



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ, ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ  
ΙΝΣΤΙΤΟΥΤΟ ΤΕΧΝΟΛΟΓΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΕΚΔΟΣΕΩΝ ΔΙΟΙΚΗΤΙΚΗΣ ΥΠΗΡΕΣΙΑΣ (ΙΤΥΣ)

Πανεπιστήμιο Πειραιώς

Εκδοτικός Επιχειρησμός:

Βιβλίο Παιδίο και Τροφή (Κατακλιτικό)

ΕΠΙΣΤΗΜΟΛΟΓΙΚΗ ΕΡΕΥΝΑ

Παναγιώτα Κωνσταντοπούλου



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΤΡΑΤΗΓΙΚΗ

ακαδημαϊκό έτος : 2010 - 2011

**«ΕΙΚΟΝΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ : ΝΟΜΙΚΟ  
ΠΛΑΙΣΙΟ ΚΑΙ ΠΡΟΣΤΑΣΙΑ  
ΚΑΤΑΝΑΛΩΤΩΝ»**

Η εργασία υποβάλλεται για την μερική κάλυψη των απαιτήσεων με στόχο  
την απόκτηση του διπλώματος

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ

Από το

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΑΓΙΩΤΑ ΜΥΛΩΝΟΠΟΥΛΟΥ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ	
ΑΡ. ΕΙΣ.	
ΟΜΡ.	
ΤΑΞΗ	658.84 ΜΥΛ
ΒΙΒΛΙΟΘΗΚΗ	



## ΠΕΡΙΛΗΨΗ

Το ηλεκτρονικό έγκλημα διαπράττεται με τη χρήση τεχνολογίας υπολογιστών. Είναι διαρκώς αυξανόμενο λόγω διάδοσης της τεχνολογίας, των μέσων πληροφορικής και της επιχειρηματικής δράσης στο Διαδίκτυο. Παρουσιάζει δυσκολίες ως προς την αντιμετώπισή του και ιδιαιτερότητες αναλόγως της γεωγραφικής θέσης μιας χώρας, της ισχύουσας νομοθεσίας σε αυτήν.

Στην παρούσα εργασία επιχειρείται η ολοκληρωμένη παρουσίαση του νομικού πλαισίου λειτουργίας αλλά και της προστασίας των καταναλωτών σε ότι αφορά στις επιχειρήσεις που δραστηριοποιούνται στο χώρο του ηλεκτρονικού επιχειρείν. Ο στόχος της παρούσας εργασίας είναι η πλήρης καταγραφή και παρουσίαση του συνόλου του νομοθετικού πλαισίου που διέπουν αυστηρά τα ηλεκτρονικά καταστήματα. Ακόμη η καταγραφή και παρουσίαση των ειδών του ηλεκτρονικού εγκλήματος και απάτης στο πλαίσιο δράσης στο ηλεκτρονικό επιχειρείν τόσο από τη σκοπιά του ιδιοκτήτη/διαχειριστή όσο και του καταναλωτή αλλά και η αναφορά στις προφυλάξεις και τα μέσα προστασίας από το ηλεκτρονικό έγκλημα.

Η δομή της εργασίας έχει ως ακολούθως.

Στο 1<sup>ο</sup> εισαγωγικό κεφάλαιο παρουσιάζονται οι βασικές έννοιες του ηλεκτρονικού επιχειρείν και τα μεγέθη ανάπτυξης του στην Ελληνική αγορά.

Στο 2<sup>ο</sup> κεφάλαιο παρουσιάζονται στοιχεία για το ηλεκτρονικό έγκλημα, η ιστορικότητα και τρόποι εμφάνισής του, καθώς και χαρακτηριστικές περιπτώσεις ηλεκτρονικής απάτης. Στο ίδιο κεφάλαιο αναφέρονται οι φορείς προστασίας των καταναλωτών.



Το 3<sup>ο</sup> κεφάλαιο πραγματεύεται το σύνολο των νομοθετημάτων που ρυθμίζουν την λειτουργία των εικονικών επιχειρήσεων στην Ελλάδα, στην ΕΕ, στις ΗΠΑ και στο Ηνωμένο Βασίλειο. Ειδικά για την Ελλάδα, παρουσιάζεται συγκεντρωτικά η ισχύουσα νομοθεσία που θα πρέπει να λάβει υπόψη μια εικονική επιχείρηση.

Το τελευταίο κεφάλαιο, το 4<sup>ο</sup>, παρουσιάζει διεξοδικότερα όλα τα μέτρα προστασίας των επιχειρήσεων αλλά και των καταναλωτών από τα ηλεκτρονικά εγκλήματα. Αναλύονται τα τεχνολογικά, τα νομοθετικά αλλά και τα προληπτικά μέτρα προστασίας από είδη κακόβουλων ενεργειών. Στο τέλος του κεφαλαίου αναφέρονται χαρακτηριστικά παραδείγματα ελληνικών ηλεκτρονικών καταστημάτων με συνήθη-ορθή αλλά και ιδιαίτερη πολιτική προστασίας καταναλωτών.

Πανεπιστήμιο Πειραιώς

## ABSTRACT

Cybercrime is usually committed using computer technology. It is increasing due to diffusion of technology, the extended use of computer equipment and due to the growing e-business environment. Compared to the physical crime, it is difficult to handle and it is mostly depended on the peculiarities and the existing legislation between different countries.

This study attempts a comprehensive review of the existing legal framework that holds in companies operating in e-business and for the protection of consumers. The main objective of this study is the complete recording and presentation of the entire legislative framework governing strictly online stores. Moreover, it attempts a classification and presentation of the different types of electronic crime and fraud from both the perspective of the owner / operator of a e-business company and the consumers.

The structure of work is as follows. The first introductory chapter presents the basic concepts of e-business development and size of the Greek electronic market. The second chapter presents information and references for the electronic crime, its historical appearance and typical cases of online fraud. The same chapter mentions the existing organizations for the consumer protection.

The third chapter deals with all legislation governing the operation of virtual enterprises in Greece, EU, U.S. and UK. Especially for Greece, a summary of the required legislation that should be taken into account from a virtual enterprise, is given.

The last fourth chapter presents all measures to protect businesses and consumers of electronic crimes. At the end of this chapter, a number of characteristic examples of Greek electronic stores with typical and exceptional consumer policy are mentioned.

Πανεπιστήμιο Πειραιώς

## ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον κύριο Ιωάννη Σμυρλή για την καθοδήγηση, την υποστήριξη και τη βοήθεια του καθ' όλη τη διάρκεια διεκπεραίωσης της παρούσας διπλωματικής μελέτης. Επίσης θα ήθελα να τον ευχαριστήσω για το ενδιαφέρον του και το χρόνο που αφιέρωσε για τη διόρθωση της παρούσας εργασίας.

Τέλος θα ήθελα να ευχαριστήσω θερμά την οικογένεια μου και τους γονείς μου για την ηθική συμπαράσταση όχι μόνο κατά τη διάρκεια της εκπόνησης της διπλωματικής μου εργασίας αλλά και καθ' όλη τη διάρκεια των σπουδών μου.



## ΠΕΡΙΕΧΟΜΕΝΑ

Λίστα Γραφημάτων – Λίστα Πινάκων	11
Κεφάλαιο 1 <sup>ο</sup> : Θεωρητική Προσέγγιση των Οικονομικών Όρων	
1.1 Εισαγωγή	12
1.2 Ηλεκτρονικό Επιχειρείν	12
1.3 Ηλεκτρονικό Εμπόριο	14
1.4 Βασικές Λειτουργίες Ηλεκτρονικών Επιχειρήσεων	18
1.5 Πλεονεκτήματα – Μειονεκτήματα Ηλ.Επιχειρείν	24
1.6 Εικονικές Επιχειρήσεις – Ηλεκτρονικά Καταστήματα	31
1.7 Ανάπτυξη Εικονικών Επιχειρήσεων στην Ελλάδα	34
1.8 Στοιχεία Προτίμησης Ελλήνων Καταναλωτών προς τις Εικονικές Επιχειρήσεις	36
Κεφάλαιο 2 <sup>ο</sup> : Ηλεκτρονικό Έγκλημα και Φορείς Προστασίας	
2.1 Εισαγωγή	41
2.2 Ηλεκτρονική Εγκληματολογία	45
2.3 Ηλεκτρονικές Απάτες Καταναλωτών στο Διαδίκτυο	46
2.4 Περιπτώσεις Ηλεκτρονικών Απατών από Ηλεκτρονικές Επιχειρήσεις	52
2.5 Φορείς Προστασίας Καταναλωτών	57
Κεφάλαιο 3 <sup>ο</sup> : Νομικό Πλαίσιο Λειτουργίας Ηλεκτρονικών Επιχειρήσεων και Προστασίας Καταναλωτών	
3.1 Εισαγωγή	64
3.2 Νομικό Πλαίσιο Προστασίας Καταναλωτών – Διατάξεις Περί Ηλεκτρονικού Εγκλήματος	66
3.2.1 Η εξέλιξη του Ποινικού Δικαίου	66

3.2.2 Παγκόσμια Νομοθεσία και Πρακτικές τους	69
3.2.3 Ισχύουσα Ελληνική Νομοθεσία	72
3.3 Νομικό Πλαίσιο Σύστασης και Λειτουργίας Ηλεκτρονικής Επιχειρήσης	74
3.3.1 Νομοθεσία Σύστασης Ηλεκτρονικών Επιχειρήσεων	74
3.3.2 Νομοθεσία Λειτουργίας Ηλεκτρονικών Επιχειρήσεων	80
3.3.3 Επιμέρους Δεσμεύσεις Ηλεκτρονικών Επιχειρήσεων	83
3.3.4 Παραβάσεις της Νομοθεσίας περί Ασφάλειας Δικτύων και Ποινές	85
3.4 Ευρωπαϊκή Νομοθεσία περί Ηλεκτρονικού Εμπορίου	87
3.5 Συγκεντρωτική Νομοθεσία Περί Σωστής Πρακτικής	92
3.6 Πρωτοβουλίες Παρέμβασης Βελτίωσης Ισχύουσας Νομοθεσίας	94
Κεφάλαιο 4 <sup>ο</sup> : Προστασία Καταναλωτών	
4.1 Εισαγωγή	97
4.2 Ασφάλεια Ηλεκτρονικών Συναλλαγών	98
4.3 Τεχνολογικά Μέσα Προστασίας	101
4.4 Ευρωπαϊκή Νομοθεσία Προστασίας Ηλεκτρονικών Καταναλωτών	104
4.5 Παραδείγματα Καταστημάτων στην Ελλάδα	107
4.6 Παραδείγματα Πολιτικής Προστασίας Καταναλωτών σε ιστοσελίδες κοινωνικής δικτύωσης	125
4.7 Προληπτικά Μέσα	127
Συμπεράσματα	132
Βιβλιογραφία	135



## ΓΡΑΦΗΜΑΤΑ

ΣΧΗΜΑ	ΤΙΤΛΟΣ	ΣΕΛΙΔΑ
Σχήμα 1	Ηλεκτρονικό Εμπόριο: Ά τρίμηνο 2006-2010	37
Σχήμα 2	Ηλεκτρονικές αγορές, κατά ηλικιακή ομάδα και φύλο:  Ά τρίμηνο 2010	38
Σχήμα 3	Ένταση βαθμού ανησυχίας για τους κινδύνους του διαδικτύου:  Απρίλιος 2009 – Μάρτιος 2010	40

## ΠΙΝΑΚΕΣ

ΠΙΝΑΚΑΣ	ΤΙΤΛΟΣ	ΣΕΛΙΔΑ
Πίνακας 1	Αγαθά και υπηρεσίες που αγοράστηκαν/παραγγέλθηκαν από το διαδίκτυο: Απρίλιος 2009 – Μάρτιος 2010	39

## ΚΕΦΑΛΑΙΟ 1<sup>ο</sup> : ΘΕΩΡΗΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ ΤΩΝ ΟΙΚΟΝΟΜΙΚΩΝ ΎΡΩΝ

### 1.1 ΕΙΣΑΓΩΓΗ

Η ανθρωπότητα βιώνει ξεχωριστά τα ερεθίσματα που δέχεται ανάλογα με τις επικρατούσες συνθήκες και συγκυρίες. Ειδικά η εποχή μας, μπορεί να ισχυρισθεί κάποιος πως διαφέρει ριζικά από παλαιότερα χρόνια, λόγω των δυνατοτήτων που ολοένα και αναπτύσσονται. Πληροφορική και Τηλεπικοινωνίες καθιστούν την καθημερινότητα ευκολότερη μα συνάμα και ταχύτερη. Οι δυνατότητες είναι αρκετές και προσδίδονται στον καθένα, είτε με άμεσο είτε με έμμεσο τρόπο. Τελικά συμπεραίνει κανείς πως με την ανάπτυξη της τεχνολογίας και του Διαδικτύου, η πληροφόρηση αποτελεί μια αστείρευτη πηγή δυνατοτήτων. Το ερώτημα όμως που τίθεται είναι η συσχέτιση όλων αυτών με το ηλεκτρονικό επιχειρείν. Η επιχειρηματικότητα σήμερα δεν εκφράζεται όπως στο παρελθόν, αποκλειστικά με τις παλαιότερες παραδοσιακές μεθόδους και σε πολύ συγκεκριμένες περιπτώσεις. Αντίθετα, καλύπτει ένα ευρύ φάσμα ανθρώπινων δραστηριοτήτων κάθε μορφής, που να για τελεσφορήσει αρκεί μια έξυπνη ιδέα, ένας καλοσχεδιασμένος στόχος και μια συγκροτημένη προσπάθεια, που όμως όλα αυτά θα πρέπει να βασίζονται σε δυνατότητες που παρέχει η σημερινή εποχή όπως είναι η βάση της, δηλαδή η πληροφορική. Οι τεχνολογίες πληροφορικής και τηλεπικοινωνιών αποτελούν το μέσον εκείνο όπου παρέχεται η δυνατότητα σχεδίασης και δημιουργίας υποδομών σε σύντομο χρονικό διάστημα και κυρίως με πολύ μικρότερο κόστος, συναρτήσει με παλαιότερα χρόνια.

### 1.2 ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΕΙΝ

Σύμφωνα με την διεθνή βιβλιογραφία, η επιχειρηματικότητα σήμερα προχωρά στα χνάρια μιας νέας εποχής, η οποία χαρακτηρίζεται και από το πεζό λατινικό γράμμα “e” που είναι το αρχικό γράμμα της λέξης “electronic”. Έτσι λοιπόν βρισκόμαστε σε επίπεδα “e-business” δηλαδή ηλεκτρονικό επιχειρείν.

Ως «Ηλεκτρονικό Επιχειρείν», νοείται κάθε επαγγελματική δραστηριότητα, με φυσική υπόσταση χώρου ή όχι, η οποία στην βάση της χρησιμοποιεί εκείνα τα ηλεκτρονικά μέσα (βάσεις δεδομένων, διαδίκτυο, e-commerce, κα.) ώστε να γίνεται αποδοτικότερη, ευρέως γνωστότερη και περισσότερο εγκλιματισμένη με την τρέχουσα τεχνολογία της εκάστοτε εποχής. Πιο απλά θα μπορούσε να χαρακτηριστεί ως μια επιχείρηση Διαδικτύου που χρησιμοποιεί εφαρμογές των τεχνολογιών πληροφοριών και επικοινωνιών για να υποστηρίξει όλες τις δραστηριότητές της. Ο όρος «ηλεκτρονικό επιχειρείν» επινοήθηκε από το τμήμα marketing της εταιρείας IBM και κάποιες ομάδες διαδικτύου εν έτει 1996. [5]

Το ηλεκτρονικό επιχειρείν αποτελεί μια καινούργια πραγματικότητα για κάθε επιχείρηση, για κάθε επιχειρηματία αλλά τελικά και για κάθε καταναλωτή. Όλες αυτές οι ομάδες έχουν στόχους που συχνά είναι αλληλοσυγκρούμενοι μα τελικά όλοι συμβάλλουν στην κινητικότητα της οικονομίας. Έτσι, επιχειρηματίες και καταναλωτές θα πρέπει να έχουν στόχους που τελικά θα συγκλίνουν με στόχο την ανταλλαγή του προϊόντος με χρήματα. Ηλεκτρονικές επιχειρηματικές μέθοδοι επιτρέπουν στις εταιρείες να συνδεθούν με εσωτερικές και εξωτερικές επεξεργασίες δεδομένων, συστήματα πιο αποτελεσματικά, να συνεργαστούν πιο στενά με τους προμηθευτές και συνεργάτες, καθώς και να ικανοποιήσουν αποτελεσματικότερα τις προσδοκίες των πελατών τους.

Οι κοινοί στόχοι των επιχειρηματιών και καταναλωτών στο χώρο του Ηλεκτρονικού Επιχειρείν είναι :

1. Αμεσότερη πληροφόρηση για τα προϊόντα και τις υπηρεσίες
2. Ελαχιστοποίηση του χρόνου συναλλαγής
3. Συναλλαγές χωρίς την φυσική παρουσία των δύο μελών
4. Ευελιξία και ευκολία στις συναλλαγές
5. Πωλήσεις κι αντιστρόφως αγορές σε ολόκληρο τον κόσμο
6. Συναλλαγές χωρίς ωράριο, 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα

Προφανώς όλα τα συμβαλλόμενα μέρη (επιχειρηματίες και καταναλωτές) θα πρέπει να είναι χρήστες του διαδικτύου ώστε να εφαρμοστεί πλήρως η όποια διαδικασία. Η έννοια του χρήστη διαφοροποιείται ποιοτικά με βάση την εξοικείωση του καθένα με το διαδίκτυο, ανάλυση όμως που θα γίνει παρακάτω. Παρατηρείται αβίαστα όμως πως η τεχνολογία των πληροφοριών και των επικοινωνιών συμβάλλει άμεσα στην υλοποίηση των παραπάνω κοινών στόχων. Διαφαίνεται ταυτόχρονα η υποχρεωτικότητα χρήσης των νέων τεχνολογιών και πως η σχέση που υπάρχει μεταξύ αυτών και της υλοποίησης της όποιας συναλλαγής, είναι άρρηκτα συνδεδεμένα. Η σχεδίαση του ηλεκτρονικού επιχειρείν όταν αυτό κτίζεται με μια συγκεκριμένη αρχιτεκτονική εφαρμογών δεν αποτελεί μόνο μια ενδιαφέρουσα ιδέα. Αντιθέτως, όσο περνούν τα χρόνια η αρχιτεκτονική δομή των ηλεκτρονικών καταστημάτων αποτελεί αναπόσπαστο κομμάτι για τη χρήση τους. Η ένταξη ολοένα και περισσότερων επιχειρήσεων στον ηλεκτρονικό κόσμο τις αναγκάζει να χρησιμοποιούν τα απαραίτητα πληροφοριακά συστήματα, να εκσυγχρονίσουν τα υποσυστήματά τους κι άρα να βρεθούν ένα βήμα πιο κοντά στον ποιοτικό ανταγωνισμό που αναπτύσσεται στο διαδίκτυο μέσω της έννοια του ηλεκτρονικού εμπορίου.

### 1.3 ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ (E-COMMERCE)

Συχνά συμβαίνει να χρησιμοποιούνται περισσότεροι από έναν όρο για την περιγραφή της ίδιας έννοιας με αποτέλεσμα να δημιουργείται σύγχυση και ασάφεια ως προς την σημασία της. Χαρακτηριστικό παράδειγμα αποτελούν οι όροι «ηλεκτρονικό εμπόριο» και «ηλεκτρονικό επιχειρείν».

Το Ηλεκτρονικό Εμπόριο είναι μία έννοια για την οποία έχουν δοθεί πολλαπλοί ορισμοί, οι οποίοι πηγάζουν κυρίως από το τρόπο με τον οποίο προσεγγίζεται από διάφορες επιστήμες και επαγγελματίες (π.χ. «επιχειρείν ηλεκτρονικά», «ο συνδυασμός Internet και EDI», κλπ). Οι διάφοροι ορισμοί αυτοί δεν καλύπτουν όλο το εύρος της έννοιας, δεδομένου ότι τα μέσα που απαιτούνται για την διενέργεια του ηλεκτρονικού εμπορίου δεν είναι μόνο ηλεκτρονικά, όπως επίσης και ότι οι τεχνολογίες Internet και EDI δεν αποτελούν αναγκαία και ικανή συνθήκη για την υλοποίησή του. Επιπλέον, οι



ορισμοί αυτοί δεν δείχνουν τις επιδιώξεις των επιχειρήσεων σχετικά με το ηλεκτρονικό εμπόριο.

Τα νοηματικά κενά των ορισμών αυτών καλύπτονται από τον εξής ορισμό: *«Ηλεκτρονικό Εμπόριο αποτελεί η χρήση ηλεκτρονικών μέσων και εφαρμογών η οποία καλύπτει οποιαδήποτε μορφή επιχειρηματικής ή διοικητικής συναλλαγής και ανταλλαγής πληροφοριών κα σκοπό έχει την δημιουργία προστιθέμενης αξίας (value added) στον πελάτη και ανταγωνιστικού πλεονεκτήματος (competitive advantage) στην εταιρία».*

Το Ηλεκτρονικό Εμπόριο καλείται να επιλύσει παραδοσιακά επιχειρηματικά προβλήματα, όπως η δυσχέρεια των έγγραφων συναλλαγών, την βελτιστοποίηση της διαχείρισης των αποθεμάτων και να προσφέρει νέες επιχειρηματικές ευκαιρίες όπως η εύρεση νέων εταίρων αλλά και προμηθευτών και πελατών σε παγκόσμια κλίμακα με μειωμένο κόστος.

Ως εκ τούτου το Ηλεκτρονικό Εμπόριο αποτελεί επιχειρηματική πρακτική που λαμβάνει διαστάσεις στρατηγικής τοποθέτησης των επιχειρήσεων-χρηστών, που επιδιώκουν την αύξηση της αξίας τους σε οικονομικό επίπεδο, σε επίπεδο ανταγωνισμού και στην αύξηση μεριδίου αγοράς. Επιπλέον, το Ηλεκτρονικό Εμπόριο συμπεριλαμβάνει πολλαπλές τεχνολογίες, αλλά και επιχειρηματικές μεθόδους, μη περιοριζόμενο στα ηλεκτρονικά μέσα μόνο. Οι τεχνολογίες και οι μέθοδοι του Ηλεκτρονικού Εμπορίου συμπεριλαμβάνουν βάσεις δεδομένων, μέσα εξόρυξης πληροφορίας (data mining και data warehousing), μέσα και κανόνες κωδικοποίησης της πληροφορίας, τεχνολογίες επικοινωνιών και μεθόδους αναδιοργάνωσης επιχειρηματικών διαδικασιών (business process re-engineering). [6]

Σε γενικότερη θεώρηση το Ηλεκτρονικό Εμπόριο καλύπτει όλο τον εμπορικό κύκλο, από την υποδοχή πρώτων υλών μέχρι την επικοινωνία με το καταναλωτή. Συμπεριλαμβάνει και τρίτους φορείς, αναγκαίους για την διενέργειά του, όπως είναι οι τράπεζες, οι υπηρεσίες των δημοσίου τομέα, μεταφορικές εταιρείες, ασφαλιστικούς οργανισμούς κλπ. Το πεδίο εφαρμογής του καλύπτει οποιοδήποτε τομέα οικονομικής δραστηριότητας, καλύπτοντας μεταξύ άλλων όλες τις μορφές εμπορίου, τη βιομηχανία, τις τράπεζες, το τουρισμό, την υγεία, το δημόσιο τομέα και τις μεταφορές.

Μια επιχείρηση για να δραστηριοποιηθεί στο ηλεκτρονικό εμπόριο χρειάζεται τουλάχιστον :

- Ένα προϊόν ή μια υπηρεσία
- Ένα δικτυακό τόπο όπου θα αγοράζουν τα προϊόντα της
- Μεθόδους προσέλκυσης του πελατειακού κοινού στην ιστοσελίδα της
- Προσωπικό εξειδικευμένο για την υποδοχή και επεξεργασία των παραγγελιών
- Μεθόδους για την είσπραξη των χρημάτων (θύρα on-line πληρωμών)
- Υπηρεσία με την οποία θα στέλνει τα προϊόντα στους πελάτες της
- Υπηρεσία επιστροφής προϊόντων
- Υπηρεσία εξυπηρέτησης πελατών

Ανακεφαλαιώνοντας, με τον όρο “Ηλεκτρονικό Εμπόριο (Electronic Commerce)” εννοούμε τη χρήση υπολογιστών και τηλεπικοινωνιακών συστημάτων και τεχνολογιών για την διεκπεραίωση μίας πλήρους εμπορικής συναλλαγής. Μία τέτοια τυπική συναλλαγή μπορεί να περιλαμβάνει

- την παρουσίαση των προϊόντων
- την προσέλκυση των πελατών (διαφήμιση, marketing)
- την αλληλεπίδραση με τον πελάτη (κατάλογοι προϊόντων, πωλήσεις)
- τη διεκπεραίωση παραγγελιών-πωλήσεων (καταγραφή παραγγελιών, πληρωμές)
- την υποστήριξη των πελατών (μετά την πώληση, παρακολούθηση παραγγελιών)
- την επικοινωνία με τους προμηθευτές

Στην πράξη το ηλεκτρονικό επιχειρείν είναι κάτι περισσότερο από ηλεκτρονικό εμπόριο. Δηλαδή το ηλεκτρονικό εμπόριο ενυπάρχει μέσα στο ηλεκτρονικό επιχειρείν. Από την άλλη πλευρά όμως το ηλεκτρονικό εμπόριο αναφέρεται σε μια πιο στρατηγική εστίαση με έμφαση στις λειτουργίες που εμφανίζονται από την χρήση των ηλεκτρονικών δυνατοτήτων. Συχνά το ηλεκτρονικό εμπόριο συνεπάγεται της

αποδοτικότερης εφαρμογής της διαχείρισης της γνώσης των συστημάτων σε μια ηλεκτρονική επιχείρηση.

Γενικότερα σύμφωνα με την μία άποψη, το Ηλεκτρονικό Εμπόριο ως όρος θεωρείται από πολλούς περιορισμένος. Συχνότερα λοιπόν χρησιμοποιείται ο όρος του Ηλεκτρονικού Επιχειρείν, που πολλοί θεωρούν ότι είναι ευρύτερος, δεδομένου ότι δεν καλύπτει αποκλειστικά τα στοιχεία του Ηλεκτρονικού Εμπορίου, τα οποία αναφέρθηκαν παραπάνω. Συγκεκριμένα, από μερίδα ειδικών υποστηρίζεται πως ο όρος Ηλεκτρονικό Επιχειρείν για μια επιχείρηση ή έναν οργανισμό περιλαμβάνει ολόκληρο τον κύκλο των οργανωσιακών διαδικασιών, οι οποίες εκτελούνται ψηφιακά κι επί πλέον περιλαμβάνει κι αυτό το ίδιο το Ηλεκτρονικό Εμπόριο, καθώς κι ολόκληρη την πληροφοριακή δομή.

Υπάρχουν διαφορετικοί τρόποι σύμφωνα με τους οποίους το ηλεκτρονικό εμπόριο μπορεί να κατηγοριοποιηθεί. Ένας από τους τρόπους αυτούς εξετάζει την φύση των συμμετεχόντων στις ηλεκτρονικές συναλλαγές. Έτσι εξάγονται διαφορετικές κατηγορίες. Οι γνωστές κατηγορίες είναι οι εξής :

1. Επιχείρηση προς Καταναλωτή (B2C)
2. Επιχείρηση προς Επιχείρηση (B2B)
3. Καταναλωτή προς Καταναλωτή (C2C)
4. Επιχείρηση προς Εργαζομένους (B2E)
5. Καταναλωτή προς Επιχείρηση (C2B)
6. Επιχείρηση προς Κράτος (B2G)
7. Καταναλωτής προς Κράτος (C2G)
8. Μεταξύ ομότιμων Συστημάτων (Απ ευθείας σύνδεση υπολογιστών χωρίς διαμεσολάβηση κεντρικού υπολογιστή) (P2P)
9. Κινητό Ηλεκτρονικό Εμπόριο (MC)

Όλες οι παραπάνω κατηγορίες έχουν οριοθετηθεί έτσι ώστε από τον τίτλο να δηλώνεται ποιος είναι ο καταναλωτής αλλά και ποιος ο προμηθευτής. Έτσι μια B2G



είναι η επιχείρηση εκείνη που αποκλειστικό πελάτη έχεις το κράτος και δεν συνεργάζεται με ιδιώτες καταναλωτές. Φυσικά μπορεί η πολιτική της επιχείρησης να μην έχει στενά όρια και τελικώς να είναι ταυτόχρονα σε παραπάνω από μία, από τις προαναφερθείσες κατηγορίες.

#### 1.4 ΒΑΣΙΚΕΣ ΛΕΙΤΟΥΡΓΙΕΣ ΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Με τον όρο **Εικονικές Επιχειρήσεις**, εννοούνται όλες εκείνες οι ηλεκτρονικές επιχειρήσεις που συντελούν στην προώθηση φυσικών ή ψηφιακών προϊόντων / υπηρεσιών με ψηφιακή διαδικασία μέσω διαδικτυακών ιστοτόπων. Συχνά όμως, ειδικά στον ελληνικό χώρο, η εικονική επιχείρηση ταυτίζεται με την ηλεκτρονική.

Όπως όλες οι επιχειρήσεις με φυσική υπόσταση, έτσι και τα ηλεκτρονικά καταστήματα διέπονται από συγκεκριμένες βασικές λειτουργίες. Αυτές είναι που θα αναλυθούν και παρακάτω υπό το πρίσμα τριών διαφορετικών προσεγγίσεων. Αρχικά θα αναλυθεί ένας τυπικός κύκλος εργασιών που έχει πλέον διαδικτυακή φύση, έπειτα οι λειτουργίες μιας εικονικής επιχείρησης για τον έμπορο και τέλος ποιος λειτουργίες αξιοποιεί ένας καταναλωτής από ένα τέτοιο ηλεκτρονικό κατάστημα.

- **Ολοκληρωμένος Κύκλος Αγορών μέσω Διαδικτύου**

Η δημιουργία ενός ολοκληρωμένου εικονικού καταστήματος συνεπάγεται αυτόματα και την μεταφορά του παραδοσιακού κύκλου αγορών στον εικονικό χώρο του Internet. Το σύνολο των κινήσεων που πραγματοποιεί ένας πελάτης όταν μπαίνει στον φυσικό χώρο ενός καταστήματος, τώρα γίνονται ηλεκτρονικά. Ο έμπορος προσπαθεί να προσομοιώσει τον παραδοσιακό κύκλο αγορών μέσω διαδικτύου, έτσι ώστε τελικά να διευκολυνθεί ο καταναλωτής και να προβεί σε αγορά του προϊόντος ή της υπηρεσίας. Παρακάτω αναλύονται κάποια από τα βασικά βήματα που συντελούνται για την ολοκλήρωση του κύκλου αγοράς:

Αρχικά ο καταναλωτής μπαίνει στην ιστοσελίδα της εικονικής επιχείρησης καταχωρώντας την διεύθυνση του διαδικτυακού τόπου που επιθυμεί. Ευθύς αμέσως

μπροστά του «ανοίγεται» μια σελίδα με συνοπτική περιγραφή των προϊόντων / υπηρεσιών που προσφέρονται στο κατάστημα, μέσω ομαδοποίησης σε κατηγορίες. Επιλέγει έπειτα την κατηγορία που τον ενδιαφέρει κι έτσι εμφανίζεται μια λίστα με τα συγκεκριμένα προϊόντα. Αν υπάρχει επιθυμία και για περαιτέρω ανάλυση, συνήθως υπάρχει λεπτομερέστερη περιγραφή του προϊόντος που ακολουθείται μάλιστα κι από πλήθος φωτογραφιών. Ενδεικτικά αναφέρεται πως οι ιστοσελίδες είναι αρχιτεκτονικά διαμορφωμένες έτσι ώστε ο κάθε χρήστης να μπορεί να πλοηγηθεί μέσα σε αυτή μόνο ως προς την κατεύθυνση που επιθυμεί χωρίς να χρειάζεται να δέχεται ανούσιες πληροφορίες όσον αφορά τον τελικό του στόχο, δηλαδή την ενημέρωσή του ως προς κάποιο συγκεκριμένο προϊόν / υπηρεσία.

Εν συνεχεία κι εφόσον ο καταναλωτής το επιθυμεί τελικά το παρεχόμενο προϊόν, το επιλέγει κι αυτό αυτόματα τοποθετείται στο «ηλεκτρονικό καλάθι» του. Το καλάθι αγορών μπορεί να δεχθεί προσθήκες ή διαγραφές προϊόντων σε όλη την διάρκεια πλοήγησης του καταναλωτή στην ιστοσελίδα του καταστήματος. Επίσης, μπορεί να ορίσει τα χαρακτηριστικά του προϊόντος του (μέγεθος, χρώμα, σχήμα, κα) καθώς και να ενεργοποιήσει τυχόν εκπωτικά κουπόνια που θα μπορούσαν να ισχύουν σε προϊόντα προσφοράς. Συνέχεια της διαδικασίας αυτής αποτελεί η διαδικασία πληρωμής. Μετά την τελική επικύρωση των αγορών του, ο καταναλωτής πρέπει να εισάγει τις πληροφορίες χρέωσης, μεταφοράς καθώς και τα στοιχεία της πιστωτικής του κάρτας στην φόρμα πληρωμής. Εδώ είναι και το σημείο που τίθεται το πρόβλημα της ασφαλούς διακίνησης πληροφοριών, θέμα όμως που θα αναλυθεί παρακάτω στην παρούσα εργασία. Ο αριθμός της πιστωτικής κάρτας κρυπτογραφείται και στέλνεται για έλεγχο της κάρτας σε πραγματικό χρόνο. Αν η αίτηση εξουσιοδότησης γίνει αποδεκτή, τότε οι πληροφορίες για τα προϊόντα / υπηρεσίες και ο τρόπος μεταφοράς, κρυπτογραφούνται και στέλνονται απευθείας στον έμπορο για την διεκπεραίωση της παραγγελίας. Αν σε οποιοδήποτε σημείο αυτής της διαδικασίας προκληθεί κάποιο σφάλμα, ο καταναλωτής καλείται να επανεισάγει τον αριθμό της κάρτας του. Σαφώς κι υπάρχουν κι άλλοι τρόποι πληρωμής στα ηλεκτρονικά καταστήματα, μα αυτή η διαδικασία είναι η συνηθέστερη, ταχύτερη και σαφώς ασφαλέστερη.

Μετά την ασφαλή παράδοση της παραγγελίας στο κατάστημα, ο κεντρικός υπολογιστής παράγει την απόδειξη πληρωμής και στέλνεται πίσω στον υπολογιστή του

πελάτη. Αυτή η απόδειξη περιλαμβάνει τον αριθμό παραγγελίας καθώς και την λίστα με τα προϊόντα / υπηρεσίες που αγόρασε ο πελάτης. [7]

### • **Λειτουργίες Καταστήματος για τον Έμπορο**

Όπως αναφέρθηκε παραπάνω, οι λειτουργίες και τα χαρακτηριστικά ενός ηλεκτρονικού καταστήματος, αφορούν και τον έμπορο αλλά και τον καταναλωτή. Έτσι θα πρέπει να ικανοποιούνται οι ανάγκες και των δύο αυτών ομάδων που είναι υπεύθυνες για την όποια οικονομική συναλλαγή. Από την πλευρά του εμπόρου, αξιολογείται η χρηστικότητα σε επίπεδο διοίκησης κι έτσι παρατίθενται οι παρακάτω λειτουργίες:

1. Δημιουργία καταλόγου προϊόντων / υπηρεσιών και διαχείριση αυτού. Έτσι μέσω αυτής της δυνατότητας μπορεί άμεσα να εμφανίζει στην ιστοσελίδα της εικονικής επιχείρησης το σύνολο των προϊόντων που εκείνος επιθυμεί να προωθήσει καθώς και να διαχειριστεί αμεσότερα τις όποιες αλλαγές θέλει να προβεί όπως εισαγωγή, διαγραφή ενημέρωση της λίστας.

2. Ανάλυση του Προφίλ και της Αγοραστικής Συμπεριφοράς του Καταναλωτή. Οι εφαρμογές του ηλεκτρονικού εμπορίου παρέχουν την δυνατότητα παρακολούθησης και καταγραφής της αγοραστικής συμπεριφοράς του καταναλωτή που επισκέπτεται την εκάστοτε σελίδα ενός ηλεκτρονικού καταστήματος. Γνωρίζοντας ο έμπορος τις προτιμήσεις του πελάτη του αλλά και τα είδη των προϊόντων που συνήθως αγοράζει, μπορεί να χαράξει διαφορετική πολιτική προώθησης προϊόντων αλλά και τιμολογιακή πολιτική για τον κάθε πελάτη ξεχωριστά. Έτσι διαχειρίζεται ευκολότερα την ποσότητα αλλά και την ποιότητα που θα μπορεί να προσφέρει, βάση των στοιχείων που παρέχονται από το αγοραστικό του προφίλ.

3. Αμεσότερος Υπολογισμός εξόδων αποστολής και παράδοσης της παραγγελίας. Κατά την διάρκεια της παραγγελίας ενός καταναλωτή και ακριβώς πριν ολοκληρωθεί η διαδικασία αυτής, ο πελάτης μπορεί να γνωρίζει το συνολικό ποσό πληρωμής. Μέσω ενός εικονικού τιμολογίου (απλός αλγόριθμος υπολογισμού τελικής τιμής μέσω μεταβλητών) γνωρίζεται στον πελάτη τα έξοδα αποστολής, ο τρόπος μεταφοράς των προϊόντων (συνήθως μέσω courier) αλλά και τελικώς το ποσό που θα κληθεί να



πληρώσει ώστε να αγοράσει το σύνολο των υπηρεσιών μέχρι το προϊόν να φτάσει στα χέρια του.

4. Παραγωγή Αναφορών και Παρακολούθηση Καταναλωτών. Τα ηλεκτρονικά καταστήματα δίνουν την δυνατότητα στους διαχειριστές τους (εμπόρους) να παράγουν έναν αριθμό προκαθορισμένων αναφορών, για την συλλογή πληροφοριών που σχετίζονται με τον αριθμό των επισκέψεων, τις πωλήσεις των προϊόντων, τον αριθμό των καταναλωτών που επισκέπτονται το κατάστημα, κα. Στην ουσία αποτελούν στατιστικά στοιχεία από τα οποία ο έμπορος μπορεί να εκμαιεύσει πληροφορίες και να προβεί στις απαραίτητες διορθώσεις αν τυχόν αντιληφθεί προβλήματα στην δομή της επιχειρησής του. Για παράδειγμα, χαμηλή επισκεψιμότητα σε προϊόντα προσφοράς θα μπορούσε να εξηγηθεί πως είτε η συγκεκριμένη κίνηση δεν ενδιαφέρει τους επισκέπτες τους ηλεκτρονικού καταστήματος είτε ότι οι τιμές είναι σε τέτοιο επίπεδο ώστε να μην είναι ανταγωνιστικά τα προϊόντα.

5. Δυνατότητα Διαφήμισης. Το κατεξοχήν χρήσιμο «όπλο» στην «φαρέτρα» ενός ιδιοκτήτη ηλεκτρονικού καταστήματος είναι η διαφήμιση άλλων καταστημάτων ή προϊόντων μέσω της δικής του ιστοσελίδας. Αυτό σημαίνει ότι κι από τις άλλες εικονικές επιχειρήσεις θα υπάρχει διαφήμιση για το δικό του ηλεκτρονικό κατάστημα. Συνάμα μπορεί να προωθεί προϊόντα που δρουν συμπληρωματικά με το δικό του προϊόν, γεγονός που ωθεί τους καταναλωτές να αγοράσουν. Έτσι δημιουργείται ένα είδος συμμαχίας μέσω αλληλοδιαφημίσεων και αλληλοστήριξης της μια εικονικής επιχείρησης με την άλλη.

6. Τιμολογιακή Πολιτική και Στοχευμένη Προώθηση Προϊόντων. Εκτός όσων δυνατοτήτων έχουν αναφερθεί, ένα ηλεκτρονικό κατάστημα δίνει την δυνατότητα στον διαχειριστή του συστήματος να προσφέρει ηλεκτρονικά κουπόνια, προσφορές σε προϊόντα και εκπτώσεις σε συγκεκριμένα τμήματα ή μεμονωμένα προϊόντα του ηλεκτρονικού καταστήματος. Αυτή η πολιτική μπορεί να εφαρμοστεί για συγκεκριμένες ημερομηνίες και χρονικές περιόδους και με ποικίλους τρόπους. Ο περιορισμός του χρονικού ορίζοντα δίνει κίνητρο στους καταναλωτές να αγοράσουν άμεσα πριν την λήξη της όποιας προσφοράς. Ταυτόχρονα ο έμπορος έχει βραχυπρόθεσμα έσοδα που ίσως να μην τα είχε αν δεν είχε επιλέξει την συγκεκριμένη προσφορά για τα προϊόντα του. Ταυτόχρονα, όπως αναφέρθηκε παραπάνω, η

τιμολογιακή πολιτική μπορεί να εφαρμοστεί προς συγκεκριμένους καταναλωτές μέσω της κατηγοριοποίησής τους, διαδικασία που αναλυθεί ακριβώς παρακάτω.

7. Επισκευσιμότητα Πελατών και Πελάτες - Αγοραστές. Η πολιτική που ακολουθείται από τις περισσότερες υπάρχουσες εφαρμογές των ηλεκτρονικών καταστημάτων επιβάλλουν την κατηγοριοποίηση των πελατών η οποία εντάσσεται στην προσπάθεια προώθησης προϊόντων και εξατομίκευσης της πολιτικής των πωλήσεων. Αυτόματα δημιουργείται η φόρμα αυτή ώστε να υπάρχει διαχωρισμός μεταξύ των πελατών που απλά επισκέπτονται το ηλεκτρονικό κατάστημα και δεν έχουν προβεί σε αγορές και σε αυτούς τους πελάτες που έχουν κάνει τουλάχιστον μια αγορά στο παρελθόν, άρα θα έχουν πρόσβαση σε πιο συγκεκριμένες εκπτώσεις. Συμπληρωματικά με την κατηγοριοποίηση των καταναλωτών, υπάρχει και η δυνατότητα εσωτερικής κατηγοριοποίησης των ήδη πελατών του καταστήματος. Η εσωτερική αυτή κατάτμηση δίνει διαφορετικά πλεονεκτήματα ανάλογα με την συχνότητα αγορών που πραγματοποιούν αλλά και από το μέγεθος των αγορών τους. Συχνές κατηγορίες που παρατηρούνται είναι οι Silver και Gold πελάτες. Έτσι διαφοροποιούνται τα επίπεδα εκπτώσεων, προσφορών και προνομίων για τον καθένα. Για την ύπαρξη αυτής της διαδικασίας, θα πρέπει ο πελάτης να έχει κάνει εγγραφή στην βάση δεδομένων του καταστήματος, συμπληρώνοντας στην αντίστοιχη φόρμα τα προσωπικά του στοιχεία.

