματικότητας της αστυνομικής δράσης»*.

Τέλος δεν θα πρέπει να ξεχνάμε άλλη μια πρόταση που έχει κατά καιρούς διατυπωθεί και αφορά στη σύσταση Δικαστικής Αστυνομίας. Πιο συγκεκριμένα [92]ο όρος ‘αστυνομία’, όπως διδάσκεται στο διοικητικό δίκαιο, έχει δύο έννοιες, την ουσιαστική και την τυπική. Με την ουσιαστική έννοια, ‘αστυνομία’ αποκαλείται η «*πολιτειακή εκείνη ενέργεια, ήτις αποβλέπει εις την αποτροπήν παντός κινδύνου διαταράξεως της δημοσίας τάξεως*». Με την τυπική έννοια, ‘αστυνομία ή αστυνομική δύναμη’ ονομάζεται «*η δημόσια εκείνη υπηρεσία στην οποία είναι ανατεθειμένη η άσκηση της πολιτειακής ενέργειας της αστυνομίας*».

Η αστυνομία με την ουσιαστική της έννοια διακρίνεται σε διοικητική (administrative) και σε δικαστική (Judiciaire) αστυνομία ή αστυνομία καταδίωξης (κατά το Γαρδίκα)[93]. Το έργο της τελευταίας έχει κυρίως κατασταλτικό χαρακτήρα, δεδομένου ότι συνίσταται σε ανίχνευση και διακρίβωση των εγκλημάτων και της ταυτότητας των εγκληματιών, συγκέντρωση των αποδεικτικών στοιχείων και γενικά σε υποβοήθηση του ανακριτικού έργου[94].

---

[92] Αλεξιάδης Σ. (1998) «*Ανακριτική*», Εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη, σελ. 122 {Η. Κυριακοπούλου (1962) «*Ελληνικόν Διοικητικόν Δίκαιον*», Τομ. Γ΄, Έκδοση δ΄, σελ. 482επ. βλ. εκτενή ανάπτυξη Α. Τάχου (1990) «*Δίκαιο της δημόσιας τάξης*», Εκδόσεις Σάκκουλα, Θεσσαλονίκη}.

[93] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 122 {Παπανικολαΐδη Δ. (1960) «*Introduction génerale á la théorie de la police administrative*», σελ.13 επ.}.

[94] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 122 {Βουγιούκα «*Ποινικό Δικονομικό Δίκαιο*», τευχ.Ι, σελ. 60επ., Παπανικολαΐδη, Introduction, σελ.16}.

Ενώ όμως η παραπάνω διάκριση της αστυνομίας με ουσιαστική έννοια, σε διοικητική και δικαστική αστυνομία, δεν φαίνεται να δημιούργησε ιδιαίτερα προβλήματα (δεδομένου ότι στηρίζεται σε ουσιαστικό κριτήριο, δηλ. τη φύση του επιτελούμενου έργου), δεν συνέβη το ίδιο με το θέμα αν η διοικητική και η δικαστική αστυνομία θα πρέπει να είναι ανατεθειμένες στην ίδια ή σε διάφορες Υπηρεσίες. Το θέμα τούτο έχει ουσιαστική σημασία, γιατί η Υπηρεσία της δικαστικής αστυνομίας όχι μόνο θα είναι στελεχωμένη με όργανα ειδικευμένα και αναπόσπαστα στο έργο τους, αλλά και γιατί ως Υπηρεσία θα υπάγεται στις δικαστικές και όχι στις διοικητικές αρχές.

Δικαστική αστυνομία με την παραπάνω έννοια έχει οργανωθεί σε ορισμένες ευρωπαϊκές χώρες. Τα περισσότερα κράτη, όμως, διαφυλάσσουν και τις παραδοσιακές τους αστυνομικές Υπηρεσίες, ιδιαίτερα όταν αυτές έχουν αποκτήσει φήμη. Στη χώρα μας η άσκηση της δικαστικής αστυνομίας ή αστυνομίας καταδίωξης από ιδιαίτερη Υπηρεσία προβλεπόταν πριν εκατόν εξήντα χρόνια από το Β.Δ. της 31-12-1836 περί δημοτικής αστυνομίας (η οποία διακρινόταν σε διοικητική και σε δικαστική αστυνομία: άρθρο 2). Η δικαστική αστυνομία ήταν «*επιφορτημένη να εξετάζη τα εγκλήματα και πλημμελήματα, να συνάζη τας αποδείξεις και ενδείξεις, να εξακριβώνη τας περιστάσεις και να καταστρώνη τακτικά πρωτόκολλα περί των αυτουργχων».*

Γρήγορα όμως η λύση της 'δικαστικής αστυνομίας' εγκαταλείφθηκε και επικρινόταν ως αντιτιθέμενη *«εις την σύγχρονον ανάγκην και έννοιαν της αστυνομίας... ως εντελώς άστοχος, διότι η αστυνομία είναι οργανισμός ενιαίος η αστυνομία τάξεως και καταδιώξεως έχουσιν άρρικτον δεσμόν αμοιβαίας συνεργασίας, ώστε είναι αδύνατον εκ του ενιαίου τούτου οργανισμού να αποσπασθή η αστυνομία καταδιώξεως»*[95].

Αντίθετα, ο Γιώτης Χ. σε σχετική του εισήγηση, θεώρησε σκόπιμο τον πλήρη χωρισμό της δικαστικής από τη διοικητική αστυνομία[96]. Αλλά η αρνητική θέση επικράτησε ως τις μέρες μας.

Πρόσφατα, όμως, το θέμα ανακινήθηκε από δύο κατευθύνσεις:

[95] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 124.
[96] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 124 {βλ. Γιώτη Χ. (1954) «*Résumé du Rapport, Revue I.D.P.»,* σελ. 231. βλ. επίσης Χορομίδη Κ. «*Η δικαστική λειτουργία (Δικαιοσύνη)*» Αρμεν. 1982, σελ. 570}.

α) Το Φεβρουάριο του 1990 πραγματοποιήθηκε στη Μαδρίτη Ευρωπαϊκή Διάσκεψη, με τη συμμετοχή εκπροσώπων των κρατών-μελών των Ευρωπαϊκών Κοινοτήτων και θέμα τη 'Δικαστική Αστυνομία'[97].

β) Εκδηλώθηκε έντονη κίνηση υπέρ της ίδρυσης δικαστικής αστυνομίας στο δικαστικό χώρο. Αρχικά, υποβλήθηκε στο Υπουργείο Δικαιοσύνης από την Ένωση Εισαγγελέων υπόμνημα αρ.74/ 12.6.1987[98], το οποίο υπογράμμιζε την αδυναμία του δικαστικού λειτουργού να δράσει άμεσα και αποτελεσματικά προς εξιχνίαση σοβαρών εγκλημάτων, επειδή τούτο πρέπει να γίνεται με παραγγελίες σε αστυνομικές αρχές, οι οποίες εκτός των άλλων υπάγονται ευθέως και αμέσως στις διαταγές προϊσταμένων Υπηρεσιών, που κατευθύνονται από την εκτελεστική εξουσία.

Λίγα χρόνια κατόπιν, η Εταιρία Δικαστικών Μελετών αφιέρωσε μία από τις συναντήσεις της στο ίδιο ζήτημα της 'Δικαστικής Αστυνομίας', όπου στη σχετική εισήγηση[99] διαπιστώθηκε η ανάγκη ίδρυσης 'Δικαστικής Αστυνομίας', με την άμεση ή σταδιακή αναγωγή της σε αυτοτελή Υπηρεσία οργανικά συναρθρωμένη με τη δικαστική λειτουργία, στην οποία και ανήκει φυσιολογικά ως δυναμικός μοχλός, αφετήριος μηχανισμός και γι αυτό αποφασιστικός παράγων στην άσκηση της ποινικής δικαιοδοσίας.

Για την επίτευξη του στόχου αυτού προτάθηκαν δύο επιλογές: α) είτε η ίδρυση σε ορισμένες μεγάλες πόλεις ειδικών τμημάτων 'Δικαστικής Αστυνομίας' στελεχωμένων με αστυνομικούς ειδικευμένους στη δίωξη του εγκλήματος, β) είτε η ίδρυση στο Υπουργείο Δικαιοσύνης αυτοτελούς υπηρεσίας δικαστικής αστυνομίας, που θα στελεχώνεται από αστυνομικούς που θα έχουν το χαρακτήρα και την υπηρεσιακή κατάσταση δικαστικών υπαλλήλων κατά τους ορισμούς του άρθρου 92 παρ.1-3 Συντ.

---

[97] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 125 {βλ. την εισήγηση της Ελληνικής αντιπροσωπείας, Αστυνομική Επιθεώρηση, Μάιος 1990, σελ. 278 επ., και κριτικό σχόλιο Βονρβούλη Α. (1991) «*Το πρόβλημα της δικαστικής αστυνομίας*», Εφημερίδα 'Καθημερινή', σελ.13}.

[98] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 125 {βλ. Ελληνική εισήγηση στη Διάσκεψη της Μαδρίτης, Αστυνομική Επιθεώρηση, Μάιος 1990, σελ. 282, και Εφημερίδα 'Μακεδονία' της 25-10-1987}.

[99] Αλεξιάδης Σ. (1998) όπ. παρ. σελ. 125 {βλ. την εισήγηση Βελλή Γ. (1991) *«Δικαστική αστυνομία»*, Υπεράσπιση σελ. 123 επ.}.

Η Εταιρία Δικαστικών Μελετών υιοθέτησε την εν λόγω εισήγηση και έκρινε ενδεδειγμένη και πραγματοποιήσιμη σε πρώτο στάδιο την υπό (α) λύση. Προφανώς υπό την πίεση, που προαναφέρθηκε, του δικαστικού σώματος, το Υπουργείο Δικαιοσύνης σε νομοσχέδιο το οποίο κατάρτισε για την τροποποίηση των ποινικών κωδίκων περιέλαβε και ειδικό κεφάλαιο για την ίδρυση και οργάνωση Δικαστικής αστυνομίας. Η πρωτοβουλία αυτή χαιρετήθηκε από την Ολομέλεια των προέδρων των Δικηγορικών Συλλόγων Ελλάδος. Το κλίμα που καλλιεργήθηκε, κατά τα προηγούμενα, θεωρήθηκε κατάλληλο κι έτσι ο Ν. 2145/1993 που ακολούθησε περιέλαβε το μακροσκελές άρθρο 36, το οποίο προβλέπει τα σχετικά με την ίδρυση και την οργάνωση 'Δικαστικής Αστυνομίας'.

Επισημαίνεται ότι στο πάγιο αυτό αίτημα των δικαστικών ενώσεων και των εισαγγελέων της χώρας -το οποίο και παραμένει για περισσότερα από 15 χρόνια κενό γράμμα- [100]η ΕΛ.ΑΣ επιχειρηματολογεί ενάντια, με το σκεπτικό ότι θα υπάρξουν δυσλειτουργίες και αλληλοεπικαλύψεις αρμοδιοτήτων. Προφανώς η ΕΛ.ΑΣ διαισθάνεται ότι η λειτουργία ανεξάρτητου σώματος δικαστικής αστυνομίας, υπό τη διεύθυνση εισαγγελικού λειτουργού, θα της στερήσει ζωτικό χώρο δράσης και θα περιορίσει την έκταση της εξουσίας της.

Κατόπιν αυτών των αντιδράσεων οι εκπρόσωποι του υπουργείου Δικαιοσύνης, τελικά βρήκαν καταφύγιο στην Ευρώπη. Κάτω από την πίεση της Ευρωπαϊκής Επιτροπής κατά της Διαφθοράς (GRECO), που έκανε στην Ελλάδα συγκεκριμένη σύσταση για δημιουργία 'Δικαστικής Αστυνομίας', ένα ακόμη νομοσχέδιο για την ίδρυση 'Δικαστικής Αστυνομίας' είναι γεγονός.