#### • **Λειτουργίες Καταστήματος για τον Καταναλωτή**

Οι συνήθεις λειτουργίες που προσφέρει ένα τυπικό ηλεκτρονικό κατάστημα στους καταναλωτές είναι :

1. (Προαιρετική) Εγγραφή στο Κατάστημα. Ο εκάστοτε καταναλωτής έχει τη δυνατότητα να εγγραφεί στο σύστημα της εικονικής επιχείρησης και να καταχωρηθεί ως μέλος της. Με αυτό τον τρόπο, καταγράφονται τα προσωπικά του στοιχεία, που καλείται να συμπληρώσει στην φόρμα, καθώς επίσης και οι προτιμήσεις του έτσι ώστε την επόμενη φορά θα εισέλθει στο κατάστημα με τον δικό του προσωπικό κωδικό (username and password). Το ηλεκτρονικό περιβάλλον του καταστήματος θα αναγνωρίσει τον πελάτη και θα αρχίσει να συνθέτει το αγοραστικό του προφίλ είτε

μέσω των προϊόντων που αγοράζει ή ακόμα κι από τα προϊόντα που ελέγχει περιηγούμενος στην ιστοσελίδα.

2. Πλοήγηση στην Ιστοσελίδα του Καταστήματος κι Αναζήτηση. Ίσως κι η σημαντικότερη λειτουργία μιας ηλεκτρονικής επιχείρησης είναι η εύκολη περιήγηση ενός δυνητικού αγοραστή στην ιστοσελίδα μέσω μιας φιλικής διεπαφής. Επιπλέον, οι χρήστες μέσω του μηχανισμού αναζήτησης, μπορούν να αναζητήσουν προϊόντα απλά πληκτρολογώντας την κατάλληλη λέξη. Έτσι εντοπίζουν το πραγματικά ζητούμενο προϊόν γρήγορα, εύκολα και έγκαιρα.

3. Καλάθι Αγορών. Όπως αναφέρθηκε και παραπάνω, η εκάστοτε εφαρμογή ηλεκτρονικού εμπορίου επιτρέπει την επιλογή προϊόντων και προσθήκη αυτών στο «καλάθι αγορών», κατά την διάρκεια της πλοήγησης των καταναλωτών στο κατάστημα. Ως καλάθι αγορών ορίζεται μια εικονική μνήμη που αποθηκεύει τις επιλογές του καταναλωτή μαζί με την αξία του προϊόντος. Ταυτόχρονα σε περίπτωση προσθήκης κι άλλων προϊόντων, ο αλγόριθμός που κρύβεται από πίσω, αθροίζει την τελική αξία πληρωμής. Έτσι όταν ο πελάτης τελειώσει τις αγορές του, προχωρά στο «τάμειο» για να πληρώσει την παραγγελία του, που ήδη ξέρει την τελική αξία της. Συνηθίζεται πλέον, όταν ένας καταναλωτής φύγει από το ηλεκτρονικό κατάστημα χωρίς να κάνει «έξοδο» (log out) από το προσωπικό του προφίλ, όταν επιστρέφει, το καλάθι αγορών του θα είναι αποθηκευμένο κι έτοιμο προς επεξεργασία.

4. Εξατομικευμένο Εμπόριο. Οι ηλεκτρονικές επιχειρήσεις παρέχουν την δυνατότητα στους καταναλωτές να ορίσουν εκείνοι τις προτιμήσεις τους. Υπάρχει επίσης δυνατότητα οριοθέτησης το εύρος τιμών που επιθυμούν να δώσουν για την αγορά ενός συγκεκριμένου προϊόντος. Έτσι μέσω μια φόρμας αναζήτησης – σύγκρισης τιμών, εμφανίζονται οι επιλογές για τον καταναλωτή.

5. Εκπτώτικα Κουπόνια. Προσφέρονται ανάλογα με την τιμολογιακή πολιτική της εταιρείας αλλά και την βαθμίδα που βρίσκεται ο καταναλωτής από την συχνή ή όχι αγορά προϊόντων από το συγκεκριμένο κατάστημα.

6. Λήψη Παραγγελίας. Ο καταναλωτής ορίζει τον τρόπο και τον τόπο λήψης της παραγγελίας του. Μέσω καταχώρησης των στοιχείων του, θα δεχτεί την παραγγελία του εκεί όπου έχει ζητήσει μέσω της διαδικασίας courier.



7. Ηλεκτρονικές Πληρωμές μέσω ψηφιακού πορτοφολιού. Τα προϊόντα τελικώς φτάνουν στην φάση της αγοράς αρκεί ο καταναλωτής να πληρώσει το αντίτιμο που απαιτείται ώστε να γίνουν δικά του. Αυτό μπορεί να γίνει είτε μέσω πιστωτικής κάρτας, όπως αναφέρθηκε ήδη, είτε μέσω ψηφιακού χρήματος προπληρωμένης κάρτας είτε μέσω αντικαταβολής.

Όλα τα ανωτέρω στοιχεία που αναφέρθηκαν συνθέτουν το τοπίο των πλεονεκτημάτων που μπορεί να έχει ένα εικονικό κατάστημα. Οι δυνατότητες – λειτουργίες που παρέχει του δίνουν ανταγωνιστικό πλεονέκτημα έναντι των υπόλοιπων επιχειρήσεων που έχουν φυσική παρουσία. Πλεονεκτήματα καθώς και τα μειονεκτήματα αναλύονται στην επόμενη παράγραφο της παρούσας εργασίας.

## 1.5 ΠΛΕΟΝΕΚΤΗΜΑΤΑ – ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΠΙΧΕΙΡΕΙΝ

Από την περιγραφή της έννοιας του Ηλεκτρονικού Επιχειρείν, διαφαίνεται πως η εξέλιξη της επιχειρηματικότητας τα προηγούμενα χρόνια προσέφερε πολλά οφέλη προς τους καταναλωτές αλλά και τους επιχειρηματίες, μα συνάμα έδρασε κι αρνητικά ως προς το σύνολο της οικονομίας. Παρακάτω θα αναλυθούν διεξοδικά το σύνολο των πλεονεκτημάτων καθώς και των μειονεκτημάτων από το Ηλεκτρονικό Επιχειρείν.

### **Μείωση των ιεραρχικών επιπέδων**

Πληθώρα επιχειρήσεων κατόρθωσαν με την χρήση της τεχνολογίας της πληροφορικής και των τηλεπικοινωνιών να μεταμορφωθούν. Συγκεκριμένα, κατάφεραν να μεταβούν από μια δυσκίνητη καθημερινότητα μπλεγμένη στην γραφειοκρατία, σε ευέλικτες, αποδοτικότερες, επιδεκτικότερες στις αλλαγές και περισσότερο ανταγωνιστικές. Αρκετές μάλιστα κατόρθωσαν να πραγματοποιήσουν μείωση του προσωπικού και των επιπέδων ιεραρχίας στην οργάνωσή τους, να μειώσουν το μέγεθός τους και να γίνουν λειτουργικότερες από κάθε άποψη. Τα δίκτυα των υπολογιστικών συστημάτων που χρησιμοποιούν, επιτρέπουν και υποστηρίζουν την εργασία σε ομάδες, που οδηγεί σε πιο επίπεδη οργάνωση. Αυτού του είδους η οργάνωση όμως θεωρείται



αποδοτικότερη και περισσότερο ελεγχόμενη ως προς την αποφυγή των όποιων παρεκκλίσεων από το οικονομικό πρόγραμμα των επιχειρήσεων. Αυτό συμβαίνει επειδή τα μέλη μιας ομάδας μπορούν να συνεργάζονται ανεξάρτητα από τις θέσεις που βρίσκονται. Οι δυνατότητες αυτές έχουν επίσης οδηγήσει και σε αντίστοιχη αναβάθμιση της λειτουργίας των ανώτερων στελεχών της εκάστοτε διοίκησης. Έτσι, τα υψηλότερα στελέχη μπορούν να διοικούν και να ελέγχουν μεγαλύτερο πλήθος εργαζομένων, να εποπτεύουν περισσότερα έργα, κάτω από οποιεσδήποτε περιστάσεις, έχοντας ταυτόχρονα καλύτερη επίγνωση των πραγμάτων που συνδράμουν τριγύρω τους.

### **Ανεξαρτησία της εργασίας από φυσικό τόπο εξέλιξης**

Η έννοια της ανεξαρτησίας από το τόπο εργασίας είναι μια έννοια ευρέως διαδοσμένη σε χώρες κυρίως του εξωτερικού όπως είναι η Αμερική. Η εργασία από απόσταση εμφανίζεται όλο και πιο συχνά σε ηλεκτρονικές και μη επιχειρήσεις. Συνεπώς, οι νέες τεχνολογίες επιτρέπουν τη συνεργασία ανεξάρτητα από τις αποστάσεις μεταξύ των εργαζομένων. Σε πολλές περιπτώσεις συγκεκριμένα τμήματα της παραδοσιακής οργάνωσης έχουν απαξιωθεί και μπορούν να καταργηθούν. Η διαχείριση αποθεμάτων με αυτοματοποιημένες διαδικασίες (logistics) που παρέχονται από λογισμικό, είναι ένα επίσης χαρακτηριστικό παράδειγμα της ανεξαρτησίας από φυσικό χώρο εργασίας. Οι προμηθευτές πλέον έχουν τη δυνατότητα να συνδέονται μέσω εξωδικτύων ή και του Διαδικτύου με τα συστήματα των επιχειρήσεων, να ενημερώνονται για τις απαιτήσεις και να προετοιμάζονται για τις παραδόσεις. Ενδεικτικό παράδειγμα αποτελεί το σύστημα της Built To Order που είχε αναπτύξει πρώτη η Dell και στην Ελλάδα είναι ευρέως γνωστή η εταιρεία Πλαίσιο. Γενικά οι επιχειρήσεις δεν περιορίζονται πλέον από τις γεωγραφικές τους θέσεις, ούτε και τις δυνατότητες οργάνωσης για να υποστηρίξουν το marketing, την ενημέρωση, τις παραγγελίες, τις πωλήσεις και πληρωμές των προϊόντων και υπηρεσιών που προσφέρουν. Η δικτυακή επιχείρηση, και γενικότερο το ηλεκτρονικό επιχειρείν, έχει την δυνατότητα να συντονίζει όλες τις σχετικές δραστηριότητες, οπουδήποτε κι αν βρίσκονται αυτές. Επί πλέον, η δικτυακή επιχείρηση μπορεί να συνδέεται άμεσα και να συντονίζεται με άλλες επιχειρήσεις, να δημιουργεί εικονικές επιχειρήσεις, που μπορούν να συνδέουν προμηθευτές, κατασκευαστές, ιδέες, περιουσιακά στοιχεία, ακόμα και

ανταγωνιστές. Συνάμα μπορεί μια ηλεκτρονική επιχείρηση να χρησιμοποιεί τις δυνατότητες άλλων συνεργαζόμενων επιχειρήσεων, χωρίς να την ανάγκη κάποιας φυσικής σύνδεσής τους. Χαρακτηριστικό παράδειγμα αποτελεί όταν η επιχείρηση μπορεί να έχει αναλάβει την σχεδίαση ενός προϊόντος ή μιας υπηρεσίας, μια άλλη την παραγωγή και την συναρμολόγησή του, μια τρίτη την οικονομική διαχείριση και μία ακόμα την διανομή του προϊόντος στα επί μέρους σημεία πώλησης στην κάθε περιοχή. Οι συνεργασίες αυτές δεν είναι συνήθως μόνιμες, αλλά διαρκούν όσο το προϊόν ή η υπηρεσία και αποφέρει κέρδη από τον επιμερισμό αυτό των διεργασιών.

### Βελτίωση της Οργάνωσης

Η ανάπτυξη νέων τεχνολογιών έχει εξελίξει αρκετές επιχειρήσεις σε όλους τους κλάδους της οικονομίας. Πιο συγκεκριμένα, στην δικτυακή επιχείρηση, η τεχνολογία της πληροφορικής και την τηλεπικοινωνιών έχει οδηγήσει στην κατάργηση πολλών χειρονακτικών διαδικασιών κι τις έχει αντικαταστήσει με νέες αυτοματοποιημένες. Άμεσο αποτέλεσμα αυτού είναι η βελτιωμένη διαχείριση της ροής των εργασιών. Αυτό το γεγονός έχει οδηγήσει στην μείωση του κόστους και στην βελτίωση της εξυπηρέτησης των πελατών. Με τον τρόπο αυτό πραγματοποιείται σχεδίαση νέων διαδικασιών η οποία συνήθως συμβάλλει με ουσιαστικό τρόπο στη βελτίωση της όλης επιχειρησιακής οργάνωσης. Επιπρόσθετα η δικτυακή επιχείρηση έχει την δυνατότητα να οργανώνεται πιο ευέλικτα και με δυνατότητες καλύτερης απόκρισης στις αλλαγές της αγοράς. Κλείνοντας το κομμάτι της βελτιστοποίησης της οργάνωσης, θα μπορούσε να ειπωθεί πως μέσω της γρηγορότερης απόκρισης της επιχείρησης, μπορεί να ωφεληθεί αμεσότερα από τις παρουσιαζόμενες επιχειρηματικές ευκαιρίες. Όπως είναι φανερό, ανεξάρτητα από το μέγεθος της επιχείρησης, εντός του διαδικτύου έχουν όλοι ίσες ευκαιρίες. Βέβαια το κόστος σε κάθε περίπτωση διευρύνει τη διαφορά εντός των δυνατοτήτων. Όμως οι επιχειρηματικές ιδέες που συνδυάζονται καταλλήλως με τη ορθή χρήση της τεχνολογίας, μπορούν να παράσχουν σε κάθε επιχείρηση, πρόσθετη ευελιξία ώστε να είναι σε θέση να αντεπεξέλθει στις δυσκολίες και στους περιορισμούς που είναι συνάρτηση του μεγέθους της.

Ταυτόχρονα τα πληροφοριακά συστήματα μιας ηλεκτρονικής επιχείρησης επιτρέπουν την κάθετη ροή των πληροφοριακών δεδομένων μεταξύ των ιεραρχικών επιπέδων και την οριζόντια μεταξύ των διαφορετικών λειτουργικών περιοχών. Με τον

τρόπο αυτό λοιπόν γίνεται μια υποτυπώδης διανομή της εξουσίας στα μεσαία και τα κατώτερα διοικητικά στελέχη της επιχείρησης, καθώς και σε ομάδες εργασίας. Παράλληλα η οριζόντια ροή των πληροφοριακών δεδομένων μεταξύ των λειτουργικών περιοχών του ίδιου ιεραρχικού επιπέδου, συμβάλλει ουσιαστικά στην πραγματική οριζόντια πληροφόρηση κάθε επιπέδου και δίνει την δυνατότητα συνεργασίας μεταξύ στελεχών του ίδιου επιπέδου αλλά διαφορετικών λειτουργικών περιοχών. Όλα τα παραπάνω, επαναπροσδιορίζουν τις διοικητικές διαδικασίες παρέχοντας στα στελέχη νέες σημαντικές ελευθερίες στον προγραμματισμό της ηγεσίας, στον έλεγχο καθώς και στην οργάνωση. Ταυτόχρονα η κάθετη ροή επιτρέπει στα διοικητικά στελέχη να πληροφορούνται για την απόδοση της επιχείρησης σε κάθε επίπεδο αλλά και σε κάθε λειτουργική περιοχή.

### **Αποδοτικότερο Marketing**

Τα οφέλη που από την εφαρμογή δικτυακού marketing στο Ηλεκτρονικό Επιχειρείν είναι τα ακόλουθα:

1. Άμεση επικοινωνία με τους πελάτες. Με ελκυστικές και καλά δομημένες παρουσιάσεις των προϊόντων, υπηρεσιών και των εφαρμογών τους, δίνεται μια ολοκληρωμένη εικόνα στους πελάτες με αποτέλεσμα την μείωση του κύκλου των πωλήσεων και τη μείωση του κόστους ενημέρωσης και επικοινωνίας.
2. Αναβάθμιση της εξυπηρέτησης μετά την πώληση, στον πελάτη και την μείωση του κόστους υποστήριξης
3. Ευελιξία προσαρμογής της επιχείρησης στις αλλαγές τις αγοράς μέσω ενημέρωσης των στοιχείων σε μια ηλεκτρονική σελίδα που είναι εύκολη και ταχύτερη ως προς την χρήση από τους καταναλωτές, λόγω φύσης του μέσου. Αντίθετα, αν η επιχείρηση θελήσει να ενημερώσει τον έντυπο κατάλογό της και να τον διανεμίει, το κόστος και ο χρόνος που θα χρειαστούν είναι σαφώς μεγαλύτερα.
4. Δυνατότητα άμεσης επικοινωνίας με τους προμηθευτές



5. Δυνατότητα σε κάθε επιχείρηση, ανεξάρτητα μεγέθους, να απευθυνθεί ανταγωνιστικά στην παγκόσμια αγορά με δυνητικό αγοραστικό κοινό που ξεπερνά τα εκατομμύρια καταναλωτών.
6. Εξυπηρέτηση Πελατών σε Πραγματικό Χρόνο
7. On line παράδοση πληροφοριακού υλικού και άλλων προϊόντων
8. Δυνατότητα άμεσης παρακολούθησης των ανταγωνιστικών προϊόντων
9. Δυνατότητα μετρήσεων αποτελεσματικότητας και διεξαγωγής ερευνών, βαθμού ικανοποίησης πελατών, επιθυμητά χαρακτηριστικά ενός νέου προϊόντος.
10. Αύξηση της αφοσίωσης του πελάτη και αναβάθμιση της επικοινωνίας της επιχείρησης με τον καταναλωτή.
11. On line συνεργασία με άλλες επιχειρήσεις
12. Χαμηλότερο κόστος προϊόντος και μικρότερος χρόνος παράδοσης

### **Χαμηλά Επίπεδα Ασφαλείας και Διασφάλισης Αυθεντικότητας**

Η μεγάλη ευκολία πρόσβασης κι επομένως το χαμηλό επίπεδο ασφάλειας, πρόσβασης σε πληροφορίες αλλά και διεκπεραίωσης των οικονομικών συναλλαγών είναι από τα βασικότερα μειονεκτήματα του Ηλεκτρονικού Επιχειρείν. Λόγω αυτής της σοβαρότατης έλλειψης ασφάλειας, συνήθως οι χρήστες χρησιμοποιούν το Διαδίκτυο για μια απλή περιήγηση, δηλαδή ουσιαστικά για πληροφόρηση κι όχι για την πραγματοποίηση αγοράς προϊόντος. Η ασφάλεια στο Ηλεκτρονικό Εμπόριο, γενικότερα, είναι πρωταρχικής σημασίας τόσο για τον πελάτη όσο και για την ίδια επιχείρηση. Η έλλειψη ενός απόλυτα ασφαλούς μοντέλου συναλλαγών στο διαδίκτυο θεωρείται σημαντικό εμπόδιο εισόδου για πολλούς καταναλωτές, αλλά και για τις επιχειρήσεις που επιθυμούν να εισέλθουν στην αγορά αυτή είτε ως αγοραστές είτε ως πωλητές αγαθών και υπηρεσιών. Το θέμα της ασφάλειας ανακύπτει από την ανάγκη αποστολής του αριθμού πιστωτικής κάρτας του πελάτη, γεγονός το οποίο όμως γίνεται και στις φυσικές συναλλαγές της καθημερινότητας, εφόσον χρησιμοποιηθεί η κάρτα. Για την αντιμετώπιση των προβλημάτων αυτών, ως ποιοτικότερη μέθοδος αποτελεί η

κρυπτογράφηση, έννοια που θα αναλυθεί παρακάτω. Έτσι, ενδεικτικά αναφέρεται, πως είτε τα δεδομένα στέλνονται κρυπτογραφημένα είτε διατηρούνται κρυπτογραφημένα σε βάσεις δεδομένων των επιχειρήσεων. Οι μέθοδοι αυτές σε συνδυασμό και με άλλες τεχνικές ασφαλείας, προσπαθούν να εκπληρώσουν τις ελάχιστες προδιαγραφές για ασφάλεια των συναλλαγών που συνοψίζονται στο εξής τετράπτυχο: Ιδιωτικότητα, Εμπιστευτικότητα, Ακεραιότητα και Δεσμευτικότητα.

### **Επίπεδα Εξοικείωσης Καταναλωτών με Τεχνολογία**

Ακόμα και σήμερα, δεν είναι δεδομένο πως όλοι οι υπονήφιοι πελάτες ή η αγορά – στόχος έχει πρόσβαση στο διαδίκτυο. Σύνολο ανθρώπων ακόμα δεν χρησιμοποιούν την τεχνολογία. Συνεπώς κάποιες επιχειρήσεις, ακόμα και αν το επιθυμούν δεν μπορούν να χρησιμοποιούν το διαδίκτυο ως αποκλειστικό μέσο προώθησης των προϊόντων τους. Ταυτόχρονα, η έλλειψη κάποιου κεντρικού συντονισμού και ευρετηρίου που να εγγυάται την ταχύτητα, την αξιοπιστία και την διαθεσιμότητα του δικτύου, μετατρέπει τις ηλεκτρονικές αγορές σε πραγματική σπασσοκεφαλιά. Το διαδίκτυο δεν διαθέτει κάποιο κεντρικό σύστημα ταξινόμησης κι ελέγχου σε μηχανές αναζήτησης. Έτσι ο χρήστης, ακόμα κι αυτός που έχει επαφή με την νέα τεχνολογία, δυσκολεύεται αρκετά στο επίπεδο συλλογής επαρκούς πληροφόρησης για την επικείμενη ηλεκτρονική αγορά που θέλει να πραγματοποιήσει. Αντιλαμβανόμεστε άμεσα λοιπόν, πως σε περίπτωση ηλεκτρονικού αναλφαριθμητισμού ή ελλιπούς εξοικείωσης από πλευράς των καταναλωτών, θα πρέπει η επιχείρηση να αλλάξει προσανατολισμό στην μορφή της και να μετατρέψει τις ηλεκτρονικές υπηρεσίες σε περισσότερο παραδοσιακές.

### **Συναλλαγματικές Ισορροπίες – Νομοθετική Κάλυψη**

Οι κυβερνήσεις προσπαθούν να ελέγχουν την εισροή και εκροή συναλλάγματος, ώστε η ψαλίδα μεταξύ τους να μην ξεπερνά κάποια προαποφασισμένα όρια. Η διάδοση των ηλεκτρονικών επιχειρήσεων άρα και του ηλεκτρονικού εμπορίου, με την πραγματοποίηση αγορών μέσω του διαδικτύου, επέφερε σημαντικές αλλαγές στις συναλλαγματικές ισορροπίες μεταξύ των κρατών καθώς και στα επίπεδα εξαγωγών. Εφόσον οι περισσότερες δικτυακές επιχειρήσεις, βάσει ερευνών βρίσκονται χωροταξικά στις ΗΠΑ, τεράστια ποσά συναλλάγματος φεύγουν από τις χώρες του κόσμου, και κυρίως από τις πιο ανεπτυγμένες όπως είναι η Ευρώπη, με προορισμό τις

ΗΠΑ. Το πρόβλημα γίνεται εντονότερο σε χώρες με ήδη βεβαρημένο συναλλαγματικό ισοζύγιο.

Από την άλλη, η σχεδόν πλήρης έλλειψη νομοθετικής κάλυψης σε θέματα που προκύπτουν από το Ηλεκτρονικό Εμπόριο και τη χρήση του διαδικτύου για επιχειρησιακές συναλλαγές, καθιστούν αυτές ως λιγότερο ελκυστικές. Κρίνεται αναγκαία η θέσπιση ειδικού νομοθετικού πλαισίου και η αναθεώρηση του ισχύοντος.

### **Ανταγωνισμός – Λογοκλοπή – Αντιγραφή**

Ίσως από τα σημαντικότερα μειονεκτήματα μιας ηλεκτρονικής επιχείρησης είναι η έννοια της «Λογοκλοπής». Η διαδικασία marketing μέσω διαδικτύου μετατρέπει την ηλεκτρονική σελίδα της κάθε επιχείρησης σε εύκολο στόχο «πειρατείας». Με τον δόκιμο αυτό όρο εννοείται η κλοπή μέρους ή ολόκληρου του περιεχομένου μιας ιστοσελίδας από χρήστες με σκοπό την αντιγραφή της. Έτσι μέσω του πλεονεκτήματος της δωρεάν δημοσιοποίησης από το Διαδίκτυο, η ηλεκτρονική εικόνα της επιχείρησης εκτίθεται σε κάθε είδους επεξεργασία μέσω της λογοκλοπής. Το συμβάν αυτό έρχεται να λειτουργήσει με επιπρόσθετο αρνητικό φορτίο αν η κατασκευή – συντήρηση της όποιας ιστοσελίδας επιβαρύνεται με ένα σημαντικό κόστος στον προϋπολογισμό της επιχείρησης. Το ύψος του ποσού επιβαρύνει την μία, ενώ ταυτόχρονα, μέσω της λογοκλοπής, μπορεί να ωφελούνται περισσότερες επιχειρήσεις.

Τέλος, άξιο αναφοράς είναι το επίπεδο του ανταγωνισμού που αναπτύσσεται στον Παγκόσμιο Ιστό. Με την έννοια παγκόσμιο, χρειάζεται να τονιστεί το μέγεθος της προσπάθειας που χρειάζεται να καταβάλει η κάθε επιχείρηση ώστε να μπορεί να επιβιώσει στον στίβο του ανταγωνισμού. Καθημερινώς αναηδούν όλο και περισσότερες επιχειρήσεις που δραστηριοποιούνται στο Ηλεκτρονικού Επιχειρείν. Το χαμηλό κόστος εισόδου, μετατρέπει το Διαδίκτυο σε μια ασφαλή αρένα ως προς την χρεωκοπία αλλά Ρωμαϊκό Κολοσσαίο ως προς τον ανταγωνισμό. Παραγγελίες για αγορές προϊόντων μέσω Διαδικτύου θεωρητικά γίνονται σε οποιονδήποτε χρόνο και από οποιονδήποτε τόπο μπορεί να βρίσκεται ο καταναλωτής. Όμως, όπως έχει φανεί, οι καταναλωτές είναι διστακτικοί στο να αγοράζουν προϊόντα από ηλεκτρονικά καταστήματα (δεν δίνουν εύκολα λ.χ. τον αριθμό της πιστωτικής τους κάρτας στο Διαδίκτυο...) ενώ δεν εμπιστεύονται και το service των ηλεκτρονικών καταστημάτων.



Σκληρός ανταγωνισμός παρατηρείται στα εγχώρια ηλεκτρονικά καταστήματα, καθώς ο ανταγωνισμός στην αγορά είναι εξοντωτικός και πολλές επιχειρήσεις βρίσκονται πλέον σε οριακό επίπεδο. Ο πόλεμος των τιμών μεταξύ των καταστημάτων, τα ιδιαίτερα χαμηλά περιθώρια καθαρού κέρδους- που πέφτουν ακόμα και κάτω του 2%-, αλλά και η είσοδος των παραδοσιακών, μεγάλων αλυσίδων στην αγορά του ηλεκτρονικού εμπορίου σφίγγουν τον κλοιό στην αγορά. [3]

## 1.6 ΕΙΚΟΝΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ – ΗΛΕΚΤΡΟΝΙΚΑ ΚΑΤΑΣΤΗΜΑΤΑ

Στην ενότητα αυτή θα αναλυθεί το Ηλεκτρονικό Κατάστημα ή Ηλεκτρονική Επιχείρηση ως ορισμός αλλά και θα αναφερθεί η ιστορικότητα καθώς και η εξέλιξη διαμέσου των ετών.

*Ηλεκτρονικό Κατάστημα (e-shop) είναι ο όρος που χρησιμοποιείται για να αναφερθεί κάποιος σε ένα Δικτυακό τόπο (site) μέσω του οποίου πραγματοποιούνται πωλήσεις διαφόρων ειδών. [1]*

Τα ηλεκτρονικά καταστήματα συγκαταλέγονται στις εφαρμογές της κατηγορίας επιχείρηση προς καταναλωτή (B2C) και αποτελούν σημεία πρόωθησης και πώλησης αγαθών μέσω του Διαδικτύου. Ένα ηλεκτρονικό κατάστημα μπορεί να αναπαραστήσει ένα φυσικό κατάστημα, καθώς και να το εμπλουτίσει, χρησιμοποιώντας τη τεχνολογία, καθιστώντας το πιο λειτουργικό, με άμεσο στόχο την ποιοτικότερη εξυπηρέτηση του καταναλωτή.. Σε αρκετές περιπτώσεις, τα e-shops λειτουργούν ως υποκαταστήματα των υφιστάμενων (φυσικών) καταστημάτων, ενώ σε άλλες περιπτώσεις αποτελούν τα μοναδικά σημεία πώλησης των προϊόντων μιας επιχείρησης. Η έννοια της μοναδικότητας που αναφέρθηκε συνεπάγεται φυσικά της ύπαρξη κάποιας αποθήκης κι ενός συστήματος διανομής των προϊόντων στους καταναλωτές, μα αποτρέπεται η ύπαρξη φυσικού χώρου με την έννοια του καταστήματος όπως την ξέρουμε μέχρι τώρα. Συνεπώς ένα ηλεκτρονικό κατάστημα μπορεί να λειτουργεί χωρίς όμως την φυσική ύπαρξη χώρου ως προς την διάθεση προϊόντων και υπηρεσιών για τους καταναλωτές. Στόχος του ηλεκτρονικού καταστήματος, δεν είναι μόνο η προβολή των προϊόντων αλλά και η εφαρμογή τεχνικών που προσδίδουν πρόσθετη αξία στην ηλεκτρονική παρουσία του εμπόρου και ωθούν τον πελάτη να προτιμήσει την ηλεκτρονική αγορά



έναντι της παραδοσιακής. Οι τεχνικές αυτές αφορούν την αποτελεσματική απόκριση στις ανάγκες του καταναλωτή μέσα από την παροχή υποστήριξης στον πελάτη, πριν καθώς και μετά την συναλλαγή. Επιπλέον, θα πρέπει να ληφθεί υπόψη και ο σχεδιασμός, η παραγωγή και η προώθηση των προϊόντων βάσει των ιδιαίτερων απαιτήσεων και αναγκών του κάθε πελάτη, μεμονωμένα, καθώς και η δυνατότητα εξοικονόμησης κόστους αλλά και χρόνου.

Ο καταστηματάρχης από την πλευρά του, εξασφαλίζει την ηλεκτρονική παρουσία του καταστήματος του σε ολόκληρο τον κόσμο με αποτέλεσμα την δημιουργία νέων διεξόδων προώθησης και πώλησης των προϊόντων του. Επιπρόσθετα, προκύπτουν νέα κανάλια επικοινωνίας με τους πελάτες αλλά και με τις άλλες επιχειρήσεις καθιστώντας ακόμα πιο ισχυρή κι άμεση την επαφή της ηλεκτρονικής επιχειρήσής του μαζί τους. Το σύνολο των αυτοματοποιημένων διαδικασιών, που αφορούν την διαχείριση αποθεμάτων και την διανομή των προϊόντων, μπορούν να υιοθετηθούν και να συντελέσουν στην εξοικονόμηση του κόστους για την επιχείρηση, γεγονός που θα μπορεί να μετακυλιστεί και στον πελάτη μέσω κάποιας μείωσης της τελικής τιμής του προϊόντος. Έτσι η επιχείρηση γίνεται ανταγωνιστικότερη καταλαμβάνοντας μεγαλύτερο μερίδιο από την «πίτα» των καταναλωτών.

Τα ηλεκτρονικά καταστήματα του Διαδικτύου, σε ένα μεγάλο ποσοστό τους, διαθέτουν χαρακτηριστικά που αφορούν την προβολή, προώθηση των προϊόντων, την δυνατότητα άμεσης παραγγελίας και αγοράς αυτών είτε με αντικαταβολή είτε μέσω πιστωτικής κάρτας. Επίσης, υιοθετούνται μέθοδοι για την αναγνώριση της ταυτότητας του πελάτη και σκιαγράφηση του προφίλ, όχι μόνο όσον αφορά τα προσωπικά του στοιχεία αλλά και τις αγοραστικές του συνήθειες. Με αυτό τον τρόπο, κάθε φορά που ο συγκεκριμένος πελάτης επισκέπτεται το κατάστημα, εμφανίζονται στην οθόνη του κάποιες διαμορφωμένες σελίδες σύμφωνα με τις απαιτήσεις και την αγοραστική του συμπεριφορά κατά την τελευταία επίσκεψή του ή στο σύνολο των επισκέψεων του. Η διαδικασία αυτή εμπίπτει σε καταστρατήγηση των προσωπικών δεδομένων μιας κι η δημιουργία καταναλωτικού προφίλ από τις επιχειρήσεις αποτελεί προϊόν συναλλαγής σε μεταγενέστερες αγορές και ομαδοποιεί τον καταναλωτή σε κατηγορίες. Έτσι τίθεται θέμα ελέγχου και παραβίασης των προσωπικών δεδομένων. Το φαινόμενο αυτό θα αναλυθεί περαιτέρω σε επόμενο κεφάλαιο της διπλωματικής αυτής εργασίας.

Σε αυτό το σημείο θα ήταν σημαντικό να αναφερθεί η ιστορική εξέλιξη και η κατηγοριοποίηση των ηλεκτρονικών καταστημάτων, από την πρώιμη μορφή που παρουσιάστηκαν στο Διαδίκτυο μέχρι την κατάσταση που βρίσκονται στην σημερινή εποχή. Με την πάροδο των ετών τα ηλεκτρονικά καταστήματα διαμορφώθηκαν και εξελίχθηκαν ως εξής:

1. Η ΠΡΩΤΗ ΓΕΝΙΑ όπου η εμφάνισή τους έγινε σχεδόν ταυτόχρονα με την ανάπτυξη του Παγκόσμιου Ιστού (www) και οι δυνατότητες που υπήρχαν ήταν σε επίπεδο δημιουργίας ηλεκτρονικών σελίδων ως μέσο διαφήμισης και προβολής στο παγκόσμιο καταναλωτικό κοινό. Με την πάροδο του χρόνου και της κατανόησης πως το Δίκτυο αποτελεί ένα από τα χρησιμότερα εργαλεία, οι επιχειρήσεις άρχισαν να επενδύουν αρκετά χρήματα προκειμένου να βελτιώσουν τις διεπαφές τους δημιουργώντας έτσι πιο προσιτές και εύχρηστες ιστοσελίδες προς όφελος των δυνητικών πελατών τους.
2. Η ΔΕΥΤΕΡΗ ΓΕΝΙΑ έχει το εξής νέο στοιχείο που είναι η Ηλεκτρονική Παραγγελία. Όπως αναλύθηκε παραπάνω, μέσω στοχευμένου marketing υπάρχει η δυνατότητα προσέγγισης καταναλωτών μέσω παραγγελίας εντός Διαδικτύου. Έτσι αυτόματα μεγαλώνει το εύρος της αγοράς κάθε επιχείρησης αφού υπάρχει πλέον η δυνατότητα να δέχεται παραγγελίες από περιοχές στις οποίες μέχρι εκείνη την στιγμή δεν υπήρχε η φυσική παρουσία ενός καταστήματος. Η επιχείρηση δηλώνει πλέον το παρόν σε αγορές που μέχρι πρότινος ήταν σαφώς ακατόρθωτο να εισχωρήσει. Μέσω της πλοήγησης των καταναλωτών στο ηλεκτρονικό κατάστημα, δημιουργείται ένα καλάθι, που ο καταναλωτής, πριν αποχωρήσει από την σελίδα μπορεί να επιβεβαιώσει την παραγγελία του και τελικά να κάνει την συναλλαγή. Η παραγγελία του αυτή αποθηκεύονταν υποτυπωδώς στην επιχείρηση κι από εκεί εκείνη πραγματοποιούσε τις επιλογές του καταναλωτή.
3. Η ΤΡΙΤΗ ΓΕΝΙΑ προσπάθησε και κατάφερε να ξεπεράσει το εμπόδιο της ολοκλήρωσης των ηλεκτρονικών σελίδων άρα και των παραγγελιών τους με τις βάσεις δεδομένων που έχει η κάθε επιχείρηση. Έτσι, γύρω στα μέσα του 1995, αναδεικνύεται η ανάγκη της ολοκλήρωσης των ηλεκτρονικών καταστημάτων με τα υπάρχοντα πληροφοριακά συστήματα. Επιχειρήσεις που διέθεταν

ηλεκτρονικά καταστήματα εγκατεστημένα στους υπολογιστές, δημιούργησαν τον τρόπο της ομαλής συνύπαρξης και λειτουργίας των δύο συστημάτων. Επιτεύχθηκε ο στόχος σύμφωνα με τον οποίο καταχωρούνταν απευθείας οι ηλεκτρονικές παραγγελίες στο πληροφοριακό σύστημα προκειμένου να διεκπεραιώνονται αμεσότερα και ορθότερα. Βέβαια, μετά την υλοποίηση ενός τέτοιου μηχανισμού, προέκυψαν κι άλλα θέματα όπως η αυτόματη ενημέρωση της αποθήκης, και η διαχείριση των προσφορών του ηλεκτρονικού καταστήματος από το υπάρχον Πληροφοριακό Σύστημα, ενώ προέκυψε και το θέμα της ηλεκτρονικής πληρωμής. Στη κατηγορία αυτή εντάσσονται και ηλεκτρονικά καταστήματα που υποστηρίζουν, την ηλεκτρονική τιμολόγηση αλλά και την ηλεκτρονική παράδοση των προϊόντων.

4. Η ΤΕΤΑΡΤΗ ΓΕΝΙΑ και τελευταία μορφή αφορά στα πλήρη ηλεκτρονικά καταστήματα, που υποστηρίζουν πλέον και το θέμα της ηλεκτρονικής πληρωμής. Μέσω ολοκληρωμένες κι ασφαλών υπηρεσιών, η συναλλαγή παίρνει πλήρη ηλεκτρονική μορφή. Εισάγονται νέες έννοιες όπως είναι το ηλεκτρονικό πορτοφόλι, ευέλικτη κοστολόγηση, εξατομικευση συμπεριφοράς καταναλωτή, επεκτασιμότητα και αυτοματοποιημένος υπολογισμός των φορολογικών συντελεστών,

## 1.7 ΑΝΑΠΤΥΞΗ ΤΩΝ ΕΙΚΟΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

Σε μια περίοδο οικονομικών προκλήσεων, όπως βρίσκεται αυτή την στιγμή η Ελλάδα, η ανάπτυξη των εικονικών επιχειρήσεων είναι κάτι παραπάνω από μια απάντηση για ένα καλύτερο οικονομικό περιβάλλον. Δεν αρκεί απλώς η μετατροπή των σημερινών υπηρεσιών σε On line υπηρεσίες. Η ανάπτυξη των εικονικών επιχειρήσεων μπορεί να διαμορφώσει μια νέα σχέση αγοράς – καταναλωτή, να συντομεύσει την απόσταση ανάμεσα στην καινοτομία και την επιχειρηματικότητα, να δώσει ευκαιρίες επιχειρηματικότητας σε γεωγραφικά απομακρυσμένες περιοχές της χώρας (ακριτικά μέρη ή αποκεντρωμένα), να συνδυάσει την έρευνα και την επιχειρηματική δραστηριότητα. Μια νέα ψηφιακή αγορά θα μπορέσει να υπερβεί τις όποιες στρεβλώσεις της ελληνικής οικονομίας, να διαρρήξει ολιγοπωλιακές και μονοπωλιακές



πρακτικές ενώ οι πολίτες θα αναπτύξουν μια νέα καταναλωτική συμπεριφορά, έχοντας περισσότερες δυνατότητες για σύγκριση και αξιολόγηση των προϊόντων. Η ανάπτυξη των εικονικών επιχειρήσεων αφορά το σύνολο των υπηρεσιών που μπορεί να λαμβάνει ο πολίτης από τον ιδιωτικό τομέα. Σήμερα η Ελλάδα βρίσκεται αρκετά πίσω σε όλους τους δείκτες που άπτονται της ψηφιακής οικονομίας, τόσο σε ότι αφορά τους καταναλωτές, όσο και τις επιχειρήσεις.

Στην ελληνική οικονομία οι αμιγώς εικονικές επιχειρήσεις δεν έχουν αναπτυχθεί ικανοποιητικά. Σε πολλές περιπτώσεις, επιχειρήσεις που ξεκίνησαν τη δραστηριότητα τους ως αποκλειστικά ηλεκτρονικές στη συνέχεια διαμόρφωσαν και χώρο πώλησης προϊόντων και off line. Χαρακτηριστικά παραδείγματα αποτελούν οι επιχειρήσεις ηλεκτρονικών (e-shop, getitnow, κα) που ενώ ξεκίνησαν ως ηλεκτρονικά καταστήματα με αποθήκες ώστε από εκεί να γίνεται η διανομή, χρειάστηκαν να προχωρήσουν στην δημιουργία καταστημάτων με φυσική υπόσταση.

Η εξήγηση για το φαινόμενο αυτό είναι σύνθετη. Η επικρατέστερη άποψη είναι πως οι Έλληνες διατηρούν μεγάλες επιφυλάξεις για τις ηλεκτρονικές συναλλαγές. Χαρακτηριστικό είναι ότι από έρευνα της Ελληνικής Στατιστικής Αρχής προέκυψε ότι, το ποσοστό των Ελλήνων που δεν πραγματοποιούν ηλεκτρονικές αγορές μέσω των ηλεκτρονικών καταστημάτων ανέρχεται στο 81,6% των χρηστών του διαδικτύου. Αν συμπεριληφθεί και το μέρος των καταναλωτών που δεν χρησιμοποιούν το διαδίκτυο, συμπεραίνουμε πως η επιφυλακτικότητα στην Ελλάδα είναι ακόμη σε πιο υψηλά επίπεδα.

Οι πιο σημαντικοί ανασταλτικοί παράγοντες για τους οποίους δεν πραγματοποιούνται άμεσες ηλεκτρονικές αγορές είναι οι ακόλουθοι:

1. Οι Έλληνες καταναλωτές προτιμούν ακόμη την αγορά προϊόντων με τον παραδοσιακό τρόπο – επειδή ταιριάζει με τη ψυχοσύνθεσή τους
2. Υπάρχει καθυστέρηση στην παράδοση των προϊόντων
3. Υπάρχει αμφιβολία για την πραγματοποίηση της παράδοσης των προϊόντων στο σπίτι



4. Σε πολλές περιπτώσεις τα προϊόντα δεν είναι συνεχώς διαθέσιμα κι ας εκτίθενται στην ιστοσελίδα
5. Υπάρχει ανησυχία στην χρήση των πιστωτικών καρτών, για λόγους ασφαλείας
6. Πολλές επιχειρήσεις δεν φροντίζουν για την ασφάλεια των προσωπικών δεδομένων κι ένα πλήθος επιχειρήσεων δεν έχουν πολιτική διαφύλαξης (privacy policy).

Όλοι αυτοί οι λόγοι, άλλος περισσότερος άλλος λιγότερο, έχουν συμβάλει στην διαμόρφωση των επιπέδων της ηλεκτρονικής επιχειρηματικότητας στα ελληνικά δεδομένα. Τέλος είναι άξιο να αναφερθεί πως και η κρίση που περνά σήμερα η χώρα μας συμβάλλει αρνητικά σε όλα τα επίπεδα της οικονομίας κι όχι μόνο στην επιχειρηματικότητα.

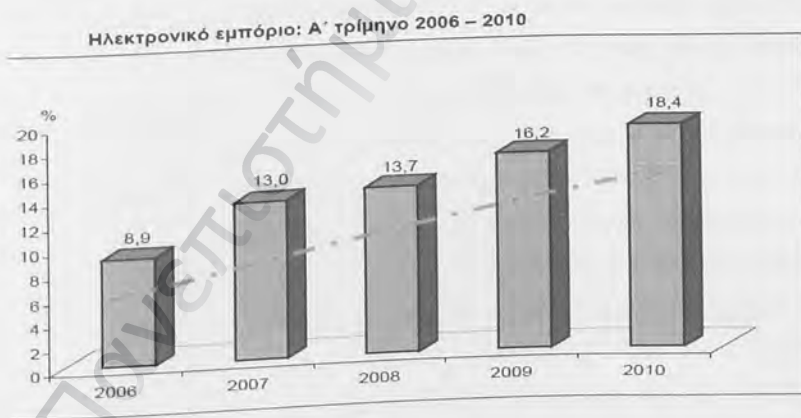
Σαφώς το κλίμα δεν είναι μόνιμα αρνητικό. Γίνονται συνεχώς θετικά βήματα προς την ανάπτυξη της ηλεκτρονικής επιχειρηματικότητας ειδικά σε νεανικές ηλικίες όπως είναι οι φοιτητές. Δράσεις και διαγωνισμοί οργανώνονται ολοένα και συχνότερα με χρηματικά αντίτιμα μα κι επενδυτικά κεφάλαια από ιδιώτες ώστε να υλοποιηθούν οι ιδέες των νικητών. Ένας από αυτούς είναι ο διαγωνισμός Global Management Challenge που αποτελεί διεθνή θεσμό τα τελευταία 32 χρόνια και διεξήχθη φέτος στην χώρα μας για 6<sup>η</sup> συναπτή χρονιά. Το σημαντικό είναι πως διεξάγεται εξ ολοκλήρου ηλεκτρονικά, δηλαδή μέσω διαδικτύου, από ομάδες φοιτητών και στελεχών που έχουν δηλώσει συμμετοχή κι οι οποίες καλούνται να διοικήσουν εικονικές επιχειρήσεις σε όλους τους λειτουργικούς τομείς, επί τη βάση ενός ιδιαίτερος εξελιγμένου λογισμικού προσομοιωτή. Η ελληνική συμμετοχή αναδείχθηκε νικήτρια από την δεύτερη θέση. [9]

#### 1.8 ΣΤΟΙΧΕΙΑ ΠΡΟΤΙΜΗΣΗΣ ΕΛΛΗΝΩΝ ΚΑΤΑΝΑΛΩΤΩΝ ΠΡΟΣ ΤΙΣ ΕΙΚΟΝΙΚΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Στην ενότητα αυτή θα παρουσιαστούν στοιχεία σχετικά με τη προτίμηση των Ελλήνων καταναλωτών προς τις εικονικές επιχειρήσεις και γενικότερα την διαδικασία ηλεκτρονικών παραγγελιών.

Σύμφωνα με τα στοιχεία έρευνας που πραγματοποίησε η Ελληνική Στατιστική Αρχή προκύπτει ότι:

1. Το ποσοστό των χρηστών του διαδικτύου που κατά το Α' τρίμηνο του 2010 πραγματοποίησαν ηλεκτρονικές αγορές, ανέρχεται στο 18,4%. Ωστόσο, όπως απέδειξε η έρευνα, οι μειωμένοι ρυθμοί αύξησης (13,6% για το χρονικό διάστημα 2009-2010, ενώ 18,2% για το 2008-2009) αντικατοπτρίζουν την επιφυλακτικότητα που διακατέχει το μεγαλύτερο σύνολο των Ελλήνων καταναλωτών. Παρόλα αυτά ο μέσος ετήσιος ρυθμός μεταβολής των αγορών μέσω διαδικτύου, ανέρχεται στο 20,8% για την πενταετία 2006-2010. (Σχήμα 1) Στο παραπάνω συμπέρασμα της επιφυλακτικότητας έρχεται να προστεθεί και το στοιχείο πως παρόλο που οι χρήστες που δεν έχουν κάνει ηλεκτρονικές αγορές ολοένα και μειώνεται, τα επίπεδα των ηλεκτρονικών αγοραστών παραμένουν αρκετά χαμηλά. Συμπέρασμα αυτού είναι πως το διαδίκτυο συνεχίζει να μην αποτελεί την συνηθέστερη πρακτική αγορών για τα ελληνικά νοικοκυριά.



2. Ως προς το προφίλ του μέσου καταναλωτή των ηλεκτρονικών επιχειρήσεων προέκυψε ότι ο μέσος πελάτης είναι στην συντριπτική του πλειοψηφία άντρας ηλικίας από 25 έως 34 ετών, μισθωτός κι απόφοιτος ανώτερης ή ανώτατης εκπαίδευσης. Αξιοσημείωτη σαφώς υπήρξε κι η μεγάλη ποσοστιαία διαφορά μεταξύ αντρών και γυναικών που πραγματοποιούν ηλεκτρονικές αγορές. Το μέγεθος αυτό φτάνει περίπου στις 30 ποσοστιαίες

μονάδες υπέρ του αντρικού φύλου. Κάτι τέτοιο σίγουρα θα μπορούσε να δηλώσει αρκετά για τις καταναλωτικές συνήθειες των γυναικών, όπως ότι εμπιστεύονται λιγότερο το διαδίκτυο ή ότι επιθυμούν οπτική επαφή με το προϊόν που θέλουν να αγοράσουν. (Σχήμα 2)



3. Τα προϊόντα ή οι υπηρεσίες που αγοράστηκαν ή παραγγέλθηκαν από το διαδίκτυο για προσωπική χρήση, κατά τη χρονική περίοδο Απρίλιος 2009 – Μάρτιος 2010, είναι, κυρίως, ηλεκτρονικές συσκευές και βιντεοκάμερες, φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεοράσεις, DVDs κλπ. (28,5%), ταξιδιωτικές υπηρεσίες, όπως εισιτήρια, ενοικίαση αυτοκινήτου κλπ. (27,8%), και είδη ένδυσης και υπόδησης – αθλητικά είδη (24,5%). Τα είδη και οι υπηρεσίες που παρουσιάζουν μεγαλύτερη αύξηση, σε σχέση με το 2009, είναι προϊόντα όπως λογισμικό για ηλεκτρονικό υπολογιστή, ηλεκτρονικές συσκευές, οικιακά είδη και είδη ένδυσης. Ταυτόχρονα ενώ τα προηγούμενα χρόνια υπηρεσίες τουρισμού είχαν την μεγαλύτερη προτίμηση των καταναλωτών, το έτος 2010 εμφάνισαν μια σταθερότητα ενώ ειδικότερα οι υπηρεσίες ταξιδιωτικών γραφείων μια μείωση της τάξης του 10%. Αναλυτικά, τα προϊόντα και οι υπηρεσίες που παραγγέλθηκαν ή αγοράστηκαν ηλεκτρονικά, κατά τη χρονική περίοδο Απρίλιος 2009 – Μάρτιος 2010, παρουσιάζονται στον πίνακα που ακολουθεί. (Πίνακας 1)
- Τα προϊόντα που αγοράζονται on-line συνεχίζουν να είναι, κατά κύριο λόγο, το λογισμικό και οι αναβαθμίσεις για ηλεκτρονικό υπολογιστή



συμπεριλαμβανομένων των computer games και video games (67,3% επί του συνόλου των παραδιδόμενων on-line προϊόντων) και ακολουθούν με 30,9% τα βιβλία, τα περιοδικά, οι εφημερίδες σε ηλεκτρονική μορφή, το υλικό ηλεκτρονικής εκμάθησης και με 19,9% οι ταινίες και η μουσική. Και εδώ, επίσης, παρουσιάζεται διαφορά μεταξύ των δύο φύλων, αφού το 80% όσων αγοράζουν και παραλαμβάνουν on-line τα προαναφερθέντα προϊόντα είναι άνδρες και μόνο το 20% γυναίκες.

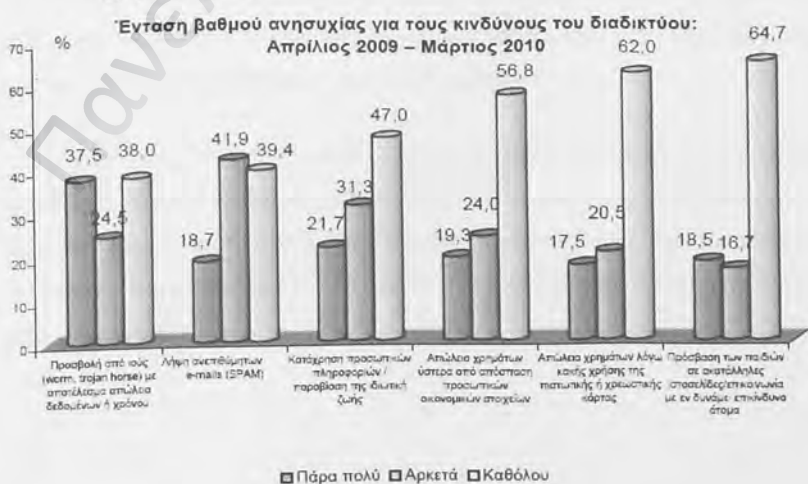
Αγαθά και υπηρεσίες που αγοράστηκαν / παραγγέλθηκαν από το διαδίκτυο: Απρίλιος 2009 – Μάρτιος 2010

ΑΓΑΘΑ – ΥΠΗΡΕΣΙΕΣ	% του συνολικού αριθμού αγορών
Ηλεκτρονικές συσκευές (βιντεοκάμερες, φωτογραφικές μηχανές, κινητά τηλέφωνα, τηλεόρασεις, DVDs κλπ.)	28,5
Ταξιδιωτικές υπηρεσίες (εισιτήρια, ενοίκιαση αυτοκινήτου κλπ.)	27,8
Είδη ένδυσης και υπόδησης – αθλητικά είδη	24,5
Εξαρτήματα και περιφερειακός εξοπλισμός (hardware) ηλεκτρονικού υπολογιστή	24,1
Διαμονή σε καταλύματα (ξενοδοχεία, δωμάτια, διαμερίσματα κλπ.)	23,3
Βιβλία (σε ηλεκτρονική ή μη μορφή), περιοδικά, εφημερίδες	20,5
Εισιτήρια για εκδηλώσεις (συναυλίες, θεατρικές παραστάσεις, κινηματογράφο κλπ.)	20,1
Λογισμικό για ηλεκτρονικό υπολογιστή (εξαιρουμένων computer games και video games) και αναβαθμίσεις αυτού	16,2
Οικιακά είδη (έπιπλα, παιχνίδια, είδη τέχνης, ηλεκτρικές οικιακές συσκευές κλπ.)	14,5
Άλλα (κοσμήματα, πληροφορίες από βάσεις δεδομένων κλπ.)	9,4
Ταινίες, μουσική (DVDs, CDs, βιντεοκασέτες κλπ.)	9,1
Παιχνίδια για ηλεκτρονικό υπολογιστή και παιχνιδιομηχανές και αναβαθμίσεις αυτών	5,8
Υλικό ηλεκτρονικής εκμάθησης	5,4
Υπηρεσίες τηλεπικοινωνιών (συνδρομές συνδρομητικής τηλεόρασης –Nona–, συνδρομές ευρυζωνικής σύνδεσης, λογαριασμοί κινητού ή σταθερού τηλεφώνου, καταβολή χρημάτων σε προπληρωμένη τηλεφωνική κάρτα κλπ.)	4,4
Είδη διατροφής – είδη παντοπωλείου	2,3
Φάρμακα	2,2
Μετοχές, οικονομικές υπηρεσίες, ασφάλειες (κάθε είδους)	1,9

4. Το διαδίκτυο, εκτός από ανεξάντλητη πηγή κάθε είδους πληροφόρησης, αποτελεί μέσο ψυχαγωγίας και ένα από τα πλέον δημοφιλή μέσα επικοινωνίας μεταξύ των νέων. Η πλοήγηση στις σελίδες του παγκόσμιου ιστού απαιτεί ιδιαίτερη προσοχή από τον χρήστη, διότι εγκυμονεί πολλαπλούς κινδύνους, τόσο για την ασφάλεια του υπολογιστή του όσο και



για την ασφάλεια των προσωπικών του δεδομένων. Η ασφάλεια στο διαδίκτυο έχει δύο μορφές, οι οποίες αποδίδονται με τους αγγλικούς όρους «security» και «safety», αντίστοιχα. Στη πρώτη περίπτωση έχουμε προστασία από κινδύνους, όπως είναι η προσβολή από ιούς, ενώ στη δεύτερη προστασία από ηλεκτρονικές απάτες και συναφή αδικήματα. Η ένταση του βαθμού ανησυχίας των χρηστών του διαδικτύου για κάθε έναν από τους πιθανούς κινδύνους απεικονίζονται στο Σχήμα 3. Σε ποσοστό 62% όσοι χρησιμοποιούν το διαδίκτυο ανησυχούν για την προσβολή από ιούς με αποτέλεσμα την απώλεια δεδομένων ή χρόνου αλλά και για τη λήψη ανεπιθύμητων e-mails (spams) 60,6%. Το χαμηλό ποσοστό (35,2%) ανησυχίας που καταγράφεται για την πρόσβαση των παιδιών σε ακατάλληλες ιστοσελίδες ή και την επικοινωνία με «εν δυνάμει» επικίνδυνα άτομα ύστερα από χρήση του διαδικτύου στην κατοικία αποδίδεται στο χαμηλό ποσοστό των νοικοκυριών της έρευνας, με μέλη παιδιά ηλικίας μικρότερης των 16 ετών, (27% επί του συνόλου των ερευνηθέντων νοικοκυριών). Ενδεικτικά, για την ηλικιακή ομάδα 35 – 54 ετών το ποσοστό ανησυχίας αγγίζει το 84,6%. Για την αντιμετώπιση των όποιων προβλημάτων 8 στους 10 χρήστες λαμβάνουν κάποιο ειδικό ηλεκτρονικό μέτρο όπως anti-virus or anti-spam or firewall. Ο γονικός έλεγχος ή το λογισμικό φίλτραρίσματος των ιστοσελίδων ως μέτρο προφύλαξης των παιδιών από ακατάλληλες ιστοσελίδες, χρησιμοποιούνται από το 6,7% των χρηστών. [11]



## ΚΕΦΑΛΑΙΟ 2<sup>ο</sup>: ΗΛΕΚΤΡΟΝΙΚΟ ΈΓΚΛΗΜΑ ΚΑΙ ΦΟΡΕΙΣ ΠΡΟΣΤΑΣΙΑΣ

### 2.1 ΕΙΣΑΓΩΓΗ

Οι ραγδαίες εξελίξεις του Διαδικτύου και άλλων συστημάτων πληροφοριών έχουν δημιουργήσει έναν εντελώς νέο οικονομικό τομέα και νέες ροές πληροφοριών, προϊόντων και υπηρεσιών οι οποίες διέρχονται διαμέσου των εσωτερικών και εξωτερικών συνόρων της Ευρωπαϊκής Ένωσης. Το γεγονός αυτό είχε βεβαίως πολυάριθμες θετικές συνέπειες για τους καταναλωτές και τους πολίτες. Εντούτοις, οι εξελίξεις αυτές έχουν επίσης ανοίξει πολλές νέες δυνατότητες για τους κακοποιούς. Είναι σαφώς ορατό το πρότυπο νέων αξιόποινων δραστηριοτήτων κατά του Διαδικτύου, ή μέσω της χρήσης συστημάτων πληροφοριών ως μέσου διάπραξης αδικημάτων.

Οι μορφές αυτών των αξιόποινων δραστηριοτήτων εξελίσσονται διαρκώς, πράγμα που καθιστά προφανώς δύσκολο για τη νομοθεσία και την επιχειρησιακή επιβολή του νόμου να ακολουθήσουν τον ίδιο ρυθμό. Ο εγγενής διασυνοριακός χαρακτήρας αυτού του νέου είδους αδικημάτων δημιουργεί επίσης την ανάγκη βελτίωσης της διασυνοριακής συνεργασίας στον τομέα της επιβολής του νόμου. Το έγκλημα στον κυβερνοχώρο πλήττει όλους τους τομείς της κοινωνίας εκ τούτου, η πολιτική για την αντιμετώπισή του θα είναι επίσης ορατή σχεδόν παντού. Δεδομένου του πολύ μεγάλου αριθμού πολιτών οι οποίοι χρησιμοποιούν ιδιωτικούς υπολογιστές, η πλειονότητα των πολιτών (ήδη υπό την ιδιότητά των δυνητικών θυμάτων) μπορεί επίσης να υπόκειται στις επιπτώσεις οποιασδήποτε πρωτοβουλίας στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

Εντούτοις, υπάρχουν επίσης σαφείς ενδείξεις σύμφωνα με τις οποίες έχουν αυξηθεί οι αξιόποινες δραστηριότητες που στρέφονται κατά συγκεκριμένων ομάδων θυμάτων. Ως εκ τούτου, μια αποτελεσματική πολιτική για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο θα μπορούσε να έχει σαφείς ευεργετικές συνέπειες για τις ομάδες αυτές.

Δεδομένης της εμβέλειας και του εύρους των απειλών για την ασφάλεια, η ανάγκη αντιμετώπισης των απειλών του εγκλήματος στον κυβερνοχώρο εξακολουθεί να υφίσταται και ενδέχεται να αυξηθεί. Τα ζητήματα ασφάλειας που συνδέονται με το έγκλημα στον κυβερνοχώρο έχουν παγκόσμια διάσταση και δεν μπορούν συνεπώς να αντιμετωπίζονται μόνο σε εθνικό επίπεδο. Η απειλή είναι διεθνής και το ίδιο διεθνής πρέπει να είναι ένα μέρος τουλάχιστον της απάντησης. Είναι αναμφισβήτητο ότι η καταπολέμηση του εγκλήματος στον κυβερνοχώρο θα εξακολουθήσει να είναι πιο σημαντική και αποτελεσματική σε εθνικό επίπεδο, υπάρχει όμως σαφής ανάγκη διασύνδεσης και ενδεχομένως συμπλήρωσης των εθνικών προσπαθειών στο ευρωπαϊκό επίπεδο.

### Το Ηλεκτρονικό Έγκλημα

Στο παρελθόν, έχουν γίνει πολλές προσπάθειες να ορισθεί το **ηλεκτρονικό έγκλημα**. Ένας παλαιότερος ορισμός προσδιορίζει το ηλεκτρονικό έγκλημα ως «*μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της*». Ωστόσο, το ηλεκτρονικό έγκλημα δεν είναι κάτι τόσο απλό, ούτε μπορούμε να το γενικεύσουμε. Υιοθετώντας μια πιο γενική προσέγγιση που τείνει να επικρατήσει σήμερα, μπορούμε να θεωρήσουμε το ηλεκτρονικό έγκλημα ως:

- μια νέα μορφή εγκλήματος, που διαπράττεται με τη χρήση της τεχνολογίας των υπολογιστών
- μια παραλλαγή των ήδη υπαρχόντων εγκλημάτων, τα οποία διαπράττονται με υπολογιστές
- μια εγκληματική πράξη στην εκδήλωση της οποίας συμμετέχουν καθ' οποιονδήποτε τρόπο τεχνολογίες πληροφορικής.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crimes) αποτελεί τον ίδιο τύπο εγκλήματος με το «κοινό» ή «συμβατικό έγκλημα» και η μόνη διαφορά που το διακρίνει από αυτό είναι ότι διαπράττεται σε διαφορετικό περιβάλλον (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον



ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μία άλλη δε κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου.

Στην αγγλική γλώσσα οι όροι που χρησιμοποιούνται για να περιγράψουν το ηλεκτρονικό έγκλημα ποικίλουν: *e-crime*, *cybercrime*, *computer-crime*, *internet related crime* και *hitech-crime* είναι οι συχνότερα χρησιμοποιούμενοι. Οι διαφορές των ανωτέρω όρων είναι ελάχιστες. Μπορούμε να θεωρήσουμε τους όρους *computer crime*, *e-crime*, *hitech-crime* ως γενικότερους και τους όρους *cybercrime* και *internet related crime* ως ειδικότερους, καθότι στην δεύτερη περίπτωση περιλαμβάνεται υποχρεωτικά και το στοιχείο του Διαδικτύου.

Αντιστοίχως, στην ελληνική γλώσσα οι όροι που χρησιμοποιούνται είναι *ηλεκτρονικό έγκλημα*, *δικτυακό έγκλημα* και *έγκλημα του κυβερνοχώρου*. Το στοιχείο της δικτύωσης περιλαμβάνεται στους δύο τελευταίους όρους. Βασικό συστατικό στοιχείο του ηλεκτρονικού εγκλήματος, αποτελεί η ύπαρξη μιας συσκευής ηλεκτρονικής επεξεργασίας δεδομένων, όπως ηλεκτρονικός υπολογιστής, κινητό τηλέφωνο, palmtop, notepad κλπ. Κυρίαρχο ρόλο διαδραματίζει ο υπολογιστής, ο οποίος μπορεί :

- Να αποτελεί τον στόχο κάποιας επίθεσης όπου σε αυτήν την περίπτωση αυτή μπορούμε να πούμε ότι ο υπολογιστής είναι το «θύμα» της επίθεσης
- Να αποτελεί το μέσο διάπραξης κάποιας επίθεσης, δηλαδή το εργαλείο που χρησιμοποιεί ο επιτιθέμενος για να πραγματοποιήσει τον εγκληματικό σκοπό του (π.χ. εισβάλλοντας σε κάποιο άλλο υπολογιστή)
- Να αποτελεί ένα βοηθητικό μέσο για τη διάπραξη του εγκλήματος, π.χ. να αποθηκεύονται σε αυτόν στοιχεία ή πληροφορίες που αφορούν άτομα τα οποία συμμετέχουν σε παράνομες δραστηριότητες.

Υπό το πρίσμα της Νομικής επιστήμης, ο όρος Ηλεκτρονικό έγκλημα ή Ηλεκτρονική εγκληματικότητα αποτελεί μια ευρεία έννοια στην οποία εμπίπτουν όλες εκείνες οι αξιόποινες πράξεις που τελούνται με τη χρήση ενός συστήματος ηλεκτρονικής επεξεργασίας δεδομένων. [12]



Ο όρος αυτός διακρίνεται σε στενή και σε ευρεία έννοια. Η μεν στενή έννοια, ηλεκτρονική εγκληματικότητα, αναφέρεται στις αξιόποινες πράξεις όπως είναι η ηλεκτρονική απάτη, η χωρίς άδεια απόκτηση δεδομένων, η παραποίηση δεδομένων και η δολιοφθορά δηλαδή εγκλήματα όπου ο ηλεκτρονικός υπολογιστής αποτελεί κύριο μέσο τέλεσης των εγκλημάτων. Αντίθετα με την ευρεία έννοια η εγκληματικότητα μέσω τεχνολογίας πληροφορικής περιλαμβάνει όλα εκείνα τα αδικήματα για την τέλεση των οποίων ο ηλεκτρονικός υπολογιστής ή παρόμοιος εξοπλισμός χρησιμοποιείται ως βοηθητικό μέσο.

Άξιο αναφοράς αποτελούν εν τάχει οι μορφές του ηλεκτρονικού εγκλήματος υπό γενικότερη οπτική γωνία:

- 1) Απάτη απλή - συμπεριλαμβάνει όλες εκείνες τις απάτες που πραγματοποιούνται και εκτός του κυβερνοχώρου
- 2) Τηλεπικοινωνιακή απάτη
- 3) Κυβερνο-σφετερισμός (cybersquatting) – Πρόκειται για ένα φαινόμενο του Internet, όπου διάφοροι επιτήδριοι, τον πρώτο καιρό που το Διαδίκτυο είχε αρχίσει να γίνεται δημοφιλές για εμπορική χρήση, έσπευσαν να κατοχυρώσουν σ' αυτό εμπορικά σήματα εταιρειών (επωνυμίες ή και διακριτικούς τίτλους), αποκτώντας το αντίστοιχο όνομα χώρου (domain name), με απώτερο στόχο να τα πωλήσουν (μεταβιβάσουν) στους νόμιμους ιδιοκτήτες τους όταν αυτοί θελήσουν αργότερα να δραστηριοποιηθούν στο Internet.
- 4) Προσβολή της προσωπικότητας- δυσφήμιση
- 5) Πορνογραφία, προσβολή της δημοσίας αιδούς, προστασία ανηλικών
- 6) Προσβολή των δικαιωμάτων πνευματικής ιδιοκτησίας
- 7) Παράνομη πρόσβαση σε δεδομένα (hacking, cracking)
- 8) Αλλοίωση ή διαγραφή δεδομένων με ιούς
- 9) Παράνομη επεξεργασία προσωπικών δεδομένων
- 10) Η αποστολή πολυάριθμων e-mails με διαφημιστικό περιεχόμενο (Spamming)

## 2.2 ΗΛΕΚΤΡΟΝΙΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ

Η απαρχή του ηλεκτρονικού εγκλήματος θα μπορούσε να ταυτιστεί και με την εμφάνιση των ηλεκτρονικών υπολογιστών καθώς από τότε υπήρξαν οι πρώτες προσπάθειες επίδοξων εγκληματιών ώστε να βρουν και να εκμεταλλευτούν τις νέες τεχνολογίες εις βάρος των καταναλωτών. Καθίσταται προφανές πως σε αυτό το πρώιμο στάδιο, το ηλεκτρονικό έγκλημα ήταν σπάνιο καθώς και ο απόλυτος αριθμός αλλά και η χρήση των ηλεκτρονικών υπολογιστών βρίσκονταν σε ακόμη χαμηλά επίπεδα. Οι υπολογιστές τότε αποτελούσαν προϊόν πολυτελείας. Με το πέρασμα του χρόνου το μεγαλύτερο ποσοστό των πολιτών στις ανεπτυγμένες χώρες έχει πρόσβαση σε ηλεκτρονικό υπολογιστή. Ουσιαστικά, η μεγαλύτερη ανάπτυξη του ηλεκτρονικού εγκλήματος, με την σημερινή έννοια, συντελείται με την εμφάνιση των δικτύων που δημιουργούν νέες διόδους πρόσβασης προς την πληροφορία. Είναι σαφές πως η ραγδαία ανάπτυξη της τεχνολογίας έχει δώσει το έδαφος για νέες ευκαιρίες στην ανάπτυξη της ηλεκτρονικής εγκληματικότητας με γεωμετρική πρόοδο. Αρχικά θα πρέπει να επισημανθούν οι ορισμοί της Εγκληματολογικής επιστήμης γενικότερα αλλά και της ηλεκτρονικής ειδικότερα. [12]

**Η Εγκληματολογική Επιστήμη** (Forensic Science), ασχολείται με την ανακάλυψη, ανάλυση και νομική τεκμηρίωση των αποδείξεων, που συνδέουν μια αξιόποινη πράξη με ένα πρόσωπο, ή γενικότερα πρόσωπα και αποδεικτικά στοιχεία. Η ανάλυση του DNA και η εξέταση των δακτυλικών αποτυπωμάτων είναι μερικές από τις δυνατότητες της επιστήμης αυτής.

**Η Ηλεκτρονική Εγκληματολογία** (Computer Forensic Science), είναι «η επιστήμη που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων κατά τρόπο νομικά αποδεκτό». Όλο και πιο συχνά, οι αποδείξεις μιας αξιόποινης πράξης είναι κρυμμένες σε έναν υπολογιστή. Είναι αρκετά δύσκολο, όχι μόνο να εντοπίσουμε τις αποδείξεις, αλλά και να τις συγκεντρώσουμε με τέτοιο τρόπο ώστε να είναι αποδεκτές στο δικαστήριο. Οι δικαστικές αρχές πρέπει να αποδείξουν, ότι τα στοιχεία που συλλέχθηκαν από τη σκηνή διάπραξης του εγκλήματος, διατηρήθηκαν αναλλοίωτα και τεκμηριώνουν την ενοχή του κατηγορουμένου. Παράλληλα, θα πρέπει να βεβαιώσουν ότι δεν έγινε κάποια παράλειψη που κατέστρεψε αποδείξεις σχετικές με την αθωότητα του κατηγορουμένου.

Πατέρας της εγκληματολογικής επιστήμης θεωρείται ο Αρχιμήδης (287-212 π.Χ.). Μετά τον Αρχιμήδη, η πρώτη γνωστή εφαρμογή της εγκληματολογικής επιστήμης πραγματοποιήθηκε από έναν Άραβα μηχανικό, τον 7ο αιώνα, ο οποίος χρησιμοποιούσε τα δαχτυλικά αποτυπώματα για να αποδείξει την ταυτοπροσωπία δανειστών και δανειοληπτών. Το ίδιο αιώνα, τα δαχτυλικά αποτυπώματα χρησιμοποιήθηκαν και από τους Κινέζους. Συστηματική εφαρμογή της εγκληματολογικής επιστήμης στον ευρωπαϊκό χώρο παρατηρείται αρχικά τον 16ο αιώνα, όταν η ιατρική επιστήμη άρχισε να χρησιμοποιεί τις γνώσεις της για τον προσδιορισμό της αιτίας θανάτου, σε περιπτώσεις ανθρωποκτονιών. Από τον 18ο αιώνα και άλλες επιστήμες, όπως η φυσική και χημεία, άρχισαν να χρησιμοποιούνται στην διερεύνηση των εγκλημάτων. Στους αιώνες που ακολούθησαν η εγκληματολογική επιστήμη εδραιώθηκε στον τομέα της διερεύνησης του εγκλήματος. Σήμερα η έρευνα του συνόλου των εγκλημάτων, στηρίζεται κατά μεγάλο ποσοστό στην εγκληματολογική επιστήμη.

Περνώντας ειδικότερα στο στάδιο του ηλεκτρονικού εγκλήματος, μια πρώτη αναφορά παγκοσμίως έγινε τον 18<sup>ο</sup> αιώνα μΧ. και συγκεκριμένα το 1820, στην Γαλλία. Εκείνη την εποχή ο Γάλλος ύφαντουργός Joseph-Marie Jacquard, ο οποίος ήταν πρωτοπόρος τον τομέα του, κατασκεύασε έναν συγκεκριμένο τύπο αργαλειού με μεγαλύτερες αποδόσεις και στόχους για μαζικότερη παραγωγή. Επί της ουσίας η μηχανή αυτή επέτρεπε την επανάληψη μιας σειράς όμοιων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό καθώς κι η διορατικότητα των υπαλλήλων του, δημιούργησε έντονη ανησυχία. Έτσι, επειδή φοβήθηκαν πως απειλείται η παραδοσιακή τους εργασία, προκαλούσαν συχνά δολιοφθορές στο μηχάνημα ώστε εν τέλει να επιτύχουν την αποθάρρυνση του Joseph-Marie Jacquard, να χρησιμοποιήσει αυτή την νέα τεχνολογία.

### 2.3 ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ ΚΑΤΑΝΑΛΩΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι διάφορες μορφές ηλεκτρονικού εγκλήματος, κατηγοριοποιούνται σε δύο (2) μεγάλες κατηγορίες. Στην πρώτη εντάσσονται τα λεγόμενα «γνήσια» ηλεκτρονικά εγκλήματα, των οποίων η εμφάνιση συμπίπτει με αυτή των υπολογιστών και του



διαδικτύου. Η δεύτερη κατηγορία είναι τα παραδοσιακού τύπου εγκλήματα που προϋπήρχαν των υπολογιστών όμως μέσω της ανάπτυξης του διαδικτύου αναπτύχθηκε η εφαρμογή τους και σε άλλα τμήματα της οικονομίας.

Κάθε τύπος των παρακάτω εγκλημάτων που θα αναλυθούν μπορούν να εφαρμοστούν από τις ηλεκτρονικές επιχειρήσεις προς τους καταναλωτές, άλλοτε περισσότερο άλλοτε λιγότερο. Αυτό συμβαίνει με τα γνήσια ηλεκτρονικά εγκλήματα. Τα συμβατικά όμως εγκλήματα που τελούνται και χωρίς την χρήση του υπολογιστή, δεν μπορούν να εφαρμοστούν από τα ηλεκτρονικά καταστήματα εις βάρος των καταναλωτών. Για λόγους πληρότητας θα αναφερθούν απλώς παρακάτω:

1. Διαδικτυακή Τρομοκρατία
2. Πειρατεία Λογισμικού
3. Παιδική Πορνογραφία
4. Ξέπλυμα Χρήματος.

Τα κυριότερα και πιο διαδεδομένα εγκλήματα που περιλαμβάνονται στην κατηγορία των γνήσιων ηλεκτρονικών εγκλημάτων είναι τα εξής:

1. Κακόβουλες εισβολές σε δίκτυα (hacking , cracking)
2. Ανεπιθύμητη Αλληλογραφία (spamming)
3. Διασπορά κακόβουλου λογισμικού ( viruses, Trojan horses)
4. Spyware – Adware - Malware
5. Πειρατεία ονομάτων χώρου (domain names privacy)
6. Ηλεκτρονικό Ψάρεμα (phising – pharming)
7. Απάτη με την Νιγηριανή Επιστολή
8. Επιθέσεις Άρνησης Εξυπηρέτησης

## Hacking

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση και η χωρίς δικαίωμα διείσδυση σε συστήματα ηλεκτρονικού υπολογιστή, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά ή η καταστροφή κι αποκόμιση οικονομικού οφέλους, αλλά η ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση ικανότητας του να εισβάλει κανείς σε ένα υπολογιστικό σύστημα. Η έννοια του hacking είναι ευρεία και μπορεί να πραγματοποιείται με ειδικά εργαλεία λογισμικού ή προγράμματα που απαιτούν διαφορετικές ικανότητες και να μπορούν να οριστούν ως παράνομες και εγκληματικές. Η εισβολή στο εσωτερικό δίκτυο μιας επιχείρησης ή οργανισμού ακόμα κι αν δεν είναι κακόβουλη, μπορεί να αναφερθεί πως ενέχει κακόβουλο χαρακτήρα. Αυτό γιατί ο επιτιθέμενος εισχωρώντας στο σύστημα της εκάστοτε επιχείρησης, ηλεκτρονικού καταστήματος κλπ, αποκτά γνώσεις για την ασφάλειά του κι έτσι έχει την δυνατότητα στο να διαπράξει μελλοντικά ένα ηλεκτρονικό έγκλημα.

Ο καλύτερος τρόπος πρόκλησης ζημιάς σε μια ιστοσελίδα είναι αναμφισβήτητα το hacking. Ένας επιτιθέμενος hacker μπορεί να εισέλθει σε ένα σύστημα ως «υπερχρήστης» και να προκαλέσει ζημιά, παραβιάζοντας το απόρρητο της ηλεκτρονικής αλληλογραφίας, μπλοκάροντας τις υπηρεσίες του συστήματος ή υποκλέπτοντας ή καταστρέφοντας πολύτιμα αρχεία και δεδομένα της επιχείρησης. Αναλύοντας λοιπόν το ηλεκτρονικό έγκλημα του hacking , ο καταναλωτής έχει τα ίδια ποσοστά να πέσει θύμα όσο και μια ηλεκτρονική επιχείρηση. Η διαφοροποίηση έγκειται πως η ιστοσελίδα της επιχείρησης λειτουργεί ως «Δούρειος Ίππος» για να μπορεί να εισέλθει ο hacker στα στοιχεία του καταναλωτή. Συνεπώς η επιχείρηση ή το ηλεκτρονικό κατάστημα συμβάλει στην εξαπάτηση του καταναλωτή της, χωρίς να το επιδιώκει.

## Cracking

Το **Cracking** αποτελεί παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα, την αλλαγή των σχετικών κωδικών πρόσβασης, και άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. Σε αντίθεση με το hacking, εδώ βασικός σκοπός είναι, μέσω της μη εξουσιοδοτημένης πρόσβασης στο σύστημα, να υποκλέψει πληθώρα πληροφοριών και να προκαλέσει οικονομικές και

κάθε είδους ζημιές. Ίσως το γνωστότερο παράδειγμα κακόβουλης επίθεσης μέσω cracking είναι η υποκλοπή κωδικού πιστωτικής κάρτας και τον οποίο ο επιτήδειος τον χρησιμοποιεί προς όφελός του.

Σε αυτό ακριβώς το σημείο είναι όπου μπορεί αυτή καθεαυτή η ηλεκτρονική επιχείρηση να εξαπατήσει τον καταναλωτή. Για παράδειγμα σε μια δεδομένη φόρμα αγοράς, ζητούνται προσωπικά στοιχεία όπως είναι κι ο αριθμός πιστωτικής κάρτας, προκειμένου να ολοκληρωθεί η οικονομική συναλλαγή. Καθώς ο καταναλωτής συμπληρώνει τα στοιχεία του, αυτά δεν εμφανίζονται στην οθόνη του αλλά ούτε και στο σύστημα του ιδιοκτήτη της ιστοσελίδας. Σε περίπτωση όμως που η επιχείρηση λειτουργεί ως cracker τότε έχει δώσει το πρώτο βήμα για να μπορέσει να υποκλέψει τα στοιχεία του καταναλωτή της. Μετά από την ολοκλήρωση της αγοράς από τον καταναλωτή, ο επιτήδειος αφήνει ένα χρονικό περιθώριο ώστε να μην φανεί η αγορά από το κατάστημά του ως ύποπτη, και σε οποιονδήποτε άλλο χρόνο, χρησιμοποιεί τα στοιχεία της πιστωτικής κάρτας που υπέκλεψε για δικό του όφελος. Φυσικά, όπως και πριν, μπορεί να γίνει κλοπή προσωπικών στοιχείων αλλά ο θύτης να μην έχει ουδεμία σχέση με το ηλεκτρονικό κατάστημα που έκανε την αγορά του ο καταναλωτής.

#### Ανεπιθύμητη Αλληλογραφία (SPAMMING)

**Η ανεπιθύμητη αλληλογραφία ή spamming** αποτελεί τη μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι αυτό ο όρος είναι δόκιμος για αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για τον παραλήπτη που εν προκειμένω είναι ένας καταναλωτής.

Η δυνατότητα που προσφέρει το διαδίκτυο για φθηνή κι άμεση αποστολή εκατομμυρίων μηνυμάτων, ωθεί τις ανά τον κόσμο εταιρείες (ειδικά τα ηλεκτρονικά καταστήματα) στην επιλογή τέτοιων μεθόδων για την προώθηση των προϊόντων τους. Η διαδικασία συλλογής των ηλεκτρονικών διευθύνσεων πραγματοποιείται με διάφορους τρόπους όπως :



1. Με χρήση ειδικού λογισμικού παράγει τεράστιες λίστες με τυχαίες διευθύνσεις
2. Από καταλόγους μεγάλων εταιρειών παροχής ίντερνετ (ISP)
3. Από εταιρείες που χρησιμοποιούν λογισμικό harvester το οποίο σαρώνοντας το διαδικτυο συλλέγει διευθύνσεις από καταλόγους με newsgroup που έχουν ήδη εγγραφεί τα θύματα της ανεπιθύμητης αλληλογραφίας
4. Από καταλόγους εταιρειών που διαθέτουν ηλεκτρονικό κατάστημα

Καθίσταται σαφές λοιπόν πως το σύνολο των ηλεκτρονικών επιχειρήσεων είναι δυνατόν να χρησιμοποιήσουν αυτού του είδους την ηλεκτρονική απάτη προς δικό τους όφελος. Θεωρώντας πως η μαζική αποστολή μηνυμάτων αποτελεί συνετή κι αποτελεσματική τακτική e- marketing, οι εταιρίες γεμίζουν το διαδικτυο με τέτοιου είδους διαφημιστικό υλικό. Με την ταυτόχρονη χρήση άλλων κακόβουλων λογισμικών όπως είναι τα malware – adware, που θα αναλυθούν παρακάτω, μια εταιρία ή ένας ιδιώτης μπορεί να υποκλέψει από τους πελάτες της τα στοιχεία επαφών του στο ηλεκτρονικό του ταχυδρομείο αποκτώντας έτσι μια αρκετά μεγάλη βάση δεδομένων που σίγουρα αξιοποιείται για εμπορικούς και οικονομικούς σκοπούς. Παρόλο που δεν προκαλεί φθορά στον υπολογιστή του πελάτη της, η διαδικασία αυτή αποτελεί απάτη από την επιχείρηση προς τον επικείμενο πελάτη της. Spam μηνύματα, σύμφωνα με την Οδηγία 2002/58/EC του Ευρωπαϊκού Κοινοβουλίου, δεν είναι αυτά που προέρχονται από επώνυμο αποστολέα ή αυτά που δίνουν τη δυνατότητα διαγραφής του παραλήπτη από τη λίστα αποδεκτών.

### Ιοί (VIRUSES)

Ο **ιός** είναι ένας βλαβερός εκτελέσιμος κώδικας, ο οποίος επιζεί με το να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο κατ' αντιστοιχία με τους βιολογικούς ιούς. Έχουν παρασιτική συμπεριφορά καθώς επιζούν μολύνοντας άλλα αρχεία, ακολουθώντας έτσι πιστά την ανάλογη συμπεριφορά των οργανικών ιών. Ο ιός έχει την δυνατότητα να αναπαράγει τον εαυτό του και να τον μεταφέρει σε άλλους υπολογιστές μέσω των αρχείων. Σκοπός ενός ιού είναι η καταστροφή, ανεξαρτήτως μεγέθους, αρχείων ή σε λογισμικού προγράμματος. Συνηθέστερος τρόπος μετάδοσης είναι η διανομή μέσω ηλεκτρονικού ταχυδρομείου.