Η αρχική ιδέα ήταν να ενταχθεί το σώμα αυτό στη δομή της ΕΛ.ΑΣ, ώστε να μην υπάρξουν προβλήματα επικάλυψης αρμοδιοτήτων. Τελικά, όμως, εκπονήθηκε σχέδιο νόμου για αυτοτελές σώμα. Οι βασικές αρχές του νομοσχεδίου αυτού προβλέπουν:

- Ίδρυση 'Δικαστικής Αστυνομίας', αρχικά στις μεγάλες εισαγγελίες, υπό τη διοίκηση και εποπτεία του προϊσταμένου των εισαγγελιών.

[100] Ζέρβας Χ. (2005) «*Η 'ΕΛ.ΑΣ.' της Σχολής Ευελπίδων*», Εφημερίδα 'Ελευθεροτυπία'.

- Συμμετοχή σε αυτή επιλεγμένου αριθμού υπαλλήλων της εισαγγελίας αλλά και ένστολων, ένοπλων υπαλλήλων που θα προσλαμβάνονται με τις διαδικασίες που ίσχυσαν για τους υπαλλήλους του σώματος εξωτερικής φρούρησης των φυλακών (βαθμολόγηση ειδικών προσόντων, όπως πτυχίων, γνώσης ξένων γλωσσών και αθλητικές εξετάσεις).
- Σύμφωνα με τις πρώτες εκτιμήσεις, για τη στελέχωση του νέου σώματος αλλά και για την αποτελεσματική λειτουργία του θα απαιτηθούν στο αρχικό στάδιο τουλάχιστον 300 υπάλληλοι.
- Η βασική απασχόληση του σώματος θα γίνεται σε επιδόσεις δικαστικών εγγράφων, εκτελέσεις αποφάσεων δικαστηρίων και διενέργεια προανακρίσεων με εντολή εισαγγελέα. Οι αρμοδιότητες αυτές θα ανακουφίσουν την αστυνομία από ανεπιθύμητα βάρη και θα προσδώσουν στις ανακριτικές ενέργειες μεγαλύτερη αξιοπιστία.
- Θα υπάρξει πρόβλεψη να ανατεθεί στη δικαστική αστυνομία αποκλειστικά η διενέργεια ερευνών για θέματα διαφθοράς, όπως είναι υποθέσεις δωροδοκίας, ξεπλύματος βρόμικου χρήματος κ.ά.
- Στα στελέχη του νέου σώματος θα ανατεθεί, επίσης, η φρούρηση των δικαστηρίων και η επιβολή της τάξης εντός των χώρων απονομής της δικαιοσύνης, γεγονός που θα επιτρέψει στην ΕΛ.ΑΣ την καλύτερη αξιοποίηση των δικών της στελεχών.

Το νομοσχέδιο φαίνεται να είναι έτοιμο προς κατάθεση, αλλά τα σενάρια που εκπορεύονται και πάλι από το Υπουργείο Δικαιοσύνης θέλουν το νέο σώμα παράρτημα της ΕΛ.ΑΣ.

Λαμβάνοντας υπόψη όλα τα παραπάνω που αφορούν στους επίσημους μηχανισμούς δίωξης θα ήταν άδικο να παραλείψουμε να αναφερθούμε στις δράσεις - αντιδράσεις στο ηλεκτρονικό έγκλημα που έχουν αναλάβει Μη Κυβερνητικές Οργανώσεις (ΜΚΟ), όπως λ.χ. αυτή του ‘Web Police’ και φυσικά να ελπίσουμε, χωρίς περαιτέρω αναλύσεις, στη συνέχιση του έργου τους και γιατί όχι στην ενδυνάμωσή τους.

5.1.2 Συνεργασία - Ανταλλαγή γνώσης και εμπειρίας κατά της εγκληματικής τεχνολογίας

Οι κοινωνίες πάντοτε αντιδρούσαν με τον έναν ή των άλλον τρόπο σε αυτό που καλείται εγκληματικό φαινόμενο, [101]καθώς κανένα εθνικό χαρακτηριστικό, κανένα πολιτικό σύστημα, κανένα κοινωνικο-οικονομικό σύστημα, κανένα νομικό σύστημα, καμία τιμωρία ή μεταχείριση απάλλαξαν ποτέ μια χώρα από το φαινόμενο αυτό. Αντίθετα παρατηρούμε την αύξησή του, την εμφάνιση νέων μορφών, συνοδευομένων μάλιστα, από τη βία.

Η αντίδραση αυτή σήμερα φαίνεται να επικεντρώνεται στο ηλεκτρονικό έγκλημα ως νέα μορφή εγκλήματος. Στο 'νέο αυτό εχθρό' μπορούμε να αντιτάξουμε όπλα, όχι αναγκαστικά 'υπερσύγχρονα' αλλά κλασικά. Αρκεί λοιπόν να ανατρέξουμε στο παλιό μας οπλοστάσιο όπου κρύβεται ένα σημαντικό όπλο που διαθέτουμε σαν κοινωνία δικαίου και δεν είναι άλλο από τους 'συμμάχους'.

Λέγοντας σύμμαχους εννοούμε όλους αυτούς που εργάζονται προς την ίδια κατεύθυνση την αντιμετώπιση δηλαδή των εγκληματικών δράσεων. Θεωρούμε λοιπόν ότι η όποια αντίδραση θα πρέπει να στηρίζεται και να ενισχύεται στη βάση της συνεργασίας και ανταλλαγής γνώσης των εμπλεκόμενων κάθε φορά διωκτικών οργάνων, προκειμένου αφενός να συγκεντρώνονται πληροφορίες και εμπειρία, αναφορικά με τις χρησιμοποιούμενες από τους δράστες εγκληματικές μεθόδους, αφετέρου να γνωστοποιούνται οι εφαρμογές των εγκληματολογικών (forensic) τεχνικών στην αντιμετώπιση της κατά περίπτωση εγκληματικής δράσης.

Σχετικό με τα παραπάνω είναι και το κείμενο της πολυσυζητημένης Συμφωνίας μεταξύ Ελλάδας - Τουρκίας που αν και [102]αναφέρεται στην καταπολέμηση της τρομοκρατίας, στο άρθρο 2 προβλέπει η συνεργασία μεταξύ των δύο Μερών να πραγματοποιείται -σύμφωνα με την εθνική νομοθεσία- μέσω: α) ανταλλαγής πληροφοριών και πείρας σε τομείς κοινού ενδιαφέροντος, β) ανταλλαγής πείρας στη χρησιμοποίηση εγκληματολογικής τεχνολογίας, καθώς και

[101] Φαρσεδάκης Ι. (1996) όπ. παρ., σελ. 11.
[102] Νικολακόπουλος Δ. (1999) «*Η αντιτρομοκρατική συμφωνία μεταξύ Ελλάδας και Τουρκίας*», Εφημερίδα 'Το Βήμα', σελ. Α05, κωδικός άρθρου: Β12792Α051, ID: 199194.

στις μεθόδους και στα μέσα της εγκληματολογικής έρευνας, γ) ανταλλαγής πληροφοριών, γνώσης και πείρας στον τομέα των μεθοριακών ελέγχων προκειμένου να ανακαλυφθούν παραποιημένα ταξιδιωτικά έγγραφα και για την πρόληψη παράνομης εισόδου και παράνομης μετανάστευσης, δ) ανταλλαγής φυλλαδίων, εκδόσεων και αποτελεσμάτων επιστημονικών ερευνών σε τομείς που καλύπτονται από τη Συμφωνία, με σχεδιοποίηση και λήψη μέτρων κοινού ενδιαφέροντος κ.λ.π.

Αντιλαμβανόμαστε λοιπόν με βάση την παραπάνω Συμφωνία, που παρατέθηκε ενδεικτικά, την ιδιαίτερη σημασία που δίδεται στη συνεργασία και την ανταλλαγή γνώσης και πείρας για την πρόληψη και την καταστολή του κατά περίπτωση εγκλήματος.

Ειδικά στον τομέα της εγκληματολογικής τεχνολογίας και προκειμένου να επιτευχθεί η επιδιωκόμενη εναρμόνιση των χρησιμοποιούμενων εγκληματολογικών τεχνικών η βελτίωση της ποιότητάς τους, αλλά και η απαιτούμενη ενημέρωση για τις τρέχουσες ‘εξελίξεις’ εγκληματολογικής δράσης, η Διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας έχει ενταχθεί στο Δίκτυο Εγκληματολογικών Ινστιτούτων (European Network of Forensic Science Institutes - E.N.F.S.I).

Το E.N.F.S.I[103] αριθμεί 53 εγκληματολογικά εργαστήρια που προέρχονται από 31 χώρες συμπεριλαμβανομένων των: Αυστρία, Βέλγιο, Βουλγαρία, Κροατία, Κύπρος, Τσεχία, Δανία, Εσθονία, Φινλανδία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιρλανδία, Ιταλία κ.λ.π.

[Κατωτέρω παρατίθεται χάρτης επί του οποίου εμφαίνονται τα προαναφερόμενα εργαστήρια].

[103] http://www.enfsi.org

[104]Σύμφωνα με το καταστατικό του, στόχος είναι: *«να κατοχυρωθεί η ποιότητα του έργου ανάπτυξης και παραγωγής αποτελεσμάτων της εγκληματολογικής επιστήμης σε όλη την Ευρώπη και να διατηρηθεί το προβάδισμα σε παγκόσμιο επίπεδο».* Το E.N.F.S.I επιτυγχάνει τους στόχους του με την πραγματοποίηση σχετικών συνεδριάσεων και με τις εργασίες των 15 ομάδων εργασίας εμπειρογνωμόνων, στις οποίες εξετάζονται όλες οι πτυχές των διαφόρων ειδικευμένων θεματικών πεδίων της εγκληματολογικής επιστήμης.

Τα εργαστήρια εγκληματολογικών ερευνών των κρατών μελών της Ευρωπαϊκής Ένωσης ενίσχυσαν τα τελευταία χρόνια σε σημαντικό βαθμό -στο πλαίσιο των εργασιών του E.N.F.S.I- τόσο τη συνεργασία μεταξύ τους, όσο και με τα εγκληματολογικά εργαστήρια των άλλων ευρωπαϊκών χωρών.

Τι άλλο όμως εξασφαλίζει η συνεργασία μεταξύ των αρμόδιων για την πρόληψη και την καταστολή οργανισμών; Στις περισσότερες χώρες, συμπεριλαμβανομένων των κρατών μελών της Ε.Ε, ισχύουν ελάχιστες τυπικές απαιτήσεις στα θέματα των ποιοτικών κανόνων που πρέπει να τηρούν τα εγκληματολογικά εργαστήρια. Πρόκειται για μία κατάσταση διαμετρικά αντίθετη από το καθεστώς που διέπει τον κλάδο των ειδών διατροφής και των ποτών, την έγκριση των νέων φαρμακευτικών ιδιοσκευασμάτων κ.λ.π. Σε όλους αυτούς τους τομείς, υπάρχουν ε-

[104] Βρυξέλλες, 18.5.2004 COM(2004) 376 τελικό (http://eur-lex.europa.eu/LexUriServ/site/el/com/2004/com2004_0376el01.doc).

πίσημοι φορείς οι οποίοι επιφορτίζονται με το έργο του ελέγχου της τήρησης των σχετικών προτύπων ποιότητας, πράγμα που έχει ως συνέπεια τα σχετικά αποτελέσματα των εργαστηριακών δοκιμών να είναι υπεράνω πάσης εύλογης αμφιβολίας και να μπορεί να γίνονται αποδεκτά αποτελώντας τη βάση για αποφάσεις που έχουν συνήθως έχουν πολύ σοβαρές επιπτώσεις.

Ένα πρώτο σημαντικό βήμα για τη βελτίωση του ποιοτικού επιπέδου των εργαστηρίων εγκληματολογικών ερευνών στην Ε.Ε είναι το αίτημα, από τη δεκαετία του 1980 και μετά, της επιβολής συγκεκριμένων ποιοτικών απαιτήσεων. Τα σχετικά πρότυπα υπάρχουν ήδη εδώ και πολλά χρόνια και συμπεριλαμβάνουν τόσο τις τεχνικές, όσο και τις οργανωτικές πτυχές οι οποίες είναι αναγκαίες για την κατοχύρωση ενός ορισμένου ελάχιστου ποιοτικού επιπέδου.