### Δούρειο Ίπποι (Trojan Horses)

Ένας δούρειος ίππος είναι ειδική μορφή ιού και δρα σε συνδυασμό με ένα κεντρικό υπολογιστή, ο οποίος μεταφέρει τον βασικό κώδικα του κακόβουλου λογισμικού. Οι δούρειοι ίπποι είναι προγράμματα κρυμμένα μέσα σε άλλα χρήσιμα προγράμματα (ονομάζονται ξενιστές) και στις κατάλληλες συνθήκες εκτελούν μια εκ πρώτης όψεως αφανή λειτουργία που όμως μπορεί να έχει καταστροφικές συνέπειες για τον υπολογιστή του καταναλωτή. Συνήθως μέσω αυτής της ηλεκτρονικής απάτης, επιδιώκονται καταστροφικοί σκοποί όπως η διαγραφή αρχείων από σκληρό δίσκο. Γενικότερα όμως, μέσω ενός Trojan horse, επιτρέπεται στον επιτιθέμενο να αποκτήσει δικαιώματα προσπέλασης στο σύστημα μιας επιχείρησης ή ενός ηλεκτρονικού καταστήματος, παρακάμπτοντας τις συνήθεις διαδικασίες ελέγχου προσπέλασης. Αν λοιπόν cracking, όπως αναφέρθηκε παραπάνω, είναι το σύνολο της διαδικασίας που έχει κακόβουλη πρόθεση, ένα από τα εργαλεία της αποτελεί ο «Δούρειος Ίππος».

### Spyware – Adware – Malware

**Spyware** είναι ένα πρόγραμμα που χρησιμοποιείται για να παρακολουθεί τις δραστηριότητες του προσβεβλημένου υπολογιστή. Ένας υπολογιστής που έχει προσληφθεί από spyware, παρακολουθείται με σκοπό να υποκλέπτονται στοιχεία τα οποία πληκτρολογούνται, όπως για παράδειγμα κωδικοί χρήσης ή passwords.

**Adware** είναι τα προγράμματα ηλεκτρονικής απάτης που αναδύουν παράθυρα διαφημίσεων με κακόβουλο τρόπο, χωρίς ο καταναλωτής να έχει επιβεβαιώσει τα στοιχεία του για την παρουσίαση τέτοιου υλικού. Χρησιμοποιούν την ταχύτητα του διαδικτύου από το οικιακό δίκτυο του θύματος ώστε να χαμηλώσουν την ταχύτητά του, στέλνοντας συνεχώς διαφημιστικά μηνύματα. Ταυτόχρονα αυτού του είδους το κακόβουλο προϊόν είναι σε θέση να συλλέγει πληροφορίες από την επισκεψιμότητα του καταναλωτή στις διάφορες ιστοσελίδες δημιουργώντας έτσι το καταναλωτικό του προφίλ. Έπειτα αυτό το σύνολο πληροφοριών επεξεργάζεται κι έτσι οι αναδυόμενες διαφημίσεις δεν είναι από τυχαία προϊόντα αλλά στοχευμένο marketing σε προϊόντα που έχει αναζητήσει παλαιότερα ο καταναλωτής. Η διεργασία αυτή της ηλεκτρονικής απάτης δημιουργεί τεράστιες βάσεις δεδομένων οι οποίες είναι και επεξεργάσιμες αλλά κι εμπορεύσιμες από και προς διάφορες ηλεκτρονικές και μη επιχειρήσεις.

Ο όρος **Malware** αναφέρεται σε όλα μαζί τα παραπάνω προγράμματα που αναφέρθηκαν. Είτε μπορεί να καταστρέψουν τον υπολογιστή του θύματος, είτε να κατασκοπεύσουν τις δραστηριότητές του, είτε να ενοχλήσουν μέσω διαφημιστικών μηνυμάτων, είτε τελικώς να προκαλέσουν την οποιαδήποτε άλλη κακόβουλη ενέργεια στο σύστημα του υπολογιστή του.

Τα υπόλοιπα ηλεκτρονικά εγκλήματα που αναφέρθηκαν στην αρχή αυτής της ενότητας (Πειρατεία ονομάτων χώρου, Ηλεκτρονικό Ψάρεμα, Απάτη με την Νιγηριανή Επιστολή, Επιθέσεις Άρνησης Εξυπηρέτησης) παρόλο που αποτελούν κακόβουλες ενέργειες, δεν μπορούν να συνδυαστούν άμεσα με τις ηλεκτρονικές επιχειρήσεις, ούτε αυτές μπορούν να τις χρησιμοποιήσουν εις βάρος των πελατών τους.

## 2.4 ΠΕΡΙΠΤΩΣΕΙΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΠΑΤΗΣ

Στην ενότητα αυτή θα παρατεθούν κάποια χαρακτηριστικά παραδείγματα περιπτώσεων ηλεκτρονικής απάτης τόσο σε παγκόσμιο όσο και σε εθνικό επίπεδο.

Με βάση τα στοιχεία της Υποδιεύθυνσης Ηλεκτρονικού Εγκλήματος [13] στο 8ο βαλκανικό security forum επισημαίνεται ότι η εντύπωση ότι τα άτομα υψηλού μορφωτικού επιπέδου δεν αποτελούν θύματα ηλεκτρονικής απάτης καταρρίπτεται, καθώς τέτοιο άτομο έδωσε 6.000 ευρώ για υπόθεση που αποτελεί το παλαιότερο παράδειγμα ηλεκτρονικής απάτης, όπου ζητείται προκαταβολή για τα έξοδα έναντι υπόσχεσης για απολαβές εκατομμυρίων. Τρία ακόμη άτομα επείσθησαν ηλεκτρονικά να καταβάλουν προκαταβολή 5.000 ευρώ έναντι της αγοράς αυτοκινήτου, το οποίο δεν παρέλαβαν ποτέ, ενώ επιχειρηματίας από θεσσαλική πόλη διαπίστωσε ότι είχε αναρτηθεί “ροζ” αγγελία με το τηλέφονό της. Εικάζεται ότι η ενέργεια θα πρέπει να αποδοθεί σε επαγγελματικό ανταγωνιστή της. Σε μία άλλη περίπτωση, σύζυγος έλαβε φωτογραφία της συζύγου του σε ερωτικές στιγμές, η οποία όμως αποδείχθηκε φωτομοντάζ. [13]

Επίσης, σε έναν άλλον φορέα όπως είναι το Safeline, που ο ρόλος του θα αναλυθεί παρακάτω, ο αριθμός των καταγγελιών που έλαβε το 2010, έφτασε τις 4204



(αύξηση 136.44% σε σχέση με το 2009). Οι αιτίες της γοργής αύξησης στον αριθμό των καταγγελιών, που παρατηρείται από το 2008, είναι δύσκολο να προσδιοριστούν, σίγουρα όμως περιλαμβάνουν την αύξηση του αριθμού των χρηστών του Ίντερνετ και την βελτίωση της συνειδητοποίησής τους. [14]

Εκτός των κλασικών περιπτώσεων ηλεκτρονικής απάτης που αναφέρθηκαν σε προηγούμενη ενότητα, οι καταναλωτές μπορούν να υποπέσουν και σε άλλων μορφών απάτες από τα ηλεκτρονικά καταστήματα, που αυτές κιάλας είναι οι συνηθέστερες. Αναφέρονται ενδεικτικά οι εξής:

1. Μη έγκυρος τρόπος επιβεβαίωσης της εγκυρότητας της ιστοσελίδας του ηλεκτρονικού καταστήματος
2. Περίπτωση υποκλοπής στοιχείων πιστωτικής κάρτας την ώρα καταχώρισης
3. Μη διαφύλαξη προσωπικών δεδομένων από κάθε χρήση
4. Παραλαβή διαφορετικού προϊόντος από αυτό που απεικονιζόταν ή από αυτό που περιείχε η παραγγελία του καταναλωτή
5. Παραλαβή ελαττωματικού προϊόντος
6. Καθυστερήση παράδοσης της παραγγελίας
7. Μη απάντηση έγκυρης παραγγελίας από το ηλεκτρονικό κατάστημα προς τον καταναλωτή, με την δημιουργία φόβου η παραγγελία να μην παραδοθεί
8. Μη ακύρωση παραγγελίας από πλευράς καταναλωτή με ενδεχόμενο να πληρώσει κάτι που τελικά δεν χρειαζόταν
9. Χρέωση διαφορετικού ποσού στην πιστωτική κάρτα του καταναλωτή, απ αυτό που χρειαζόταν για την παραλαβή του προϊόντος
10. Κρυφές χρεώσεις για την αποστολή του προϊόντος, για την απόδοση του Φ.Π.Α. και διαφοροποίηση τιμής λίγο πριν την ολοκλήρωση της παραγγελίας με κάθε είδους δικαιολογία

Όλα τα παραπάνω έχουν συναντηθεί αρκετές φορές τόσο στην παγκόσμια όσο και στην εγχώρια οικονομία. Τα παραδείγματα ποικίλα αλλά ελάχιστα, συναρτήσει των περιπτώσεων που δημιουργούνται καθημερινώς, έχουν αναρτηθεί δημοσίως στο διαδίκτυο προκειμένου να ενημερωθούν διεξοδικά οι καταναλωτές ώστε να αναπτύξουν δικλίδες ασφαλείας ως προς τα ηλεκτρονικά καταστήματα. Στην συνέχεια της παρούσας εργασίας, θα παρατεθούν περιπτώσεις αυτού του είδους της απάτης και πως τελικά αντέδρασαν οι αρμόδιοι φορείς.

### Περίπτωση στο Ηλεκτρονικό Κατάστημα E – BAY

Οι ηλεκτρονικές δημοπρασίες έχουν τους κινδύνους τους, όπως ισχύει φυσικά και για τις δημοπρασίες σε πραγματικό χρόνο. Αυτό το συνειδητοποίησε με οδυνηρό τρόπο ένας Αυστριακός, ο οποίος αγόρασε μέσω του eBay χρυσό, που ποτέ δεν του εστάλη. Το αποτέλεσμα ήταν αυστριακό δικαστήριο να επιβάλει πρόστιμο 16.463 ευρώ στην αμερικανική ιστοσελίδα, γιατί δεν προστάτησε τον πελάτη της. Είναι η πρώτη δικαστική απόφαση στον κόσμο με τέτοιο αντικείμενο, που πλήττει το eBay. Ο εξαπατηθείς Αυστριακός αγόρασε ένα κιλό χρυσού από τη γερμανική εταιρία ML Agentur το Σεπτέμβριο του 2007, μέσω του eBay, όμως ποτέ δεν παρέλαβε τις ράβδους χρυσού μετά την πληρωμή τους. Η ML Agentur, που έχει προϊστορία με απάτες και διαθέτει σχετικό φάκελο στη γερμανική αστυνομία, έχει έκτοτε χρεοκοπήσει και ο πελάτης δεν μπορεί να διεκδικήσει πίσω τα χρήματά του. Το eBay διαφήμιζε τη γερμανική εταιρία ως ιδιαίτερα «αξιόπιστο πωλητή», σύμφωνα με τα κριτήρια της επιχείρησης online δημοπρασιών, παρόλο που είχε δεχτεί και στο παρελθόν παράπονα αγοραστών, ιδίως για καθυστερήσεις στην παραλαβή των εμπορευμάτων που είχαν αγοράσει από την ML Agentur. Το αυστριακό δικαστήριο επέβαλε το πρόστιμο κρίνοντας ότι το site των δημοπρασιών γνώριζε την προϊστορία της γερμανικής εταιρίας, πριν γίνει η συναλλαγή με τον χρυσό, και παραμέλησε να προστατεύσει τον ανυποψίαστο αγοραστή. Η ML Agentur, πριν κλείσει, είχε παρουσιάσει μηνιαίες πωλήσεις άνω των 400.000 ευρώ το 2007 και το eBay είχε εισπράξει ένα ποσοστό από αυτά τα έσοδα. Οι επικριτές του eBay κατέκριναν την ιστοσελίδα ότι έχει χαλαρή πολιτική προστασίας των αγοραστών, επειδή παίρνει ποσοστά από τους πωλητές. [13]

Όπως εύλογα μπορεί να παρατηρηθεί από το παραπάνω συμβάν, περισσότερες από μία απάτες που πραγματοποιήθηκαν μέσα σε μία μόνο καταγγελία. Συνεπώς ο

καταναλωτής δεν πρέπει να εφησυχάζεται, πρέπει να είναι συνεχώς υποψιασμένος και να γνωρίζει την ορθή διαδικασία παραγγελίας μέσω διαδικτύου.

### Περίπτωση σε Τράπεζες – Ν.Π.Δ.Δ. – Δ.Ε.Κ.Ο.

Τα συστήματα των τραπεζών δέχονται καθημερινά επιθέσεις, οι οποίες στην Ελλάδα είναι αυξημένες κατά 20% και στο εξωτερικό σχεδόν 100%, σε σύγκριση με τα επίπεδα πριν από την κρίση. Κάθε χρόνο στην Ελλάδα πέφτουν θύματα ηλεκτρονικής απάτης περίπου 2.500 καταναλωτές με κόστος 4 εκατ. ευρώ. Κατά το τρέχον έτος 2011 τα θύματα αναμένεται να ξεπεράσουν τα 3.000 ευρώ και το κόστος να αγγίξει τα 5 δισ. ευρώ. Η έξαρση του φαινομένου άρχισε να παρατηρείται από το πρώτο εξάμηνο του 2008, όταν έπεσαν θύματα απάτης με πιστωτικές κάρτες 700 Έλληνες, έναντι 135 το αντίστοιχο εξάμηνο του 2007. Τραπεζικά στελέχη που ασχολούνται με την ασφάλεια των συστημάτων επισημαίνουν ότι τον τελευταίο χρόνο έχουν αυξηθεί όλα τα είδη απάτης, που ξεκινούν από την κλοπή στοιχείων πιστωτικών καρτών και φτάνουν μέχρι τις ληστείες και την εξαπάτηση πελατών τραπεζών. Χαρακτηριστική περίπτωση είναι το πρόσφατο κρούσμα επιτηδείων στην Κρήτη, όπου εμφανίζονταν ως σύμβουλοι επιχειρήσεων και αποσπούσαν φορολογικά στοιχεία εταιρειών. Πριν από μερικούς μήνες η Ελληνική Ένωση Τραπεζών με ανακοίνωσή της επεσήμανε νέες μορφές εξαπάτησης πελατών τραπεζών στα ΑΤΜ, ενώ επέστησε την προσοχή στα λεγόμενα spam, δηλαδή τα ενοχλητικά-παραπλανητικά email, τα οποία έχουν ως στόχο να αποσπάσουν προσωπικά δεδομένα (τραπεζικό λογαριασμό, κωδικούς κ.λπ.) από αφελείς. Το πιο δημοφιλές προϊόν στη μαύρη αγορά είναι τα στοιχεία πιστωτικών καρτών, ενώ ακολουθούν οι τραπεζικοί λογαριασμοί και οι λογαριασμοί ηλεκτρονικού ταχυδρομείου.

Ένα άλλο στοιχείο που διαπιστώνεται στην έκθεση είναι ότι πλέον έχει αλλάξει η ταυτότητα των κλεφτών. Αν κάποτε ήταν νεαροί ερασιτέχνες που σκορπούσαν τον τρόμο στο Διαδίκτυο, σήμερα οι συμμορίες του κυβερνοχώρου συνδέονται με το οργανωμένο έγκλημα. Και όποιος δεν υπακούει στους κανόνες, μπορεί να αποκλειστεί από μια μελλοντική δουλειά, να δεχθεί μια ανελέητη ηλεκτρονική επίθεση ή ακόμη και απειλές για τη σωματική του ακεραιότητα. Γενικότερα θα πρέπει οι καταναλωτές να είναι υποψιασμένοι αλλά και ταυτόχρονοι σίγουροι πως η τράπεζα δεν ζητεί από τον χρήστη εμπιστευτικά προσωπικά δεδομένα, όπως τον κωδικό User ID, το μυστικό



Password, αριθμούς λογαριασμών ή καρτών κ.λπ. μέσω του ηλεκτρονικού ταχυδρομείου (e-mail), ούτε στέλνει στους χρήστες εμπιστευτικές πληροφορίες μέσω αυτού.

### Περίπτωση Απάτης με e-mail

Ίσως το πιο πρόσφατο παράδειγμα απάτης «νέας» γενιάς είναι ένα e-mail απάτη με φερόμενο ως αποστολέα το Υπουργείο Οικονομικών. Μάλιστα, για να γίνεται πιο πιστευτό, στο μήνυμα περιλαμβάνεται το λογότυπο του Υπουργείου, το δε κείμενο είναι στα Ελληνικά, και μάλιστα σε ικανοποιητική ποιότητα –αν και δεν λείπουν κάποια οφθαλμοφανή λάθη που το προδίδουν, όπως για παράδειγμα η μετάφραση του PIN ως ... καρφίτσα. Σε κάθε περίπτωση, με το e-mail αυτό ο παραλήπτης ενημερώνεται ότι δήθεν δικαιούται κάποιο ποσό ως επιστροφή φόρου και για να το παραλάβει άμεσα θα πρέπει να συμπληρώσει τα στοιχεία του στην ηλεκτρονική φόρμα που του δίδεται. Και βέβαια, όπως συμβαίνει σε όλες αυτές τις περιπτώσεις, για να το καταφέρει θα πρέπει να συμπληρώσει όλα τα προσωπικά δεδομένα του (ονοματεπώνυμο, διεύθυνση κατοικίας, ΑΦΜ, κ.α.), στοιχεία πρόσβασης στον τραπεζικό του λογαριασμό (όνομα χρήστη και συνθηματικό, αριθμός λογαριασμού κλπ), καθώς και όλα τα στοιχεία της πιστωτικής του κάρτας.

Ένα άλλο είδος απάτης που χρησιμοποίησε τον Δήμο Άνω Λιοσίων, προς αύξηση της εμπιστευτικότητας του, αποτελούσε ένα μήνυμα όπου χαρακτηριστικά αναφέρονταν τα ονόματα των γονέων που είχαν ένα παιδί με καρδιακή ανεπάρκεια και πως χρειαζόνταν χρήματα προκειμένου να εγχειρισθεί. Συνάμα, μέσα στην επιστολή αναφέρονταν κι ο Μ.Κ.Ο. «Χαμόγελο του Παιδιού» πλην του Δήμου Άνω Λιοσίων. Η ελεημοσύνη μέσω Ιντερνετ είναι μία πρόσφατη μορφή ηλεκτρονικής απάτης στην Ελλάδα. Κατά τη διάρκεια των τελευταίων τεσσάρων χρόνων, έχουν καταγγελθεί στη χώρα μας οκτώ περιπτώσεις απάτης στο Διαδίκτυο με τη μορφή έμμεσης ελεημοσύνης, δηλαδή κάποιος επιχειρεί να πουλήσει ένα προϊόν (π.χ. μια τηλεόραση ή ένα κινητό τηλέφωνο) σε χαμηλή τιμή. Το θύμα καταβάλλει το ποσό με πιστωτική κάρτα ή μέσω τράπεζας, αλλά το προϊόν δεν καταλήγει ποτέ στα χέρια του. Μάλιστα, σε μία περίπτωση, ο αγοραστής αντί να λάβει το κινητό που παρήγγειλε, έλαβε μία πέτρα. [15]

Όπως παρατηρείται σε όλες τις περιπτώσεις, οι επιτήδευοι χρησιμοποιούν διάφορα μέσα προς την εξαπάτηση των καταναλωτών. Κύρια μέσα πειθούς αποτελεί είτε η επίκληση αξιόπιστου δικτυακού τόπου (e-bay) που αποτελούσε αξιόπιστο μέσο αγοροπωλησιών είτε η επίκληση στο συναίσθημα (ελεημοσύνη λόγω προβλήματος υγείας). Ο τρόπος που στήνεται όμως η παγίδα είναι κυρίως μέσω της μαζικής αποστολής e-mails σε όλα τα ανυποψίαστα θύματα, με την ελπίδα πως όλο και περισσότεροι θα εξαπατηθούν, ανταποκρινόμενοι στις απαιτήσεις του κάθε κειμένου (στέλνοντας στοιχεία, προωθώντας το μήνυμα ,κα.). Η έκβαση αφού κάποιος ενδώσει στην όποια παγίδα, είναι λίγο πολύ γνωστό με συνήθη στόχο την πιστωτική του κάρτα.

## 2.5 ΦΟΡΕΙΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑΝΑΛΩΤΩΝ – Ρόλος, Αρμοδιότητες και Συνήθης Πρακτική

Η άνηθηση ή ακόμα καλύτερα η έξαρση του ηλεκτρονικού εγκλήματος ολόένα κι αυξάνει τα ποσοστά παρουσίας της σε όλα τα επίπεδα της κοινωνίας όπως είναι ανήλικοι, έφηβοι ακόμη κι ενήλικες οι οποίοι έχουν γνώσεις χρήσης των Ηλεκτρονικών Υπολογιστών. Οι καταναλωτές, όπου σε αυτή την ομάδα του κύκλου πωλήσεων εντάσσονται τα περισσότερα θύματα, δεν θα μπορούσαν να αντιμετωπίσουν την οποιαδήποτε μορφή ηλεκτρονικής εξαπάτησης, αν δεν υπήρχαν οι αρμόδιοι φορείς οργάνωσης και προστασίας. Αυτοί είναι οι Φορείς Προστασίας Καταναλωτών.

Με τον όρο **Φορέας Προστασίας Καταναλωτών**, εννοούμε την Μη Κυβερνητική Οργάνωση που αποσκοπεί στο να προστατεύσει, να ενημερώσει και να ασχοληθεί νομικά με θέματα εξαπάτησης καταναλωτών. Αυτοί οι φορείς λειτουργούν προσθετικά με το αρμόδιο Υπουργείο του κράτους και την Γενική Γραμματεία Καταναλωτή και η συμβολή τους αποτελεί αρωγό στην αποτελεσματικότερη καταπολέμηση της όποιας μορφής εγκλήματος είτε οικονομικού είτε ηλεκτρονικού. Συνήθως αυτά τα προγράμματα είναι επιδοτούμενα από την Ευρωπαϊκή Ένωση καθώς επίσης κι από εθελοντές κι ιδιώτες που συμβάλλουν οικονομικώς με την δική τους συνδρομή. Τα μέλη ενασχόλησης είναι επίσης εθελοντές και δεν τίθεται θέμα μισθού.

Τόσο σε παγκόσμιο όσο κι σε ελληνικό επίπεδο, υπάρχει πληθώρα τέτοιων φορέων που συμβάλλουν στην θωράκιση των αξιόπιστων συναλλαγών προστατεύοντας τους καταναλωτές. Προβαίνοντας σε μια ιστορική αναδρομή για την πάταξη του ηλεκτρονικού εγκλήματος θα μπορούσε να αναφερθεί πως η Interpol ήταν ο πρώτος διεθνής οργανισμός που προσέγγισε το ηλεκτρονικό έγκλημα και την ποινική νομοθεσία σε σχέση με αυτό το 1979 στο Τρίτο Διεθνές Συμπόσιο για την Απάτη που πραγματοποιήθηκε στο Παρίσι [16]. Επίσης ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.) παρουσίασε ένα ψήφισμα σχετικό με τη νομοθεσία γύρω από το ηλεκτρονικό έγκλημα στο 8ο Συνέδριο για την Πρόληψη του Εγκλήματος και τη Μεταχείριση των Παραβατών. Πρόκειται για το Εγχειρίδιο για την πρόληψη και τον έλεγχο του ηλεκτρονικού εγκλήματος που εκδόθηκε το 1994. Στο συγκεκριμένο κείμενο αναλύεται το φαινόμενο της ηλεκτρονικής εγκληματικότητας, οι βασικότερες μορφές του και η σχετική νομοθεσία διαφόρων χωρών. Αναπτύσσονται προτάσεις για την πληρέστερη και αποτελεσματικότερη αντιμετώπιση. Αποτελεί την πρώτη μεθοδική διεθνή προσπάθεια προσέγγισης νομοθετικού πλαισίου για το ηλεκτρονικό έγκλημα και έτσι θεωρείται βάση πάνω στην οποία μπορούν να γίνουν περεταίρω αναθεωρήσεις και τροποποιήσεις ανάλογα με τις τρέχουσες κάθε φορά τεχνολογικές αλλά και νομικές εξελίξεις.

Σε ευρωπαϊκό επίπεδο, η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης στο Στρασβούργο το 1976 στις εργασίες του Συνεδρίου για τις Εγκληματολογικές πλευρές του οικονομικού εγκλήματος, όπου για πρώτη φορά παρουσιάζονται οι μορφές του ηλεκτρονικού εγκλήματος. Το 1996 το Συμβούλιο της Ευρώπης προέβη στην έκδοση τριών Οδηγιών οι οποίες παρά το γεγονός ότι δεν έχουν δεσμευτική ισχύ για τα κράτη-μέλη, παρέχουν κατευθυντήριες γραμμές και υποδείξεις προς την υιοθέτηση μιας συγκεκριμένης συμπεριφοράς. Πρόκειται για την Οδηγία Νο R (1989) που αναφέρεται στο έγκλημα που διαπράττεται με τον υπολογιστή. Έπεται μια Οδηγία μεγάλης σπουδαιότητας γιατί καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο γενικές δικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων. Είναι η Οδηγία Νο R(1995) για τα δικονομικά ζητήματα που σχετίζονται με την τεχνολογία των πληροφοριών. Ακολουθεί η πιο πρόσφατη Οδηγία Νο R(2001) σχετικά με την αυτορρύθμιση σε θέματα διαδικτύου. Οι συστάσεις αυτές αποτέλεσαν



συστατικά κομμάτια για την σύνταξη της Σύμβασης στον Κυβερνοχώρο. Το σύνολο των συστάσεων που αναφέρθηκαν ενδεικτικά, θα αναλυθούν περαιτέρω σε παρακάτω κεφάλαιο της παρούσας διπλωματικής εργασίας.

Στην Ελλάδα έχουν δημιουργηθεί διάφοροι φορείς προστασίας καταναλωτών, οι κυριότεροι των οποίων αναφέρονται στη συνέχεια.

#### IN στιούτο ΚΑ ταναλωτών (INKA)

Η επίσημη ονομασία του είναι INKA/ Γενική Ομοσπονδία Καταναλωτών Ελλάδος [17] με ημερομηνία ιδρύσεως την 15 Μαρτίου 1995. Το INKA/ΓΟΚΕ είναι ένας ανεξάρτητος, μη κερδοσκοπικός, και μη κυβερνητικός οργανισμός. Η Ομοσπονδία, ως προς τους κανονισμούς που τη διέπουν, είναι σύμφωνη με την εθνική νομοθεσία για την Προστασία Καταναλωτών(νόμος 2251/1994). Το INKA/ΓΟΚΕ είναι επισήμως καταγεγραμμένο ως Ομοσπονδία, σύμφωνα με την ελληνική νομοθεσία με την απόφαση 2393/25-8-1995 του πρωτοδικείου Αθηνών. Το INKA είναι η πρώτη καταναλωτική οργάνωση της χώρας. Ιδρύθηκε το 1970. Η Ομοσπονδία INKA/Γενική Ομοσπονδία Καταναλωτών Ελλάδος ιδρύθηκε το 1995. Σήμερα αριθμεί 46 μέλη-οργανώσεις σε όλη την Ελλάδα, αποτελώντας το μεγαλύτερο δίκτυο καταναλωτικών οργανώσεων της χώρας, και αντιπροσωπεύοντας το 94των πολιτών-καταναλωτών που συμμετέχουν ενεργά στο Ελληνικό Καταναλωτικό Κίνημα. Το Μάιο 2003 το INKA επιλέγεται από τη Γενική Δ/ση Υγεία και Προστασία Καταναλωτή της Ευρωπαϊκής Επιτροπής για να υλοποιήσει το Ευρωπαϊκό Κέντρο Καταναλωτή, κέντρο πληροφόρησης και υποστήριξης των καταναλωτών-πολιτών της Ευρωπαϊκής Ένωσης και εθνικό κόμβο ενός Δικτύου 15 κέντρων σε 13 κράτη μέλη της ΕΕ. Τα παράπονα ή τις καταγγελίες τους οι καταναλωτές μπορούν να τις αποστείλουν στο mail της ιστοσελίδας κι έπειτα ο οργανισμός, ανάλογα με τον φόρτο παραπόνων, δρα κι ενημερώνει την Νομαρχία που «ανήκει» το συμβάν, προκειμένου κι εκείνοι με την σειρά τους να πράξουν τα δέοντα.

Συμπληρωματικά υπάρχει και το Νέο INKA [18] όπου είναι ένας ανεξάρτητος, μη κερδοσκοπικός και μη κυβερνητικός οργανισμός, που μπορεί και εκπροσωπεί τους καταναλωτές σε Εθνικούς και Ευρωπαϊκούς φορείς. Αποτελεί την παλαιότερη και μεγαλύτερη καταναλωτική οργάνωση στην Ελλάδα με περισσότερα από 10.000 ενεργά

μέλη. Λειτουργεί ανεξάρτητα από βιομηχανικά, εμπορικά και πολιτικά συμφέροντα και κύριο μέλημα τους είναι η προστασία των συμφερόντων των καταναλωτών. Υποστηρίζει διαδικασίες διαλόγου με τους κοινωνικούς φορείς, τα κόμματα αλλά και την εκάστοτε κυβέρνηση, πάνω από όλα όμως υποστηρίζει, αναζητά και επιδιώκει την επικοινωνία με τους καταναλωτές, που αποτελούν και την κινητήριου δύναμη τους.

Οι στόχοι δράσης είναι οι εξής:

- Η ενίσχυση των δράσεων ενημέρωσης των πολιτών σε θέματα που αφορούν στην Υγεία και Προστασία του Καταναλωτή και συγκεκριμένα σε κάθε τομέα, ο οποίος συνδέεται με το κόστος και την ποιότητα ζωής, όπως και στην προστασία του περιβάλλοντος, στη βελτίωση των υπηρεσιών της Δημόσιας Διοίκησης και γενικά σε όλα τα θέματα που αφορούν στο κοινωνικό σύνολο και στο δημόσιο συμφέρον.
- Η πληροφόρηση και η ευαισθητοποίηση των καταναλωτών και ιδιαίτερα των νέων καταναλωτών σε σχέση με την αγορά ασφαλών προϊόντων στο πλαίσιο της Εσωτερικής Ενιαίας Αγοράς.
- Η εκπαίδευση των καταναλωτών και ιδιαίτερα των νέων καταναλωτών στο πώς να ασκούν τα δικαιώματά τους όταν αυτά θίγονται.
- Η ευαισθητοποίηση των εκπαιδευτικών σε προβλήματα που σχετίζονται με τα καταναλωτικά προϊόντα, και ιδιαίτερα εκείνα που αφορούν περισσότερο τους νέους.
- Η διαμόρφωση προϋποθέσεων διαλόγου και συνεργασίας των κοινωνικών εταίρων της αγοράς, με σκοπό τη βελτίωση της διαφάνειας της αγοράς.

### SaferInternet

Η Δράση Ενημέρωσης *Saferinternet.gr* [19] του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου και η εκστρατεία ενημέρωσης και επαγρύπνησης που διεξάγεται στη χώρα μας από το 2004, υλοποιούνται υπό την αιγίδα της Ευρωπαϊκής Επιτροπής στο πλαίσιο του προγράμματος Safer Internet.

Οι κύριοι στόχοι της δράσης *Saferinternet.gr* είναι:

- Η προστασία των ανήλικων χρηστών του Διαδικτύου από ακατάλληλο ή επιβλαβές για αυτούς περιεχόμενο, ή από ακατάλληλη ή επιβλαβή συμπεριφορά.
- Η ενημέρωση των γονέων για τους τρόπους με τους οποίους μπορούν να προστατευθούν αλλά και να προστατεύσουν αποτελεσματικά τα παιδιά τους από τους κινδύνους που εγκυμονούν από τη μη ορθή χρήση των διαδραστικών τεχνολογιών, όπως είναι το Διαδίκτυο ή το κινητό τηλέφωνο.
- Η προώθηση των θετικών πλευρών των διαδραστικών τεχνολογιών, ως εργαλεία της καθημερινής μας ζωής.
- Η εκπαίδευση των εκπαιδευτικών για την ασφαλή χρήση του Διαδικτύου και του κινητού τηλεφώνου, ενημερώνοντας τόσο για τα πολλαπλά οφέλη όσο και για τους πιθανούς κινδύνους, με στόχο τη δημιουργία πολλαπλασιαστικής δράσης μέσα στην τάξη.
- Η ενθάρρυνση του διαλόγου μεταξύ ανήλικων και γονέων σχετικά με τη χρήση του Διαδικτύου, η προώθηση του ψηφιακού αλφαριθμητισμού και της κριτικής σκέψης.
- Η υποστήριξη, γονέων, εκπαιδευτικών, αλλά και ανήλικων χρηστών με κατάλληλο ενημερωτικό υλικό.

Για την επίτευξη των παραπάνω στόχων, το *Saferinternet.gr* υλοποιεί σειρά δραστηριοτήτων όπως διοργάνωση ενημερωτικών εκδηλώσεων για το κοινό, σεμινάρια προς εκπαιδευτικούς, προώθηση θεμάτων που σχετίζονται με την ασφάλεια στο Διαδίκτυο στα ΜΜΕ, δημιουργία πολυμορφικού online και έντυπου ενημερωτικού υλικού, καθώς και τηλεοπτικές και ραδιοφωνικές καμπάνιες. Το *Saferinternet.gr* συνεργάζεται με εκπροσώπους του κράτους, της βιομηχανίας των νέων τεχνολογιών καθώς και με Μη Κυβερνητικές Οργανώσεις στην Ελλάδα και το εξωτερικό με πρωταρχικό σκοπό την εξασφάλιση ενός ασφαλέστερου διαδικτυακού περιβάλλοντος.



Η δράση Saferinternet.gr αποτελεί τον εθνικό εκπρόσωπο του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης *Insafe*, με 30 μέλη στην Ευρώπη. Στα πλαίσια του *Insafe* το *Saferinternet.gr* ανταλλάσσει απόψεις, εμπειρίες, βέλτιστες πρακτικές και πληροφοριακό υλικό με τα άλλα Ευρωπαϊκά Κέντρα.

Το *Saferinternet.gr* αποτελεί μια από τις τρεις δράσεις του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, δίπλα στην Γραμμή Καταγγελιών *Safeline* και τη Γραμμή Βοηθείας *ΥποΣΤΗΡΙΞΩ*. Υλοποιείται από την αστική μη κερδοσκοπική εταιρία Safer Internet Hellas.

### SafeLine

Η SafeLine [14] ξεκίνησε τη λειτουργία της στις 14 Απριλίου 2003. Είναι η μοναδική ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο και επίσημο μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) από τις 18 Οκτωβρίου 2005. Βασική μέριμνα της SafeLine είναι η εξάλειψη φωτογραφιών και βίντεο που απεικονίζουν κακοποίηση ανηλίκων, καθώς και η προάσπιση του δικαιώματος της ασφαλούς πλοήγησης του παιδιού στο Διαδίκτυο. Στα παραπάνω προστίθεται και η αντιμετώπιση της παρενόχλησης του μέσω του κυβερνοχώρου ή του κινητού τηλεφώνου αλλά και η αντιμετώπιση περιεχομένου που αφορά τη βία, το ρατσισμό, την ξενοφοβία και γενικά καθετί το οποίο αντιβαίνει στην Ελληνική Νομοθεσία. Το 2008, η SafeLine ένωσε τις δυνάμεις της με τον Ελληνικό Κόμβο Επαγρύπνησης. Παράλληλα, δημιουργήθηκε η Γραμμή Βοηθείας ΥποΣΤΗΡΙΞΩ (helpline) της Μονάδας Εφηβικής Υγείας του Νοσοκομείου «Αγλαΐα Κυριακού». Οι τρεις δράσεις δημιούργησαν τον Ελληνικό Κόμβο Ασφαλούς Διαδικτύου με στόχο μια πιο πολύπλευρη και οργανωμένη προσπάθεια που ενσωματώνει την ενημέρωση & αφύπνιση του κοινού, την καταγγελία, καθώς και την πρόληψη & βοήθεια κάτω από το ίδιο κοινό έργο.

Το σύνολο των φορέων, όσο κι αξιόλογο έργο κι αν επιθυμούν να πραγματοποιήσουν, σίγουρα θα δυσκολεύονταν αν δεν προϋπήρχε η ανάλογη νομοθεσία περί των ηλεκτρονικών εγκλημάτων. Νομοθεσία που συνεχώς εξελίσσεται, σχεδόν παράλληλα με την τεχνολογία, και εφαρμόζεται σε παγκόσμιο επίπεδο χρήσης

των υπολογιστών. Στο παρακάτω κεφάλαιο θα γίνει περαιτέρω ανάλυση του Νομοθετικού ατού πλαισίου λειτουργίας των εικονικών επιχειρήσεων αλλά και της προστασίας των καταναλωτών από αυτές.

Πανεπιστήμιο Πειραιώς

## ΚΕΦΑΛΑΙΟ 3<sup>ο</sup> : ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΛΕΙΤΟΥΡΓΙΑΣ ΕΙΚΟΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑΝΑΛΩΤΩΝ

### 3.1 ΕΙΣΑΓΩΓΗ

Η Κοινωνία της πληροφορίας δεν είναι μόνο μία κοινωνία γνώσης και ανάπτυξης καθώς εμφανίζονται και στο Διαδίκτυο ανάλογα προβλήματα με αυτά που παρουσιάζονται στη κοινωνία. Ένα από αυτά είναι η εγκληματικότητα, η οποία όπως έχει ήδη αναφερθεί σε προηγούμενη ενότητα, έχει διάφορες μορφές, όπως :

- επίθεση κατά πληροφορικών συστημάτων
- διάδοση παιδικής πορνογραφίας
- απάτη
- παραβιάσεις πνευματικής ιδιοκτησίας
- προσβολές της ιδιωτικότητας
- υποστήριξη της διάπραξης παραδοσιακών εγκλημάτων όπως η διακίνηση ναρκωτικών ή το δουλεμπόριο

Πρέπει να σημειωθεί ο ιδιαίτερα ευάλωτος χαρακτήρας της σημερινής κοινωνίας της πληροφορίας: η οικονομία, η διοίκηση και η κοινωνία είναι σε πολύ υψηλό βαθμό εξαρτημένες από την αποτελεσματικότητα και την ασφάλεια των πληροφορικών συστημάτων. Είναι μία κοινωνία υψηλών ευκαιριών και ευχερειών αλλά ταυτόχρονα μία κοινωνία κινδύνων.

Η ανωνυμία ως βασικό χαρακτηριστικό του Διαδικτύου έχει σοβαρές συνέπειες για το ποινικό δίκαιο. Δεν δυσχεραίνει απλώς τη διαλεύκανση των εγκλημάτων αλλά δημιουργεί σοβαρό πρόβλημα και ως προς τις αποδείξεις. Ένα άλλο σοβαρό κοινωνιολογικό-εγκληματολογικό στοιχείο είναι ότι η ανωνυμία ενθαρρύνει τους χρήστες του Διαδικτύου να επιχειρήσουν εγκληματικές πράξεις τις οποίες δεν θα επιχειρούσαν παρά μόνο στον κυβερνοχώρο καθώς στον χώρο αυτό δεν φαίνεται να έχει διαμορφωθεί μία ηθική τάξη και δομή με σαφείς κανόνες δεοντολογίας, επιταγές και απαγορεύσεις.



Η διάδοση της τεχνολογίας των υπολογιστών σε όλες τις πλευρές της ζωής, η διασύνδεση των υπολογιστών σε διεθνή δίκτυα έχουν καταστήσει το έγκλημα πιο διαφοροποιημένο, πιο επικίνδυνο και διεθνοποιημένο. Τα νέα συστήματα έχουν ειδικά χαρακτηριστικά που διευκολύνουν τους δράστες αλλά δυσχεραίνουν το έργο των διωκτικών αρχών (πολλαπλά συστήματα λογισμικού και hardware, έλλειψη εμπειρίας πολλών χρηστών, ανωνυμία, κρυπτογράφηση, διεθνής κινητικότητα).

Αποτέλεσμα :

- η παραβατικότητα καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο.
- τα εγκλήματα αυτά μπορούν να πραγματοποιηθούν από τον καθένα και να πλήξουν τον καθένα. Δεν χρειάζεται καν να εγκαταλείψει κανείς τον χώρο του σπιτιού του.
- το ηλεκτρονικό έγκλημα έχει αποκτήσει κινητικότητα και διεθνή χαρακτήρα

Το σύνολο του ηλεκτρονικού εγκλήματος είναι αρκετά μεγάλο τόσο σε πλήθος περιπτώσεων όσο και σε πολυμορφία. Οι παρακάτω ενότητες θα επικεντρωθούν κυρίως στο ηλεκτρονικό έγκλημα υπό το πρίσμα του ηλεκτρονικού επιχειρείν. Οι εξελίξεις αυτές θέτουν σοβαρότατα ζητήματα για το ποινικό δίκαιο καθώς τα μεθοδολογικά του παραδείγματα και οι κατηγορίες του τίθενται σε αμφισβήτηση ως προς τη ρυθμιστική τους ικανότητα. Πέραν όμως του ποινικού δικαίου σε περίπτωση εξαπάτησης καταναλωτή από το ηλεκτρονικό έγκλημα, άξιο αναφοράς αποτελεί και το σύνολο του ποινικού κώδικα που διέπει την σύσταση και την λειτουργία των εικονικών επιχειρήσεων τόσο σε παγκόσμιο επίπεδο όσο και σε εγχώριο. Σκοπός αυτού του κεφαλαίου είναι η παράθεση όλων εκείνων των νόμων που οριοθετούν και ρυθμίζουν τόσο τις εικονικές επιχειρήσεις ως προς την λειτουργία αλλά κι εκείνων των νόμων που ενεργοποιούνται σε περίπτωση εξαπάτησης διαδικτυακού καταναλωτή.

## 3.2 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑΝΑΛΩΤΩΝ – ΔΙΑΤΑΞΕΙΣ ΠΕΡΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

### 3.2.1 Η εξέλιξη του Ποινικού Δικαίου της Κοινωνίας της Πληροφορίας

Η εξέλιξη του ποινικού δικαίου του κυβερνοχώρου χαρακτηρίζεται από τέσσερα στάδια τα οποία αναλύονται παρακάτω:

- α) Στη δεκαετία του '70 και του '80 το πρώτο κύμα νομοθεσίας αφορούσε στην προστασία της ιδιωτικότητας και των προσωπικών δεδομένων.
- β) Στη δεκαετία του '80 ένα δεύτερο κύμα τροποποιήσεων των νόμων αφορούσε στην καταστολή του οικονομικού ηλεκτρονικού εγκλήματος
- γ) Η τρίτη σειρά στη διάρκεια της δεκαετίας του '80 αφορούσε στην προστασία της πνευματικής ιδιοκτησίας
- δ) Μετά τα μέσα του '90 σημειώνεται ένα τέταρτο κύμα νομοθετικών τροποποιήσεων που αφορά στο παράνομο και αθέμιτο περιεχόμενο.

#### Προστασία Ιδιωτικότητας

Οι νόμοι για την προστασία προσωπικών δεδομένων περιέχουν ποινικές διατάξεις που αφορούσαν κατά πρώτο λόγο στα ηλεκτρονικά αρχεία αλλά που βαθμιαία επεκτάθηκαν και στα χειρόγραφα αρχεία. Υπάρχουν ωστόσο διαφοροποιήσεις ως προς τις συμπεριφορές που ποινικοποιούνται. Στη νομοθεσία των ΗΠΑ, Καναδά και Ιαπωνίας συναντάται περιορισμένος αριθμός τέτοιων εγκλημάτων. Αντίθετα στις ευρωπαϊκές χώρες ο σχετικός κατάλογος είναι σαφώς μακρύτερος και αφορά σε :

- α) προσβολή ουσιαστικών δικαιωμάτων (παράνομη διάδοση, διαβίβαση προσωπικών δεδομένων, παράνομη καταχώριση, τροποποίηση, παραποίηση αλλά και χρήση προσωπικών δεδομένων,
- β) παραβάσεις υποχρεώσεων εκ του νόμου π.χ. ο ιταλικός νόμος για την προστασία δεδομένων προβλέπει ως ποινικό αδίκημα τη μη συμμόρφωση σε αποφάσεις της αρχής ελέγχου ή την άρνηση επίδειξης εγγράφων ή παροχής πληροφοριών.

γ) προσβολή δικαιωμάτων πρόσβασης του υποκειμένου στα δεδομένα που το αφορούν. (π.χ. νόμοι Λουξεμβούργου, Δανίας, Σουηδίας)

δ) μη τήρηση των υποχρεώσεων ασφαλείας (data security measures) που επιβάλλει ο νόμος (π.χ. νόμοι Δανίας, Ιταλίας)

### Οικονομικό Ποινικό Δίκαιο

Η τροποποίηση πολλών ρυθμίσεων του ποινικού δικαίου κρίθηκε σε πολλές χώρες αναγκαία προκειμένου να αντιμετωπιστούν οι νέες μορφές προσβολής παραδοσιακών αγαθών αλλά και η προσβολή άυλων αγαθών όπως π.χ. μία τραπεζική κατάθεση ή ένα πρόγραμμα. Στην αρχή η νομοθεσία επικεντρώθηκε στην ηλεκτρονική απάτη αλλά στην πορεία προστέθηκαν διατάξεις που αφορούσαν το σαμποτάζ, την κατασκοπεία, την παράνομη πρόσβαση κλπ.

### Παράνομο κι Αθέμιτο Περιεχόμενο

Σε σχέση με το παράνομο και αθέμιτο περιεχόμενο προκύπτουν δύο κρίσιμα νομικά ζητήματα :

α) αν και ποιοί περιορισμοί μπορούν να επιβληθούν στην παραγωγή, διάδοση και χρήση του περιεχομένου δεδομένου ότι πρέπει να ληφθεί υπόψη η άσκηση και ο σεβασμός και άλλων δικαιωμάτων όπως η ελευθερία της έκφρασης και το δικαίωμα πληροφόρησης.

Ως προς αυτό το κρίσιμο νομικό ζήτημα και κυρίως σε ότι αφορά σε σελίδες πολιτικού ή ιδεολογικού περιεχομένου, η αντιμετώπιση ποικίλλει ανάλογα με την ιστορική, πολιτική και συνταγματική παράδοση κάθε χώρας. Το πρόσφατο παράδειγμα της αντιμετώπισης εκ μέρους της YAHOO της απόφασης γαλλικού δικαστηρίου σχετικά με την φιλοξενία σελίδων με φιλοναζιστικό περιεχόμενο είναι χαρακτηριστικό: η εταιρία ως προς το γαλλικό “τμήμα” της συμμορφώθηκε με την απόφαση καθώς αυτό επιβαλλόταν από τη γαλλική νομοθεσία ενώ η YAHOO στις ΗΠΑ δήλωσε ότι δεν μπορεί να εμποδίσει τη διάδοση του συγκεκριμένου περιεχομένου γιατί αυτό θα συνιστούσε περιορισμό της ελευθερίας της έκφρασης. Το θέμα της κρίσης του περιεχομένου υπό το πρίσμα της ελευθερίας της έκφρασης και της πληροφόρησης συναρτάται άμεσα και με το ζήτημα της ευθύνης. Σοβαρά ζητήματα εγείρονται σε



σχέση με το εάν μπορεί να ανατεθεί στο πάροχο υπηρεσιών δικτύου κλπ. να ελέγχει - κυρίως εκ των προτέρων - το περιεχόμενο των σελίδων που φιλοξενεί. Δεν είναι δηλαδή αυτονόητο να ανάγεται μία τέτοια εταιρία σε παράγοντα που σταθμίζει και κρίνει συνταγματικά δικαιώματα όπως η ελευθερία της σκέψης ή/και συνταγματικές αρχές και αξίες όπως η δημοκρατική αρχή, ο σεβασμός του πολιτεύματος, η προστασία της αξίας και της προσωπικότητας του ανθρώπου. Θα μπορούσε να επιβληθεί η οποιαδήποτε αλλαγή στο ζήτημα της υποχρέωσης συμμόρφωσής της μόνο στην περίπτωση που υπάρξει σχετική δικαστική ή διοικητική απόφαση. Ορισμένες χώρες προσπαθούν να λύσουν αυτά τα προβλήματα, αφενός δηλαδή της σύγκρουσης της ελευθερίας της γνώμης και της πληροφόρησης και της διαφύλαξης ζωτικών συμφερόντων - αξιών και αφετέρου να ενθαρρύνουν τον αυτοέλεγχο και την εκπόνηση κωδίκων δεοντολογίας από τους φορείς και τις εταιρείες που παρέχουν τέτοιες υπηρεσίες.

Ένα άλλο πρόβλημα, που ανάγεται στο ίδιο κενό νόμου που υπάρχει, σχετίζεται με το περιεχόμενο, δηλαδή την παιδική πορνογραφία. Σε πολλές χώρες υπάρχει νομοθεσία που τιμωρεί την πορνογραφία και αποσκοπεί στην προστασία των ανηλίκων από την εκμετάλλευση αλλά και στην προστασία της πνευματικής και ηθικής τους ανάπτυξης. Αποσκοπεί περαιτέρω στην προστασία των χρηστών ηθών αλλά και της ανθρώπινης αξιοπρέπειας. Σήμερα στις περισσότερες χώρες προβλέπεται προστασία και ο ποινικός κολασμός αυτών των πράξεων και πολλές νομοθεσίες έχουν τροποποιηθεί προκειμένου να συμπεριλαμβάνονται ρητά στο πεδίο εφαρμογής των σχετικών διατάξεων η ηλεκτρονική καταχώριση και διάδοση πορνογραφικού υλικού. Οι πράξεις που τιμωρούνται αφορούν συνήθως την διάδοση, την προμήθεια του σχετικού υλικού και τη δημοσίευσή του. Τα τελευταία χρόνια καταγράφεται η τάση να επεκταθούν οι ποινικές ρυθμίσεις και στην κατοχή τέτοιου υλικού.

β) τα ζητήματα ευθύνης αφενός του παρόχου περιεχομένου και αφετέρου του παρόχου υπηρεσιών, του οποίου το δίκτυο ή ο κεντρικός υπολογιστής χρησιμοποιείται από τρίτους για τη διάδοση τέτοιου περιεχομένου.

Ως προς αυτό το νομικό ζήτημα, της ποινικής ευθύνης αυτών που παρέχουν υπηρεσίες για το περιεχόμενο που διαδίδεται μέσω των συστημάτων και των δικτύων τους, τα προβλήματα είναι νέα και εξαιρετικά σύνθετα. Η νομοθεσία αλλά και η

επιστημονική συζήτηση διαχωρίζει σε επιμέρους μέρη την ευθύνη όσον αφορά τους παροχείς υπηρεσιών διαδικτύου. (ευθύνη αν είναι δικό τους το περιεχόμενο, καταχώρηση περιεχομένου χωρίς έλεγχο δικαιωμάτων)

Η συζήτηση αλλά και οι τελικοί νόμοι έχουν πλέον καταλήξει πως η ευθύνη επιμερίζεται μεταξύ του συγγραφέα αλλά κι εκείνου που διαθέτει το όποιο αθέμιτο περιεχόμενο. Για όλα τα υπόλοιπα αδικήματα υπάρχει διαφοροποίηση ως προς : α) αυτών που καταχωρούν σε δικούς τους υπολογιστές το περιεχόμενο τρίτου προσώπου και β) αυτών που απλά παρέχουν πρόσβαση (μεσάζοντες) μέσω υπηρεσιών δικτύου και απλώς μεταφέρουν το περιεχόμενο (μέσω ιστο – συνδέσμων)

Ως προς την πρώτη κατηγορία η κυρίαρχη τάση φαίνεται να ευνοεί τον περιορισμό της ποινικής ευθύνης μόνο στις περιπτώσεις που ο πάροχος υπηρεσιών γνώριζε την ύπαρξη του συγκεκριμένου παράνομου περιεχομένου στον server του και ήταν τεχνικό εφικτό και εύλογα αναμενόμενο ότι θα διαγράψει αυτό το περιεχόμενο. Ως προς τη δεύτερη κατηγορία φαίνεται να υπάρχει γενική συμφωνία ότι δεν υπέχουν ποινική ευθύνη λόγω των τεχνικών και νομικών συνθηκών που δεν επιτρέπουν την εποπτεία και τον έλεγχο του περιεχομένου που διακινούν

Η κοινοτική νομοθεσία περιόρισε σημαντικά την ευθύνη των παρόχων υπηρεσιών πρόσβασης και δικτύου.

### 3.2.2 Παγκόσμια Νομοθεσία και Πρακτικές τους

#### Η ΝΟΜΟΘΕΣΙΑ ΣΤΙΣ Η.Π.Α.

Στις Η.Π.Α. το 1984 θεσπίζεται ο πρώτος νόμος για το ηλεκτρονικό έγκλημα. Πρόκειται για τον Computer Fraud and Abuse Act, ο οποίος δεν κατάφερε ικανοποιητικά να θέσει ένα βασικό πλαίσιο για την αντιμετώπιση της ηλεκτρονικής εγκληματικότητας. Οι λόγοι ήταν αρκετοί όπως η αδυναμία προσδιορισμού της δικαιοδοσίας των δικαστηρίων και η έλλειψη ορολογίας σχετιζόμενης με την τεχνολογία των ηλεκτρονικών υπολογιστών και του διαδικτύου. Επιπλέον, ο νόμος περιοριζόταν στην προστασία αποκλειστικά και μόνο των κρατικών υπολογιστικών συστημάτων από τη μη εξουσιοδοτημένη πρόσβαση και που είχε ως άμεσο σκοπό την απόκτηση απόρρητων πληροφοριών που θα μπορούσαν να απειλήσουν τις Η.Π.Α. Η

πρώτη τροποποίηση έγινε δύο χρόνια αργότερα, το 1986, παρά το γεγονός ότι αναφερόταν πάλι σε κρατικά υπολογιστικά συστήματα, με σαφέστερη πλέον τεχνική ορολογία. Στη συνέχεια έγιναν και άλλες αναθεωρήσεις με πιο ουσιαστική αυτή του 1994. Το νομοθετικό πλαίσιο επεκτείνεται και σε υπολογιστές του διαπολιτειακού εμπορίου. Ενέργειες όπως επιθέσεις άρνησης εξυπηρέτησης και διασπορά κακόβουλου λογισμικού κρίνονται παράνομες. Τον Οκτώβριο του 1996, ο νόμος Computer Fraud and Abuse Act συμπληρώνεται με την National Information Infrastructure Protection Act (NIIPA). Είναι μια σειρά νόμων θεσπιζόμενη από την κυβέρνηση των Η.Π.Α. Η σημαντικότερη διάταξη αυτού του νομοθετήματος<sup>40</sup> προβλέπει ότι ο κάθε μεμονωμένος χρήστης, εισερχόμενος σε έναν υπολογιστή προστατευμένο, είναι υπεύθυνος για τις πράξεις του αλλά και για τις συνέπειες αυτών. Στην περίπτωση που η πρόσβαση του είναι εξουσιοδοτημένη ευθύνεται ποινικά μόνο όταν σκοπίμως προσπαθεί να προκαλέσει βλάβη στο θύμα. Οι παραπάνω διατάξεις ισχύουν και σήμερα με κάποιες μικρές τροποποιήσεις και έχουν ενσωματωθεί στο κεφάλαιο 18 παράγραφος 1030 του Ποινικού Κώδικα των Η.Π.Α. (18 U.S.C. §1030 Fraud and Related Activity in Connection with Computers).

### Η ΝΟΜΟΘΕΣΙΑ ΣΤΟ ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ

Ο πρώτος νόμος για το ηλεκτρονικό έγκλημα στο Ηνωμένο Βασίλειο ψηφίστηκε από το Κοινοβούλιο είναι ο «Computer Misuse Act» και αποτέλεσε οδηγό για τις νομοθεσίες πολλών άλλων χωρών όπως του Καναδά και της Ιρλανδίας. Διακρίνονται τρεις βασικές κατηγορίες εγκλημάτων:

1. Μη εξουσιοδοτημένη πρόσβαση με σκοπό διάπραξη αδικημάτων.
2. Μη εξουσιοδοτημένη τροποποίηση πληροφοριών που είναι αποθηκευμένες σε υπολογιστικό σύστημα .
3. Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες που είναι αποθηκευμένες σε υπολογιστές.

Στο «Computer Misuse Act» περιλαμβάνονται και διατάξεις που αναφέρονται στον τρόπο απονομής της δικαιοσύνης αλλά και στη δικαιοδοσία των δικαστηρίων.



Η ΝΟΜΟΘΕΣΙΑ ΣΤΗ ΛΟΙΠΗ ΕΥΡΩΠΗ

Σε ευρωπαϊκό επίπεδο, [21] η πρώτη προσπάθεια νομικής προσέγγισης του ηλεκτρονικού εγκλήματος πραγματοποιήθηκε από το Συμβούλιο της Ευρώπης στο Στρασβούργο το 1976 στις εργασίες του Συνεδρίου για τις Εγκληματολογικές πλευρές του οικονομικού εγκλήματος, όπου για πρώτη φορά παρουσιάζονται οι μορφές του ηλεκτρονικού εγκλήματος. Το 1996 το Συμβούλιο της Ευρώπης πρόβη στην έκδοση τριών Συστάσεων οι οποίες παρά το γεγονός ότι δεν έχουν δεσμευτική ισχύ για τα κράτη- μέλη, παρέχουν κατευθυντήριες γραμμές και υποδείξεις προς την υιοθέτηση μιας συγκεκριμένης συμπεριφοράς. Πρόκειται για τη Σύσταση Νο R (1989) που αναφέρεται στο έγκλημα που διαπράττεται με τον υπολογιστή. Έπεται μια Σύσταση μεγάλης σπουδαιότητας γιατί καθιερώνονται για πρώτη φορά σε διεθνές νομικό κείμενο γενικές οικονομικές αρχές που πρέπει να ισχύουν κατά την έρευνα των ηλεκτρονικών εγκλημάτων. Είναι η Σύσταση Νο R(1995) για τα δικονομικά ζητήματα που σχετίζονται με την τεχνολογία των πληροφοριών. Ακολουθεί η πιο πρόσφατη Σύσταση Νο R(2001) σχετικά με την αυτορρύθμιση σε θέματα διαδικτύου. Οι συστάσεις αυτές αποτέλεσαν συστατικά κομμάτια για την σύνταξη της Σύμβασης στον Κυβερνοχώρο. Η Διεθνής Σύμβαση για τον κυβερνοχώρο, με αντικείμενο την καταπολέμηση της εγκληματικής δραστηριότητας στους κόλπους του διαδικτύου, καταρτίστηκε στις 23/11/2001 στη Βουδαπέστη. Ήδη οι εργασίες για τη δημιουργία αυτής της σύμβασης ξεκίνησαν τον Απρίλιο του 1997, με τη σύσταση μιας επιτροπής ειδικών στον τομέα του ηλεκτρονικού εγκλήματος, με αρχικό χρονοδιάγραμμα περάτωσης τα τέλη του 1999. Λόγω όμως των ιδιαίτερων προβλημάτων που προέκυψαν (ταχύτατη εξέλιξη της τεχνολογίας), οι εργασίες της σύμβασης παρατάθηκαν έως το τέλος του 2000 και τελικά ολοκληρώθηκε ακόμα πιο μετά (Νοέμβριος 2001). Η Σύμβαση έως σήμερα έχει υπογραφεί από τα περισσότερα μέλη του Ευρωπαϊκού Συμβουλίου, καθώς και από τις Η.Π.Α., τον Καναδά, την Ιαπωνία και τη Νότια Αφρική. Ο βασικότερος σκοπός της «Σύμβασης για το Έγκλημα στον κυβερνοχώρο» είναι η εναρμόνιση των εθνικών νομοθεσιών των κρατών-μελών που έχουν υπογράψει, στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Επίσης, με τη σύμβαση παρέχεται το νομοθετικό πλαίσιο του δικονομικού δικαίου που είναι απαραίτητο για τη διερεύνηση και τη δίωξη των εγκλημάτων του κυβερνοχώρου. Με τη σύμβαση αυτή θέτονται οι βάσεις για μια αποτελεσματική συνεργασία για το ηλεκτρονικό έγκλημα.

Η «Σύμβαση για το Έγκλημα στον κυβερνοχώρο» περιλαμβάνει:

1. Διατάξεις ουσιαστικού ποινικού δικαίου:
  - διατάξεις που αναφέρονται σε εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων και συστημάτων,
  - διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές
  - διατάξεις για εγκλήματα σχετικά με το περιεχόμενο,
  - διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων
2. Διατάξεις ποινικού δικονομικού δικαίου:
  - Ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστή
  - Ταχεία διαφύλαξη και γνωστοποίηση διακινουμένων δεδομένων
  - Εντολή παροχής πληροφοριών
  - Έρευνα και κατάσχεση αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή
  - Πραγματικός χρόνος συλλογής διακινουμένων δεδομένων
  - Παγίδευση και υποκλοπή περιεχομένου δεδομένων:
3. Διατάξεις διεθνούς δικαστικής συνεργασίας
  - Έκδοση
  - Γενικές αρχές σχετικές με την αμοιβαία συνδρομή,
  - Παροχή αυθόρμητων πληροφοριών,
  - Ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών
  - Ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων

Σε επόμενη ενότητα της παρούσας εργασίας αναλύεται διεξοδικά η νομοθεσία και οι συγκεκριμένες οδηγίες της Ευρωπαϊκής Ένωσης σχετικά με τα εγκλήματα που εξειδικεύονται στο ηλεκτρονικό εμπόριο.

### 3.2.3. Ισχύουσα Ελληνική Νομοθεσία

Στην ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά στα ηλεκτρονικά εγκλήματα. Παρόλα αυτά έχουν γίνει πληθώρα προσπαθειών ώστε να εναρμονιστεί η ελληνική νομοθεσία σύμφωνα με τις ευρωπαϊκές επιταγές.

- Ο Ν.1805/88 αφορά εγκλήματα που διαπράττονται με υπολογιστή και έχει τροποποιήσει τις σχετικές διατάξεις του Ποινικού Κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) οι οποίες σχετίζονται με τη διάπραξη εγκλημάτων με τη χρήση υπολογιστή.
- Το άρθρο 370Α αναφέρεται στην παραβίαση του απορρήτου των τηλεπικοινωνιών και το άρθρο 348Α στην πορνογραφία ανηλίκων. Τα παραπάνω άρθρα του Ποινικού Κώδικα δεν είναι αρκετά για να καλύψουν τις ανάγκες δίωξης της ηλεκτρονικής εγκληματικότητας, η οποία παράλληλα πάντα με τις τεχνολογικές εξελίξεις εμφανίζεται με νέες μορφές. Άλλωστε στα συγκεκριμένα άρθρα δεν έχει προβλεφτεί η ύπαρξη του διαδικτύου το οποίο πλέον δίνει νέες διαστάσεις στο ζήτημα. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν με βάση την ισχύουσα στην Ελλάδα νομοθεσία. Αυτό το κενό βέβαια αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, εφόσον ο εικονικός κόσμος του διαδικτύου θεωρηθεί απλά ως ένα ακόμα μέσο για τη διάπραξη εγκλημάτων.
- Ακόμα, διατάξεις που σχετίζονται με το ηλεκτρονικό έγκλημα περιλαμβάνονται στο Π.Δ. 131/2003 που αναφέρεται στην ανεπιθύμητη αλληλογραφία (spamming) και στην ευθύνη των παρεχόμενων υπηρεσιών διαδικτύου για πράξεις των χρηστών που είναι συνδρομητές τους. Το συγκεκριμένο Π.Δ. θεσπίστηκε σε εφαρμογή της κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο.
- Επίσης ο Ν.2867/2000 για την «οργάνωση και λειτουργία του τομέα των Τηλεπικοινωνιών», οι Ν.2774/1999 και Ν.2472/1997 «περί προσωπικών δεδομένων» και ο Ν.2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» σχετίζονται με κάποιες πτυχές του ηλεκτρονικού εγκλήματος. Ο τελευταίος μάλιστα αντικαταστήθηκε με τον Ν.3115/2003 και αναφέρεται στην ίδρυση της «Εθνικής Επιτροπής του Απορρήτου των Επικοινωνιών». Στόχο έχει την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε τρόπο και την τήρηση των όρων και διαδικασιών άρσης του απορρήτου.



### 3.3 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΣΥΣΤΑΣΗΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΕΙΚΟΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Στην παραπάνω ανάλυση, αναφέρθηκε το σύνολο της νομοθεσίας που διέπει παραβάσεις που εμπίπτουν στο ηλεκτρονικό έγκλημα καθώς επίσης και το σύνολο των κυρώσεων που προβλέπει ο νόμος για κάθε περίπτωση ξεχωριστά. Πληθώρα ηλεκτρονικών εγκλημάτων αναπτύσσονται και σε ηλεκτρονικές επιχειρήσεις. Η παρακάτω ανάλυση θα επικεντρωθεί στην παράθεση του νομικού πλαισίου για την σύσταση αλλά και την λειτουργία εικονικών επιχειρήσεων στην Ελλάδα. Θα παρατεθούν ομοιότητες και διαφορές αυτού του είδους επιχειρήσεων με το υπόλοιπο σύνολο επιχειρήσεων που αναπτύσσονται στον ελλαδικό χώρο.

#### 3.3.1 Νομοθεσία Σύστασης Ηλεκτρονικής Επιχείρησης

Όσον αφορά την σχετική νομοθεσία σύστασης ενός τέτοιου είδους επιχείρησης, οι μελλοντικοί επιχειρηματίες μπορούν να προβούν στην δημιουργία της, χωρίς διαφορετικές διαδικασίες από μια κοινή επιχείρηση. Αυτό επιφέρει αρκετά πλεονεκτήματα όσον αφορά την ταχύτητα δημιουργίας της, χωρίς περαιτέρω γραφειοκρατικές διαδικασίες, αλλά επίσης και στην ασφάλεια της υπάρχουσας γνώσης, μιας και δεν διαφέρει επί της ουσίας με του άλλου είδους επιχειρήσεις. [2]

Σε ένα πρώτο στάδιο θα πρέπει να προσδιοριστεί η Νομική Μορφή της επιχείρησης. Μπορεί είτε να είναι Ατομική είτε Εταιρική. Στην περίπτωση της εταιρικής μορφής επιχείρησης, μπορεί να διακριθεί σε 4 υποκατηγορίες που αναλυθούν συνοπτικά παρακάτω. Το σημαντικό συμπέρασμα που θα ανακύψει κι από την ανάλυση είναι πως η νομική μορφή των ηλεκτρονικών επιχειρήσεων είναι ακριβώς ίδια με τις φυσικές επιχειρήσεις.

**Ατομική επιχείρηση:** Η μορφή αυτή είναι ιδιαίτερα διαδεδομένη. Κύριο πλεονέκτημά της είναι η μεγάλη ευελιξία ως προς τις επιχειρηματικές αποφάσεις που αφορούν στο είδος της δραστηριότητας, στην επιλογή των τεχνικών μεθόδων και, ως ένα βαθμό, στο μέγεθος της παραγωγής. Τα πλεονεκτήματα αυτά είναι ουσιώδη, κυρίως για τις μικρές και μέσου μεγέθους αγροτικές, βιοτεχνικές και εμπορικές επιχειρήσεις, στις οποίες η προσωπική επίβλεψη και πρωτοβουλία είναι μεγάλης σημασίας. Όταν όμως το είδος

της δραστηριότητας επιβάλλει την ανάπτυξη μεγάλου μεγέθους, τότε η εταιρική μορφή της επιχείρησης είναι συχνά η πιο κατάλληλη.

**Εταιρική επιχείρηση:** Η εταιρική επιχείρηση ανήκει σε δύο ή περισσότερα άτομα, τους εταίρους, που συνδέονται με ειδική σχέση μεταξύ τους, την εταιρική, που καθορίζεται ανάλογα με το είδος της εταιρείας. Βασικές μορφές της εταιρικής επιχείρησης είναι: ομόρρυθμη, ετερόρρυθμη, ανώνυμη εταιρεία και εταιρεία περιορισμένης ευθύνης.

Στις ομόρρυθμες (Ο.Ε.) όλοι οι εταίροι είναι αλληλέγγυα υπεύθυνοι με όλη τους την περιουσία για τη δραστηριότητα και τα χρέη της εταιρείας. Επιπλέον υπόκεινται σε προσωπική κράτηση όταν βρίσκονται σε αδυναμία να εξοφλήσουν τους πιστωτές τους.

Στις ετερόρρυθμες (Ε.Ε.) ένας τουλάχιστον εταίρος είναι υπεύθυνος με όλη του την περιουσία για τα χρέη της εταιρείας και υπόκειται σε προσωπική κράτηση για τη μη εξόφλησή τους.

Στις ανώνυμες εταιρείες (Α.Ε.), που είναι μετοχικές, κάθε εταίρος (μέτοχος) είναι υπεύθυνος μόνο για το ποσοστό συμμετοχής του, δηλαδή για τον αριθμό των μετοχών τις οποίες διαθέτει. Ο μέτοχος συμμετέχει στην εκλογή της διοίκησης της εταιρείας, στη διαμόρφωση των γενικών αρχών της πολιτικής και στα κέρδη, ανάλογα με τον αριθμό των μετοχών που διαθέτει. Στη γενική συνέλευση των μετόχων κάθε μέτοχος διαθέτει τόσους ψήφους όσες είναι οι μετοχές που κατέχει. Σε περίπτωση ζημιών ή πτωχεύσεως είναι υπεύθυνος μέχρι του ποσού που έχει καταβάλει για τις μετοχές του, δηλαδή, στη χειρότερη περίπτωση, οι μετοχές του χάνουν τελείως την αξία τους.

Οι εταιρείες περιορισμένης ευθύνης (Ε.Π.Ε.) είναι ένας ενδιάμεσος τύπος μεταξύ των προσωπικών εταιρειών (Ο.Ε. και Ε.Ε.) και της ανώνυμης εταιρείας. Το κύριο γνώρισμα των εταιρειών αυτών είναι το μικρό κεφάλαιο που χρειάζεται για τη σύστασή τους και η περιορισμένη ευθύνη των εταίρων τους μέχρι το ύψος του κατατεθειμένου εταιρικού κεφαλαίου, όπως ακριβώς συμβαίνει και με τις ανώνυμες εταιρείες, σε αντίθεση με τις προσωπικές εταιρείες. [20]

Στο στάδιο της σύστασης μιας επιχείρησης, ο κάθε τύπος έχει τις δικές του γραφειοκρατικές διαδικασίες ώστε να έγκειται νομότυπα σύμφωνα με τα άρθρα του Εμπορικού Νόμου. Οι διαφορές ανά τύπο είναι σημαντικές και κυρίως έγκεινται στην σύσταση του κεφαλαίου αλλά και στον καθορισμό του προσώπου αναλαμβάνει τον κίνδυνο μιας επικείμενης πτώχευσης της επιχείρησης. Παρακάτω θα αναλυθούν ενδεικτικά οι προϋποθέσεις σύστασης του κάθε τύπου καθώς και τα βασικά χαρακτηριστικά του.

#### Ο.Ε.

Για την ίδρυση ομόρρυθμης εταιρείας πρέπει να συμπράξουν δύο τουλάχιστον μέρη ή κατά την έκφραση του νόμου υποχρεούνται αμοιβαίως στην επιδίωξη κοινού σκοπού (άρθρο 741, Αστικού Κώδικα).

Τα ιδρυτικά μέλη της ομόρρυθμης εταιρείας μπορεί να είναι φυσικά ή νομικά πρόσωπα. Τα φυσικά πρόσωπα πρέπει να έχουν συμπληρώσει το δέκατο όγδοο (18ο) έτος της ηλικίας τους (σύμφωνα με το άρθρο 127 του Αστικού Κώδικα, όπως τροποποιήθηκε με το άρθρο 3 του Ν.1329/83). Συμμετοχή ανηλίκου στην ίδρυση προσωπικής εταιρείας επιτρέπεται μόνο κατόπιν δικαστικής άδειας. Τα βασικά χαρακτηριστικά της είναι τα εξής:

1. Οι εταίροι της ομόρρυθμης εταιρείας ευθύνονται με ολόκληρη την περιουσία τους για όλες τις υποχρεώσεις της εταιρείας, με αλληλέγγυα ευθύνη τους.
2. Με τη λύση της εταιρείας δεν παύει η ευθύνη των εταίρων για τυχόν υπάρχοντα χρέη της εταιρείας.
3. Η ομόρρυθμη εταιρεία δεν χρειάζεται συμβολαιογραφικό έγγραφο για την κατάρτισή της, αντιθέτως αρκεί ένα ιδιωτικό συμφωνητικό.

#### Ε.Ε.

Για την ίδρυση ετερόρρυθμης εταιρείας πρέπει να συμπράξουν δύο τουλάχιστον μέρη ή κατά την έκφραση του νόμου υποχρεούνται αμοιβαίως στην επιδίωξη κοινού σκοπού (άρθρο 741, Αστικού Κώδικα).



Τα ιδρυτικά μέλη της ετερόρρυθμης εταιρείας μπορεί να είναι φυσικά ή νομικά πρόσωπα. Τα φυσικά πρόσωπα πρέπει να έχουν συμπληρώσει το δέκατο όγδοο (18ο) έτος της ηλικίας τους (σύμφωνα με το άρθρο 127 του Αστικού Κώδικα, όπως τροποποιήθηκε με το άρθρο 3 του Ν.1329/83). Συμμετοχή ανηλίκου στην ίδρυση προσωπικής εταιρείας επιτρέπεται μόνο κατόπιν δικαστικής άδειας. Τα βασικά χαρακτηριστικά της είναι τα εξής:

1. Διαίρεση των εταίρων της ετερόρρυθμης εταιρείας σε δύο κατηγορίες: τους ομόρρυθμους και τους ετερόρρυθμους. Η ευθύνη των ομόρρυθμων εταίρων απέναντι στους πιστωτές της εταιρείας είναι αλληλέγγυα και απεριόριστη. Η ευθύνη των ετερόρρυθμων εταίρων είναι περιορισμένη και δεν μπορεί να υπερβεί το ποσό της εισφοράς του στην εταιρεία.
2. Η ετερόρρυθμη εταιρεία δεν χρειάζεται συμβολαιογραφικό έγγραφο για την κατάρτισή της, αντιθέτως αρκεί ένα ιδιωτικό συμφωνητικό.

#### Α.Ε.

Για την ίδρυση ανώνυμης εταιρείας πρέπει να συμπράξουν δύο τουλάχιστον μέλη ή κατά την έκφραση του νόμου το κεφάλαιο αυτής πρέπει να αναληφθεί από δύο τουλάχιστον ιδρυτές (άρθρο 8, Κ.Ν. 2190/20). Η αναλογία συμμετοχής των ιδρυτών δεν ορίζεται.

Τα ιδρυτικά μέλη της ανώνυμης εταιρείας μπορεί να είναι φυσικά ή νομικά πρόσωπα. Τα φυσικά πρόσωπα πρέπει να έχουν συμπληρώσει το δέκατο όγδοο (18ο) έτος της ηλικίας τους (σύμφωνα με το άρθρο 127 του Αστικού Κώδικα, όπως τροποποιήθηκε με το άρθρο 3 του Ν.1329/83). Συμμετοχή ανηλίκου στην ίδρυση ανώνυμης εταιρείας επιτρέπεται μόνο κατόπιν δικαστικής άδειας.

Κατώτερο όριο γενικώς για την ίδρυση Ανώνυμης Εταιρείας είναι τα είκοσι εκατομμύρια (20.000.000) δρχ. (άρθρο 8, παρ.2 Κ.Ν. 2190/20, όπως αντικαταστάθηκε από το άρθρο 11 παρ.1 του Ν.2579/98), ενώ υπάρχουν περιπτώσεις που ο νόμος απαιτεί πολύ μεγαλύτερο ποσό κεφαλαίου. Π.χ. οι προερχόμενες από συγχώνευση ή μετατροπή κατά τις διατάξεις του Ν.Δ. 1297/72 και του Ν. 2166/93 ανώνυμες εταιρείες πρέπει να έχουν ελάχιστο ύψος μετοχικού κεφαλαίου 100.000.000 δρχ. Σύμφωνα με το

N.2842/2000, το ελάχιστο μετοχικό κεφάλαιο για την ίδρυση Α.Ε. από 1/1/2002 ορίζεται στα 60.000 Euro (20.445.000 δρχ.). Για τις ήδη υπάρχουσες εταιρείες προβλέπεται η δυνατότητα να συνεχίσουν να λειτουργούν με 2.5% χαμηλότερο κεφάλαιο (δηλ. 58.500 Euro). Τα βασικά χαρακτηριστικά της είναι τα εξής:

1. Το μεγάλο σχετικά κεφάλαιο που απαιτείται για την ίδρυσή της
2. Η διαίρεση του κεφαλαίου σε ίσα μερίδια, που ενσωματώνονται σε έγγραφα, τις μετοχές
3. Οι αυστηροί όροι δημοσιότητας κατά την ίδρυσή της αλλά και καθ' όλη τη διάρκεια της ζωής της
4. Η μακρά διάρκειά της (συνήθως 50 ετών)
5. Η περιορισμένη ευθύνη των μετόχων
6. Η λήψη αποφάσεων κατά πλειοψηφία
7. Η ύπαρξη δύο οργάνων, ήτοι της Γενικής Συνέλευσης των μετόχων και του Διοικητικού Συμβουλίου.

#### Ε.Π.Ε.

Σύμφωνα με το άρθρο 3 του Ν.3190/1955, η εταιρεία περιορισμένης ευθύνης είναι εμπορική, έστω και αν ο σκοπός αυτής δεν είναι εμπορική επιχείρηση, ωστόσο απαγορεύεται η άσκηση ορισμένων δραστηριοτήτων, όπως τραπεζικές, ασφαλιστικές, χρηματιστηριακές, διαχείριση χαρτοφυλακίου αξιόγραφων, διαχείριση αμοιβαίων κεφαλαίων, χρηματοδοτική μίσθωση, πρακτορεία επιχειρηματικών απαιτήσεων, προώθηση και υλοποίηση επενδύσεων υψηλής τεχνολογίας (μόνο venture capital) και αθλητικές δραστηριότητες.

Για την ίδρυση εταιρείας περιορισμένης ευθύνης απαιτείται εταιρικό κεφάλαιο το οποίο δεν μπορεί να είναι μικρότερο των 6.000.000 δρχ., ενώ θα πρέπει να έχει καταβληθεί ολόκληρο κατά την υπογραφή του Καταστατικού (άρθρο 4 παρ.1 του Ν.3190/1955 όπως αντικαταστάθηκε με την παρ.3 του αρθρ.11 του Ν.2579/1998). Το μισό τουλάχιστον του ποσού αυτού πρέπει να είναι καταβλημένο σε μετρητά. Περιορισμός ως προς το ύψος του κεφαλαίου δεν υπάρχει.

Σύμφωνα με το N.2842/2000, το ελάχιστο κεφάλαιο για την ίδρυση Ε.Π.Ε. από 1/1/2002 ορίζεται στα 18.000 Euro (6.133.500 δρχ). Για τις ήδη υπάρχουσες εταιρείες προβλέπεται η δυνατότητα να συνεχίσουν να λειτουργούν με 2,5% χαμηλότερο κεφάλαιο (δηλ. 17.550 Euro).

Σύμφωνα με το άρθρο 43α του Ν.3190/1955 που τροποποιήθηκε με το άρθρο 2 του Π.Δ. 279/1993, Εταιρεία Περιορισμένης Ευθύνης μπορεί να συστήσει και ένα μόνο πρόσωπο ή μία ήδη συνιστάμενη ΕΠΕ να μετατραπεί σε μονοπρόσωπη. Ωστόσο, η μονοπρόσωπη ΕΠΕ είναι άκυρη, αν ο εταίρος (φυσικό ή νομικό πρόσωπο) που τη συνέστησε είναι και μοναδικός εταίρος σε άλλη μονοπρόσωπη ΕΠΕ, ή αν έχει συσταθεί από άλλη μονοπρόσωπη ΕΠΕ. Τα βασικά χαρακτηριστικά της είναι τα εξής:

1. Η διαίρεση του κεφαλαίου σε “μερίδες συμμετοχής” κάθε μία εκ των οποίων αποτελείται από εταιρικά μερίδια, από τα οποία το καθένα δεν μπορεί να είναι μικρότερο των 10.000 δρχ.
2. Συγκεκριμένοι όροι δημοσιότητας κατά την ίδρυσή της αλλά και καθ’ όλη τη διάρκεια της ζωής της
3. Η ορισμένη διάρκειά της (αν και η παράλειψη αναγραφής της διάρκειας δεν αποτελεί λόγο ακυρότητας της εταιρείας)
4. Η περιορισμένη ευθύνη των εταίρων
5. Η λήψη αποφάσεων κατά πλειοψηφία πλέον του μισού του όλου αριθμού των εταίρων, που εκπροσωπούν πλέον του μισού του όλου εταιρικού κεφαλαίου
6. Η ύπαρξη δύο οργάνων, ήτοι της Γενικής Συνέλευσης των εταίρων και του διαχειριστή ή διαχειριστών.

Ξεπερνώντας το στάδιο της επιλογής του τύπου της ηλεκτρονικής επιχείρησης που θα καλεστεί ο ιδιοκτήτης να επιλέξει, έπονται μια πληθώρα από διοικητικές διαδικασίες. Αρχικά αφού επιλεγεί η έδρα της επιχείρησης, ακόμα και της ηλεκτρονικής, τα φυσικά πρόσωπα ή οι εταίροι – μέλη των νομικών προσώπων πρέπει να εγγραφούν στο Επιμελητήριο της περιοχής όπου ορίζεται η έδρα της επιχείρησης. Αυτό αποτελεί ένα από τα σημαντικά βήματα της σύστασης για τον λόγο ότι σε περίπτωση εγγραφής στον ασφαλιστικό φορέα των εμπόρων, επαγγελματικών και βιοτεχνών (ΟΑΕΕ) απαιτούνται και στοιχεία προσδιορισμού της έδρας της επιχείρησης.



Στην συνέχεια κάθε εργοδότης που απασχολεί προσωπικό, υπάγεται στην ασφάλιση του ΙΚΑ – ΕΤΑΜ κι υποχρεούται να απογράφεται και στο Μητρώο Εργοδοτών του ΙΚΑ – ΕΤΑΜ.

Τέλος, στο στάδιο σύστασης μιας επιχείρησης, αποτελεί η υπαγωγή της εταιρείας στο φορολογικό μητρώο του ΦΠΑ που αυτό μπορεί να γίνει στην αρμόδια εφορία (ΔΟΥ) ανάλογα με την έδρα της επιχείρησης. [20]

### 3.3.2. Νομοθεσία Λειτουργίας Ηλεκτρονικής Επιχείρησης

Από την παραπάνω ανάλυση καθίσταται σαφές πως μια ηλεκτρονική επιχείρηση, τουλάχιστον ως προς την σύσταση, δεν διαφέρει καθόλου από οποιαδήποτε άλλη επιχείρηση που φέρει φυσική υπόσταση όπως είναι ένας χώρος εγκατάστασης. Παρόμοιες καταστάσεις επικρατούν όμως και στην απαραίτητη νομοθεσία για την λειτουργία μιας ηλεκτρονικής επιχείρησης. Όσοι νόμοι διέπουν τις υπόλοιπες επιχειρήσεις ως προς την ορθότητα και την νομιμότητα λειτουργίας τους, οι ίδιοι νόμοι διέπουν και τις ηλεκτρονικές επιχειρήσεις στην ελληνική οικονομία. Η μοναδική διαφοροποίηση έγκειται στο ότι οι ηλεκτρονικές επιχειρήσεις ρυθμίζονται κι από νόμους που αφορούν την τεχνολογία αλλά και την προστασία των καταναλωτών από τα ηλεκτρονικά εγκλήματα που αναλύθηκαν παραπάνω. Στην παρούσα ενότητα θα αναλυθούν εκείνοι οι επιπρόσθετοι νόμοι που ρυθμίζουν τις ηλεκτρονικές επιχειρήσεις.

#### Αρχή Προστασίας Προσωπικών Δεδομένων

Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο. Η αρχή αυτή, που ιδρύθηκε το 1997 και ονομάστηκε Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ) έχει ποικίλες αρμοδιότητες μεταξύ των οποίων είναι να εκδίδει οδηγίες και αποφάσεις και να γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Οι σημαντικότερες Οδηγίες της ΑΠΠΔ είναι :

☛ Η Οδηγία 1122/2000 για τα κλειστά κυκλώματα τηλεόρασης και

- ☛ Η Οδηγία 115/2001 για την επεξεργασία δεδομένων των εργαζομένων όπου επειδή αποτελεί και την ουσία της συγκεκριμένης εργασίας παρατίθεται στο Παράρτημα Α.