Κατ' αρχήν υπάρχει το πρότυπο NEN-EN-ISO/IEC 17025 που δεν έχει βέβαια ειδική εφαρμογή μόνο για τα εργαστήρια των εγκληματολογικών ερευνών. Επίσης υπάρχει το πρότυπο ILAC-G19:2002, το οποίο διευκρινίζει το πρότυπο 17025 σε συνάρτηση με τα εργαστήρια των εγκληματολογικών ερευνών.

Η θέσπιση του συστήματος διασφάλισης του ποιοτικού επιπέδου είναι δαπανηρή και χρονοβόρα. Για το λόγο αυτό, πρέπει να παραχωρηθεί στα εργαστήρια ένα αποδεκτό χρονικό διάστημα, για να συμμορφωθούν με τα εν λόγω πρότυπα.

Μέχρις στιγμής, υπάρχουν μόλις 6 εργαστήρια μέλη του E.N.F.S.I που διαθέτουν ένα επίσημο αναγνωρισμένο σύστημα διασφάλισης της ποιότητας με βάση τα δύο προαναφερθέντα πρότυπα ποιότητας. Ένα πρώτο σημαντικό βήμα για βελτίωση της ποιότητας των εργαστηρίων εγκληματολογικών ερευνών όλης της Ένωσης είναι κατά συνέπεια η αποδοχή από όλα τα εγκληματολογικά εργαστήρια της Ε.Ε ενός συστήματος διασφάλισης της ποιότητας που θα βασίζεται σε αυτά τα δύο πρότυπα και η αναγνώρισή τους από τους εθνικούς οργανισμούς τους έγκρισης.

Το E.N.F.S.I αποτελεί ένα χρήσιμο όργανο συνεργασίας για την εγκληματολογική επιστήμη στην Ευρωπαϊκή Ένωση. Καθώς όμως στους κόλπους του συμπεριλαμβάνει και μέλη που δεν ανήκουν στην Ευρωπαϊκή Ένωση, δεν είναι δυνατόν για την Ε.Ε να χρησιμοποιεί το

E.N.F.S.I ως το επίσημο όργανο που εκπροσωπεί τα συμφέροντά της στο χώρο της εγκληματολογικής επιστήμης. Συνεπώς, προτείνεται τα μέλη από την Ευρωπαϊκή Ένωση του E.N.F.S.I να συγκροτήσουν μία επίσημη επιμέρους ομάδα στο πλαίσιο του E.N.F.S.I, με την οποία η Ευρωπαϊκή Ένωση θα είναι σε θέση να επικοινωνεί επισήμως.

Στο επίπεδο της Ευρωπαϊκής Ένωσης υπάρχουν μόνο δύο νομικές πράξεις που σχετίζονται με την εγκληματολογική επιστήμη: πρόκειται για το ψήφισμα του Συμβουλίου της 9ης Ιουνίου 1997 σχετικά με την ανταλλαγή αποτελεσμάτων ανάλυσης του DNA[105] και το ψήφισμα του Συμβουλίου της 25ης Ιουνίου 2001 για το ίδιο θέμα[106].

Επιλέξαμε στη σύντομη αυτή αναφορά μας να παραθέσουμε, συνοπτικά, ορισμένα στοιχεία για το E.N.F.S.I, χωρίς αυτό να σημαίνει ότι δεν υπάρχουν και άλλοι αξιόλογοι φορείς συνεργασίας, διότι θεωρούμε ότι είναι χαρακτηριστικό παράδειγμα και πρότυπο συνεργασίας με πολύ αξιόλογο έργο. Στόχος και βαθύτατη επιθυμία μας είναι να γίνει αντιληπτή από τον αναγνώστη η αναγκαιότητα συνεργασίας, συντονισμού και ανταλλαγής γνώσης είτε μέσω συνεδριών είτε μέσω συναντήσεων - επισκέψεων κ.λ.π. των εμπλεκόμενων στο εγκληματικό φαινόμενο φορέων, προκειμένου η τεχνολογία να βοηθήσει με τις εφαρμογές της στον πόλεμο κατά του ηλεκτρονικού εγκλήματος.

5.2 Μέτρα πρόληψης διαφόρων φορέων

5.2.1 Χρηματοοικονομικά ιδρύματα

Πάνω στο θέμα λήψης προληπτικών μέτρων, θα εστιάσουμε στα χρηματοοικονομικά ιδρύματα για να δούμε, μέσα από ένα εξαιρετικό άρθρο των: Rebecca Sausner, Jennifer Robin Dunn & Michael Sisk, που δημοσιεύτηκε στο Περιοδικό 'Επιστημονικό Μάρκετινγκ', τεύχος

[105] ΕΕ C 193 της 24ης Ιουνίου 1997.
[106] ΕΕ C 187 της 3ης Ιουλίου 2001.

Απριλίου 2006[107], τις αντιδράσεις των τραπεζών στο πρόβλημα που λέγεται ηλεκτρονική απάτη και πλαστογραφία.

Σύμφωνα λοιπόν με την Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC) οι οικονομικές ζημιές από απάτες που πραγματοποιούνται με κλοπή ταυτότητας (identity theft) και άλλου είδους ηλεκτρονικές απάτες και πλαστογραφίες, φτάνουν στις ΗΠΑ τα 48 δισ. δολάρια. Ανεξάρτητα από την ακρίβεια αυτών των στοιχείων, ελάχιστα χρηματοοικονομικά ιδρύματα κυνηγούν με αποφασιστικότητα τους δράστες. Σύμφωνα με την Avivah Litan, αναλύτρια της Gartner[108] μόλις 1 στις 700 υποθέσεις κλοπής ταυτότητας και ηλεκτρονικής απάτης που σημειώνονται στις τράπεζες φτάνει στα δικαστήρια και ο ένοχος τιμωρείται. Αυτός είναι και ο λόγος που τα περιστατικά αυξάνονται.

Φυσικά, υπάρχουν τράπεζες όπως η Wachovia που δεν κρατούν παθητική στάση. Ο Brian McGinley, διευθυντής του Τμήματος Διαχείρισης Ζημιών της Wachovia, εκτιμά ότι αυτόν το χρόνο θα οδηγήσει 200 υπαλλήλους της τράπεζας στη Δικαιοσύνη με την κατηγορία διάπραξης ηλεκτρονικής απάτης, χάρη στην εξελιγμένη 'Τεχνολογία Ανίχνευσης Οικονομικών Εγκλημάτων' που απλώνει το δίχτυ της μέχρι τα ταμεία της τράπεζας. Με τα συστήματα ασφαλείας που έχει υιοθετήσει, η τράπεζα έχει γλιτώσει περισσότερα από 1.000.000$.

Άλλες τράπεζες όμως προτιμούν να προφυλάσσουν το όνομά τους και αποφεύγουν να δημοσιοποιούν αυτά τα περιστατικά. Πιστεύουν ότι το μέγεθος της οικονομικής ζημιάς δεν δικαιολογεί το κόστος της έρευνας και της νομικής δίωξης. Ωστόσο η στάση αυτή εξοργίζει τις Διωκτικές Αρχές που δεν ενδιαφέρονται μόνο να τιμωρήσουν τους ενόχους, αλλά και να αποθαρρύνουν άλλους που θα θελήσουν να ακολουθήσουν το παράδειγμά τους.

Σύμφωνα με τις διωκτικές αρχές, ο μόνος τρόπος για να συνετιστούν οι τράπεζες και να αλλάξουν στάση είναι να υποχρεωθούν με τη θέσπιση νέων Νόμων. Πρόκειται για ένα ενδεχόμενο του οποίου τις συνέπειες οι τράπεζες πρέπει να λάβουν σοβαρά υπόψη. Εξάλλου, μάλλον δεν έχουν ξεχάσει τις συνέπειες των αναρίθμητων Νόμων σχετικά με τη διαφύλαξη των

[107] http://www.morax.gr/ article_show.php?article _id=921
[108] Μία από τις μεγαλύτερες εταιρείες ερευνών και συμβουλευτικών υπηρεσιών στο χώρο του IT.

προσωπικών δεδομένων ή της κατευθυντήριας οδηγίας που ορίζει ότι οι τράπεζες πρέπει μέχρι το τέλος του 2006 να έχουν υιοθετήσει 'Τεχνολογία Διπλής Ταυτοποίησης του χρήστη για τις Διαδικτυακές Τραπεζικές Συναλλαγές'.

Πέρα όμως από το ζήτημα των τραπεζών που προτιμούν να κρύβουν το πρόβλημα, είναι και η διαφωνία που υπάρχει όσον αφορά το μέγεθος του προβλήματος. Οι στατιστικές σχετικά με τις απάτες έχουν γίνει κινούμενοι στόχοι και δεν υπάρχει κανείς που να συμφωνεί είτε με τον αριθμό των περιστατικών είτε με το μέγεθος της οικονομικής ζημιάς. Η FTC δηλώνει ότι κατά το 2003 υπήρξαν 10.000.000 θύματα κλοπής ταυτότητας, ένας αριθμός με τον οποίο οι περισσότερες τράπεζες διαφωνούν γιατί σ' αυτόν περιλαμβάνονται και τα θύματα απάτης με πιστωτικές κάρτες, όπως και οι νέοι λογαριασμοί που ανοίχτηκαν με πλαστά στοιχεία. Γιατί όμως το ανέχονται, οι τράπεζες;

Σε γενικές γραμμές υπάρχουν δύο κατηγορίες οικονομικών εγκλημάτων. Αυτά που ενορχηστρώνονται από οργανωμένα κυκλώματα και αυτά που διαπράττονται από ανεξάρτητα άτομα για προσωπικό κέρδος. Και οι δύο κατηγορίες συμβάλλουν στη διάβρωση της εμπιστοσύνης του καταναλωτή. Δεν είναι τυχαίο ότι έρευνες δείχνουν ότι η επιφυλακτικότητα των καταναλωτών απέναντι στις ηλεκτρονικές συναλλαγές αυξάνεται συνεχώς, αν και στην πραγματικότητα ο μεγάλος όγκος των οικονομικών εγκλημάτων αυτής της μορφής διαπράττεται στο φυσικό και όχι στο δικτυακό χώρο.

Οι μικροεγκληματίες είναι σχετικά εύκολο να εντοπιστούν από τις αστυνομικές αρχές. Ωστόσο αυτό που ανησυχεί ιδιαίτερα τις αρχές είναι τα οργανωμένα κυκλώματα, καθώς μια χούφτα εγκληματίες μπορούν να προκαλέσουν ζημιά σε εκατοντάδες εκατομμύρια ανθρώπων. Και όσο κι αν η ιδέα είναι ανατριχιαστική, δυστυχώς οι συνθήκες δημιουργούν το κατάλληλο περιβάλλον.

Ωστόσο, η Wachovia έχει απτές αποδείξεις για τον αποτρεπτικό χαρακτήρα των 'Συστημάτων Ανίχνευσης Οικονομικών Εγκλημάτων' που εφαρμόζει στα καταστήματά της. Σύμφωνα με πληροφοριοδότες και ανθρώπους που έχουν συλληφθεί, οι εγκληματίες αποφεύγουν συ-

γκεκριμένες τράπεζες γιατί ο κίνδυνος σύλληψης είναι αυξημένος. Η αλήθεια είναι ότι **η τράπεζα που τηρεί αυστηρή στάση απέναντι στο οικονομικό έγκλημα δεν αποτρέπει εντελώς τον κίνδυνο, αλλά σίγουρα τον περιορίζει**.

Ωστόσο, για να αυξηθεί ο αριθμός των συλλήψεων σε επίπεδο ανάλογο του αριθμού των οικονομικών εγκλημάτων που αναφέρονται κάθε χρόνο, πρέπει να δοθούν λύσεις στα ακόλουθα ζητήματα:

α) Όγκος και Συνεργασία

Ο όγκος των εγκλημάτων, ανεξάρτητα από τις όποιες εκτιμήσεις, είναι τεράστιος σε σύγκριση με τις δυνατότητες των διωκτικών αρχών. Αντικειμενικά, δεν διαθέτουν ούτε το ανάλογο ανθρώπινο δυναμικό, ούτε τους ανάλογους οικονομικούς πόρους για να ασχοληθούν παρά με ένα ελάχιστο ποσοστό των περιστατικών.

Ένα άλλο σημαντικό εμπόδιο στην αντιμετώπιση των οικονομικών εγκλημάτων είναι η έλλειψη επικοινωνίας και συνεργασίας μεταξύ των εμπλεκομένων φορέων. Πολλές τράπεζες δυσκολεύονται να συνεργαστούν με τις διωκτικές αρχές, αλλά ακόμη και μεταξύ τους. Και σαν να μην έφτανε αυτό, συχνά οι τράπεζες και οι δικηγόροι τους δεν έχουν τις γνώσεις να χειριστούν τις νομικές διαδικασίες, με αποτέλεσμα να καθυστερούν και να περιπλέκουν τη δίωξη.

Ωστόσο έχουν σημειωθεί κάποια θετικά βήματα στο μέτωπο της συνεργασίας. Το Κέντρο Αρωγής Κλοπής Ταυτότητας (ITAC), το οποίο έχει ιδρυθεί από 48 τράπεζες, συμφώνησε πρόσφατα να θέσει στη διάθεση των αρχών τη βάση δεδομένων των περιστατικών που παρακολουθεί. Το πρόβλημα είναι ότι το ITAC διαχειρίζεται ένα σχετικά μικρό αριθμό περιστατικών και τα στοιχεία που φτάνουν στα χέρια των αρχών είναι μετά την πάροδο κάποιων μηνών. Επιπρόσθετα ορισμένες τράπεζες αντιμετωπίζουν τα Συστήματα Καταπολέμησης Οικονομικού Εγκλήματος που διαθέτουν ως Στρατηγικό Ανταγωνιστικό Πλεονέκτημα και σε πολλές περιπτώσεις δεν δέχονται να μοιραστούν τη γνώση και την εμπειρία τους με άλλους ανταγωνιστές.

Όπως είναι φυσικό, οι τεχνολογικές λύσεις που έχουν αναπτυχθεί για την αποτροπή των οικονομικών εγκλημάτων είναι πολλές. Μία λύση που ήδη χρησιμοποιείται από αρκετές τράπεζες είναι ο μηχανισμός ID Score της εταιρείας ID Analytics.

Με τη συγκεκριμένη τεχνολογία, αναλύεται η βάση δεδομένων της εταιρείας, στην οποία είναι καταχωρημένα εκατομμύρια περιστατικά και αξιολογείται αν αυτός που αιτείται την πίστωση είναι αυτός που πραγματικά υποστηρίζει ότι είναι. Σύμφωνα με την εταιρεία, οι τράπεζες που χρησιμοποιούν το ID Score έχουν μειώσει κατά 45%-60% τα περιστατικά πλαστών αιτήσεων.

Το πλεονέκτημα της συγκεκριμένης λύσης είναι ότι σταματά την απάτη εν τη γενέσει της και προστατεύει την τράπεζα ή τον έμπορο από τον απατεώνα που θα εμφανιστεί σαν νόμιμος πελάτης. Το μειονέκτημα είναι ότι αν ο απατεώνας αποτύχει μάλλον θα πάει στη διπλανή τράπεζα ή σε έναν άλλο δικτυακό τόπο, αναζητώντας έναν στόχο που δεν χρησιμοποιεί την τεχνολογία ID Score.

Σύμφωνα με τις εκτιμήσεις της ID Analytics, η βάση των πελατών της αναμένεται να αυξηθεί κατά τα επόμενα χρόνια και να φτάσει στο 80% με 90% των ιδρυμάτων που χορηγούν πιστωτικά προϊόντα στις ΗΠΑ. Αν πράγματι η εκτίμηση αυτή αποδειχθεί αληθινή, η εταιρεία θα είναι σε θέση να αποτρέψει το 80% των οικονομικών εγκλημάτων που έχουν σχέση με χρήση πλαστής ταυτότητας. Και όταν γίνει αυτό, οι διωκτικές αρχές θα έχουν το περιθώριο να εστιάσουν και να ασχοληθούν με τα λίγα -συγκριτικά- περιστατικά που θα έχουν σημειωθεί.

Μήπως όμως οι διωκτικές αρχές θα έπρεπε να έχουν πρόσβαση στις πληροφορίες που συγκεντρώνει η ID Analytics και αφορούν τις απόπειρες εξαπάτησης; Είναι αλήθεια ότι κάποιοι είναι υπέρ αυτής της άποψης υποστηρίζοντας ότι η συγκεκριμένη τεχνολογία είναι η μόνη αποτελεσματική που υπάρχει αυτή τη στιγμή για να συλληφθούν οι απατεώνες. Ωστόσο η ID Analytics έχει διαφορετική άποψη. Σύμφωνα με την εταιρεία, η τεχνολογία που χρησιμοποιεί εστιάζει στην αποτροπή του εγκλήματος και δεν υπάρχουν μηχανισμοί για τον εντοπισμό και τη σύλληψη των δραστών.

β) Δικτυακές Εφαρμογές

Στην πράξη, το ζήτημα της ασφάλειας των δικτύων έχει λυθεί. Το μέτωπο που μένει ακόμη ανοιχτό είναι οι εφαρμογές που 'βλέπουν' στο Διαδίκτυο. Πριν μερικούς μήνες, μία εταιρεία της Wall Street υπήρξε όμηρος ενός χάκερ που απείλησε να θέσει εκτός λειτουργίας το δικτυακό της τόπο αν δεν κατέβαλε λύτρα. Πράγματι, ο δικτυακός τόπος τέθηκε εκτός λειτουργίας, η εταιρεία αναγκάστηκε να καταβάλει λύτρα και τώρα το FBI ερευνά την υπόθεση.

Όσοι εμπλέκονται στο συγκεκριμένο περιστατικό τηρούν σιγήν ιχθύος, αψευδής μαρτυρία της έντασης που υπάρχει σήμερα σε σχέση με το ζήτημα της ασφάλειας των εφαρμογών. Πριν πέντε χρόνια το μεγάλο ζήτημα ήταν η ασφάλεια των δικτύων σήμερα είναι οι εκατοντάδες εφαρμογές των εταιρειών που 'βλέπουν' στο Διαδίκτυο. Σε έκθεση του 2004 της Gartner (μίας από τις μεγαλύτερες εταιρείες ερευνών και συμβουλευτικών υπηρεσιών στον χώρο του IT) αναφερόταν ότι 70% των κενών ασφαλείας παρουσιάζονταν σε επίπεδο εφαρμογών και όχι σε επίπεδο δικτύων. Σε έκθεση που δημοσίευσε η Gartner ισχυρίζεται ότι περίπου τα 2/3 των εφαρμογών που τρέχουν σε Web-servers έχουν 'τρωτά σημεία που μπορεί κάποιος να εκμεταλλευτεί'.

Η καρδιά του προβλήματος βρίσκεται στο ότι η ανάπτυξη των εφαρμογών αυτών γίνεται από τους προγραμματιστές των εταιρειών. Οι προγραμματιστές αυτοί συνήθως δεν έχουν ούτε την κατάλληλη εκπαίδευση ούτε τις γνώσεις για να κάνουν τις εφαρμογές ασφαλείς. Για να καλυφθεί αυτό το κενό, τις περισσότερες φορές οι εταιρείες αναθέτουν σε εξωτερικές Ομάδες Ειδικευμένων Προγραμματιστών να ελέγξουν κατά πόσο οι εφαρμογές που ανέπτυξαν είναι ασφαλείς.

Η ζήτηση στο χρηματοοικονομικό κλάδο είναι τόσο μεγάλη ώστε πολλές από τις εταιρείες που ειδικεύονται στον έλεγχο των νέων εφαρμογών δυσκολεύονται να ανταποκριθούν στην αυξημένη ζήτηση. Δεν είναι λίγες οι περιπτώσεις, όπου στις εφαρμογές που ελέγχονται εντοπίζονται αρκετά κενά ασφαλείας, με αποτέλεσμα το προϊόν να επιστρέφει στην Ομάδα Προγραμματιστών που το ανέπτυξε για να το διορθώσει.

Ωστόσο, η προσέγγιση του εκ των υστέρων ελέγχου της ασφάλειας των εφαρμογών φαίνεται να μην επαρκεί για την αντιμετώπιση του προβλήματος. Το ειδικό λογισμικό που χρησιμοποιείται, συχνά ανακαλύπτει μόνο τα εμφανή κενά ασφαλείας. Αν συνυπολογίσουμε ότι οι χάκερ ανακαλύπτουν κάθε στιγμή νέους τρόπους επίθεσης και ότι οι εταιρείες όταν αναβαθμίζουν μία εφαρμογή, σπάνια επανελέγχουν την ασφάλειά της, καταλαβαίνουμε ότι η θωράκιση των εφαρμογών είναι διάτρητη.

Σύμφωνα με τους ειδικούς, ο έλεγχος της ασφάλειας των εφαρμογών πρέπει να ενσωματωθεί στο στάδιο ανάπτυξης της εφαρμογής, ώστε ο τελικός κώδικας να μην έχει πολλά κενά ασφαλείας κάτι που οι εταιρείες δυσκολεύονται να πετύχουν.

Μία προσέγγιση είναι να οριστεί ένας ή δύο από τους βασικούς προγραμματιστές της εταιρείας ως σύνδεσμος με την ομάδα ασφαλείας και μαζί να αναλάβουν τον συντονισμό της **εκπαίδευσης** των υπολοίπων προγραμματιστών της ομάδας. Μία άλλη προσέγγιση είναι η ανάπτυξη εφαρμογών με τη χρήση κομματιών κώδικα που ήδη έχει εγκριθεί ως ασφαλής. Είναι κάτι που δυστυχώς δεν γίνεται συχνά, με αποτέλεσμα να μειώνεται το επίπεδο ασφαλείας των εφαρμογών.

γ) Ανακαλύπτοντας τις Εξωτερικές Συσκευές

Οι πολιτικές πρόσβασης στο δίκτυο είναι η μία πλευρά του νομίσματος. Ωστόσο, αυτό που πραγματικά αλλάζει την εξίσωση είναι ο έλεγχος των εξωτερικών συσκευών που οι εργαζόμενοι μπορούν να συνδέσουν στους υπολογιστές τους.

Το δίκτυο κάθε εταιρείας έχει τόσα κενά ασφαλείας όσες και οι θύρες USB που υπάρχουν σε κάθε PC και φορητό υπολογιστή του δικτύου της. Σε κάθε μία από αυτές τις θύρες κάποιος μπορεί να συνδέσει κάτι τόσο κοινότυπο όσο ένας εκτυπωτής, μέχρι κάτι φινετσάτο όπως ένα iPod Mini. Το τελικό αποτέλεσμα θα είναι το ίδιο: Κλοπή Ευαίσθητων Εταιρικών Δεδομένων.

Ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζουν οι τράπεζες είναι η χαρτογράφηση όλων των δεδομένων που βρίσκονται στους υπολογιστές τους και η προστασία των δεδομένων από φορητές συσκευές. Σύμφωνα με τον Davis Mainer, διευθυντή του Τμήματος Χρηματοοικονομικών Λύσεων της Symantec, 60%-65% των ευαίσθητων πληροφοριών των εταιρειών βρίσκονται σε προσωπικούς υπολογιστές.

Το χρηματιστήριο της Φιλαδέλφειας είναι ένας από τους φορείς που προσπαθεί να δώσει λύση στο πρόβλημα. Χρησιμοποιεί ένα νέο προϊόν της Safend, το Safend Protector. Πρόκειται για μία εφαρμογή που επιτρέπει στους μάνατζερ να ορίσουν δικαιώματα πρόσβασης από τις θύρες επικοινωνίας των υπολογιστών, όπως τις θύρες USB, FireWire, BlueTooth, υπερύθρων, καθώς και τους οδηγούς CD ή DVD. Το προϊόν ενσωματώνει τεχνολογία προστασίας, ώστε οι χρήστες να μην μπορούν να παρακάμψουν τις πολιτικές ασφαλείας.