Οι σπουδαιότερες αποφάσεις της ΑΠΠΔ, που έχουν φυσικά συνάφεια με το αντικείμενο της συγκεκριμένης εργασίας, είναι οι εξής:

- ☛ Η Απόφαση 50/2000 σχετικά με τους όρους για την νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της άμεσης εμπορίας ή διαφήμισης και της διαπίστωσης πιστοληπτικής ικανότητας.
- ☛ Η Απόφαση 120/2001 για την επεξεργασία Προσωπικών Δεδομένων σχετικά την παροχή υπηρεσιών καρτοκινητής τηλεφωνίας
- ☛ Η Απόφαση 1469/2000 για τη συλλογή προσωπικών δεδομένων από εταιρείες τηλεπικοινωνιακών δραστηριοτήτων.
- ☛ Η Απόφαση 147/2001 για την χρήση ευαίσθητων δεδομένων ενώπιον δικαστηρίου
- ☛ Η Απόφαση 8/2003 σχετικά με την πρόσβαση τρίτου σε δεδομένα εταιρείας κινητής τηλεφωνίας για άσκηση δικαιώματος υπεράσπισης ενώπιον δικαστηρίου.

Οι πιο άξιες προσοχής, τέλος, γνωμοδοτήσεις της ΑΠΠΔ είναι:

- ☛ Η Γνωμοδότηση 71/2002 σχετικά με την επεξεργασία προσωπικών δεδομένων στην αυτόματη αναγνώριση της ταυτότητας του συνδρομητή καλούσας γραμμής σε ψηφιακά δίκτυα ενοποιημένων υπηρεσιών (ISDN),
- ☛ Η Γνωμοδότηση 78/2002 για τις προϋποθέσεις διασταύρωσης προσωπικών δεδομένων στο χώρο της σταθερής τηλεφωνίας,
- ☛ Η Γνωμοδότηση 86/2001 σχετικά με την είσοδο και παραμονή αλλοδαπών στην ελληνική επικράτεια,
- ☛ Η Γνωμοδότηση 15/2001 σχετικά με την ανάλυση γενετικού υλικού για σκοπούς εξιχνίασης εγκλημάτων και ποινικής δίωξης.

Αρχή Διασφάλισης του Απορρήτου των Τηλεπικοινωνιών

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) προβλέπεται από το Ν.3115/2003. Είναι ανεξάρτητη αρχή με διοικητική αυτοτέλεια και έχει ως σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στο πλαίσιο αυτό, η Α.Δ.Α.Ε. είναι η αρμόδια αρχή για τον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. Η δράση της διέπεται πάντοτε από τις αρχές της διαφάνειας, της αντικειμενικότητας και της αμεροληψίας.

Η Α.Δ.Α.Ε. αποτελείται από 7 μέλη και ισάριθμα αναπληρωματικά, τα οποία απολαμβάνουν κατά την άσκηση των καθηκόντων τους πλήρη προσωπική και λειτουργική ανεξαρτησία. Ωστόσο, έχουν καθήκον εχεμύθειας, το οποίο υφίσταται και μετά την αποχώρησή τους. Τα πρόσωπα που θα γίνουν μέλη της Α.Δ.Α.Ε. επιλέγονται από τη Βουλή και πρέπει να τυγχάνουν ευρείας κοινωνικής αποδοχής και να διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στο νομικό τομέα ή στον τεχνικό τομέα των επικοινωνιών.

Η Α.Δ.Α.Ε. στο πλαίσιο εκπλήρωσης του σκοπού της, μπορεί:

- ☛ Να διενεργεί απευαγγέλτως ή έπειτα από καταγγελία τακτικούς ή έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημόσιων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.
- ☛ Να καλεί σε ακρόαση τις διοικήσεις, τους νόμιμους εκπροσώπους και τους υπαλλήλους των ως άνω δημοσίων υπηρεσιών ή ιδιωτικών εταιριών.
- ☛ Να συνεργάζεται με άλλες αρχές της χώρας, με αντίστοιχες αρχές άλλων κρατών και με ευρωπαϊκούς ή διεθνείς οργανισμούς.
- ☛ Να γνωμοδοτεί και να απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.



Τα μέλη και το προσωπικό της Α.Δ.Α.Ε., για να διαπιστώσουν παράβαση της νομοθεσίας για την προστασία του απορρήτου, μπορούν να ελέγχουν τα βιβλία και στοιχεία των ελεγχόμενων υπηρεσιών, οργανισμών και επιχειρήσεων, καθώς και πάσης φύσεως αρχεία, βιβλία, στοιχεία και λοιπά έγγραφα των προσώπων που ελέγχουν. Επιπλέον, έχουν δικαίωμα να ενεργούν έρευνες στα γραφεία και τις λοιπές εγκαταστάσεις των ελεγχόμενων και να διενεργούν ένορκες και μη καταθέσεις, με την επιφύλαξη του επαγγελματικού απορρήτου των εξεταζόμενων προσώπων.

Σε περίπτωση που κατά τον έλεγχο διαπιστωθεί παραβίαση του απορρήτου, τα μέλη της Α.Δ.Α.Ε. μπορούν να κατασχέσουν τα μέσα με τα οποία πραγματοποιείται η παραβίαση αυτή, ενώ παράλληλα καταστρέφουν τις πληροφορίες, τα δεδομένα ή τα στοιχεία που αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών. Για τα μέσα που κατάσχονται, ορίζεται μεσεγγυούχος ωστόσο αποφανθούν τα αρμόδια δικαστήρια. [23]

### 3.3.3. Επιμέρους Δεσμεύσεις για Ηλεκτρονικές Επιχειρήσεις

Η συλλογή και επεξεργασία προσωπικών δεδομένων εξελίσσεται σε συστατικό στοιχείο των ενδοδικτυακών συναλλαγών. Προσωπικά δεδομένα συλλέγονται συνήθως ήδη κατά την αρχική φάση σύνδεσης του ενδιαφερόμενου καταναλωτή με το δικτυακό χώρο της επιχείρησης, συχνά μέσω εντύπων που συμπληρώνει ψηφιακά ο πλοηγός-αγοραστής. Η συλλογή δεδομένων, συνήθως με απώτερο σκοπό τη δημιουργία του προφίλ του «πελάτη», γίνεται συχνά και με άλλους τρόπους, όπως εγκατάσταση cookies, τεχνικές εξόρυξης δεδομένων κλπ.. Η χρήση τέτοιων τεχνικών παρουσιάζεται συνήθως ως αναγκαιότητα για τη διαμόρφωση των πολιτικών και της στρατηγικής των επιχειρήσεων.

Ωστόσο, όσοι δραστηριοποιούνται στο πεδίο των ηλεκτρονικών συναλλαγών οφείλουν να γνωρίζουν πως ό,τι είναι τεχνικά δυνατό δεν είναι αυτονόητα και νόμιμο ή θεμιτό. Η συλλογή και επεξεργασία προσωπικών δεδομένων στο πλαίσιο του ηλεκτρονικού επιχειρείν υπόκειται στις ρυθμίσεις, τις προϋποθέσεις και απαγορεύσεις των νόμων 2472/97 για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων και 2774/99 για την προστασία προσωπικών δεδομένων στον

τηλεπικοινωνιακό τομέα και τις επιμέρους ερμηνευτικές Οδηγίες που έχει εκδώσει η Αρχή Προστασίας Προσωπικών Δεδομένων. [22]

Ένα κρίσιμο στοιχείο είναι ότι η συλλογή και επεξεργασία προσωπικών δεδομένων επιτρέπεται καταρχήν μόνο με συγκατάθεση του χρήστη-πελάτη ή στο πλαίσιο της εκπλήρωσης μιας σύμβασης που ήδη συνδέει την επιχείρηση με αυτόν. Σε άλλη περίπτωση η συλλογή τέτοιων δεδομένων είναι νόμιμη εφόσον αυτά προέρχονται από καταλόγους και πηγές δημόσια προσβάσιμες που απευθύνονται στο ευρύ κοινό καθώς και προηγούμενες συναλλακτικές επαφές στο πλαίσιο συναφών σκοπών.

Τα προσωπικά δεδομένα των αντισυμβαλλόμενων ή των ενδιαφερομένων επισκεπτών των ιστοσελίδων μιας επιχείρησης πρέπει να συλλέγονται με τρόπο νόμιμο, θεμιτό και διαφανή. Όπως τονίζεται στην νέα Οδηγία 2002/58/ΕΚ «σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» λογισμικό παρακολούθησης, δικτυακοί «κοριοί», κρυφά αναγνωριστικά στοιχεία και άλλες παρόμοιες διατάξεις που μπορούν να εισέλθουν στο τερματικό του χρήστη εν αγνοία του με σκοπό την πρόσβαση σε πληροφορίες, την αποθήκευση αθέατων πληροφοριών ή την ανίχνευση των δραστηριοτήτων του χρήστη, συνιστούν ενδεχόμενη σοβαρή παραβίαση της ιδιωτικής ζωής του χρήστη. Η χρησιμοποίηση τέτοιων διατάξεων θα πρέπει να επιτρέπεται μόνο για θεμιτούς σκοπούς και εφόσον τα γνωρίζουν οι χρήστες αυτοί.

Η ενημέρωση των χρηστών κατά το στάδιο της συλλογής των προσωπικών δεδομένων που τους αφορούν, έχει κεφαλαίωδη σημασία για την προστασία των προσωπικών δεδομένων αλλά και για τη νομιμότητα της επεξεργασίας τους και δε συνιστά μόνο αυτοτελή υποχρέωση που έχει εισαγάγει η νομοθεσία για την προστασία προσωπικών δεδομένων, αλλά αποτελεί ταυτοχρόνως και προϋπόθεση για την έγκυρη συγκατάθεση του χρήστη. Η συγκατάθεση στην ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων νοείται ως «ενημερωμένη συγκατάθεση» (informed consent).

Η ενημέρωση πρέπει να αναφέρεται καταρχήν στο γεγονός καθαυτό της συλλογής και επεξεργασίας προσωπικών δεδομένων και τη βάση στην οποία αυτή θεμελιώνεται (συγκατάθεση, σύμβαση). Οποσδήποτε πρέπει να περιλαμβάνει την (online και offline) ταυτότητα αυτού που συλλέγει τα δεδομένα, το σκοπό για τον οποίο

συλλέγονται τα δεδομένα, καθώς και πληροφορίες για τους τυχόν περαιτέρω αποδέκτες των δεδομένων. Είναι επίσης αναγκαίο και σκόπιμο να ενημερώνονται οι επισκέπτες/συναλλασσόμενοι για τα δικαιώματα που τους παρέχει η νομοθεσία για την προστασία προσωπικών δεδομένων (δικαίωμα πρόσβασης, διόρθωσης, αντίταξης κλπ.).

Εφόσον οι επιχειρήσεις έχουν εκπονήσει πολιτικές Ασφαλείας της ιδιωτικότητας είναι χρήσιμο και εξυπηρετεί ταυτόχρονα τους σκοπούς της ενημέρωσης, να ανακοινώνονται σε εμφανή σημεία των αντίστοιχων ηλεκτρονικών σελίδων. Είναι αυτονόητο ότι αυτές οι πολιτικές πρέπει να είναι σύμφωνες και να εναρμονίζονται με το γράμμα και το πνεύμα της νομοθεσίας για την προστασία προσωπικών δεδομένων. Η ενημέρωση είναι απαραίτητη και στην περίπτωση της εγκατάστασης «cookies» ή άλλων συναφών διατάξεων. Όταν οι διατάξεις αυτές προορίζονται για σκοπούς που η έννομη τάξη κρίνει ως θεμιτούς, η χρησιμοποίησή τους επιτρέπεται μόνο υπό τον όρον ότι παρέχονται στους χρήστες σαφείς και ακριβείς πληροφορίες για τον προορισμό των «cookies» ή τυχόν ανάλογων διατάξεων, ώστε να εξασφαλίζεται ότι είναι εν γνώσει του χρήστη οι πληροφορίες που αποθηκεύονται στον τερματικό υπολογιστή που χρησιμοποιεί και να παρέχεται στους χρήστες η δυνατότητα να αρνηθούν την αποθήκευση «cookies» ή παρόμοιων διατάξεων στον τερματικό τους εξοπλισμό. Οι τρόποι της παροχής πληροφοριών, της παροχής του δικαιώματος άρνησης ή αίτησης συγκατάθεσης θα πρέπει να είναι όσο το δυνατόν πιο προσιτοί για το χρήστη.

### **3.3.4. Παραβάσεις της Νομοθεσίας περί Ασφαλείας Δικτύων και Ποινές**

Η τήρηση των επιταγών και απαγορεύσεων που σχετίζονται με την επεξεργασία αλλά και την ασφάλεια των προσωπικών δεδομένων επιβάλλεται από την οικεία νομοθεσία. Τυχόν παράβαση των υποχρεώσεων αυτών για προστασία και ασφάλεια των δεδομένων ενδέχεται να έχει ως αποτέλεσμα την επιβολή διοικητικών κυρώσεων από την Αρχή Προστασίας Προσωπικών Δεδομένων (όπως 11 πρόστιμα, αναστολή επεξεργασίας, καταστροφή αρχείων κλπ.) ή/και τη γέννηση αξιώσεων και υποχρεώσεων αποζημίωσης ή χρηματικής ικανοποίησης των προσώπων που θίγονται από τις παραβάσεις των νομοθετικών διατάξεων και των υποχρεώσεων ασφαλείας.

Όποιος παραβιάζει με οποιονδήποτε τρόπο το απόρρητο των επικοινωνιών ή τους όρους και τη διαδικασία άρσης αυτού, τιμωρείται με ποινή φυλάκισης



τουλάχιστον ενός έτους και χρηματική ποινή από 15.000 έως 60.000 ευρώ. Σε περίπτωση που ο παραβάτης ανήκει στο προσωπικό υπηρεσίας, οργανισμού, νομικού προσώπου ή επιχείρησης που ασχολείται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση ή την επικοινωνία, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον 2 ετών και η χρηματική ποινή τουλάχιστον 30.000 ευρώ.

Συγκεκριμένες παραβάσεις συνιστούν μάλιστα ποινικά αδικήματα και επισύρουν και ποινικές κυρώσεις. Ωστόσο, η μεγαλύτερη κύρωση είναι η δυσπιστία των συναλλασσομένων. Πολλές πρόσφατες μελέτες έχουν αποδείξει ότι πολλοί άνθρωποι απέχουν από ηλεκτρονικές συναλλαγές από φόβο για τη μεταχείριση και την τύχη των προσωπικών τους δεδομένων. Η επένδυση σε τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy Enhancing Technologies), η ύπαρξη, τήρηση και διαφήμιση πολιτικών για την προστασία της ιδιωτικότητας δεν είναι απλά συμμόρφωση προς το νόμο. Είναι ανταγωνιστικό πλεονέκτημα. Είναι προϋπόθεση για να αποκτηθεί η εμπιστοσύνη των καταναλωτών.

Εκτός από την Ελληνική δικαιοσύνη και την Αρχή Προστασίας Προσωπικών Δεδομένων που επιβάλλει κυρώσεις σε περιπτώσεις άρσης του απορρήτου στην επικοινωνία μέσω τηλεπικοινωνιακών δικτύων ή δικτύων υπολογιστών, και η Αρχή Διατήρησης της Ακεραιότητας των Επικοινωνιών μπορεί να επιβάλει στον παραβάτη διοικητικές κυρώσεις. Η απόφασή της πρέπει να είναι πλήρως αιτιολογημένη και πάντοτε ύστερα από προηγούμενη κλήτευση και ακρόαση του φερόμενου ως υπαιτίου, ο οποίος μπορεί να παραστεί μετά ή διά πληρεξουσίου δικηγόρου, εκτός αν ο Πρόεδρος της Α.Δ.Α.Ε. διατάξει την αυτοπρόσωπη παρουσία του. Οι διοικητικές κυρώσεις που μπορεί να επιβάλει η Αρχή είναι :

- ☛ Σύσταση για συμμόρφωση σε συγκεκριμένη διάταξη της νομοθεσίας με προειδοποίηση επιβολής κυρώσεων σε περίπτωση υποτροπής του παραβάτη.
- και
- ☛ Πρόστιμο από 15.000 έως 1.500.000 ευρώ.

### 3.4 ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ ΠΕΡΙ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΜΠΟΡΙΟΥ

Η Ευρωπαϊκή Ένωση έχει ασχοληθεί ενδελεχώς με το θέμα της ρύθμισης των ηλεκτρονικών επιχειρήσεων και γενικότερο με το κομμάτι του Ηλεκτρονικού Εμπορίου. Μέσω των κοινοτικών οδηγιών δημιουργεί τις κατευθυντήριες γραμμές προκειμένου να υπάρχει μια εναρμόνιση στο σύνολο της Ευρωζώνης. Από τις πρώτες οδηγίες που αποτέλεσε την βάση στον τομέα αυτό είναι η οδηγία 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 8<sup>ης</sup> Ιουνίου 2000, για νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά της εκάστοτε χώρας. Αυτός είναι κι ο λόγος που θα αναλυθεί εν τάχει η συγκεκριμένη οδηγία.

Η οδηγία αυτή στηρίζεται στις κατευθύνσεις που περιέχονται στην ανακοίνωση της Επιτροπής με το ηλεκτρονικό εμπόριο, με στόχο τη σύσταση ενός συνεκτικού, σε ευρωπαϊκή κλίμακα, νομικού πλαισίου για το ηλεκτρονικό εμπόριο. Η υιοθετούμενη προσέγγιση αποβλέπει, ειδικότερα, στην αποφυγή των υπερβολικών κανονιστικών ρυθμίσεων, στηριζόμενη στις ελευθερίες της εσωτερικής αγοράς, λαμβανομένων υπόψη των πραγματικών εμπορικών συνθηκών και εξασφαλίζοντας μια αποτελεσματική προστασία των στόχων γενικού ενδιαφέροντος. Η παρούσα οδηγία ανταποκρίνεται επίσης στη βούληση εξάλειψης των αποκλίσεων μεταξύ των νομολογιών των κρατών μελών ούτως ώστε να κατοχυρωθεί ένα επίπεδο ασφάλειας ικανό να αυξήσει την εμπιστοσύνη των καταναλωτών και των επιχειρήσεων.

Όσον αφορά το πεδίο εφαρμογής της, η οδηγία καλύπτει όλες τις υπηρεσίες της κοινωνίας της πληροφορίας υπηρεσίες μεταξύ επιχειρήσεων, τις υπηρεσίες μεταξύ επιχειρήσεων και καταναλωτών, τις δωρεάν υπηρεσίες που χρηματοδοτούνται, για παράδειγμα, από διαφημιστικά έσοδα ή έσοδα προερχόμενα από χορηγίες και τις υπηρεσίες που επιτρέπουν τη διεκπεραίωση ηλεκτρονικών συναλλαγών σε απευθείας σύνδεση (και ιδίως τη διαλογική τηλεπώληση αγαθών και υπηρεσιών και τις σε απευθείας σύνδεση αγορές από ηλεκτρονικά καταστήματα). Καλύπτει επίσης τις εξής υπηρεσίες και δραστηριότητες σε απευθείας σύνδεση (on-line): on-line εφημερίδες και περιοδικά, on-line βάσεις δεδομένων, on-line χρηματοπιστωτικές υπηρεσίες, on-line επαγγελματικές υπηρεσίες (δικηγόρων, γιατρών, λογιστών, κτηματομεσιτών), on-line ψυχαγωγικές υπηρεσίες (π.χ. βιντεοταινίες κατά παραγγελία), on-line marketing και

διαφήμιση, υπηρεσίες πρόσβασης στο Internet. Η οδηγία έχει εφαρμογή αποκλειστικά στους φορείς παροχής υπηρεσιών που είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση (ΕΕ). Εντούτοις, προκειμένου να μην παρακωλύσει το παγκόσμιο ηλεκτρονικό εμπόριο, δεν περιλαμβάνει διατάξεις ασύμβατες με τα νομικά πλαίσια και τις διαδικασίες που ισχύουν σε άλλες περιφέρειες του κόσμου.

Χαρακτηριστικά, η οδηγία δεν επιτρέπει στα κράτη μέλη να υπαγάγουν τις υπηρεσίες της κοινωνίας της πληροφορίας σε ειδικά καθεστάτα αδειοδότησης τα οποία δεν εφαρμόζονται επίσης και σε παρόμοιες υπηρεσίες που παρέχονται με άλλα μέσα. Κατά συνέπεια, θα ήταν αντίθετη προς τις διατάξεις της οδηγίας η υπαγωγή της δημιουργίας ιστοθέσεων σε διαδικασία αδειοδότησης. Σε περίπτωση ωστόσο που η υπόψη ιστοθέση αφορά δραστηριότητες υποκείμενες σε κανονιστικές ρυθμίσεις (για παράδειγμα on-line τραπεζικές και χρηματοπιστωτικές υπηρεσίες), η δημιουργία της μπορεί να υπαχθεί σε καθεστώς αδειοδότησης. Ακόμα οι εμπορικές επικοινωνίες πρέπει να είναι σαφώς αναγνωρίσιμες και μη επιδεχόμενες παρερμηνειών (άρθρο 6) ούτως ώστε να αυξηθεί η εμπιστοσύνη των καταναλωτών και να διασφαλιστούν θεμιτές εμπορικές πρακτικές. Επιπλέον, οι εμπορικές επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου πρέπει να είναι σαφώς αναγνωρίσιμες ευθύς ως περιέρχονται στον αποδέκτη. Τα κράτη μέλη οφείλουν εξάλλου να λάβουν μέτρα με τα οποία να εξασφαλίζεται ότι οι φορείς παροχής υπηρεσιών που προβαίνουν σε ανεπίκλητες εμπορικές επικοινωνίες μέσω ηλεκτρονικού ταχυδρομείου συμβουλευόμαστε τακτικά τα μητρώα «επιλογών» (σύστημα opt-out) στα οποία μπορούν να εγγράφονται τα φυσικά πρόσωπα που δεν επιθυμούν να λαμβάνουν τέτοιες εμπορικές επικοινωνίες και σέβονται την επιλογή αυτών των προσώπων. Η οδηγία δεν απαγορεύει ωστόσο στα κράτη μέλη να επιλέξουν το σύστημα προγενέστερης συγκατάθεσης (opt-in)

Κλείνοντας για την εφαρμογή της οδηγίας, τα κράτη μέλη και η Επιτροπή ενθαρρύνουν την κατάρτιση κωδίκων δεοντολογίας σε κοινοτικό επίπεδο, από τις επαγγελματικές ενώσεις ή οργανώσεις, με σκοπό να συμβάλουν στην ορθή εφαρμογή της οδηγίας. Ωστόσο, η Επιτροπή μεριμνά ώστε οι εν λόγω κώδικες να τηρούν τις αρχές του κοινοτικού δικαίου και να εξασφαλίζεται η διαφάνειά τους σε κοινοτικό επίπεδο. Οι ενώσεις καταναλωτών πρέπει να συμμετέχουν στη διαδικασία κατάρτισης και εφαρμογής των κωδίκων δεοντολογίας (άρθρο 16). Σε περιπτώσεις διαφωνίας μεταξύ



ενός φορέα παροχής και ενός αποδέκτη μιας υπηρεσίας της κοινωνίας της πληροφορίας, τα κράτη μέλη μεριμνούν ώστε η νομοθεσία τους να επιτρέπει την ουσιαστική χρήση μηχανισμών εξώδικης επίλυσης και με τα κατάλληλα ηλεκτρονικά μέσα. Τα κράτη μέλη οφείλουν να εξασφαλίζουν ότι τα αρμόδια όργανα εξώδικης επίλυσης των διαφορών εφαρμόζουν τις αρχές της ανεξαρτησίας, της διαφάνειας, της εκατέρωθεν ακρόασης, της αποτελεσματικότητας της διαδικασίας, της νομιμότητας της απόφασης, της ελευθερίας των μερών και της αντιπροσώπευσης (άρθρο 17). Τα κράτη μέλη μεριμνούν ώστε οι δραστηριότητες υπηρεσιών της κοινωνίας της πληροφορίας να αποτελούν αντικείμενο αποτελεσματικών μέσωσν έννομης προστασίας που να επιτρέπουν την λήψη μέτρων με σκοπό την επανόρθωση της εικαζόμενης παράβασης και την αποφυγή πρόκλησης περαιτέρω ζημίας στα διακυβευόμενα συμφέροντα (άρθρο 18). Τα κράτη μέλη μεριμνούν ώστε οι αρμόδιες αρχές τους να διαθέτουν τις κατάλληλες εξουσίες ελέγχου και έρευνας που απαιτούνται για την αποτελεσματική εφαρμογή της οδηγίας. Μεριμνούν επίσης ώστε οι αρμόδιες αρχές τους να συνεργάζονται με τις εθνικές αρχές των άλλων κρατών μελών και να ορίζουν, προς το σκοπό αυτόν, αρμόδιο για επικοινωνία του οποίου τα στοιχεία κοινοποιούν στα άλλα κράτη μέλη και στην Επιτροπή (άρθρο 19).

Μια δεύτερη κοινοτική οδηγία είναι η 2002/38/ΕΚ θεσπίζει κανόνες σχετικά με τη φορολόγηση υπηρεσιών οι οποίες παρέχονται σε ηλεκτρονική μορφή μέσω ηλεκτρονικών δικτύων (ενημερωτικές, πολιτιστικές, καλλιτεχνικές, αθλητικές, επιστημονικές, εκπαιδευτικές, ψυχαγωγικές και άλλες παρόμοιες υπηρεσίες, καθώς και λογισμικό, ηλεκτρονικά παιχνίδια και υπηρεσίες πληροφορικής).

Συγκεκριμένα έχει προβλεφθεί ειδικό καθεστώς για υπηρεσίες που παρέχονται ηλεκτρονικά. Επιγραμματικά η οδηγία αναφέρει τα εξής :

1. Τα κράτη μέλη επιτρέπουν σε μη εγκατεστημένο υποκείμενο στο φόρο ο οποίος παρέχει ηλεκτρονικές υπηρεσίες σε μη υποκείμενο στο φόρο, ο οποίος είναι εγκατεστημένος ή έχει τον τόπο της κατοικίας του ή της συνήθους διαμονής του σε κράτος μέλος, να χρησιμοποιεί το ειδικό καθεστώς σύμφωνα με τις ακόλουθες διατάξεις. Το ειδικό καθεστώς ισχύει για όλες αυτές τις παροχές εντός της Κοινότητας.

2. Ο μη εγκατεστημένος υποκείμενος στο φόρο δηλώνει στο κράτος μέλος εγγραφής την έναρξη των δραστηριοτήτων του, ως υποκείμενου στο φόρο, την παύση ή τη μεταβολή αυτών, εφόσον ως αποτέλεσμα έχουν να μην εμπίπτει πλέον στο ειδικό καθεστώς. Η δήλωση αυτή υποβάλλεται ηλεκτρονικά.

Οι πληροφορίες που παρέχει ο μη υποκείμενος στο φόρο προς το κράτος μέλος εγγραφής, όταν αρχίζουν οι φορολογικές του δραστηριότητες, περιέχει τα ακόλουθα στοιχεία φορολογικής ταυτότητας: ονοματεπώνυμο, ταχυδρομική διεύθυνση, ηλεκτρονικές διευθύνσεις και ιστοσελίδες, τυχόν εθνικό αριθμό φορολογικού μητρώου και δήλωση σύμφωνα με την οποία το συγκεκριμένο πρόσωπο δεν διαθέτει αριθμό φορολογικού μητρώου ΦΠΑ εντός της Κοινότητας. Ο μη εγκατεστημένος υποκείμενος στο φόρο κοινοποιεί στο κράτος μέλος εγγραφής, κάθε τυχόν αλλαγή των πληροφοριών που έχει υποβάλει.

3. Το κράτος μέλος εγγραφής χορηγεί στο μη εγκατεστημένο υποκείμενο στο φόρο προσωπικό αριθμό φορολογικού μητρώου. Βασιζόμενα στις πληροφορίες που χρησιμοποιούνται για τη χορήγηση του αριθμού αυτού φορολογικού μητρώου, τα κράτη μέλη κατανάλωσης μπορούν να διατηρούν δικά τους συστήματα εγγραφής.

Το κράτος μέλος εγγραφής κοινοποιεί με ηλεκτρονικά μέσα, στο μη εγκατεστημένο υποκείμενο στο φόρο, τον αριθμό φορολογικού μητρώου που του χορηγήθηκε.

4. Το κράτος μέλος εγγραφής διαγράφει το μη εγκατεστημένο υποκείμενο σε φόρο από το φορολογικό μητρώο, εάν:

- α) το εν λόγω πρόσωπο κοινοποιήσει ότι δεν παρέχει πλέον ηλεκτρονικές υπηρεσίες ή
- β) μπορεί άλλως πως να συναχθεί ότι η φορολογητέα του δραστηριότητα έχει τερματισθεί ή
- γ) δεν πληροί πλέον τις απαραίτητες προδιαγραφές που του επιτρέπουν να χρησιμοποιεί το ειδικό καθεστώς ή
- δ) έχει επανειλημμένα παραλείψει να συμμορφωθεί προς τους κανόνες που αφορούν το ειδικό καθεστώς.

5. Ο μη εγκατεστημένος υποκείμενος στο φόρο υποβάλλει με ηλεκτρονικό τρόπο, στο κράτος μέλος εγγραφής, δήλωση φόρου προστιθεμένης αξίας για κάθε τρίμηνο, είτε έχει παρασχεθεί ηλεκτρονική υπηρεσία είτε όχι. Η δήλωση υποβάλλεται εντός είκοσι ημερών από το τέλος της φορολογικής περιόδου, την οποία καλύπτει η δήλωση.

Στη δήλωση φόρου προστιθεμένης αξίας παρατίθεται ο αριθμός φορολογικού μητρώου και, για κάθε κράτος μέλος κατανάλωσης στο οποίο οφείλεται φόρος, η συνολική αξία, χωρίς το φόρο προστιθεμένης αξίας, της παροχής ηλεκτρονικών υπηρεσιών, για την φορολογική περίοδο, και το συνολικό ποσό του φόρου που αντιστοιχεί. Αναφέρονται επίσης οι ισχύοντες φορολογικοί συντελεστές και το συνολικό ποσό του φόρου που οφείλεται.

6. Η δήλωση του φόρου προστιθεμένης αξίας συμπληρώνεται σε ευρώ. Τα κράτη μέλη που δεν έχουν υιοθετήσει το ευρώ μπορούν να απαιτούν τη συμπλήρωση της δήλωσης αυτής στο εθνικό τους νόμισμα. Εάν η παροχή υπηρεσιών έχει πραγματοποιηθεί σε άλλα νομίσματα, κατά τη συμπλήρωση της δήλωσης φόρου προστιθεμένης αξίας χρησιμοποιείται η συναλλαγματική ισοτιμία που ισχύει την τελευταία ημέρα της φορολογικής περιόδου. Η μετατροπή γίνεται σύμφωνα με τις συναλλαγματικές ισοτιμίες που δημοσίευσε η Ευρωπαϊκή Κεντρική Τράπεζα την ημέρα εκείνη ή, εάν δεν υπήρξε δημοσίευση τη συγκεκριμένη ημέρα, τις ισοτιμίες της επόμενης ημέρας δημοσίευσης.

7. Ο μη εγκατεστημένος υποκείμενος στο φόρο καταβάλλει το φόρο προστιθεμένης αξίας συγχρόνως με την υποβολή της δήλωσης. Η πληρωμή γίνεται σε τραπεζικό λογαριασμό σε ευρώ, που ορίζεται από το κράτος μέλος εγγραφής. Τα κράτη μέλη που δεν έχουν υιοθετήσει το ευρώ, μπορούν να απαιτούν να γίνεται η πληρωμή σε τραπεζικό λογαριασμό στο νόμισμά τους.

8. Παρά το άρθρο 1 παράγραφος 1 της οδηγίας 86/560/ΕΟΚ, στο μη εγκατεστημένο υποκείμενο στο φόρο ο οποίος χρησιμοποιεί το ειδικό αυτό καθεστώς, αντί εκπτώσεων δυνάμει του άρθρου 17 παράγραφος 2 της παρούσας οδηγίας, χορηγείται επιστροφή σύμφωνα με την οδηγία 86/560/ΕΟΚ. Το άρθρο 2 παράγραφοι 2 και 3 και το άρθρο 4 παράγραφος 2 της οδηγίας 86/560/ΕΟΚ δεν εφαρμόζονται στις επιστροφές που



συνδέονται με ηλεκτρονικές παροχές υπηρεσιών καλυπτόμενες από αυτό το ειδικό καθεστώς.

9. Ο μη εγκατεστημένος υποκείμενος στο φόρο καταγράφει με επαρκείς λεπτομέρειες τα στοιχεία των συναλλαγών που καλύπτονται από το ειδικό αυτό καθεστώς, ώστε να μπορούν οι φορολογικές αρχές του κράτους μέλους καταπόνησης να επαληθεύουν την ακρίβεια της δήλωσης του φόρου προστιθεμένης αξίας της παραγράφου 5. Τα στοιχεία αυτά θα πρέπει να διατίθενται ηλεκτρονικά, κατόπιν αίτησης, στο κράτος μέλος εγγραφής και στο κράτος μέλος καταπόνησης. Τα στοιχεία αυτά διατηρούνται επί διάστημα δέκα ετών, αρχής γενομένης από το τέλος του έτους κατά το οποίο έγινε η συναλλαγή.

10. Το άρθρο 21 παράγραφος 2 στοιχείο β) δεν εφαρμόζεται στους μη εγκατεστημένους υποκείμενους στο φόρο, οι οποίοι έχουν επιλέξει το ειδικό αυτό καθεστώς.

### 3.5 ΣΥΓΚΕΝΤΡΩΤΙΚΗ ΑΝΑΦΟΡΑ ΤΗΣ ΝΟΜΟΘΕΣΙΑΣ

Η νομοθεσία της Ελλάδος, όπως παρουσιάστηκε και παραπάνω, παρέχει ικανοποιητικό πλέγμα προστασίας για τους καταναλωτές και τις επιχειρήσεις. Στην παρούσα παράγραφο παρουσιάζεται συγκεντρωτικά η νομοθεσία που διέπει ένα ηλεκτρονικό κατάστημα προκειμένου να είναι σύννομο και ως προς την λειτουργία του αλλά κι ως προς τους ίδιους τους καταναλωτές του.

Οι τρεις (3) βασικοί άξονες της νομοθεσίας που θα πρέπει να τηρεί μια επιχείρηση που δραστηριοποιείται στο χώρο του ηλεκτρονικού εμπορίου είναι οι εξής :

#### 1. **Νομοθεσία που αφορά στη νομική μορφή της επιχείρησης (εμπορικό δίκαιο)**

Αρχικά θα πρέπει η επιχείρηση, ακόμη και αν είναι ένα ηλεκτρονικό κατάστημα χωρίς φυσική υπόσταση χώρου, να λειτουργεί σύμφωνα με τους κανόνες που επιβάλλει η νομική μορφή και που διέπει όλες τις επιχειρήσεις της μορφής αυτής. Οι διατάξεις

αυτές έχουν να κάνουν με το εμπορικό δίκαιο λειτουργίας μιας επιχείρησης, ανεξαρτήτως μορφής, ηλεκτρονικής ή όχι.

## 2. Προστασία προσωπικών δεδομένων των υπαλλήλων της εταιρείας

Η διαδικτυακή φύση των ηλεκτρονικών καταστημάτων τα υποχρεώνει να ρυθμίζονται από την Α.Π.Π.Δ. Τα προσωπικά δεδομένα, όπως και παρουσιάστηκε, έχουν αυστηρή νομοθεσία λόγω της ευαισθητοποίησης που υπάρχει ως προς αυτά. Συγκεκριμένα η οδηγία 115/2001 όπου ρυθμίζει την επεξεργασία δεδομένων των υπαλλήλων της κάθε επιχείρησης. Αυτά πρέπει να τηρούνται σε βάσεις δεδομένων της εκάστοτε επιχείρησης, για ένα συγκεκριμένο χρονικό διάστημα, ακόμα κι αν ο υπάλληλος έχει απολυθεί από την επιχείρηση.

## 3. Προστασία προσωπικών δεδομένων των καταναλωτών

Στο πλαίσιο της διαφύλαξης των προσωπικών δεδομένων υπάρχουν οι νόμοι Ν.2774/99 και Ν.2472/97. Επιπλέον από αυτούς ισχύει η απόφαση 50/2000 της Α.Π.Π.Δ που πραγματεύεται με την νόμιμη επεξεργασία των προσωπικών δεδομένων αλλά και η οδηγία 147/2001 της ΕΕ που ρυθμίζει την χρήση ευαίσθητων προσωπικών δεδομένων των καταναλωτών ενώπιον του δικαστηρίου.

Επίσης μια επιχείρηση ρυθμίζεται κι από τις διατάξεις της Α.Δ.Α.Ε. μα η πλειοψηφία των ρυθμίσεων της έγκειται στις τηλεπικοινωνίες, που δεν καλύπτουν απαραίτητα τις ηλεκτρονικές επιχειρήσεις.

Τέλος, με κατεύθυνση πάλι προς την προστασία των καταναλωτών του ηλεκτρονικού καταστήματος εφαρμόζεται το Π.Δ. 131/2003 περί spamming. Σε αυτό προστίθεται και ο νόμος Ν.2225/94 ο οποίος ρυθμίζει τη προστασία ελευθερίας της ανταπόκρισης της επικοινωνίας των καταναλωτών προς τα καταστήματα αλλά και αντιστρόφως. Η τεχνολογική κάλυψη των επιχειρήσεων προς τους πελάτες τους είναι η χρησιμοποίηση cookies της ίδιας της εταιρείας προκειμένου να εξασφαλιστεί η ακεραιότητα των μηνυμάτων που στέλνουν.

Η ανωτέρω νομοθεσία είναι απαραίτητη ώστε το ηλεκτρονικό κατάστημα ή η ηλεκτρονική επιχείρηση να λειτουργεί νομικώς ορθά αλλά και να καλύπτει το σύνολο

των προϋποθέσεων εκείνων όπου ο καταναλωτής θα εμπιστευτεί αλλά κι ο ίδιος θα είναι ασφαλής, από την επεξεργασία των προσωπικών του δεδομένων.

### 3.6 ΠΡΩΤΟΒΟΥΛΙΕΣ ΠΑΡΕΜΒΑΣΗΣ ΒΕΛΤΙΩΣΗΣ ΤΗΣ ΙΣΧΥΟΥΣΑΣ ΝΟΜΟΘΕΣΙΑΣ

#### Πρωτοβουλία eEurope

Η πρωτοβουλία eEurope [24] προτάθηκε αρχικά από την Ευρωπαϊκή Επιτροπή στο τέλος του 1999 και επικυρώθηκε από το Ευρωπαϊκό Συμβούλιο ως τμήμα της Στρατηγικής της Λισαβόνας για να εκσυγχρονίσει την Ευρωπαϊκή Οικονομία. Ο στόχος του eEurope ήταν φιλόδοξος: να συνδέσει στο Διαδίκτυο τον κάθε πολίτη, την εκπαίδευση και τις επιχειρήσεις, καθώς και να εκμεταλλευτεί τις δυνατότητες τις νέας οικονομίας για την ανάπτυξη, την απασχόληση και την άρση των αποκλεισμών. Το πρώτο σχέδιο δράσης eEurope, που έλαβε χώρα το 2000-2002, είχε 3 σκοπούς: το φθηνότερο, γρηγορότερο και ασφαλέστερο Διαδίκτυο, την επένδυση στις ικανότητες των ανθρώπων και την προώθηση της χρήσης του Διαδικτύου. Αποτελούνταν από 64 στόχους και σχεδόν όλοι επιτεύχθηκαν πριν από το τέλος το 2002. Η δεύτερη φάση αποτελείται από το Σχέδιο Δράσης eEurope 2005, που επικυρώθηκε από το Ευρωπαϊκό Συμβούλιο στη Σεβίλλη. Στόχος του 2005 είναι ότι η Ευρώπη πρέπει πλέον να αποκτήσει σύγχρονες on-line δημόσιες υπηρεσίες (ηλεκτρονική διακυβέρνηση, υπηρεσίες e-learning, τηλεϊατρική και υπηρεσίες υγείας) και ένα δυναμικό περιβάλλον ηλεκτρονικού εμπορίου και e-επιχειρείν. Για να καταστεί δυνατή η πραγματοποίηση των παραπάνω, είναι απαραίτητη η ευρέως διαδεδομένη διαθεσιμότητα Ευρωζωνικής Πρόσβασης σε ανταγωνιστικές τιμές καθώς και η ασφαλής υποδομή πληροφοριών. Το eEurope 2005 έχει πλέον αντικατασταθεί από την στρατηγική i2010.

#### Στρατηγική i2010

Η στρατηγική i2010, που έρχεται να αντικαταστήσει το eEurope 2005, δίνει έμφαση στην αγορά, στις επενδύσεις και στην ποιότητα ζωής. Η ευρωπαϊκή στρατηγική



"i2010" που συνδιαμορφώνεται με την Ευρωπαϊκή Ένωση, περιλαμβάνει τρεις ερμηνείες του προθέματος "i", οι οποίες ταυτίζονται σε σημαντικό βαθμό με τις προτάσεις που κατατέθηκαν από την Ειδική Γραμματεία ΚτΠ. Η πρώτη ερμηνεία - στόχος του προθέματος "i" στην ευρωπαϊκή στρατηγική "i2010" για την Κοινωνία της Πληροφορίας, αποτελεί το "internal market for information services", δηλαδή τη δημιουργία ενός κοινού Ευρωπαϊκού χώρου για την Κοινωνία της Πληροφορίας, όπου η ευρωπαϊκή τεχνογνωσία και τεχνολογία διαχέονται στο εσωτερικό της Ευρώπης με μεγαλύτερη ταχύτητα και αξιοποιούνται από όλους τους Ευρωπαίους πολίτες. Η δεύτερη ερμηνεία-στόχος του προθέματος "i" στη νέα ευρωπαϊκή στρατηγική "i2010" για την Κοινωνία της Πληροφορίας, αποτελεί το "investment in ICT innovation for competitiveness", δηλαδή επενδύσεις σε καινοτομία για την αξιοποίηση των νέων τεχνολογιών πληροφορικής και επικοινωνιών, προκειμένου να βελτιωθεί η ευρωπαϊκή και εθνική ανταγωνιστικότητα. Η τρίτη ερμηνεία-στόχος του προθέματος "i" στη νέα ευρωπαϊκή στρατηγική "i2010", αποτελεί το "inclusion and better quality of life", δηλαδή η ισότιμη συμμετοχή των Ευρωπαίων πολιτών και η εξασφάλιση καλύτερης ποιότητας ζωής, μέσω των δυνατοτήτων της Κοινωνίας της Πληροφορίας.