Ένα από τα θετικά χαρακτηριστικά του Safend Protector είναι ότι το προϊόν μπορεί να επιτρέψει ή να απαγορεύσει την πρόσβαση σε εξωτερικές συσκευές με κριτήριο τον αριθμό σειράς της συσκευής. Η δυνατότητα αυτή είναι τεράστιας σημασίας αν αναλογιστούμε το πλήθος των εξωτερικών συσκευών με τεράστιες χωρητικότητες μνήμης που έχουν κατακλύσει την αγορά.

Κι αν αυτή ήταν η μία όψη του νομίσματος ας δούμε και την άλλη μέσα από τη ‘ζωντανή’ αφήγηση ενός θύματος απάτης, με την ελπίδα να γίνει κατανοητή η αναγκαιότητα και η άμεση εφαρμογή όλων των παραπάνω προτάσεων.

«Όταν δέχθηκα το πρώτο τηλεφώνημα από εισπρακτική εταιρεία, πίστεψα ότι είχαν καλέσει σε λάθος αριθμό. Όχι, δεν έζησα ποτέ στην Αριζόνα ούτε έχω πιστωτική κάρτα Discover. Στο δεύτερο τηλεφώνημα άρχισα να ανησυχώ, και μετά το τρίτο άρχισα σαν τρελή να τηλεφωνώ και να στέλνω φαξ ζητώντας αντίγραφα της κίνησης του λογαριασμού μου. Μέχρι τη στιγμή που έφτασαν στα χέρια μου, είχα δεχθεί 22 κλήσεις από εισπρακτικές εταιρείες και τράπεζες για χρεώσεις ύψους 48.000$.

Πίστεψα αφελώς, ότι δεδομένης της έκτασης που έχουν στις ΗΠΑ οι οικονομικές απάτες με κλοπή προσωπικών στοιχείων, οι τράπεζες, οι εισπρακτικές εταιρείες και οι εταιρείες διαχείρισης δεδομένων οικονομικής συμπεριφοράς (το αντίστοιχο του Τειρεσία) θα ήταν τόσο εξοικειωμένες ώστε το ξεκαθάρισμα της υπόθεσης θα ήταν απλό. Τεράστιο λάθος.

Έψαξα στο Διαδίκτυο και συμβουλεύτηκα φίλους. Γρήγορα όμως έγινε φανερό ότι ο δρόμος που είχα μπροστά μου ήταν μακρύς και δύσκολος. Οι πιστωτές δεν έδειχναν καμία συμπάθεια στο πρόβλημά μου και όποιος έχει βρεθεί στη θέση μου μπορεί να καταλάβει το Γολγοθά μου. Κατάλαβα ότι δεν μπορούσα να δώσω μόνη μου αυτή τη μάχη. Ένιωθα τελείως απροστά-

τευτη. Δεν έκανα τίποτε κακό και όμως ήμουν υποχρεωμένη να υφίσταμαι ακόμη και 50 τηλεφωνήματα την ημέρα από εισπρακτικές εταιρείες. Τηλεφωνούσαν συνέχεια και με στόλιζαν με πρόστυχα επίθετα. Τότε αποφάσισα να προσλάβω δικηγόρο. Μετά από ένα χρόνο και αρκετές μηνύσεις, η μάχη δεν έχει τελειώσει. Γνωρίζατε ότι ανάλογα με τη νομοθεσία κάθε Πολιτείας, δεν αρκεί να παρουσιάσετε αντίγραφο της έκθεσης της αστυνομίας για να καθαρίσει το αρχείο με τα δεδομένα της οικονομικής σας συμπεριφοράς; Γνωρίζατε ότι οι τράπεζες δεν υποχρεώνονται από τον νόμο να λαμβάνουν υπόψη τους τη δήλωση της απάτης που προστίθεται στο προσωπικό σας αρχείο οικονομικής συμπεριφοράς; Με άλλα λόγια, ακόμη και αν εσείς έχετε δηλώσει το περιστατικό, οι απάτες και οι πλαστογραφίες μπορεί να συνεχίζονται.

Η πρόσβαση σε προσωπικές πληροφορίες είναι ευκολότερη από ποτέ. Η άνεση με την οποία μπορεί κάποιος να συλλέξει τα προσωπικά σας στοιχεία είναι τρομακτική. Με τον ένα ή τον άλλο τρόπο, όλα τα προσωπικά μας στοιχεία, από τον αριθμό της ταυτότητάς μας μέχρι τους αριθμούς των τραπεζικών μας λογαριασμών και των πιστωτικών μας καρτών, είναι προσβάσιμα και περιμένουν κάποιον να τα κλέψει.

Μιλώντας εκ πείρας σας εγγυούμαι ότι αν πέσετε θύμα απάτης με κλοπή προσωπικών στοιχείων, θα ταλαιπωρηθείτε, θα σας κάνουν να νιώσετε εγκληματίας, θα υποβληθείτε σε τεράστια έξοδα, θα ξοδέψετε ατέλειωτες ώρες, και τελικά δεν θα είστε σίγουρος ότι δεν θα ξαναπέσετε θύμα. Οι καταναλωτές είναι απροστάτευτοι. Ανεξάρτητα από την πιστοληπτική σας αξιολόγηση πριν το συμβάν, στη συνέχεια θα επιβαρυνθείτε με υψηλότερους τόκους, ίσως δυσκολευτείτε να πάρετε δάνειο ή πιστωτική κάρτα, και μπορεί να χρειαστεί να περιμένετε ακόμη και δέκα χρόνια για να σταματήσουν οι επιπτώσεις.

Αν και δεν μπορώ να απαλλάξω τους καταναλωτές από το μερίδιο της ευθύνης τους, για να μπει ένα φρένο στις απάτες με κλοπή προσωπικών στοιχείων πρέπει η επιχειρηματική κοινότητα να τεθεί ενώπιον των δικών της ευθυνών. Το συγκεκριμένο έγκλημα ξεκινά με την απόκτηση, τη χρήση, την αποθήκευση και την πρόσβαση σε πληροφορίες που οι καταναλωτές δίνουν στις επιχειρήσεις και τις δημόσιες Υπηρεσίες. ***Το έγκλημα δεν πρόκειται να σταματήσει αν οι ίδιες οι επιχειρήσεις δεν προστατέψουν τα προσωπικά στοιχεία που τους έχουμε εμπιστευτεί****. Αυτή τη στιγμή προετοιμάζω μήνυση ενάντια στην εταιρεία που πιστεύω ότι ήταν υπεύθυνη για τη διαρροή των προσωπικών μου στοιχείων. Ενθαρρύνω όλα τα θύματα να δραστηριοποιηθούν ας αποδώσουμε τις ευθύνες εκεί που πραγματικά ανήκουν, στις επιχειρήσεις και όχι στον καταναλωτή.».*

5.2.2 Μέτρα πρόληψης ευρέως διαδεδομένα

Θα πρέπει να παραδεχθούμε πως η ψηφιακή εγκληματικότητα είναι η ουσία της ανασφάλειας των πληροφοριακών συστημάτων της ψηφιακής κοινωνίας, του 21^{ου} αιώνα που διανύουμε, γι' αυτό και η αντιμετώπισή της προβάλλει επιτακτική. Τα συστατικά της στοιχεία που την ευνοούν, αποτελούν, κατά τη γνώμη μας, ένα συνδυασμό της ταυτόχρονης ύπαρξης των ακόλουθων τριών τουλάχιστον παραγόντων (βλ. σχετ. Felson M. [2002] «*Crime and Everyday Life*» όπου γίνεται λόγος για τη θεωρία 'Routine Activity Theory'):

α) ενός δράστη με τις κατάλληλες τεχνολογικές γνώσεις και τα απαραίτητα κίνητρα -όπως κι αν ονομάζεται αυτός, hacker,cracker κλπ.- για να διαπράξει ένα ψηφιακό έγκλημα,

β) ενός πιθανού στόχου - θύματος, που είναι το πληροφοριακό σύστημα μιας επιχείρησης, ενός οργανισμού, ακόμα κι ενός απλού ιδιώτη - χρήστη και

γ) η απουσία ή η ανεπάρκεια των μέσων προφύλαξης, όπως τα συνήθη μέτρα ασφαλείας (δηλ. τα 'τείχη προστασίας/firewalls' και τα antivirus προγράμματα) του πληροφοριακού συστήματος - υποψήφιου θύματος.

Λαμβάνοντας υπόψη θα σταθούμε στο (γ) παράγοντα και θα επιχειρήσουμε να αναφερθούμε συνοπτικά σε ορισμένα από τα προϊόντα προφύλαξης που διατίθενται στην αγορά, δίνοντας έμφαση στη βιομετρική τεχνολογία.

[109]**α) Anti-Spam Software**

Το συγκεκριμένο λογισμικό εμποδίζει ανεπιθύμητα εμπορικά μηνύματα, χρησιμοποιώντας χαρακτηριστικά ενός e-mail και πληροφορίες σε πραγματικό χρόνο από χρήστες σε όλο τον κόσμο ώστε να καθορίσει επακριβώς νέες πηγές spam.

β) Anti-Spyware Software

Αυτό το λογισμικό μπορεί να ανιχνεύσει, να εμποδίσει και να εξαλείψει με ασφάλεια πιθανά ανεπιθύμητα προγράμματα όπως spyware, adware, pop-ups, key loggers και προγράμματα τηλεχειρισμού.

γ) Anti-virus software

Το λογισμικό αυτό δρα κατά των ιών, ανιχνεύει υπάρχουσες προσβολές από ιούς, τις απομακρύνει εάν υπάρχουν και αποτρέπει μελλοντικές.

δ) Content filtering tools

Αυτά τα εργαλεία χρησιμοποιούνται από γονείς ώστε να μπλοκάρουν ιστοσελίδες που είναι ακατάλληλες για παιδιά. Οι περισσότεροι από τους μεγαλύτερους παροχείς υπηρεσιών Διαδικτύου προσφέρουν τα συγκεκριμένα εργαλεία ή υπηρεσίες «παιδικής ασφάλειας» στους πελάτες.

[109] http://w3.bsa.org/hellas//antipiracy/greece_cybersafety_4.cfm

ε) Device Authentication

Οι συσκευές αυτές βεβαιώνουν ότι μόνο οι εξουσιοδοτημένοι Η/Υ ή άλλες ψηφιακές συσκευές μπορούν να λειτουργήσουν σε ένα δίκτυο. Αυτά τα μηχανήματα μπορούν να χρησιμοποιηθούν μαζί με τεχνολογίες πιστοποίησης χρήστη ώστε να δημιουργηθεί μία σε βάθος άμυνα στο Διαδίκτυο και να εξασφαλιστεί ότι οι εξουσιοδοτημένοι χρήστες χρησιμοποιούν υπολογιστές που λειτουργούν σωστά.

στ) Embedded Document-Level Security

Πρόκειται για την εγκατάσταση ενός συστήματος ασφάλειας, που επιτρέπει στο δημιουργό του εγγράφου να ανταλλάξει με ασφάλεια πληροφορίες εντός και εκτός ενός firewall. Αυτές οι τεχνολογίες καθιστούν εφικτή την αυθεντικότητα του εγγράφου και διατηρούν την ακεραιότητα του περιεχομένου του. Επίσης ενισχύουν την εμπιστευτικότητα.

ζ) Encryption (κρυπτογράφηση)

Ένα μαθηματικό μέσο για την προστασία της πληροφορίας. Η κρυπτογράφηση μετατρέπει την πληροφορία σε ένα σχήμα μη διακριτό, το οποίο μπορεί να δημιουργηθεί εκ νέου μόνο με τον κατάλληλο αλγόριθμο και/ή με κλειδί. Η κρυπτογράφηση χρησιμοποιείται για την προστασία δεδομένων ή την αποφυγή μη εξουσιοδοτημένης αντιγραφής.

η) Firewall

Μία συσκευή ή λογισμικό, το οποίο υπάρχει μεταξύ του Η/Υ και του Διαδικτύου και καθορίζει εάν ένα πακέτο πνευματικής ιδιοκτησίας μπορεί να εγκατασταθεί στον Η/Υ.

θ) Intrusion Detection System

Αυτά τα συστήματα παρακολουθούν αποτυχημένες προσπάθειες καταχώρησης, ύποπτες ενέργειες αρχείων, γνωστά πρότυπα ‘επιθέσεων’ και δικτυακά όργανα ώστε να παγιώσουν την πληροφορία σε ένα δίκτυο και αυτόματα να προειδοποιήσουν για ενδεχόμενη εισβολή.

ι) Intrusion Protection Systems

Αυτά τα συστήματα αυτόματα μπορούν να ανιχνεύσουν και να αποτρέψουν τις επιθέσεις πριν προκαλέσουν οποιαδήποτε ζημιά. Τα συγκεκριμένα εργαλεία 'επαγρυπνούν' προκειμένου να εντοπίσουν ασυνήθιστη συμπεριφορά, όπως για παράδειγμα buffer overflows ή ασυνήθιστα port scans, προκειμένου αυτόματα να αποτρέψουν επιθέσεις.

ια) Logical Access Control

Ένας τρόπος καθορισμού και περιορισμένης πρόσβασης σε ένα σύστημα ή ιστοσελίδα από χρήστη, παράγοντα ή σύνολο με κοινά χαρακτηριστικά.

ιβ) User Authentication Technologies

Αυτές οι τεχνολογίες πιστοποιούν την ταυτότητα του χρήστη με τη χρήση κωδικού, ηλεκτρονικής κάρτας, συμβόλου, δικτυακή κάρτα πρόκλησης-απάντησης ή άλλων αποκλειστικών ανιχνευτών.

ιγ) Virtual Private Network (VPN)

Αυτό το δίκτυο επιτρέπει στις εταιρίες να χρησιμοποιούν δημόσια δίκτυα για ιδιωτική επικοινωνία δεδομένων. Το VPN χρησιμοποιεί μεθόδους πιστοποίησης για την ασφαλή μεταφορά δεδομένων στο Διαδίκτυο.

ιδ) Vulnerability Scanners

Οι ανιχνευτές έκθεσης είναι εργαλεία λογισμικού που εξετάζουν εάν στη δομή ενός υπολογιστή ή δικτύου υπάρχουν ελλιπείς εγκαταστάσεις αναφορικά με την ασφάλεια, τη διάρθρωση ή αν υπάρχουν ελλείψεις στις διορθώσεις.

ιε) Biometrics

Η βιομετρική τεχνολογία χρησιμοποιείται στην ανίχνευση ατομικών γνωρισμάτων όπως δακτυλικά αποτυπώματα, οπτικά δείγματα, προσωπικά χαρακτηριστικά και φωνητικά δείγματα. Τυπικά, οι ηλεκτρονικοί ανιχνευτές καταγράφουν τα γνωρίσματα και το βιομετρικό λογι-

σμικό τα αναλύει. Η βιομετρική τεχνολογία επαληθεύει την ταυτότητα του προσώπου με χαρακτηριστικά του προσώπου, αποτυπώματα, ίριδα ματιού ακόμη και DNA.

Πρόσφατη έκθεση του Ερευνητικού Κέντρου της Ευρωπαϊκής Επιτροπής στη Σεβίλλη, καταδεικνύει τα βασικά στοιχεία των βιομετρικών συστημάτων και εξετάζει επίσης όλα τα πρακτικά, ηθικά και νομικά ζητήματα που ανακύπτουν μέσα από πλασματικές αναλύσεις υποθέσεων.

Ανάμεσα στις βιομετρικές τεχνολογίες που αναπτύσσονται, η τεχνολογία των δακτυλικών αποτυπωμάτων είναι αυτή που βρίσκεται πιο κοντά στην υλοποίηση και ευρεία χρήση. Σε ορισμένες τράπεζες, όπως στη Citygroup, χρησιμοποιείται για την πιστοποίηση των υπαλλήλων. Και το ερώτημα γεννιέται '*μπορεί η βιομετρική τεχνολογία πιστοποίησης δακτυλικών αποτυπωμάτων να εφαρμοστεί στα ATM των τραπεζών*;'

Εκεί οι απαιτήσεις είναι πολύ υψηλές. Πρέπει να εξασφαλιστεί ότι οι πελάτες θα έχουν πρόσβαση στα χρήματά τους απρόσκοπτα και σε κάθε περίπτωση. Ακόμη και αν το περιθώριο σφάλματος είναι μόλις 1%, στην πράξη αυτό μεταφράζεται σε αδυναμία εκτέλεσης εκατοντάδων χιλιάδων συναλλαγών.

Οι λόγοι που μπορούν να οδηγήσουν σε λανθασμένη άρνηση εκτέλεσης της συναλλαγής είναι πολλοί. Πέρα από τους προφανείς λόγους, όπως για παράδειγμα ένα κόψιμο στο δάκτυλο, υπάρχουν και άλλοι που δεν είναι ιδιαίτερα γνωστοί. Για παράδειγμα, υπάρχουν άνθρωποι με πολύ αχνό δακτυλικό αποτύπωμα που δύσκολα αναγνωρίζεται. Φαίνεται μάλιστα το χαρακτηριστικό αυτό να συνδέεται με φυλετικά χαρακτηριστικά.

Συγκεκριμένα, σύμφωνα με έρευνες, οι Ασιάτισσες έχουν τα πιο αχνά δακτυλικά αποτυπώματα. Αν πράγματι η ακρίβεια της ανάγνωσης δακτυλικών αποτυπωμάτων εξαρτάται από χαρακτηριστικά όπως η φυλή ή το φύλο, ανοίγει ένα εντελώς νέο Κεφάλαιο. Άλλοι παράγοντες που δεν έχουν ερευνηθεί είναι τι συμβαίνει με τα δακτυλικά αποτυπώματα των ανθρώπων που εργάζονται στην ύπαιθρο ή είναι χειρώνακτες.

Αυτά τα κενά δεν είναι απλές λεπτομέρειες. Ο τραπεζικός κλάδος πρέπει να επενδύσει εκατοντάδες εκατομμύρια δολάρια πριν μπορέσει να εφαρμόσει τη βιομετρική τεχνολογία των δακτυλικών αποτυπωμάτων.

Το μόνο σίγουρο είναι ότι το κίνητρο υπάρχει. Για παράδειγμα, τον Οκτώβριο του 2005 το Ομοσπονδιακό Συμβούλιο Χρηματοοικονομικών Ιδρυμάτων (FFIEC) με επιστολή του προς όλες τις τράπεζες, ζήτησε μέχρι το τέλος του 2006 οι τραπεζικές συναλλαγές που πραγματοποιούνται μέσω Διαδικτύου να καλύπτονται από ταυτοποίηση δύο παραγόντων. Αυτοί που στοιχηματίζουν στην τεχνολογία δακτυλικών αποτυπωμάτων δεν είναι λίγοι. Η Pay By Touch Solutions (η εταιρεία που υλοποίησε τη βιομετρική μέθοδο πληρωμών της Piggly Wiggly) εξασφάλισε πρόσθετα κεφάλαια 130.000.000$ από ιδιώτες και θεσμικούς επενδυτές για την ανάπτυξη τεχνολογιών αναγνώρισης δακτυλικών αποτυπωμάτων. Τα 75.000.000 προήλθαν από Εταιρείες Διαχείρισης Κεφαλαίων, όπως η Och-Ziff Capital Management και η Farallon Capital, ενώ τα υπόλοιπα 55 προήλθαν από ιδιώτες επενδυτές και μικρές επενδυτικές εταιρείες. Πολλές φορές τα κεφάλαια που διατίθενται για τη λύση ενός προβλήματος βοηθούν. Αυτό που μένει να δούμε είναι αν θα έχουμε αποτελέσματα.

Κλείνοντας αυτή τη σύντομη αναφορά, θα παραθέσουμε ορισμένες χρήσιμες συμβουλές, που διατυπώθηκαν με αφορμή το 3^{ο} Πανελλήνιο Συνέδριο για το ηλεκτρονικό έγκλημα, τη Δικτυοπειρατεία & την Τηλεπικοινωνιακή Απάτη από το σύμβουλο Ασφαλείας Πληροφοριακών και Τηλεπικοινωνιακών Συστημάτων της εταιρείας MD5 Α.Ε, και αφορούν στην προστασία όλων μας από το ηλεκτρονικό έγκλημα.

«Κατά την πλοήγηση σας στους χώρους του Διαδικτύου είναι καλό να παίρνετε κάποια μέτρα ασφαλείας. Αποφύγετε την αποκάλυψη των προσωπικών σας ευαίσθητων δεδομένων σε τρίτους. Μην εμπιστεύεστε e-mails ή web sites που δεν έχουν αποδείξει την ταυτότητα τους. Αποφύγετε να συμπληρώνετε φόρμες με οικονομικά στοιχεία, αριθμό ταυτότητας, ΑΦΜ και λοιπά προσωπικά στοιχεία και να τις αποστέλλετε μέσω ηλεκτρονικού ταχυδρομείου χωρίς να είναι κρυπτογραφημένες. Μην επισκέπτεστε ύποπτα sites. Όσο για τις on-line συναλλαγές, βεβαιωθείτε ότι το ηλεκτρονικό κατάστημα που συναλλάσσεστε είναι αξιόπιστο (ψηφιακά υπογεγραμμένο από κάποιο ανεξάρτητο φορέα ή αρχή πιστοποίησης όπως η εταιρεία Verisign), έχει καλή φήμη και εφαρμόζει μηχανισμούς ασφαλείας όπως κρυπτογραφημένη επικοινωνία μέσω του πρωτοκόλλου SSL.
Στη χώρα μας δεν υφίσταται νομοθεσία που να δεσμεύει τους Φορείς παροχής Υπηρεσιών INTERNET(ISP) έναντι των πελατών τους. ***Πρέπει ο χρήστης να παίρνει μέτρα πρόληψης****» .*

5.2.3 Η εκπαίδευση ως εργαλείο πρόληψης

Οι νέες τεχνολογικές εξελίξεις όπως πρέπει πλέον να έχει γίνει αντιληπτό, δεν αφομοιώνονται άμεσα από τις κοινωνίες. Χρειάζονται πολλά χρόνια και ενδεχομένως και διαφορετικά εκπαιδευμένες γενιές, ώστε να γίνουν ευρύτερα αντιληπτές οι τεχνολογικές δυνατότητες αλλά και οι κίνδυνοι που πηγάζουν. Στη βάση αυτή και με γνώμονα την πρόληψη εγκλημάτων και δη της πλαστογραφίας (παραδοσιακής και με τη χρήση νέων τεχνολογιών) προτείναμε ήδη ορισμένα μέτρα πρόληψης που μπορούν να λάβουν τόσο οι ιδιώτες όσα και λοιπά χρηματοοικονομικά ιδρύματα.

Σκόπιμα επιλέξαμε να κλείσουμε το Κεφάλαιο αυτό, θίγοντας το θέμα 'εκπαίδευση' που κατά τη γνώμη μας προβάλλει ως το πλέον σημαντικό μέσο επιβίωσης από τους κινδύνους που κρύβει αυτός ο ωκεανός που ονομάζεται έγκλημα και νέες τεχνολογίες.