Συμπερασματικά, η συμβολή της έγκειται στην δεύτερη ερμηνεία που δόθηκε παραπάνω. Η αξιοποίηση νέων τεχνολογιών έχει ως πρακτική εφαρμογή τις ηλεκτρονικές επιχειρήσεις. Μέσω των παρεμβάσεων τους και την έρευνα σ αυτό τον τομέα, προωθείται η ανάπτυξη της ανταγωνιστικότητας αυτού του κλάδου τόσο σε εγχώριο τομέα, σε ηπειρωτικό αλλά και σε παγκόσμιο. Ο στόχος αυτός θέλει να καταδείξει πως τα όρια της επιχειρηματικότητας δεν μπορεί να περιοριστεί στα στενά όρια ενός γεωγραφικού τόπου και πως ο επιχειρηματίας μπορεί να μετατραπεί σε παγκόσμιο παραγωγό. Μέρος των ενεργειών τους είναι η εξάλειψη της γραφειοκρατίας στην σύσταση μιας τέτοιας επιχείρησης προκειμένου να μην χάνεται πολύτιμος χρόνος για τον επιχειρηματία αλλά και για την παγκόσμια παραγωγή. Ταυτόχρονα γίνονται κινήσεις προς ενοποίηση ή τουλάχιστον σύμπλευση των φορολογικών βαρών σε όλες τις Ευρωπαϊκές χώρες. Έτσι γνωρίζει εξ αρχής ο επιχειρηματίας το σύνολο των υποχρεώσεων του ως προς το κράτος. Παράλληλα με αυτές τις ενέργειες – στόχους, σκοπός είναι κι η επιμόρφωση των καταναλωτών ως προς τις ηλεκτρονικές επιχειρήσεις. Να ενημερωθεί κατάλληλα ο κόσμος, ώστε να αποφεύγονται σημάδια φόβου ως προς την αντικειμενικότητα αλλά και την ολοκλήρωση της παραγγελίας του

εκάστοτε καταναλωτή. Προσπαθεί, αυτή η πρωτοβουλία, να εξηγήσει πως μια επιχείρηση μπορεί να υφίσταται νομότυπα χωρίς να υπάρχει φυσική υπόσταση χώρου όπως είναι ένα κατάστημα.

Χαρακτηριστικά μέρη του *eEurope 2005 κατά το 2003*:

- σύσκεψη κορυφής για το ηλεκτρονικό επιχειρείν, στην οποία εκπρόσωποι υψηλού επιπέδου από τον επιχειρηματικό κόσμο θα περιγράψουν τις δυσκολίες που αντιμετωπίζουν όταν αναπτύσσουν επιχειρηματικές δραστηριότητες με ηλεκτρονικά μέσα
- η Επιτροπή δημιούργησε ένα δίκτυο στήριξης του ηλεκτρονικού επιχειρείν για να προαγάγει την εισαγωγή των ψηφιακών τεχνολογιών και διαδικασιών στις μικρομεσαίες επιχειρήσεις
- ο ιδιωτικός κλάδος θα πρέπει να αναπτύξει συμβατές λύσεις για τις συναλλαγές, την ασφάλεια, τις υπογραφές, τις κρατικές προμήθειες και τις πληρωμές.
- η Επιτροπή εξέτασε τους δυνατούς τρόπους για τη θέσπιση ενός πανευρωπαϊκού ηλεκτρονικού συστήματος διευθέτησης των διαφορών.

## ΚΕΦΑΛΑΙΟ 4<sup>ο</sup> : ΠΡΟΣΤΑΣΙΑ ΚΑΤΑΝΑΛΩΤΩΝ

### 4.1 ΕΙΣΑΓΩΓΗ

Η φιλολογία που έχει αναπτυχθεί γύρω από την ασφάλεια στο ηλεκτρονικό εμπόριο είναι αρκετά πλούσια, γεγονός που έχει σαν αποτέλεσμα την επιφυλακτική αντιμετώπιση του από ένα μεγάλο μέρος του αγοραστικού κοινού κι επιχειρηματικού κόσμου. Ασφαλώς το θέμα της ασφάλειας των πληρωμών στο Διαδίκτυο είναι πολύ σημαντικό αν και δεν είναι το μοναδικό. Επίσης προβληματισμό προκαλεί η ασφάλεια από την παραπλανητική πώληση προϊόντων ή ακόμη κι από την προώθηση επικίνδυνων προϊόντων φαρμακευτικής φύσης. Πολλοί είναι όμως αυτοί που αναρωτιούνται για ποιο λόγο γίνεται όλη αυτή η φασαρία, αφού δεν αναλώνεται και σημαντικό χρόνος σχετικά με την ασφάλεια των συναλλαγών που πραγματοποιούνται στο φυσικό κόσμο. Γιατί τελικά το διαδίκτυο διαφέρει τόσο πολύ και ταυτόχρονα αποτελεί πηγή έμπνευσης για τέτοιες ιστορίες, είναι ερωτήματα φιλοσοφικής βάσης.

Το βέβαιο πάντως είναι πως δεν θα πρέπει κάποιος να είναι απόλυτα αρνητικός και να υπερβάλλει, αρνούμενος να συμμετάσχει σε αγοροπωλησίες στο διαδίκτυο, απλώς και μόνο από φόβο. Κίνδυνοι υπάρχουν παντού, σε οποιαδήποτε συναλλαγή, ακόμα και στις φυσικές αγορές που μπορεί να είναι και μεγαλύτεροι. Οι κίνδυνοι από την χρήση των πιστωτικών καρτών δεν είναι συνδεδεμένοι μόνο με τις ηλεκτρονικές συναλλαγές. Είναι γνωστό ότι συμβαίνουν και στις καθημερινές μας φυσικές συναλλαγές, όπως για παράδειγμα στην ανάληψη μετρητών από τα αυτόματα μηχανήματα των τραπεζών. Συνήθως ο θόρυβος δημιουργείται πάντα γύρω από κάτι καινούργιο, όπως στην συγκεκριμένη περίπτωση είναι το Διαδίκτυο συναρτήσει του ηλεκτρονικού εμπορίου. Τα διάφορα προβλήματα, προβάλλονται και ανησυχούν την κοινή γνώμη, ενώ αν τα ίδια συμβαίνουν σε άλλες γνωστότερες παραδοσιακές καταστάσεις, δεν εντυπωσιάζουν στον ίδιο βαθμό. Αυτό βέβαια είναι φυσικό και δικαιολογείται από την άγνοια που επικρατεί γύρω από το «καινούργιο» της αγοράς. Πολλά από τα θέματα που αποκαλούνται «προβλήματα ασφαλείας» για το ηλεκτρονικό εμπόριο, είναι ακριβώς ανάλογα με τα επιχειρηματικά θέματα του πραγματικού κόσμου. Για παράδειγμα, μπορεί κάποιος να θέλει συγκεκριμένα είδη των επιχειρηματικών του επικοινωνιών να είναι ιδιωτικά, μπορεί να απαιτεί να πληρωθεί μετρητοίς ή να ζητάει προσωπικές



υπογραφές στα συμβόλαια, κλπ. Αυτές οι απαιτήσεις και τα μέσα που χρησιμοποιούνται για να ικανοποιηθούν έχουν αναπτυχθεί εδώ και χιλιάδες χρόνια κατά την διάρκεια της ιστορίας του εμπορίου. Στο Διαδίκτυο τα θέματα αυτά αντιμετωπίζονται μέσα σε ένα διαφορετικό περιβάλλον και γίνονται προσπάθειες ώστε να γίνουν σαφή και κατανοητά καθώς και να αναπτυχθούν νέες λύσεις σε σύντομο σχετικά χρονικό διάστημα.

Συνεπώς θα πρέπει κανείς να είναι συνετός, να αντιμετωπίζει τους κινδύνους με λογική και σύνεση, όχι με φόβο και άρνηση, δεδομένου ότι αυτό τον αφήνει έξω από διαδικασίες που τελικά, όπως έχει αναλυθεί και παραπάνω στην παρούσα εργασία, ωφελούν τους συμμετέχοντες, όποιο ρόλο αν έχουν είτε του αγοραστή δηλαδή αλλά είτε και του πωλητή.

#### 4.2 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Η ανάλυση οφείλει να εμβαθύνει περισσότερο στο θέμα που είναι οι «ασφαλείς» συναλλαγές. Ξεκινώντας με τη θέση ότι «απόλυτα ασφαλείς συναλλαγές» δεν υπάρχουν πουθενά, στη συνέχεια θα περιγραφεί και θα εξηγηθεί το πλαίσιο προστασίας ώστε να μειώνεται ή να ελαχιστοποιείται ο κίνδυνος των ηλεκτρονικών συναλλαγών.

Η ασφάλεια στο ηλεκτρονικό εμπόριο θεωρείται ένα μείζον θέμα να έχει επικρατήσει ότι οι όροι «ασφάλεια ή κίνδυνος» αναφέρονται μόνον στις διαδικασίες πληρωμών. Όπως για παράδειγμα, το ότι κατά την διάρκεια μιας ηλεκτρονικής συναλλαγής, ο αγοραστής ανεξάρτητα από τον τρόπο και την ασφάλεια πληρωμής, παρέχει στον πωλητή πολλές άλλες πληροφορίες. Τέτοιες πληροφορίες αναφέρονται σε διάφορα από τα προσωπικά του δεδομένα, όπως π.χ. η διεύθυνσή του. Βέβαια, μερικές από τις πληροφορίες αυτές μπορεί να είναι σημαντικές ως και απαραίτητες για την πραγματοποίηση της συναλλαγής ή και για τον πωλητή, ώστε να είναι κι αυτός σίγουρος πως ο καταναλωτής του είναι φερέγγυος. Ο κίνδυνος όμως καταχρηστικής ή παράνομης χρήσης των πληροφοριών αυτών είναι υπαρκτός. Ο κίνδυνος υποκλοπής των πληροφοριών είναι κι αυτός επίσης υπαρκτός. Επί πλέον η παράνομη χρήση τους είτε από τον πωλητή είτε από αυτόν που υπέκλεψε τις πληροφορίες, είναι κι αυτός

υπαρκτός. Αυτά όμως δεν θα πρέπει να εκπλήσσουν τους καταναλωτές, δεδομένου ότι και το παραδοσιακό εμπόριο δεν τα εμποδίζει. Συγκεκριμένα, υπάρχουν σχετικές έρευνες που υποστηρίζουν ότι το ποσοστό των κρουσμάτων σε σχέση με την χρήση των πιστωτικών καρτών στο παραδοσιακό εμπόριο είναι κατά πολύ μεγαλύτερο από το αντίστοιχο που διαπιστώνεται στο ηλεκτρονικό εμπόριο. Σε έρευνα που διενεργήθηκε το 2010 από την Στατιστική Αρχή [11], σε ποσοστό 62% των ερωτηθέντων δήλωσαν ότι δεν ανησυχούν για τυχόν απώλεια χρημάτων από κακή χρήση της πιστωτικής κάρτας ή εξαπάτησής τους. Η προβολή όμως στην περίπτωση του ηλεκτρονικού εμπορίου είναι, για τους λόγους που αναφέρθηκαν παραπάνω, τουλάχιστον υπερβολική. Σημειώνεται επίσης ότι συντριπτική πλειοψηφία των καταναλωτών που χρησιμοποιούν το ηλεκτρονικό εμπόριο, δηλώνουν πως δεν έχουν αντιληφθεί κρούσματα στις συναλλαγές τόσο των ίδιων όσο και των γνωστών τους.

Οι λόγοι που συμβάλλουν στην έλλειψη ισχυρής ασφάλειας ως προς τους καταναλωτές αλλά και ως προς τους αγοραστές είναι κυρίως τεχνολογικοί και συνοψίζονται στην παρακάτω ανάλυση.

Αρχικά είναι γνωστό πως οι υπολογιστές είναι διασυνδεδεμένοι. Ενώ παλαιότερα υπήρχε περισσότερη ασφάλεια, μέσω του Διαδικτύου όμως, επιτρέπεται σε οποιονδήποτε στον κόσμο να χρησιμοποιήσει τους υπολογιστές ενός οργανισμού. Έτσι έχει δημιουργηθεί μια «τρύπα» στην ασφάλεια του οργανισμού και πρέπει οι αρμόδιοι να είναι πολύ προσεκτικοί κατά την σχεδίαση, υλοποίηση και λειτουργία του συστήματος τους για να διασφαλιστούν. Αυτό συμβαίνει επειδή το δίκτυο είναι δημόσιο αγαθό. Αυτό που κρατά το Διαδίκτυο ενωμένο είναι μια συμφωνία σε κοινά πρωτόκολλα που χρησιμοποιούνται και στο γεγονός ότι τα δίκτυα επιτρέπουν την κίνηση μεταξύ τους. Παλαιότερα οι χειριστές των τηλεφωνικών κέντρων, ιδιαίτερα στις μικρές πόλεις, μπορούσαν –και το έκαναν- να ακούνε τις τηλεφωνικές συνομιλίες. Με την πάροδο των χρόνων, οι τεχνολογίες και οι οργανισμοί άλλαξαν έτσι ώστε τώρα να απαιτείται το απόρρητο των συνδιαλέξεων. Το δίκτυο ψηφιοποιήθηκε. Ακόμα και να έχει κάποιος πρόσβαση στο τηλεφωνικό σύστημα είναι δύσκολο ή τουλάχιστον χρονοβόρο να πάρει χρήσιμες πληροφορίες ακούγοντας τηλεφωνικές συνδιαλέξεις. Ο υπολογιστής όμως μπορεί να ψάχνει τις συνδιαλέξεις για συγκεκριμένες φράσεις, όπως

οι αριθμοί πιστωτικών καρτών χωρίς ο εισβολέας να χρειάζεται να κάνει κάποια παραπάνω δουλειά.

Πρόβλημα επίσης αποτελεί ότι γίνεται συλλογή πληροφοριών μέσω ενός υπολογιστή. Ένας εισβολέας με πρόσβαση στο χώρο που κρατάει ο πωλητής τα αρχεία του μπορεί να πάει σε καθένα από αυτά και να συλλέξει μια λίστα από αριθμούς πιστωτικών καρτών. Τα υπολογιστικά συστήματα είναι συνήθως έτσι: οι επιθυμητές (και ευαίσθητες) πληροφορίες είναι εύκολα προσπελάσιμες ενώ υπάρχουν προγράμματα που μπορούν να χρησιμοποιηθούν για αναζητήσεις. Επίσης οι υπολογιστές μπορούν να προγραμματιστούν και για άλλες παράνομες δραστηριότητες: για επιβεβαίωση εκατοντάδων παράνομων παραγγελιών, ή για εύρεση τρόπων πρόσβασης σε άλλα υπολογιστικά συστήματα. Οι πιο έμπειροι εισβολείς μπορούν να γράψουν και να διανείμουν προγράμματα σε αρχάριους εισβολείς κάνοντας τους επικινδύνους. Έτσι, σε ένα όχι ασφαλές υπολογιστικό σύστημα μια επίθεση μπορεί να μην αφήσει ίχνη σε αντίθεση με τα εγκλήματα στο φυσικό κόσμο πάντα αφήνουν κάποιες φυσικές αποδείξεις (ένας μάρτυρας, δαχτυλικά αποτυπώματα, εικόνες σε κάμερες ασφαλείας κλπ.).

Στο κομμάτι των αρνητικών στοιχείων χρησιμοποίησης των ηλεκτρονικών καταστημάτων προστίθεται η μη αντικατάσταση του ανθρώπου από τον υπολογιστή. Ο υψάλτηλος είναι πιο ευέλικτος στην επικοινωνία του με ένα πελάτη ή μπορεί να εντοπίσει κάτι ασυνήθιστο στις παραγγελίες. Οι μηχανές δεν έχουν αυτή την ευελιξία. Τέλος είναι πιθανόν κάποιοι άνθρωποι να είναι πιο πρόθυμοι να πουν ψέματα σε ένα υπολογιστικό σύστημα παρά σε ένα άτομο, με αποτέλεσμα οι ενδεχόμενοι εισβολείς να είναι πολλοί περισσότεροι. Ακόμη, οι διακινούμενες πληροφορίες είναι πολύ εύκολο να αντιγραφούν, να μεταβληθούν και να διανεμηθούν.

Είναι σημαντικό να παρατηρηθεί πως χρειάζεται αναδιοργάνωση το ισχύον νομικό σύστημα. Το νομικό σύστημα βασίζεται σε διάφορες φυσικές αποδείξεις (χαρτογραφημένα συμβόλαια, υπογραφές, διευθύνσεις, κλπ.) κατά την εξέταση κάθε υπόθεσης. Στις περισσότερες περιπτώσεις (αν όχι σε όλες), χρησιμοποιούνται ψηφιακές υπογραφές. Πρόκειται βέβαια για μια σχετικά νέα τεχνολογία που απαιτεί κάποια προσπάθεια για να κατανοηθούν τα «λεπτά» σημεία της. Επίσης, πολλά άλλα νομικά θέματα εμπλέκονται καθώς οι τεχνολογίες αλλάζουν.



Κλείνοντας, άξιο αναφοράς αποτελεί και η ασφάλεια. Τα υπολογιστικά συστήματα έχουν αποδειχθεί αρκετά ευαίσθητα στο παρελθόν σε επιθέσεις, έτσι θα πρέπει να δοθεί ιδιαίτερη προσοχή με τα νέα συστήματα ηλεκτρονικού εμπορίου. Η ασφάλεια στο Διαδίκτυο έχει απασχολήσει τα πρωτοσέλιδα των διεθνών μέσων, έτσι ώστε αρκετοί άνθρωποι (και πωλητές και αγοραστές) να ενημερωθούν σχετικά με ζητήματα ασφαλείας. Ακόμα και αν οι κίνδυνοι φαίνονται μικρότερης σημασίας από ότι στον πραγματικό κόσμο, σήμερα επικρατεί η αντίληψη ότι οι κίνδυνοι είναι πιο σοβαροί και είναι ιδιαίτερα σημαντικό να ληφθούν υπόψη τόσο στο σχεδιασμό όσο και στην υλοποίηση των συστημάτων ηλεκτρονικού εμπορίου.

### 4.3 ΤΕΧΝΟΛΟΓΙΚΑ ΜΕΣΑ ΠΡΟΣΤΑΣΙΑΣ

Όπως διαπιστώνεται κι από την παραπάνω θεωρητική ανάλυση περί της ασφάλειας των καταναλωτών, επίκεντρο αποτελούν ο τρόπος έκβασης των διαδικτυακών συναλλαγών κυρίως στο κομμάτι της πληρωμής. Οι πιστωτικές κάρτες δηλαδή κι ο τρόπος χρέωσής τους από τα ηλεκτρονικά καταστήματα, αποτελούν το μείζον πρόβλημα για τον αποφυγή των ηλεκτρονικών αγορών από τον μέσω καταναλωτή. Τα ακόλουθα τέσσερα βασικά σημεία αναφέρονται στην έννοια της ασφάλειας στο ηλεκτρονικό σύστημα πληρωμών:

1. **ΕΓΚΡΙΣΗ:** Αναφέρεται στις μεθόδους προσδιορισμού της ταυτότητας του αγοραστή πριν από την έγκριση πληρωμής
2. **ΚΡΥΠΤΟΓΡΑΦΗΣΗ:** Περιγράφει τις διαδικασίες δημιουργίας και διαχείρισης κρυπτογραφημένων μηνυμάτων με πληροφοριακά δεδομένα, τα οποία αναφέρονται σε στοιχεία προσωπικών δεδομένων του αγοραστή, ώστε να είναι δυνατόν να αποκρυπτογραφηθούν και να αξιοποιηθούν μόνο από όσους έχουν αρμοδιότητα
3. **ΑΚΕΡΑΙΟΤΗΤΑ:** Περιγράφει τις διαδικασίες που χρησιμοποιούνται για διασφάλιση των πληροφοριακών δεδομένων, από ενδεχόμενες αλλαγές, είτε αυτές είναι τυχαίες είτε σκόπιμες

4. **ΕΠΙΒΕΒΑΙΩΣΗ:** Προσδιορίζει τις διαδικασίες που πρέπει να πραγματοποιούνται για την ασφαλή καταχώρηση των δεδομένων μιας συναλλαγής, με σκοπό την κατά το δυνατόν εξασφάλιση κάθε νόμιμου συμφέροντος τόσο του πωλητή, όσο και του αγοραστή.

Εκτός από τα παραπάνω, υπάρχουν κι άλλα πολύ βασικά κι εξειδικευμένα στοιχεία σε θέματα ασφαλείας των ηλεκτρονικών συναλλαγών, τα οποία έχουν αναπτυχθεί και χρησιμοποιούνται από επιχειρήσεις που επιδίδονται ενεργά στο ηλεκτρονικό εμπόριο. Τα στοιχεία αυτά που είναι σχεδόν απαραίτητα και περιλαμβάνονται σε όλα τα πρωτόκολλα και τα προγράμματα ασφαλείας, περιγράφονται παρακάτω:

1. Ιδιωτική Κρυπτογράφηση (secret key cryptography). Είναι μια μορφή κρυπτογράφησης, που βασίζεται σε ένα μυστικό κλειδί, που είναι γνωστό μόνο στον αποστολέα των κρυπτογραφημένων μηνυμάτων και στον παραλήπτη
2. Δημόσια Κρυπτογράφηση (public key cryptography). Στην περίπτωση αυτή τα δύο μέρη που επικοινωνούν διαθέτουν και χρησιμοποιούν ένα κλειδί ιδιωτικής κρυπτογράφησης, που γνωρίζουν μόνο οι ίδιοι και χρησιμοποιούν επίσης ένα δημόσιο κλειδί κρυπτογράφησης. Η κρυπτογράφηση πραγματοποιείται σε δύο φάσεις, πρώτα με εφαρμογή της ιδιωτικής και στην συνέχεια με την χρήση δημόσιου κλειδιού, για διπλά ασφάλεια.
3. Ψηφιακή Υπογραφή (digital signature). Χρησιμοποιεί τη δημόσια κρυπτογράφηση και αναφέρεται στην χρησιμοποίηση του αντίστροφου δημόσιου κλειδιού. Όσοι έχουν το δημόσιο κλειδί, έχουν και την δυνατότητα να αποκρυπτογραφούν το σχετικό μήνυμα. Αυτό όμως που έχει σημασία είναι ότι ο παραλήπτης (που διαθέτει το δημόσιο κλειδί) βεβαιώνεται για την ταυτότητα του αποστολέα
4. Ψηφιακά Πιστοποιητικά (certificates). Αναφέρονται στην αυθεντικοποίηση μηνυμάτων. Βασίζεται σε μια ακολουθία δεδομένων, π.χ. σε διαδοχικούς ακέραιους αριθμούς ή σε ειδικά κρυπτογραφημένα δεδομένα, που εκδίδονται αποκλειστικά από διαπιστευμένους φορείς ή εταιρείες. Οι φορείς αυτοί

επιβεβαιώνουν την αυθεντικότητα των μηνυμάτων και των συναλλασσομένων. Κάθε πιστοποιητικό είναι μοναδικό για κάθε ηλεκτρονική συναλλαγή, δηλαδή για κάθε ζεύγος συναλλασσομένων.

5. Τροποποιημένο Μήνυμα (message digest). Σε πολλές περιπτώσεις ένα μήνυμα πρέπει να είναι και με συμβατό με κανόνες που ισχύουν σε συγκεκριμένες ηλεκτρονικές εφαρμογές. Οι κανόνες αναφέρονται σε διάφορα θέματα όπως για παράδειγμα το μήκος των μηνυμάτων, που ίσως πρέπει να είναι σταθερό. Σε αντίθετη περίπτωση, το μήκος θα πρέπει να αυξομειωθεί.
6. Ακεραιότητα Μηνύματος. Περιλαμβάνει το σύνολο των διαδικασιών σχετικά με την δυνατότητα διασφάλισης ότι το μήνυμα που αποστέλλεται φθάνει στον προορισμό του, χωρίς την παραμικρή αλλαγή των δεδομένων που μεταφέρει κατά τη διαδρομή του από τον αποστολέα στον παραλήπτη.
7. Αρχές Αυθεντικοποίησης (certificate authorities). Είναι οι φορείς ή και οι οργανισμοί που εκδίδουν πιστοποιητικά αυθεντικοποίησης. Μεσολαβούν και παρέχουν υπηρεσίες αυθεντικοποίησης των μηνυμάτων που ανταλλάσσονται μεταξύ των πιστοποιημένων μερών.
8. Πιστοποίηση συναλλαγής (transaction certificate). Είναι η καταγραφή της πλήρους διαδικασίας μιας συναλλαγής. Περιλαμβάνει μια μοναδική ακολουθία δεδομένων που δεν είναι δυνατόν να αλλάξει και χρησιμοποιεί συχνά και χρονικές σημάνσεις. (time stamps). Μοιάζει με τα πιστοποιητικά με την διαφορά ότι αναφέρεται στις συναλλαγές κι όχι στους συναλλασσόμενους.

Εκτός των πρωτοκόλλων γενικότερης ασφάλειας που ακολουθούν τα ηλεκτρονικά καταστήματα στις συναλλαγές τους, η τεχνολογία ασφαλείας εξειδικεύτηκε και στο μείζον θέμα ασφάλειας των ηλεκτρονικών πληρωμών. Έτσι δημιουργήθηκαν και τα αντίστοιχα πρότυπα ασφαλείας. Παρά λοιπόν την ύπαρξη πλέον αρκετά ισχυρών συστημάτων ηλεκτρονικών πληρωμών με πιστωτικές κάρτες, θα πρέπει να αναπτυχθεί κάποιο κοινό πρότυπο που να επιτρέπει στα συστήματα πληρωμών να μπορούν να επικοινωνούν μεταξύ τους. Η έλλειψη διαλειτουργικότητας που παρατηρείται σήμερα,



ίσως να ελαττώσει την αποδοχή των συστημάτων ηλεκτρονικών πληρωμών. Παρόλα αυτά υπάρχουν ήδη, δύο σημαντικά πρότυπα υπό ανάπτυξη, τα οποία θα καταστήσουν την διαλειτουργικότητα αυτών των συστημάτων πιο εύκολη.

Το πρώτο από αυτά αφορά το Secure Electronic Transactions (SET) που αναπτύχθηκε από την Visa και την Mastercard. Το SET χρησιμοποιεί τα λεγόμενα ψηφιακά πιστοποιητικά, που αναλύθηκαν παραπάνω, για την πιστοποίηση της ταυτότητας των συμμετεχόντων σε μια συναλλαγή. Επίσης, κρυπτογραφεί τις πληροφορίες των πιστωτικών καρτών πριν την μετάδοσή τους στο Διαδίκτυο.

Το δεύτερο πρότυπο αφορά το Joint Electronic Payments Initiative (JEPI) που αναπτύχθηκε από την CommerceNet και το World Wide Web Consortium. Το JEPI αποτελεί μια προσπάθεια για προτυποποίηση των διαφορετικών μηχανισμών πληρωμών, πρωτοκόλλων και μεταφοράς. Τέτοια παραδείγματα πληρωμών περιλαμβάνουν οι πιστωτικές κάρτες, οι χρεωστικές κάρτες, το ψηφιακό χρήμα καθώς κι οι ηλεκτρονικές επιταγές. Τα πρωτόκολλα πληρωμών περιλαμβάνουν το STT και το SEPP. Στην ουσία ορίζουν την μορφή του μηνύματος και την διαδικασία που απαιτείται για την ολοκλήρωση της πληρωμής. Το JEPI παρέχει την δυνατότητα στον πελάτη να χρησιμοποιήσει μια μόνο εφαρμογή και μόνο διεπαφή χρήστη για την διεκπεραίωση των συναλλαγών.

#### 4.4 ΕΥΡΩΠΑΪΚΗ ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΑΣΤΙΑΣ ΚΑΤΑΝΑΛΩΤΩΝ

Η οδηγία 2000/31/ΕΚ καλύπτει την ευθύνη των φορέων παροχής υπηρεσιών με έδρα στην ΕΕ για παρεχόμενες υπηρεσίες (υπηρεσίες μεταξύ επιχειρήσεων, υπηρεσίες μεταξύ επιχειρήσεων και καταναλωτών, δωρεάν υπηρεσίες οι οποίες χρηματοδοτούνται, για παράδειγμα, από διαφημιστικά έσοδα ή έσοδα προερχόμενα από χορηγίες), επιγραμμικές ηλεκτρονικές συναλλαγές (διαδραστικές τηλεπωλήσεις αγαθών και υπηρεσιών και επιγραμμικές αγορές από ηλεκτρονικά καταστήματα), επιγραμμικές δραστηριότητες όπως εφημερίδες, βάσεις δεδομένων, χρηματοπιστωτικές υπηρεσίες, επαγγελματικές υπηρεσίες (δικηγόρων, γιατρών, λογιστών, κτηματομεσιτών), ψυχαγωγικές υπηρεσίες (βιντεοταινίες κατά παραγγελία), ενεργητική εμπορική προώθηση και διαφήμιση και υπηρεσίες πρόσβασης στο Διαδίκτυο.

Σημαντικότερο σημείο αυτής αποτελεί το τμήμα 3, που αναλύει την νομοθεσία περί συμβάσεων που εκτελούνται με ηλεκτρονικά μέσα και περιέχει τα άρθρα 9, 10 και 11.

### Άρθρο 9

1. Τα κράτη μέλη μεριμνούν ώστε το νομικό τους σύστημα να επιτρέπει τη σύναψη συμβάσεων με ηλεκτρονικά μέσα. Τα κράτη μέλη εξασφαλίζουν, ιδίως, ότι οι νομικές προϋποθέσεις που ισχύουν για τη διαδικασία σύναψης των συμβάσεων δεν παρακωλύουν τη χρήση των συμβάσεων που συνάπτονται με ηλεκτρονικά μέσα ούτε αποστερούν τις συμβάσεις αυτές εννόμου αποτελέσματος ή ισχύος λόγω του ότι έχουν συναφθεί με ηλεκτρονικά μέσα.

2. Τα κράτη μέλη μπορούν να προβλέψουν ότι η παράγραφος 1 δεν εφαρμόζεται στις ακόλουθες συμβάσεις:

α) στις συμβάσεις που θεμελιώνουν ή μεταβιβάζουν δικαιώματα επί ακινήτου περιουσίας, εκτός από τα δικαιώματα μίσθωσης·

β) στις συμβάσεις οι οποίες απαιτούν εκ του νόμου την προσφυγή σε δικαστήριο, δημόσιες αρχές ή επαγγέλματα που ασκούν δημόσια εξουσία·

γ) στις συμβάσεις εγγυοδοσίας και συναφούς ασφαλείας από πρόσωπα που επιδιώκουν στόχους μη εντασσόμενους στο πλαίσιο της εμπορικής ή επαγγελματικής τους δραστηριότητας·

δ) στις συμβάσεις οι οποίες εμπίπτουν στο οικογενειακό ή κληρονομικό δίκαιο.

3. Τα κράτη μέλη ανακοινώνουν στην Επιτροπή τις κατηγορίες συμβάσεων που αναφέρονται στην παράγραφο 2 επί των οποίων δεν εφαρμόζουν την παράγραφο 1. Τα κράτη μέλη υποβάλλουν κάθε πέντε χρόνια έκθεση στην Επιτροπή σχετικά με την εφαρμογή της παραγράφου 2, στην οποία εξηγούν τους λόγους για τους οποίους θεωρούν αναγκαία τη διατήρηση της κατηγορίας που αναφέρεται στην παράγραφο 2 στοιχείο β), επί της οποίας δεν εφαρμόζουν την παράγραφο 1.

## Άρθρο 10

### Παρεχόμενες πληροφορίες

1. Εκτός από άλλες απαιτήσεις παροχής πληροφοριών οι οποίες προβλέπονται από το κοινοτικό δίκαιο, τα κράτη μέλη εξασφαλίζουν ότι, εφόσον δεν έχουν συμφωνήσει διαφορετικά τα συμβαλλόμενα μέρη που δεν είναι καταναλωτές, ο φορέας παροχής υπηρεσιών πρέπει να παρέχει τουλάχιστο τις ακόλουθες πληροφορίες κατά τρόπο σαφή, κατανοητό και αδιαφιλονίκητο, πριν από την ανάθεση της παραγγελίας από τον αποδέκτη της υπηρεσίας:

α) τα διάφορα τεχνικά στάδια έως τη σύναψη της σύμβασης·

β) εάν ο φορέας παροχής υπηρεσιών θα αρχειοθετήσει ή όχι τη σύμβαση μετά τη σύναψή της και εάν προβλέπεται δυνατότητα πρόσβασης σε αυτήν·

γ) τα τεχνικά μέσα που θα επιτρέπουν τον εντοπισμό και τη διόρθωση σφαλμάτων ηλεκτρονικού χειρισμού πριν από την ανάθεση της παραγγελίας·

δ) τις γλώσσες στις οποίες μπορεί να συναφθεί η σύμβαση.

2. Τα κράτη μέλη εξασφαλίζουν ότι, εφόσον δεν έχουν συμφωνήσει διαφορετικά τα συμβαλλόμενα μέρη που δεν είναι καταναλωτές, ο φορέας παροχής υπηρεσιών δηλώνει τους σχετικούς κώδικες δεοντολογίας στους οποίους υπόκειται, καθώς και τα στοιχεία που επιτρέπουν την πρόσβαση στους εν λόγω κώδικες με ηλεκτρονικά μέσα.

3. Συμβατικοί όροι και γενικοί όροι που προβλέπονται για τον αποδέκτη πρέπει να διατίθενται κατά τρόπο επιτρέποντα την αποθήκευση και την αναπαραγωγή τους.

4. Οι παράγραφοι 1 και 2 δεν εφαρμόζονται σε συμβάσεις που συνάπτονται αποκλειστικά μέσω ανταλλαγής ηλεκτρονικών μηνυμάτων ή ισοδύναμων ατομικών επικοινωνιών.



## Άρθρο 11

### Παραγγελία

1. Τα κράτη μέλη εξασφαλίζουν ότι, εφόσον δεν έχουν συμφωνήσει διαφορετικά τα συμβαλλόμενα μέρη που δεν είναι καταναλωτές, όταν ένας αποδέκτης υπηρεσίας αναθέτει παραγγελία με τεχνολογικά μέσα, ισχύουν οι ακόλουθες αρχές:

- ο φορέας παροχής υπηρεσιών οφείλει να αποστέλλει αποδεικτικό παραλαβής της παραγγελίας του αποδέκτη χωρίς περιττή καθυστέρηση και με ηλεκτρονικά μέσα,
- η παραγγελία και το αποδεικτικό παραλαβής θεωρείται ότι έχουν παραληφθεί όταν τα μέρη στα οποία απευθύνονται έχουν πρόσβαση σε αυτά.

2. Τα κράτη μέλη εξασφαλίζουν ότι, εφόσον δεν έχουν συμφωνήσει διαφορετικά τα συμβαλλόμενα μέρη που δεν είναι καταναλωτές, ο φορέας παροχής θέτει στη διάθεση του αποδέκτη της υπηρεσίας κατάλληλα, αποτελεσματικά και προσιτά μέσα που θα του επιτρέψουν να επισημάνει και να διορθώσει τα λάθη του κατά τον ηλεκτρονικό χειρισμό πριν από την ανάθεση της παραγγελίας.

3. Η παράγραφος 1 πρώτη περίπτωση και η παράγραφος 2 δεν εφαρμόζονται σε συμβάσεις που συνάπτονται αποκλειστικά με την ανταλλαγή ηλεκτρονικών μηνυμάτων ή μέσω ισοδύναμων ατομικών επικοινωνιών. [24]

### 4.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΚΑΤΑΣΤΗΜΑΤΩΝ ΣΤΗΝ ΕΛΛΑΔΑ

Η ανάπτυξη των ηλεκτρονικών καταστημάτων στην Ελλάδα είναι σε ικανό επίπεδο ώστε να δεχτούν και να χρησιμοποιούν τις ηλεκτρονικές αγορές σχεδόν στην καθημερινότητά τους [4]. Το ερώτημα που γεννάται όμως είναι αν όντως από την μεριά τους τα ηλεκτρονικά καταστήματα έχουν συμμορφωθεί με το πλήθος των νομοθετημάτων που τα διέπουν, κι αν η πολιτική προστασίας των καταναλωτών, που ακολουθούν, τελικά όντως προστατεύει τους καταναλωτές τους. Παρακάτω θα

παρουσιασθούν κι θα αναλυθούν περιληπτικά περιπτώσεις που ακολουθούν τη συνήθη πολιτική προστασίας των καταναλωτών και ένα παράδειγμα ιδιαίτερης πρακτικής.

## Συνήθης Πολιτική Προστασίας Καταναλωτών

Η πληθώρα των ηλεκτρονικών καταστημάτων ακολουθούν ενιαία στρατηγική στο θέμα της προστασίας των δεδομένων που καταχωρούν οι καταναλωτές τους. Ενδεικτικά θα αναφερθούν τα ηλεκτρονικά καταστήματα της εταιρείας Γερμανός, Multirama καθώς και τα Media Markt. Με σκοπό την παροχή ποιοτικών υπηρεσιών, συλλέγονται από τους πελάτες τους τα απαιτούμενα στοιχεία για την ασφαλή και αποτελεσματική διενέργεια των συναλλαγών τους, έναντι των οποίων οι εταιρείες ακολουθούν τους όρους και τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα του Ν. 2472/1997, όπως ισχύει σήμερα. Οι εταιρείες που προσπαθούν να κινούνται εντός αυστηρών ορίων νομικού πλαισίου, διατηρούν και μετά την απομάκρυνση από την ιστοσελίδα, το δικαίωμα να μεταβάλλουν τους όρους προστασίας των προσωπικών δεδομένων αφού πρώτα όμως ενημερώσουν τους καταναλωτές τους.

### 1. ΗΛΕΚΤΡΟΝΙΚΟ ΚΑΤΑΣΤΗΜΑ GERMANOS [29]

Στο ηλεκτρονικό αυτό κατάστημα αναφέρονται χαρακτηριστικά :

#### ➤ Όροι Προστασίας Προσωπικών Δεδομένων

*Με σκοπό την παροχή ποιοτικών υπηρεσιών, συλλέγονται από τους πελάτες μας τα απαιτούμενα στοιχεία για την ασφαλή και αποτελεσματική διενέργεια των συναλλαγών τους, έναντι των οποίων η ΓΕΡΜΑΝΟΣ ακολουθεί τους όρους του παρόντος τμήματος και τις αρχές προστασίας των δεδομένων προσωπικού χαρακτήρα του Ν. 2472/1997, όπως ισχύει σήμερα. Η ΓΕΡΜΑΝΟΣ - κινούμενη πάντοτε εντός του νομικού πλαισίου - διατηρεί το δικαίωμα να μεταβάλλει τους όρους προστασίας των προσωπικών δεδομένων μετά από ενημέρωση των χρηστών/επισκεπτών της παρούσας ιστοσελίδας.*

#### ✓ Τι πληροφορίες συλλέγουμε και για ποιους σκοπούς

Όταν δίνετε μια παραγγελία, προκειμένου να συνδεθείτε με το ηλεκτρονικό κατάστημα και να λάβετε ταυτότητα χρήστη (password), ζητάμε από σας να συμπληρώσετε το ονοματεπώνυμο σας, την ηλεκτρονική σας διεύθυνση (e-mail), την διεύθυνση κατοικίας σας και το σταθερό σας τηλέφωνο. Η ΓΕΡΜΑΝΟΣ συλλέγει και χρησιμοποιεί τα ανωτέρω στοιχεία για :

- τις ανάγκες υποστήριξης και ολοκλήρωσης της συναλλαγής που επιθυμούν οι πελάτες να κάνουν με την Εταιρεία και το Δίκτυο Καταστημάτων της (π.χ. επιβεβαίωση της παραγγελίας κ.λ.π.).
- για σκοπούς εμπορικής επικοινωνίας/προώθησης πωλήσεων (ενημέρωση για νέα προϊόντα και υπηρεσίες της Εταιρείας ή του Ομίλου Εταιρειών ΓΕΡΜΑΝΟΣ, προσφορές κ.λ.π.)
- για την άντληση στατιστικών και μόνο καταστάσεων όσον αφορά τους πελάτες του ή / και τις αγορές τους στο e-germanos.gr.

✓ Αποδέκτες δεδομένων

Για τα στοιχεία σχετικά με την αγορά αγαθών ή/και υπηρεσιών μέσα από το ηλεκτρονικό κατάστημα ή τα καταστήματα του Δικτύου Καταστημάτων ΓΕΡΜΑΝΟΣ που επιλέγετε για την εκτέλεση της ή των παραγγελιών σας, Η ΓΕΡΜΑΝΟΣ ενδέχεται να αναθέσει σε τρίτη συνεργαζόμενη μ' αυτήν επιχείρηση την παροχή υπηρεσιών υποστήριξης για τον σκοπό της εμπορικής επικοινωνίας της Εταιρείας με τους πελάτες του ηλεκτρονικού καταστήματος. Όταν γίνεται ανάθεση υπηρεσιών υποστήριξης σε τρίτη επιχείρηση, η ΓΕΡΜΑΝΟΣ απαιτεί και δεσμεύει τέτοια επιχείρηση να συμμορφώνεται με τις αρχές εχεμύθειας που τηρεί η ΓΕΡΜΑΝΟΣ ως προς τα προσωπικά δεδομένα των πελατών/χρηστών. Σε κάθε περίπτωση, για την εμπορική επικοινωνία με τους πελάτες απαιτείται η προηγούμενη συγκατάθεση τους, η οποία δηλώνεται προαιρετικά στην φόρμα συλλογής των στοιχείων κατά την εγγραφή.

✓ Διαφημιστικά μηνύματα

Το e-germanos.gr δεν θα κάνει κατάχρηση της δυνατότητας του να επικοινωνεί με τους χρήστες στην ηλεκτρονική ή ταχυδρομική τους διεύθυνση ή δια του τηλεφώνου για λόγους



προώθησης νέων προϊόντων και υπηρεσιών ή ενημέρωσης περί προσφορών. Παράλληλα δίνεται ανά πάσα στιγμή στους χρήστες η δυνατότητα διακοπής της λήψης τέτοιων μηνυμάτων.

✓ Έλεγχος προϋποθέσεων χρήσης των προσωπικών δεδομένων

Η Εταιρεία μας τηρεί αρχείο με τα ανωτέρω στοιχεία, για όσο χρονικό διάστημα είσαστε εγγεγραμμένο μέλος του e-germanos.gr. Οι χρήστες του e-germanos.gr έχουν το δικαίωμα της πρόσβασης στα προσωπικά τους στοιχεία (άρθρο 12 Ν. 2472/1997), καθώς και το δικαίωμα να ζητήσουν την αλλαγή ή και την διαγραφή ακόμα των προσωπικών τους στοιχείων και δύνανται εν γένει να προβάλλουν οποτεδήποτε αντιρρήσεις για την επεξεργασία των δεδομένων που τους αφορούν (άρθρο 13 Ν.2472/1997).