Εκπαίδευση όχι γενική και αόριστη, αλλά προσανατολισμένη στην κεντρική θεματική μας που δεν είναι άλλη από το έγκλημα της πλαστογραφίας. Θα λέγαμε λοιπόν ότι η εκπαίδευση θα πρέπει (σε πρώτη φάση τουλάχιστον) να αφορά κυρίως τους Δικαστές και Εισαγγελείς, επιβάλλεται να καθιερωθούν ειδικά σεμινάρια τόσο στη Σχολή Δικαστών όσο και στη Σχολή Μετεκπαίδευσης Δικαστικών Λειτουργών, αλλά και τους εργαζόμενους που εμπλέκονται άμεσα και συχνά με 'έγγραφα' που δύνανται να πλαστογραφηθούν αλλά και τους Αυτό βέβαια δεν σημαίνει ότι ανάλογη 'εκπαίδευση' δεν θα ήταν χρήσιμη και για όλους τους υπόλοιπους εργαζόμενους ή μη.

Λαμβάνοντας υπόψη τα παραπάνω και χάριν συντομίας θα αναφερθούμε στα αποτελέσματα σχετικής αναζήτησής μας στο Διαδίκτυο. Διαπιστώσαμε λοιπόν ότι η [110]εταιρεία 'ISON' αναλαμβάνει το σχεδιασμό και την οργάνωση σεμιναρίων για την ανάπτυξη δεξιοτήτων χρήσιμων στο σύγχρονο περιβάλλον εργασίας. Η εταιρεία αυτή που απευθύνεται τόσο σε μεμονωμένους επαγγελματίες & ιδιώτες, όσο και σε οργανισμούς που επιθυμούν να τα υλο-

[110] http://www.ison.gr/Seminars/Seminars_1.htm

ποιήσουν ενδοεπιχειρησιακά, εκπονεί -μεταξύ άλλων- εκπαίδευση υπό μορφή σεμιναρίων, με θέμα τον **'Έλεγχο της γνησιότητας αξιών & εγγράφων'**.

Πιο συγκεκριμένα σχετικά με την εκπαίδευση αυτή αναφέρεται ότι η πλαστογράφηση αξιών και εγγράφων αποτελεί μια από τις πιο συχνές απειλές του οικονομικού μας συστήματος. Εκτός από τις οδηγίες για τον έλεγχο της γνησιότητας των χαρτονομισμάτων, κάθε εργαζόμενος που παραλαμβάνει έγγραφα βάσει των οποίων παίρνονται οικονομικές αποφάσεις, πρέπει να μπορεί να διακρίνει τις μικρές λεπτομέρειες που διαχωρίζουν το πλαστό από το γνήσιο έγγραφο. Ο έλεγχος γνησιότητας αξιών και εγγράφων θα πρέπει να γίνεται στο πρώιμο στάδιο κάθε συναλλαγής, ώστε να αποφεύγονται τυχόν δυσλειτουργίες που μπορούν να προκύψουν και να επηρεάσουν ολόκληρο το σύστημα.

Προσδοκώμενα οφέλη, ο εγκυρότερος έλεγχος της γνησιότητας των αξιών και εγγράφων, η άμεση ανίχνευση πλαστών εγγράφων, η πρόληψη και αποφυγή διακίνησης πλαστών αξιών και εγγράφων.

Σε αυτή την εκπαίδευση προτείνεται να συμμετάσχουν: Διευθυντές Τραπεζών, επιλεγμένα στελέχη, Διευθυντές Ασφάλειας, ταμίες και υπάλληλοι που παίρνουν αποφάσεις βάσει εγγράφων, τα οποία τους παρουσιάζονται από πελάτες. Παράλληλα, σύμφωνα πάντα με τη σχετική ιστοσελίδα της εταιρείας, εισηγητές είναι έμπειροι αξιωματικοί, πιστοποιημένοι εμπειρογνώμονες ελέγχου πλαστών εγγράφων. Στο περίγραμμα ύλης προβλέπεται να αναπτυχθούν τα εξής θέματα:

- Παραχάραξη χαρτονομισμάτων, πλαστογραφία, επεξήγηση εννοιών.
- Χαρτί, είδη, κατασκευή και σύνθεση αυτού. Άλλα υλικά ασφάλειας, με τα οποία κατασκευάζονται έγγραφα.
- Χαρακτηριστικά μέτρα ασφάλειας στο στάδιο κατασκευής του χαρτιού ασφαλείας.
- Μελάνες, εκτυπωτικές μέθοδοι ασφαλείας.
- Πρόσθετα μέτρα ασφάλειας μετά την εκτύπωση.

- Έγγραφα αποδεικτικά ταυτότητας (ταυτότητες, άδειες ικανότητας οδήγησης κ.λ.π.) και ταξιδιωτικά έγγραφα (διαβατήρια, προξενικές θεωρήσεις κ.λ.π.). Τεχνικές προδιαγραφές κατασκευής.
- Προσωποποίηση των εγγράφων, φωτογραφία κατόχων, τρόποι προστασίας της φωτογραφίας. Σύγχρονες μέθοδοι προστασίας σελίδας με τα στοιχεία κατόχου ταξιδιωτικών εγγράφων.
- Έλεγχος γνησιότητας εγγράφων αποδεικτικών ταυτότητας, ταξιδιωτικών εγγράφων.

Τέλος στην εν λόγω εκπαίδευση περιλαμβάνεται πρακτική εξάσκηση στην ανίχνευση πλαστών ταξιδιωτικών εγγράφων και εγγράφων ταυτότητας εν γένει, μακροσκοπικά.

Από μια πρώτη αξιολόγηση θα λέγαμε ότι το παραπάνω εκπαιδευτικό πρόγραμμα είναι κάτι πρωτοποριακό και σίγουρα θέτει κάποιες βάσεις πάνω στις οποίες θα μπορούσε να πραγματοποιηθεί ένα πιο συλλογικό εγχείρημα εκπαίδευσης. Περαιτέρω κρίσεις σχετικά με την εταιρεία και τις εκπαιδεύσεις που υλοποιεί, κρίνουμε αφενός ότι δεν είναι δίκαιο να πραγματοποιηθούν αφού δεν έχουμε παρακολουθήσει από κοντά τις εν λόγω εκπαιδεύσεις, αφετέρου ξεφεύγει της κεντρικής θεματικής που αναλύουμε στην παρούσα εργασία. Στόχος είναι να προβάλλουμε κάτι υλοποιήσιμο σχετικά με αυτό που οραματιζόμαστε ως ‘εκπαίδευση εργαζομένων’ ξεφεύγοντας από την απλή θεωρητική προσέγγιση των πραγμάτων.

..//..

ΕΠΙΛΟΓΟΣ

Η διαπίστωση αντίρροπων συνεπειών από την τεχνολογία, ωφελημάτων και προβλημάτων, επιβάλλει την ειρηνική συμφιλίωση μαζί της, καθώς η άκρα προσκόλληση και εξιδανίκευση σε κάθε τι που ανήκει στο παρελθόν σημαίνει αυτόματα υποθήκευση του μέλλοντος.

Η αλήθεια είναι ότι η καθημερινότητα όπως τη βιώνει ο καθένας από εμάς, τελικά υποδεικνύει και την πιο ορθολογική αντίδραση στις νέες τεχνολογίες. Προχωράς με δειλά βήματα μπροστά ρίχνοντας κλεφτές ματιές προς τα πίσω. Σερφάρεις στο Διαδίκτυο, αλλά ετοιμάζεις χειρόγραφα μια ευχετήρια κάρτα προς τη μητέρα σου. Τι κι αν η ηλεκτρονική γραφή με copy paste και η αυτόματη διευθέτηση φαντάζει πιο εύκολη; Πάντοτε υπάρχει χρόνος και διάθεση για χειρόγραφη γραφή. Κι αν τελικά το παρακάνεις με το γράψιμο, ξυπνάει το μούδιασμα στον καρπό, απόδειξη και συγχρόνως παραδοχή ότι ναι έχει ανατείλει μια νέα, διαφορετική εποχή.

Μια εποχή που η ταχύτητα της τεχνολογικής ανάπτυξης βηματοδοτεί και τη συχνότητα των κοινωνικών μεταβολών. Για να συλλάβουμε δε την έννοια των κοινωνικών μεταβολών, αρκεί να αναλογιστούμε πως οι τρόποι ζωής και οι θεσμοί που χαρακτηρίζουν τη σύγχρονη εποχή απομακρύνθηκαν απότομα από τους τύπους της κοινωνικής οργάνωσης με τους οποίους ζούσαν οι άνθρωποι για χιλιάδες χρόνια. Όπως παρατηρεί και ο Hobsbawm[111] «*τέτοια ήταν η ταχύτητα της αλλαγής, ώστε ο ιστορικός χρόνος θα πρέπει να συντμηθεί σε μικρότερα διαστήματα για να την αποτυπώσει*.»

Στη βάση αυτή των κοινωνικών μεταβολών, που επηρεάζουν σαφώς και το εγκληματικό φαινόμενο, απομονώσαμε με πολύ προσοχή ένα μικρό τμήμα που αφορά στο έγκλημα της πλαστογραφίας με τη χρήση νέων τεχνολογιών. Προσπαθήσαμε, όπως εισαγωγικά είχαμε δεσμευθεί, να αποφύγουμε ακραίες ‘τεχνο-φοβικές’ ή ‘τεχνο-φιλικές’ απολυτότητες. Κατά πόσο το εγχείρημά μας στέφθηκε τελικά με επιτυχία ή αποτυχία είναι κάτι που τίθεται στην κρίση σας, με κριτήριο -σε μια εποχή που οι εξελίξεις τρέχουν- το χρόνο που δαπανήθηκε κατά τη μελέτη της εργασίας αυτής και αν τελικά είναι αντάξιος και δικαιώνει την αποκτηθείσα γνώση.

[111] Hobsbawm E. (2002) «*Η εποχή των άκρων. Ο Σύντομος Εικοστός Αιώνας 1914-1991*», Έκδοση Στ΄, Εκδόσεις Θεμέλιο, Αθήνα, σελ. 370.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική & Ξένη

1. Αγγελής Ι. «*Η προς ψήφιση σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο: Η σχέση της με την ελληνική έννομη τάξη*» (http://www.lawnet.gr/pages/eofn /2/cybercrime.asp).
2. Αγγελής Ι. (2000) «*Διαδίκτυο και Ποινικό Δίκαιο*», Ποιν. Χρονικά.
3. Αλεξιάδης Σ. (1998) «*Ανακριτική*», Εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη.
4. Αρτινοπούλου Β. «*Ηλεκτρονικό Έγκλημα και Θυματοποίηση*» Ict Forum, Αθήνα 29-10-2007.
5. Anderson R. (2001) «*Security Engineering: A guide to building dependable distributed systems*», New York: John Wiley and Sons, Inc.
6. Βασιλάκη Ειρ. (1993) «*Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών*», Εκδόσεις Αντ. Ν. Σάκκουλα.
7. Βιδάλη Σ. (2001) «*Η ελληνική αστυνομία του 21^{ου} αιώνα: ένα μεσογειακό μοντέλο αντεγκληματικής πολιτικής*», στο Πανούσης Γ. - Βιδάλη Σ. (2001) «*Κείμενα για την αστυνομία και την αστυνόμευση*», Εκδόσεις Α.Ν. Σάκκουλας, σειρά Εγκληματο-Λογικά, Αθήνα.
8. Βλαχόπουλος Κ. (2007) «*Ηλεκτρονικό Έγκλημα*», Νομική Βιβλιοθήκη.
9. Bernard M., Peacock J. & Berrie C. (1997) «*Τεχνολογία παραγωγής εντύπου*», μτφρ. Γ. Χατήρης, Επιμέλεια ελληνικής έκδοσης Καραγιάννης Β., Εκδόσεις Ιων.
10. Brunelle R. & Cantu A. (1987) «*A Critical evaluation of Current Ink Dating Techniques*». Journal of Forensic Sciences, JFSCA, Vol. 32, No.6.
11. Bauman Z. (2004) «*Παγκοσμιοποίηση. Οι συνέπειες για τον άνθρωπο*», Εκδόσεις Πολύτροπον, Αθήνα.

12. Γιαννόπουλος Θ. (1986) « *Όψεις και Προβλήματα Ηλεκτρονικής Εγκληματικότητος*», Νομική Βιβλιοθήκη.
13. Delmas - Marty M. (1998) «*Πρότυπα και Τάσεις Αντεγκληματικής Πολιτικής*», Νομική Βιβλιοθήκη, Αθήνα.
14. Ένωση Ελλήνων Δικονομολόγων (1994) «*Τα έγγραφα στην πολιτική δίκη*», Πρακτικά του 17ου Πανελλήνιου Συνεδρίου (Χανιά 3-6 Οκτωβρίου 1991), Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή.
15. Ζάννη Αν. (2005) «*Το διαδικτυακό έγκλημα*», Εκδόσεις Σάκκουλα, Αθήνα.
16. Ζαραφωνίτου Χ. (2002) «*Ο φόβος του εγκλήματος*», Εκδόσεις Α.Ν. Σάκκουλας, Αθήνα.
17. Ζέρβας Χ. (2005) «*Η 'ΕΛ.ΑΣ' της Σχολής Ευελπίδων*», Εφημερίδα 'Ελευθεροτυπία'.
18. Gencavage J. (1986) «*Facsimile Signatures Produced by Gelatin transfer Duplicator – Recognition and Identification*», Journal of Forensic Sciences, JFSCA, Vol. 31, No1.
19. Higounet C. «*Η Γραφή*», Εκδόσεις Δαίδαλος -Ι. Ζαχαρόπουλος Α.Ε. χ.χ.
20. Hobsbawm. E. (2002) «*Η εποχή των άκρων. Ο Σύντομος Εικοστός Αιώνας 1914-1991, στ΄ έκδοση*», Εκδόσεις Θεμέλιο, Αθήνα.
21. Θεοδωράκης Γ. (1990) «*Ποινικό δίκαιο: ειδικό μέρος: η πλαστογραφία (άρθρο 216 ΠΚ)»,* Εκδόσεις Α. Σάκκουλας, Αθήνα - Κομοτηνή.
22. Ιγγλεζάκης Ι. (2006) «*Εισαγωγή στο δίκαιο της πληροφορικής*», Εκδόσεις Σάκκουλα, Αθήνα.
23. Jess D. (1998) «*Document Examiner Textbook*», Pantex International Ltd.
24. Καιάφα-Γκμπάντι Μ. (2000) «Το ποινικό δίκαιο στην καμπή του 2000: Με το βλέμμα προς το μέλλον χωρίς αποτίμηση του παρελθόντος;», Υπεράσπιση.
25. Κανελλόπουλος Δ. (2007) «*Ηλεκτρονικά εγκλήματα στον κυβερνοχώρο*», Περιοδικό 'Εκπαίδευση & Νέες Τεχνολογίες', τεύχος 5ο (http://www.eeep.gr/5_teyxos_ekpaideysi_kai_nees_texnologies.pdf).

26. Καρράς Α. (1998) «*Ποινικό Δικονομικό Δίκαιο*», β΄ έκδοση, Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή.

27. Καφαντάρης Τ. (2004) «*Η κιβωτός της γνώσης*», Εφημερίδα 'Βήμα Science', σελ. Η01, κωδικός άρθρου: Β14188Η011, ID: 263464.

28. Κουράκης Ν. & Πατεράκης Ν. (2001) «*Το έγκλημα της απάτης»,* Νομική Βιβλιοθήκη.

29. Κυριακάκης Ε. «*Επιστημονικές – τεχνικές δυνατότητες της Δ-νσης Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) στην καταπολέμηση του εγκλήματος*», Περιοδικό 'Προβληματισμοί' της Ελληνικής Εταιρείας Στρατηγικών Μελετών, τεύχος 16.

30. Κωνσταντινίδης Α. (2000) «*Η έννοια και λειτουργία του εγγράφου στο Ουσιαστικό & Δικονομικό Ποινικό Δίκαιο*», Εκδόσεις Δίκαιο & Οικονομία Π.Ν. Σάκκουλας.

31. Kovacich L. & Boni W. (2000) «*High-Technology-Crime Investigator's Handbook*» {Τσουραμάνης Χρ. «*Ψηφιακή κοινωνία, ψηφιακή εγκληματικότητα και θυματοποίηση*» (http://www.teimes.gr/spoudastirio/yifiaki_eglimatikotita.doc)}.

32. Kuranz R. (1986) «*Technique for transferring Ink from a Written Line to a Thin-Layer Chromatographic Sheet*», Journal of Forensic Sciences, JFSCA, Vol.31, No.2.

33. Λάζος Γ. (2001) «*Οι hackers και η φιλοσοφία τους - Ποιος ποινικοποιεί δράσεις στο Δίκτυο;*», Εφημερίδα 'Ελευθεροτυπία'.

34. Λάζος Γ. (2001) «*Πληροφορική και έγκλημα*», Νομική Βιβλιοθήκη, Αθήνα.

35. Λακόπουλος Γ. (2001) «*Αφύλακτη Πολιτεία Φοβισμένοι και ανεκπαίδευτοι αστυνομικοί, αδίστακτοι και αποφασισμένοι οι κακοποιοί*», Εφημερίδα 'Το Βήμα', σελ. Α03, κωδικός άρθρου: Β13196Α031 ID: 232917.

36. Λαμπρόπουλος Γ. Β. (2001) «*Οι ψηφιακοί ντετέκτιβ της ΕΛ.ΑΣ. Πώς οι έλληνες και οι βρετανοί ειδικοί 'χαρτογραφούν' την οργάνωση '17 Νοέμβρη'»*, Εφημερίδα 'Το Βήμα', σελ. Α32, κωδικός άρθρου: Β13245Α321, ID: 234759.

37. Levy St. (1984) «*Hackers: Heroes of the Computer Revolution*» 3rd ed., New York: Penguin Books.

38. Μαγκάκης Γ. (1984) «*Ποινικό Δίκαιο Διάγραμμα γενικού μέρους*», Έκδοση Γ΄, Εκδόσεις Παπαζήση, Αθήνα.

39. Μαρνέλλος Γ. & Κυριακόπουλος Κ. (2001) «*Το Δίκτυο των παρανόμων*», Εφημερίδα 'Ελευθεροτυπία'.

40. Μιχαλοπούλου Α. (2007) «*Αντηχήσεις Οι παλαιοί των ημερών*», Εφημερίδα 'Καθημερινή'.

41. Μπίτσικα Π. (1997) «*Πώς η τεχνολογία μπορεί να γίνει σύμμαχος της εγκληματικότητας Οι ηλεκτρονικοί «φαντομάδες*», Εφημερίδα 'Το Βήμα', σελ. Α42, κωδικός άρθρου: Β12414Α421, ID: 4675.

42. Μπούμπουκα Α. (2006) «*Τυφλή η Θέμιδα στο Διαδίκτυο*», Εφημερίδα 'Κυριακάτικη Ελευθεροτυπία'.

43. Μυλωνόπουλος Χρ. «*Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο*», Σειρά Ποινικά, Νο 33, σελ. 14.

44. Moore D. (1978) «*Determing the Sequence of Ball-Point Pen Writings - A New Method?*», Journal of Forensic Sciences, JFSCA, Vol.23, No.1, σσ.142-148.

45. Moore D, (1988) «*The electrostatic Detection Apparatus (ESDA) and Its Effects on Latent Prints on Paper*», Journal of Forensic Sciences, JFSCA, Vol. 33, No.2, σσ. 357-377.

46. Νικολακόπουλος Δ. (1999) «*Η αντιτρομοκρατική συμφωνία μεταξύ Ελλάδας και Τουρκίας*», Εφημερίδα 'Το Βήμα', σελ. Α05, κωδικός άρθρου: Β12792Α051, ID: 199194.

47. Νικολακόπουλος Δ. (1997) «*Οι κομμουνιστοφάγοι έγιναν detectives Οι κοινωνικές και πολιτικές εξελίξεις μετά τη μεταπολίτευση άλλαξαν και τον έλληνα αστυνομικό*», Εφημερίδα 'Το Βήμα', σελ. Α24, κωδικός άρθρου: Β12429Α241 ID: 11530.

48. Πανούσης Γ. (1986) «*Ο ρόλος των ποινικών επιστημών στον κοινωνικό μετασχηματισμό*», σε Μνήμη Ν. Χωραφά, Η. Γάφου, Κ. Γαρδίκα, τόμος Β΄, Εκδόσεις Α.Ν. Σάκκουλας, Αθήνα.

49. Παπαθεοδώρου Θ. (2002) «Δημόσια *ασφάλεια και αντεγκληματική πολιτική. Συγκριτική Προσέγγιση»*, Νομική Βιβλιοθήκη, Αθήνα.

50. Παπαντωνίου Α. & Σερκετζής Ν. «*Το έγκλημα παραμένει έγκλημα ακόμα και όταν πραγματοποιείται ηλεκτρονικά*» (http://www.ekato.org/gr/Conference_Speeches/ANTONIS_PAP ANTONIOY.pdf).

51. Παπανεοφύτου Α. (1998) «*Ποινικό δίκαιο και ποινικό δόγμα υπό το πρίσμα των σύγχρονων αξιώσεων προστασίας από τους κινδύνους της τεχνολογικής εξέλιξης*», Ποινικά Χρονικά, τεύχος ΜΗ.

52. Ραφτόπουλος Π. (1996) «*Ποινικό Δίκαιο*», (χεο), Αθήνα.

53. Σόφος Θ. (2001) «*Η Θέμιδα τώρα 'βλέπει' προς την οθόνη*», Εφημερίδα 'Ελευθεροτυπία'.

54. Σπινέλλη Κ. (1982) «*Η Γενική Πρόληψη των εγκλημάτων. Θεωρητική και εμπειρική διερεύνηση μορφών κοινωνικού ελέγχου*», Εκδόσεις Α.Ν. Σάκκουλας, σειρά Ποινικά, Αθήνα.

55. Stewart L. (1985) «*Ballpoint Ink Age Determination by Volatile Componet Comparison - A Preliminary Study»,* Journal of Forensic Sciences, JFSCA, Vol.30, No.2, σσ.405-411.

56. Τσουραμάνης Χ. (2001) «*Ποινική Δικαιοσύνη και Εγκληματολογία στο Διαδίκτυο*», Ποινικός Λόγος, τεύχος 3.

57. Τσουραμάνης Χ. «*Ψηφιακή Κοινωνία, ψηφιακή εγκληματικότητα και θυματοποίηση*» (http://www.teimes.gr/ spoudastirio/yifiaki_eglimatikotita.doc).

58. Φαρσεδάκης Ι. (1996) «*Στοιχεία εγκληματολογίας*», Αθήνα, Νομική Βιβλιοθήκη.

59. Χριστοδούλου Κ. (2001) «*Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία*», Εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα - Κομοτηνή.

60. Χρυσοχοΐδης Μ. (2001) «*Προετοιμαζόμαστε για τον κυβερνοπόλεμο*», Εφημερίδα 'Ελευθεροτυπία'.

Διαδίκτυο

1. http://el.wikipedia.org
2. http://inventors.about.com/library/weekly/aa101697.htm
3. http://www.live-pedia.gr
4. http://www.in.gr
5. http://inventors.about.com/library/inventors/blcomputer_printers.htm
6. http://www.tmth.edu.gr/el/kiosks/typography/technology/typo_t2.html
7. http://www.Computertriti.gr
8. http://www.e-pcmag.gr/modules/news/article.php?storyid=925
9. http://www.pcproblems.gr/pcfaq/index.php?action=artikel&cat=4&id=8&artlang=el
10. http://www.yassas.com/Newsletter/1307/1307a.html
11. http://www.euro2day.gr/articles/132106
12. http://www.dart.gov.gr
13. http://www.mcconnellinternational.com/services/cybercrime.htm
14. http://www.enfsi.org
15. http://w3.bsa.org/hellas//antipiracy/greece_cybersafety_4.cfm
16. http://www.ison.gr/Seminars/Seminars_1.htm
17. http://www.marinos.com.gr/bbpdf/pdfs/msg50.pdf
18. http://www.morax.gr/ article_show.php?article _id=921
19. http://www.findlaw.com.au/article/1408.htm