✓ Αποδοχή των όρων και προϋποθέσεων για τα προσωπικά δεδομένα

Το e-germanos.gr σύμφωνα με τις διατάξεις του Νόμου περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, παρέχει στους χρήστες τη δυνατότητα, κατά τη συμπλήρωση των ατομικών τους στοιχείων στην ειδική ηλεκτρονική φόρμα, να μη χορηγήσουν τη συγκατάθεση τους για την επεξεργασία των προσωπικών τους δεδομένων για λόγους προώθησης πωλήσεων.

✓ Cookies

Δύο διαφορετικά cookies χρησιμοποιούνται στο e-germanos.gr. Το πρώτο αφορά αποκλειστικά τη συλλογή στατιστικών στοιχείων σχετικά με την επισκεψιμότητα στον κόμβο και δεν συνδέεται με τα προσωπικά σας στοιχεία. Το δεύτερο απαιτείται για τη λειτουργία του καλαθιού αγορών και ισχύει μόνο κατά το χρονικό διάστημα που είστε log-in στο e-germanos.gr, μετά δε την αποχώρησή σας από την ιστοσελίδα σβήνονται αμέσως και δεν αποθηκεύονται στο σκληρό σας δίσκο.

✓ Προστασία παιδιών

Το e-germanos.gr ακολουθεί αυστηρά τις σαφείς πολιτικές υπέρ των παιδιών.

α) Η συλλογή, χρήση και διάθεση των προσωπικών τους δεδομένων καθώς και των δεδομένων της οικογενείας τους γίνεται μόνο μετά από ρητή γραπτή έγκριση των κηδεμόνων τους.

β) Το e-germanos.gr διαβεβαιώνει τους πελάτες του ότι έχει λάβει όλα τα απαιτούμενα μέτρα ώστε το περιεχόμενο των διαφημίσεων / διαφημιστικών μηνυμάτων:

Να μην επηρεάζει τα παιδιά αρνητικά σε πνευματικό και ηθικό επίπεδο

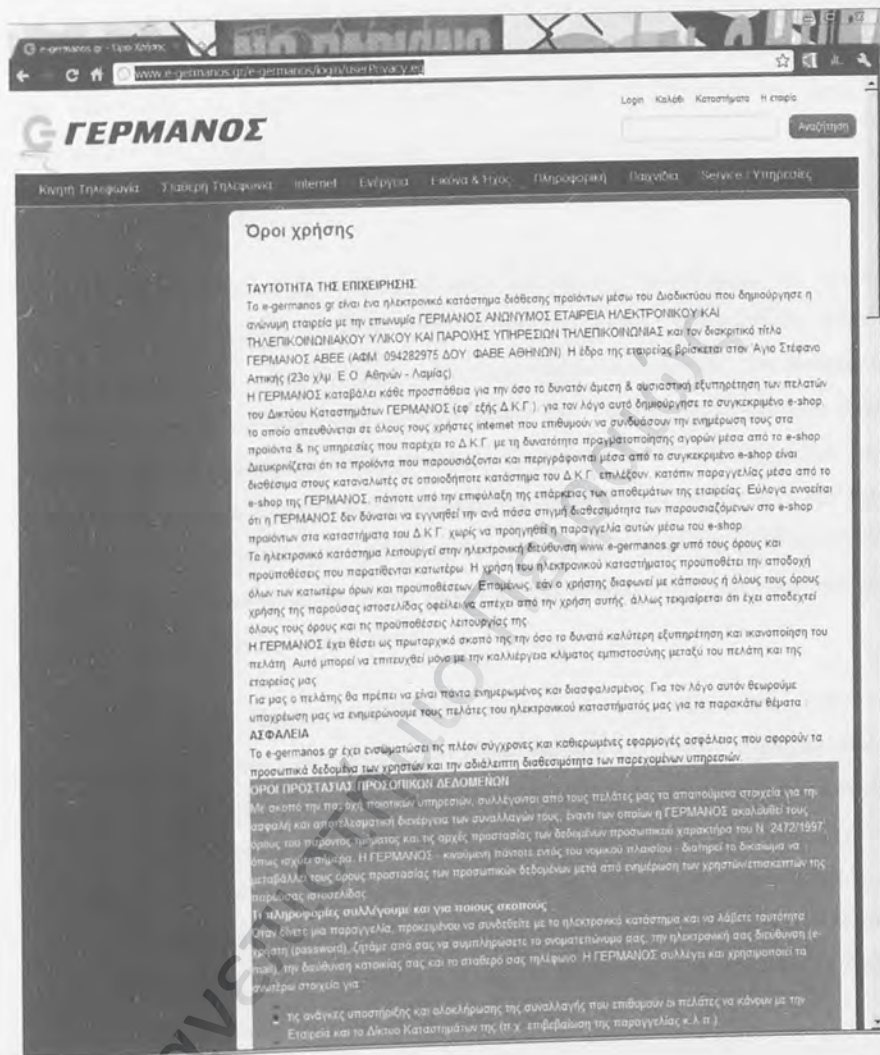
Να μην δίνεται παραπλανητική εικόνα της ποιότητας, του μεγέθους της αξίας ή της απόδοσης των διαφημιζόμενων εμπορευμάτων στα παιδιά.

✓ Η ενημέρωση των πελατών και το είδος των παρεχομένων πληροφοριών

Το e-germanos.gr δεσμεύεται ως προς την ποιότητα, την πληρότητα και την εγκυρότητα των πληροφοριών που παρατίθενται στο site, μόνον όσον αφορά την ταυτότητα του e-germanos.gr και των παρεχομένων απ' αυτό υπηρεσιών.

Ειδικότερα:

Κατά νόμο υπεύθυνη ως προς την λήψη παραγγελίας και την αποστολή εμπορεύματος στα καταστήματα GERMANOS, είναι η GERMANOS ABEE. Για την περαιτέρω ολοκλήρωση του κύκλου της συναλλαγής (παράδοση εμπορεύματος, πληρωμή οφειλομένου τιμήματος, έκδοση παραστατικού) την ευθύνη φέρει το εκάστοτε κατάστημα GERMANOS που έχει επιλέξει ο καταναλωτής. Η GERMANOS ABEE δεν φέρει ευθύνη για δήλωση αναληθών ή ανακριβών στοιχείων που αφορούν τα εμπορεύματα προμηθευτών της. Η σχετική ευθύνη περιγραφής των εμπορευμάτων βαρύνει αποκλειστικά τους επί μέρους προμηθευτές της.»



## ΗΛΕΚΤΡΟΝΙΚΟ ΚΑΤΑΣΤΗΜΑ MEDIAMARKT

Στο ηλεκτρονικό αυτό κατάστημα αναφέρονται χαρακτηριστικά :



*«Η χρήση αυτού του δικτυακού τόπου υποδηλώνει ανεπιφύλακτη συμφωνία με τους όρους χρήσης. Παρακαλούμε διαβάστε προσεκτικά τους όρους αυτούς προτού χρησιμοποιήσετε την ιστοσελίδα. Η διαχειρίστρια ΕΤΑΙΡΕΙΑ διατηρεί το δικαίωμα να μεταβάλλει οποτεδήποτε τους όρους χρήσης.»*

#### ✓ Πνευματική Ιδιοκτησία

*Η επωνυμία, ο διακριτικός τίτλος, το σήμα, οι εικόνες, τα γραφικά, τα διακριτικά γνωρίσματα, τα κείμενα και κάθε άλλο τι που περιέχεται στη δικτυακή τοποθεσία [www.mediamark.gr](http://www.mediamark.gr) αποτελούν προστατευόμενα αγαθά πνευματικής και βιομηχανικής ιδιοκτησίας της ΕΤΑΙΡΕΙΑΣ και των εταιρειών του Ομίλου Media-Saturn. Σήματα, ονόματα, ή άλλα δικαιώματα πνευματικής και βιομηχανικής ιδιοκτησίας τρίτων μερών, που εκτίθενται στην ιστοσελίδα της ΕΤΑΙΡΕΙΑΣ προστατεύονται σύμφωνα με την κείμενη νομοθεσία. Απαγορεύεται στον χρήστη η αντιγραφή, αναπαραγωγή, διάδοση, διάθεση, μετάδοση ή η με οιονδήποτε τρόπο χρήση αυτών, πέραν των χρήσεων που ρητώς ορίζονται στον παρόντα δικτυακό τόπο.*

*Ειδικότερα, επί του λογισμικού, μουσικών κομματιών, κ.λπ., όπως και εφόσον αυτά καθίστανται διαθέσιμα προς λήψη και επισημαίνονται ως τέτοια, παραχωρείται στο χρήστη ένα μη αποκλειστικό και μη μεταβιβάσιμο δικαίωμα χρήσης στη συμφωνηθείσα έκταση ή, εφόσον δεν έχει υπάρξει σχετική συμφωνία, σε έκταση που αντιστοιχεί στον επιδιωκόμενο σκοπό από την Εταιρεία με αυτή τη διάθεση και παραχώρηση. Δεν υφίστανται άλλα δικαιώματα χρήσης και εκμετάλλευσης. Ιδίως δε, δεν επιτρέπεται στο χρήστη να αναπαράγει σε αντίτυπα, να διαθέτει, να μεταδίδει ή να επιτρέπει τη δημόσια πρόσβαση στο λογισμικό, τα μουσικά κομμάτια, κ.λπ.*

#### ✓ Προστασία Προσωπικών Στοιχείων

*Η ΕΤΑΙΡΕΙΑ έχει το δικαίωμα να διατηρεί αρχείο και να επεξεργάζεται τυχόν δεδομένα προσωπικού χαρακτήρα των επισκεπτών του παρόντος δικτυακού τόπου, στο μέτρο που αυτό απαιτείται για την σωστή λειτουργία και ανάπτυξη της. Ο επισκέπτης διατηρεί το δικαίωμα ενημέρωσης (βλέπε Πολιτική Προστασίας Δεδομένων), πρόσβασης και αντίρρησης στην περαιτέρω επεξεργασία σύμφωνα με τα άρθρα 12 και 13 του Ν. 2472/97 για την προστασία δεδομένων προσωπικού χαρακτήρα.*

✓ Σύνδεσμοι με άλλες ιστοσελίδες

Οι σύνδεσμοι (links) που βρίσκονται στο site [www.mediamarkt.gr](http://www.mediamarkt.gr) πιθανόν να μεταφέρουν τον χρήστη εκτός του δικτύου της σε ιστοσελίδες που δεν ελέγχονται με οποιονδήποτε τρόπο από την ΕΤΑΙΡΕΙΑ.

Στην περίπτωση αυτή, η ΕΤΑΙΡΕΙΑ δεν φέρει καμία ευθύνη για το περιεχόμενο, την ακρίβεια, τη λειτουργία, τις μεταδόσεις, καθώς και για τυχόν μεταγενέστερες αλλαγές στις ιστοσελίδες αυτές. Δεν αναλαμβάνει ουδεμία ευθύνη για τα περιεχόμενα προσφορών τρίτων. Οι διαδικτυακοί τόποι, στους οποίους παραπέμπει άμεσα μέσω εξωτερικών συνδέσμων, επιλέγονται από την Εταιρεία με τη δέουσα προσοχή πριν την ανάρτηση του εκάστοτε συνδέσμου. Εν τούτοις, η Εταιρεία δεν ασκεί ουδεμία επιρροή σε μεταγενέστερες αλλαγές στους άμεσα συνδεδεμένους διαδικτυακούς τόπους, καθώς και σε περιεχόμενα επακόλουθων διαδικτυακών τόπων τρίτων παρόχων. Ως εκ τούτου αποστασιοποιείται η Εταιρεία ρητώς από μεταγενέστερες αλλαγές άμεσα συνδεδεμένων διαδικτυακών τόπων, από περιεχόμενα επακόλουθων διαδικτυακών τόπων και τους παρόχους τους.

✓ Ευθύνη Χρήστη

Κάθε χρήστης της ιστοσελίδας συμφωνεί με τους Όρους Χρήσης και την Πολιτική Προστασίας Δεδομένων και, υποχρεούται να μη χρησιμοποιεί αυτή ή οποιοδήποτε στοιχείο, πληροφορία ή άλλο τι εκτίθεται ή πηγάζει ή συνθέτει αυτή, εμπιστευτικού ή μη, κεκρυμμένου ή φανερού χαρακτήρα, με κανένα τρόπο –ενδεικτικά με δημοσίευση, επέμβαση, (ανά)μετάδοση, αντιγραφή, μεταφορά δεδομένων, στοιχείων, μηνυμάτων, ιών, λογισμικού, υλικού, αρχείου κ.λπ.- για την τέλεση πράξεων, οι οποίες θα μπορούσαν να προκαλέσουν ή θα προκαλούσαν προσβολή, ζημία ή βλάβη περιουσιακών αγαθών ή προσωπικών δικαιωμάτων της ΕΤΑΙΡΕΙΑΣ, του Ομίλου Εταιρειών της Media Saturn ή οποιουδήποτε τρίτου, ή θα αποτελούσαν παραβίαση της ισχύουσας νομοθεσίας, ανεξαρτήτως υπαιτιότητας.

✓ Ευθύνη Εταιρείας

Δεν ευθύνεται η Εταιρεία ως προς την επικαιρότητα, την ορθότητα, την πληρότητα ή την ποιότητα των αναφερόμενων πληροφοριών στο [Mediapedia](http://Mediapedia). Αξιώσεις αποζημίωσης

λόγω αστικής ευθύνης εναντίον της Εταιρείας, οι οποίες αφορούν σε υλικές ή ηθικές βλάβες που έχουν προκληθεί από τη χρήση ή τη μη χρήση των αναφερόμενων πληροφοριών ή/και τη χρήση ανακριβών και ελλιπών πληροφοριών, αποκλείονται γενικά, εφόσον δεν προβλέπεται από τη νομοθεσία σχετική υποχρέωση για κάλυψη αστικής ευθύνης. Επιφυλάσσεται η Εταιρεία ρητώς του δικαιώματος τροποποίησης, συμπλήρωσης ή διαγραφής τμημάτων των επιμέρους σελίδων ή στο σύνολο, ή της προσωρινής ή οριστικής διακοπής της δημοσίευσης χωρίς προειδοποίηση.

### Ηλεκτρονικό κατάστημα MULTIRAMA

Στο ηλεκτρονικό αυτό κατάστημα αναφέρονται χαρακτηριστικά :

#### **Όροι χρήσεως**

Καλώς ήλθατε στις ιστοσελίδες της εταιρίας μας. Κάνοντας χρήση του site μας, συμφωνείτε με τους κάτωθι όρους, τους οποίους θα πρέπει να διαβάσετε προσεκτικά.

Οποιοδήποτε λογισμικό διατίθεται για φόρτωση (down-loading) από αυτόν τον διακομιστή, αποτελεί πνευματική ιδιοκτησία της MULTIRAMA ΑΕΒΕ. Η χρήση τέτοιων εγγράφων από αυτόν τον διακομιστή περιορίζεται αποκλειστικά για πληροφοριακούς και μη εμπορικούς σκοπούς ή είναι μόνον προσωπική και δεν θα αντιγραφούν ούτε θα τεθούν σε άλλο δίκτυο υπολογιστών, ούτε θα διανεμηθούν με άλλα μέσα επικοινωνίας. Δεν επιτρέπεται καμία απολύτως επέμβαση στα έγγραφα. Οποιαδήποτε άλλη χρήση απαγορεύεται αυστηρά από το νόμο και ενδέχεται να συνεπάγεται αυστηρές αστικές και ποινικές κυρώσεις. Οι παραβάτες θα διώκονται νομικά.

Η MULTIRAMA ΑΕΒΕ δεν δηλώνει με κανέναν τρόπο ότι οι πληροφορίες που περιλαμβάνονται στα έγγραφα και στις ανακοινώσεις που δημοσιεύονται σ'αυτόν τον διακομιστή είναι κατάλληλα για οποιονδήποτε σκοπό. Κάθε τέτοιο έγγραφο και σχετική γραφική απεικόνιση παρέχεται "ως έχει" χωρίς καμιά απολύτως εγγύηση οποιουδήποτε είδους.

Η MULTIRAMA ΑΕΒΕ δεν φέρει ευθύνη ούτε υποχρέωση αποζημίωσης για οποιαδήποτε ζημιά και ηθική βλάβη που προκύπτει από αδυναμία παροχής υπηρεσιών υποστήριξης.



Είστε ελεύθεροι να κάνετε χρήση του [www.multirama.gr](http://www.multirama.gr) σύμφωνα με τον Νόμο και τα χρηστά ήθη. Η ευθύνη για τα περιεχόμενα των συναλλαγών ανήκει αποκλειστικά σε σας. Η MULTIRAMA ΑΕΒΕ δεν ασκεί κανένα είδος διόρθωσης ή παρέμβασης στα δεδομένα που μεταφέρετε. Ζητάμε να συμπληρώνετε σωστά τα εξής πεδία (όνομα, διεύθυνση, μήνυμα) στις on-line φόρμες επικοινωνίας. Η χρήση του site της MULTIRAMA ΑΕΒΕ υπόκειται στους Ελληνικούς και τους Διεθνείς νόμους και συμφωνείτε να μην χρησιμοποιείτε το site μας με σκοπό να παραβιάσετε αυτούς τους νόμους.

## Ευθύνη του χρήστη

Οι χρήστες συμφωνούν και αναλαμβάνουν να μη χρησιμοποιούν το ηλεκτρονικό κατάστημα για

- Αποστολή, δημοσίευση, αποστολή με e-mail ή μετάδοση με άλλους τρόπους οποιουδήποτε περιεχομένου που είναι παράνομο για οποιοδήποτε λόγο, προκαλεί παράνομη προσβολή και βλάβη στην Multirama ή σε οποιοδήποτε τρίτο είτε προσβάλλει την εμπιστευτικότητα ή το απόρρητο πληροφοριών οιοδήποτε πρόσωπο
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μετάδοση με άλλους τρόπους οποιουδήποτε περιεχομένου που προκαλεί προσβολή των χρηστών ηθών, κοινωνικών αξιών, της ανηλικότητας κ.λ.π.
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μετάδοση με άλλους τρόπους οποιουδήποτε περιεχομένου για το οποίο οι χρήστες δεν έχουν δικαίωμα μετάδοσης σύμφωνα με το νόμο ή τις εν ισχύ συμβάσεις (όπως εσωτερικές πληροφορίες, ιδιοκτησιακές και εμπιστευτικές πληροφορίες που αποκτήθηκαν ή αποκαλύφθηκαν ως μέρος εργασιακών σχέσεων ή που καλύπτονται σε συμφωνίες εμπιστευτικότητας),
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μετάδοση με άλλους τρόπους οποιουδήποτε περιεχομένου το οποίο παραβιάζει οποιαδήποτε ευρεσιτεχνία, εμπορικό σήμα, εμπορικό μυστικό, πνευματικά δικαιώματα ή άλλα ιδιοκτησιακά δικαιώματα τρίτων,
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μετάδοση με άλλους τρόπους οποιουδήποτε υλικού το οποίο περιέχει ιούς λογισμικού ή οποιοσδήποτε άλλους

*κώδικες, αρχεία ή προγράμματα που έχουν σχεδιαστεί με σκοπό την διακοπή, την πρόκληση βλάβης, την καταστροφή ή τον εξοπλισμό της λειτουργίας οποιουδήποτε λογισμικού ή υλικού υπολογιστών,*

- *Ηθελυμένη ή αθέλητη παράβαση της ισχύουσας νομοθεσίας ή των διατάξεων,*
- *Παρενόχληση τρίτων με οποιοδήποτε τρόπο.*
- *Συλλογή ή αποθήκευση προσωπικών δεδομένων σχετικά με άλλους χρήστες.*

*Επίσης συμφωνούν ότι όλα τα μέλη, οι συνεργάτες, οι υπάλληλοι, η διοίκηση, οι μέτοχοι και άλλοι συνεργάτες της MULTIRAMA ΑΕΒΕ δεν ευθύνονται για οτιδήποτε προκύψει από τρίτα μέλη τα οποία χρησιμοποιούν το site της MULTIRAMA ΑΕΒΕ. Κάθε χρήση αντίθετη προς τα ανωτέρω εκτός των τυχών ή και αστικών κυρώσεων επιφέρει και διακοπή των παρεχόμενων υπηρεσιών χωρίς καμία ειδοποίηση.*

### **Πνευματικά Δικαιώματα**

*Στο site περιλαμβάνονται υλικό, trademarks, service marks, trade dress και άλλο περιεχόμενο που ανήκει στην MULTIRAMA ΑΕΒΕ και προστατεύεται από το Νόμο. Όλα τα περιεχόμενα του site (συμπεριλαμβανομένων κειμένων, γραφικών, εικόνων, φωτογραφιών και λογισμικού) είναι πνευματικής ιδιοκτησία της MULTIRAMA ΑΕΒΕ και προστατεύονται από την Ελληνική και Διεθνή Νομοθεσία. Απαγορεύεται η οποιαδήποτε αντιγραφή, αναπαραγωγή και αναμετάδοση του υλικού, χωρίς έγγραφη άδεια της εταιρίας. Η εμφάνισή του στον διαδικτυακό τόπο δεν θα πρέπει κατά κανένα τρόπο να εκληφθεί ως μεταβίβαση ή εκχώρηση άδειας ή δικαιώματος χρήσης τους.*

### **Όρια Ευθύνης**

*Χρησιμοποιώντας το site, συμφωνείτε απόλυτα ότι η χρήση γίνεται με δική σας ευθύνη. Η MULTIRAMA ΑΕΒΕ κάνει κάθε δυνατή προσπάθεια να παρέχει υπηρεσία υψηλής ποιότητας αλλά δεν μπορούμε να εγγυηθούμε ότι δεν θα υπάρξουν διακοπές ή λάθη. Οποιαδήποτε αναφορά ή και link σε άλλο site, παρέχεται για την διευκόλυνσή σας και δεν ευθυνόμαστε για τα περιεχόμενα, τα προϊόντα και τις υπηρεσίες που παρέχονται (διαφήμιση ή πώληση) στα site αυτά. Οι φωτογραφίες των προϊόντων είναι ενδεικτικές.*

## Ισχύων Νόμος

Το site έχει δημιουργηθεί και ελέγχεται από την MULTIRAMA ΑΕΒΕ, στην Αθήνα και η Ελληνική Νομοθεσία θα καθοδηγεί την χρήση του site και την ερμηνεία του. Αν επιλέξετε να έχετε πρόσβαση στο site μας από άλλη χώρα, έχετε την ευθύνη να ακολουθείτε τους Νόμους της χώρας αυτής. Οι παραπάνω όροι αποτελούν την πλήρη συμφωνία με την MULTIRAMA ΑΕΒΕ και η MULTIRAMA ΑΕΒΕ έχει το δικαίωμα να κάνει αλλαγές στο περιεχόμενο του site και στους ανωτέρους όρους χωρίς καμία προειδοποίηση.

## Δήλωση Εχεμύθειας

Η παρούσα δήλωση εχεμύθειας αφορά στο site της MULTIRAMA ΑΕΒΕ ([www.multirama.gr](http://www.multirama.gr))

Όταν στέλνετε ένα αίτημα online, η πληροφορία που μας παρέχετε χρησιμοποιείται για να σας απαντήσουμε ηλεκτρονικά στην ερώτησή σας. Θεωρούμε τις αιτήσεις που συμπληρώνετε και την ηλεκτρονική αλληλογραφία που στέλνετε απόρρητη. Δεν μεταβιβάζουμε το περιεχόμενο αυτών παρά μόνο στον άμεσα ενδιαφερόμενο αποδέκτη και στον νόμο, εφόσον αυτό μας ζητηθεί ή στην περίπτωση που το περιεχόμενο του μηνύματος θεωρούμε ότι μας θίγει.

Τέτοια ενέργεια είναι απαραίτητη προκειμένου να:

- προστατέψουμε τα δικαιώματά μας και την περιουσία μας
- προστατευθούμε ενάντια στην κακή ή στην μη εξουσιοδοτημένη χρήση του site της MULTIRAMA ΑΕΒΕ
- προστατεύσουμε την προσωπική μας ασφάλεια ή την περιουσία των χρηστών και του κοινού μας.

Παρ' όλα αυτά, εάν μας δώσετε ψευδή ηλεκτρονική διεύθυνση ή προσπαθήσετε να πάρετε τη θέση κάποιου άλλου όταν στέλνετε πληροφορίες online, όλες οι πληροφορίες - καθώς επίσης και το IP address - θα αποτελούν μέρος οποιασδήποτε έρευνας. Οι άνθρωποι της MULTIRAMA ΑΕΒΕ μπορεί να χρειαστεί να επεξεργαστούν το ηλεκτρονικό σας μήνυμα σε συνεργασία με το τεχνικό τμήμα. Επίσης, αν ζητήσετε έναν από τους υπεύθυνους εξυπηρέτησης πελατών της MULTIRAMA ΑΕΒΕ να σας βοηθήσει σε οποιαδήποτε



ηλεκτρονική αλληλογραφία, αυτός, θα μπορεί να έχει πρόσβαση σε όλο το εύρος πληροφοριών το οποίο είναι σχετικό με το αίτημά σας, συμπεριλαμβανομένων της ηλεκτρονικής σας διεύθυνσης και των μηνυμάτων σας. Η MULTIRAMA AEBE έχει συνδέσεις με άλλα sites. Δεν είμαστε υπεύθυνοι για την πολιτική ασφαλείας τους ή για τον τρόπο με τον οποίο διαχειρίζονται τους ηλεκτρονικούς τους επισκέπτες.»

#### Ασφάλεια Συναλλαγών & Προσωπικά Δεδομένα

1. Η ΕΤΑΙΡΕΙΑ αναγνωρίζει τη σημασία του θέματος της ασφαλείας των Προσωπικών Δεδομένων, καθώς και των ηλεκτρονικών συναλλαγών και έχει λάβει όλα τα απαραίτητα μέτρα, με τις πιο σύγχρονες και προηγμένες μεθόδους, ώστε να εξασφαλίζεται η μέγιστη δυνατή ασφάλεια. Όλες οι πληροφορίες, οι οποίες σχετίζονται με τα προσωπικά στοιχεία των χρηστών, διασφαλίζονται ως απόρρητες.

2. Η MULTIRAMA χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128-bit (την πιο ισχυρή σήμερα), για ασφαλείς online εμπορικές συναλλαγές. Με αυτόν τον τρόπο κρυπτογραφούνται όλες οι προσωπικές σας πληροφορίες, συμπεριλαμβάνοντας τον αριθμό της πιστωτικής κάρτας, το όνομα και την διεύθυνση σας, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλαχθούν κατά την μεταφορά τους στο Internet.

3. Το πρωτόκολλο SSL (Secure Sockets Layer), είναι σήμερα το παγκόσμιο standard στο διαδίκτυο για την πιστοποίηση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών (web servers). Μία κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να κρυπτογραφούνται από το λογισμικό αποστολής και να αποκρυπτογραφούνται από το λογισμικό αποδοχής, προστατεύοντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατεύονται από έναν μηχανισμό που αυτόματα εξακριβώνει εάν τα δεδομένα έχουν αλλάξει κατά την μεταφορά.

4. Τα στοιχεία των χρηστών (όνομα, επάγγελμα, ηλεκτρονική διεύθυνση, διεύθυνση κατοικίας, κλπ.) και των συναλλαγών των χρηστών του ηλεκτρονικού καταστήματος θεωρούνται απόρρητα, όπως και στις συνήθεις συναλλαγές σε εμπορικό κατάστημα. Οι

χρήστες κατά την παροχή των στοιχείων τους στα πλαίσια των συναλλαγών τους όπως και με το παρόν, θα ενημερώνονται από την Multirama και συναινούν και αποδέχονται την επικείμενη επεξεργασία των στοιχείων αυτών προσωπικών δεδομένων, για τις ανάγκες της ομαλής και ευχερούς μεταξύ των μερών συναλλαγής, καθώς επίσης και της διαβίβασης των στοιχείων αυτών σε αποδέκτες οι οποίοι θα προσδιορίζονται συγκεκριμένα και είναι οι υπάλληλοι και προσηθθέντες της εταιρίας στα πλαίσια της διεκπεραίωσης της καταρτιζόμενης σύμβασης. Επίσης και με τον παρόν γνωστοποιείται η ύπαρξη του δικαιώματος πρόσβασης και του δικαιώματος εναντίωσης του άρθρου 12 και 13 του του Ν. 2472/1997.

Βεβαιώνεται ότι μόνο εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση στις πληροφορίες των συναλλαγών και μόνο όποτε αυτό είναι αναγκαίο, π.χ. για τη διεκπεραίωση των παραγγελιών. Κατά τα λοιπά η Multirama δεσμεύεται να μην αποκαλύψει τα στοιχεία των πελατών και των συναλλαγών τους, εκτός αν έχει έγγραφη εξουσιοδότηση από τους ίδιους, ή αυτό επιβάλλεται από δικαστική απόφαση ή απόφαση άλλης δημόσιας αρχής. Τα προσωπικά δεδομένα που δηλώνονται στο ηλεκτρονικό κατάστημα με το εμπορικό σήμα Multirama χρησιμοποιούνται αποκλειστικά από αυτό ή συνεργαζόμενες με αυτό επιχειρήσεις, με σκοπό την υποστήριξη, προώθηση και εκτέλεση της συναλλακτικής σχέσης. Το σύνολο των εγγράφων και ηλεκτρονικών στοιχείων που θα ανταλλάχθουν μεταξύ των μερών στα πλαίσια της πώλησης θα τηρούνται από την Multirama . Ο πελάτης μπορεί να έχει πρόσβαση σε αυτά εφόσον το επιθυμεί.

The screenshot shows a web browser displaying the website of MULTIRAMA TECH EASRY. The page title is "Όροι Χρήσης Ιστοτόπου & Δήλωση Εχεμύθειας". The content includes:

**Όροι χρήσεως**  
Καλώς ήλθετε στις σελίδες της εταιρείας μας. Κάνοντας χρήση του site μας, συμφωνείτε με τους κάτωθι όρους, τους οποίους θα πρέπει να διαβάσετε προσεκτικά.

Οποιοδήποτε λογισμικό διατίθεται για φόρτωση (down-loading) από αυτόν τον δικασιμη, αποτελεί πνευματική ιδιοκτησία της MULTIRAMA AEBE. Η χρήση τέτοιων εγγράφων από αυτόν τον δικασιμη περιορίζεται αποκλειστικά για πληροφοριακούς και μη εμπορικούς σκοπούς (ή είναι μόνον προσωπική) και δεν θα αντηρρούν ούτε θα τεθούν σε άλλα δίκτυα υπολογιστών, ούτε θα δανεισθούν με άλλο μέσο επικοινωνίας, δεν επιτρέπεται καμία απολύτως εντύπωση αποσύνθεσης κειμένου, Οποιοδήποτε άλλη χρήση απαγορεύεται αυστηρά από το νόμο και ενδέχεται να συνιστάται αυστηρές ποινικές κυρώσεις. Οι παραβιάσεις θα διώκονται νομικά.

Η MULTIRAMA AEBE δεν δηλώνει με κανέναν τρόπο ότι οι πληροφορίες που περιλαμβάνονται στα έγγραφα και στις ανακοινώσεις που δημοσιεύονται σ'αυτών τον δικασιμη είναι κατάλληλα για αποσύνθεσης ακριβή. Κάθε τέτοιο έγγραφο και οπτική γραφή απεικόνιση παράσχει "ως έχει" χωρίς καμία απολύτως εντύπωση αποσύνθεσης κειμένου.

Η MULTIRAMA AEBE δεν φέρει ευθύνη ούτε υπαπόκειται αποζημίωσης για οποιοδήποτε ζημιά και ηθική βλάβη που προκύπτει από ελλιπή παροχή υπηρεσιών υποστήριξης.

Είστε ευλαβικοί να κάνετε χρήση του www.multirama.gr σύμφωνα με τον νόμο και τα χρηστά ήθη. Η εμψυχή να τη παρέχουμε των αναλαμβανόμενων αποκλειστικά σε σας, Η MULTIRAMA AEBE δεν ασεί κανένα είδος διάκρισης ή παραβίασης στα δεδομένα που μεταφέρονται. Ζητήμα με συμπληρώνεται αυτού τα εφό ταύτα (έννοια, διεύθυνση, μήνυμα) στις απ'αυτή φέρουμε επικοινωνίας. Η χρήση του site της MULTIRAMA AEBE υπόκειται στους ΕΛΛΗΝΙΚΟΥΣ ΚΑΙ ΤΟΥΣ ΔΕΦΝΙΚΟΥΣ ΝΟΜΟΥΣ και συμφωνώντας να μην χρησιμοποιήσετε το site μας με σκοπό να παραβιάσετε αυτούς τους νόμους.

**Ευθύνη του χρήστη**  
Οι χρήστες συμφωνούν και αναλαμβάνουν να μη χρησιμοποιούν το ηλεκτρονικό κατάστημα για

- Αποστολή, δημοσίευση, αποστολή με e-mail ή μεθόδους με άλλους τρόπους αποσύνθεσης περιεχομένου που είναι παράνομο να αποσύνθεσης λήνη, προκαλεί παράνομη προσβολή και βλάβη στην Multirama ή σε οποιοδήποτε τρίτο στη προσβολή την εμπιστευτικότητα ή το απόρρητο πληροφοριών οποιουδήποτε προσώπου
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μεθόδους με άλλους τρόπους αποσύνθεσης περιεχομένου που προκαλεί προσβολή των χρηστών ήθων, κοινωνικών αξιών, της ανηλικιότητας κ.λ.π.
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μεθόδους με άλλους τρόπους αποσύνθεσης περιεχομένου για το οποίο οι χρήστες δεν έχουν δικασιμη μεθόδους σύμφωνα με το νόμο ή τις αρχές συμβάσεως (όπου εσωτερικές πληροφορίες, δημοσιογραφικές και εμπιστευτικές πληροφορίες που αποκτήθηκαν ή αποκαλύφθηκαν με μίσηρ εργασιακών σχέσεων ή που καλύπτονται σε συμφωνικές εμπιστευτικότητας).
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μεθόδους με άλλους τρόπους αποσύνθεσης περιεχομένου το οποίο παραβιάζει οποιοδήποτε ευρωπαϊκό, εμπορικό σήμα, εμπορικό μυστικό, πνευματικό δικασιμη ή άλλα δικασιμη δικαιώματα τρίτων.
- Αποστολή, δημοσίευση, αποστολή με e-mail ή μεθόδους με άλλους τρόπους αποσύνθεσης υλικού το οποίο περιέχει υλικό λογισμικό ή οποιοδήποτε άλλους κωδικούς, αρχεία ή προγράμματα που έχουν σχεδιαστεί με σκοπό την διακοπή, την πρόκληση βλάβης, την καταστροφή ή τον αποκλεισμό της λειτουργίας οποιοδήποτε λογισμικού ή υλικού υπολογιστών.
- Ηλεκτρονική ή σφάλματα παράδοσης της αντιστοιχίας νομοθεσίας ή των διατάξεων.
- Παραποίηση ή τρίτων με οποιοδήποτε τρόπο.
- Συμβολή ή απόκτηση προσωπικών δεδομένων σχετικά με άλλους χρήστες.

Επίσης συμφωνούν ότι όλα τα μέλη/οι συνεργάτες, οι υπάλληλοι, οι δοκίμοι, οι μεταφορικοί και άλλοι συνεργάτες της MULTIRAMA AEBE δεν ευλαβούνται να στείλουν προέλαση από τρίτα μέλη τα οποία χρησιμοποιούν το site της MULTIRAMA AEBE. Καθή χρήση αντίθετη προς τα ανωτέρω εκτός των τυχόν ή και ορισμένων κυρώσεων επιπλέον και δικαστική των παρεχόμενων υπηρεσιών χωρίς καμία εξαίρεση.

**Πνευματικά Δικασιμη**  
Στο site περιλαμβάνονται εικόνες, trade marks, service marks, trade dress και άλλα περιεχόμενα που ανήκουν στην MULTIRAMA AEBE και προστατεύονται από το νόμο. Όλα τα περιεχόμενα του site (συμπληρωματικών κειμένων, γραφικών, ακόνων, φωτογραφιών και λογισμικού) είναι πνευματικές ιδιοκτησία της MULTIRAMA AEBE και προστατεύονται από την ΕΛΛΗΝΙΚΗ ΚΑΙ



**Ασφάλεια Συναλλαγών & Προσωπικά Δεδομένα**

1. Η ΕΤΑΡΕΙΑ αναγνωρίζει τη σημασία του θέματος της ασφαλείας των Προσωπικών Δεδομένων, καθώς και των ηλεκτρονικών συναλλαγών και έχει λάβει όλα τα απαραίτητα μέτρα, με τα οποία σίγουρες και προηγμένες μεθόδους, ώστε να εξασφαλιστεί η μέγιστη δυνατή ασφάλεια. Όλες οι πληροφορίες, οι οποίες σχετίζονται με τα προσωπικά στοιχεία των χρηστών, διασφαλίζονται ως απόρρητες.
2. Η MULTIRAMA χρησιμοποιεί το πρωτόκολλο SSL, με κρυπτογράφηση 128-bit (πέντε φορές ισχυρότερη), ως ασφαλή online-εμπορική συναλλαγή. Με αυτόν τον τρόπο κρυπτογραφούνται όλες οι προσωπικές σας πληροφορίες, συμπεριλαμβανομένων των αριθμών της πιστωτικής κάρτας, του όνομα και την διεύθυνσή σας, έτσι ώστε να μην μπορούν να διαβαστούν ή να αλλάξουν κατά την μεταφορά τους στο Internet.
3. Το πρωτόκολλο SSL (Secure Sockets Layer), είναι σήμερα το παγκόσμιο standard στο δίκτυο για την κατοχύρωση δικτυακών τόπων (web sites) στους δικτυακούς χρήστες και για την κρυπτογράφηση στοιχείων μεταξύ των δικτυακών χρηστών και των δικτυακών εξυπηρετητών (web servers). Μία κρυπτογραφημένη SSL επικοινωνία απαιτεί όλες τις πληροφορίες που αποστέλλονται μεταξύ ενός πελάτη και ενός εξυπηρετητή (server) να κρυπτογραφούνται από το λογισμικό ασφαλείας και να αποσυμπεριγραφούνται από το λογισμικό αποδέκτη, προστατώντας έτσι προσωπικές πληροφορίες κατά τη μεταφορά τους. Επιπλέον, όλες οι πληροφορίες που αποστέλλονται με το πρωτόκολλο SSL, προστατώνται από έναν μηχανισμό που αυτόματα εμβραβώνει τα δεδομένα έναντι αλλαγών κατά την μεταφορά.
4. Τα στοιχεία των χρηστών (όνομα, επώνυμο, ηλεκτρονική διεύθυνση, διεύθυνση κατοικίας, κλπ) και των συναλλαγών των χρηστών του ηλεκτρονικού καταστήματος θεωρούνται απόρρητα, όπως και στις ομήρες συναλλαγές σε εμπορικό κατάστημα. Οι χρήστες κατά την παροχή των στοιχείων τους στα πλαίσια των συναλλαγών τους όπως και με το παρόν, θα ενημερώνονται από την Multirama και ουκ ούτως ή άλλως απόδοχόντας την απεικονίσιμη απειράκιση των στοιχείων αυτών, προσαρμόζοντας από την Multirama και ουκ ούτως ή άλλως απόδοχόντας την απεικονίσιμη απειράκιση των στοιχείων αυτών σε απόδοχόντας οι οποίοι θα προσδοκούνται συμπεριφορά και όλα οι υπόλοιποι και προστηνότες της εταιρείας στα πλαίσια της διαπραράκισης της καταρτιζόμενης σύμβασης. Επίσης και με τον παρόν νυνστερησθήκη ή ύπερση του δικαιοκτύου προσδοκίας και του δικαιοκτύου εναντίωσης του άρθρου 12 και 13 του Ν. 2472/1992.

Βεβαιώνεται ότι μόνο εξουσιοδοτημένοι υπάλληλοι έχουν πρόσβαση στις πληροφορίες των συναλλαγών και μόνο όποτε αυτό είναι αναγκαίο, π.χ. για τη διαπραράκιση των παραγγέλων. Κατά τα λοιπά η Multirama δεσμεύεται να μην αποκαλύψει τα στοιχεία των πελατών και των συναλλαγών τους, όπως εν διαίτηροση εξουσιοδοτήσει από τους ίδιους, ή αυτό σφδδλονται από δικαστική απόδοχόν ή απόδοχόν άλλης δημόσιας αρχής. Τα προσωπικά δεδομένα που δηλώνονται στο ηλεκτρονικό κατάστημα με το παρόν σήμα Multirama χρησιμοποιούνται αποκλειστικά από αυτό ή συντηροζόμενες με αυτό επαρτηρικός, με σκοπό την υποστήριξη, προώθηση και οπτική της συναλλακτικής σχέσης. Τα ούνολα των ενγρόφων και ηλεκτρονικών στοιχείων που θα ανταλλάσσονται μεταξύ των μερών στο πλαίσιο της πώλησης θα προδόνται από την Multirama. Ο πελάτης μπορεί να διαρτορήσει σε αυτό σφδδν το σήμα.

**Χρήστες πληροφοριών:**  
 Δομο & Προσωπικά Πληρώματα  
 Δομο Χρήσης Ισπώρητου & Δίλωση Επαύλουθου  
 Ασφάλεια Συναλλαγών & Προσωπικά Δεδομένα  
 Τρέφια Πληρωμής

**Επικοινωνία**  
 Από σπώρητο: 801-11-15000  
 Από κινητό: 210-8181888  
 Mail: info@multirama.gr  
 Φόρμα επικοινωνίας

Βρείτε τώρα στις Multirama την πιο μεγάλη γκάμα προϊόντων τεχνολογίας σε συντηροζόμενες τιμές!

**Υπολογιστές - Notebooks - GPS:** desktop pc, laptop, netbook  
**Προϊόντα Αναδόχου:** ασύρτητες, μητρικές κάρτες, κάρτες γραφικών, μητρικές RAM  
**Εξόνη & Ήχος:** Τηλεόραση, φωτογραφικές μηχανές, βιντοκάμερες, home cinema  
**Gaming:** Κονόλες παιχνιδιών, Games, Αξισούρα Παιχνιδιών  
**Τηλεόνη - Internet:** κινητό - Τηλέφωνο, Smartphones

Copyright © 2008 Multirama. All rights reserved.

Το πρόβλημα που ανακύπτει συχνά μα δεν αποτελεί κι άμεσα νομικό παράπτωμα είναι πως αυτού του είδους τα ηλεκτρονικά καταστήματα αναθέτουν σε τρίτη συνεργαζόμενη εταιρεία, την διαχείριση και την εκμετάλλευση των στοιχείων σχετικά με την αγορά αγαθών ή/και υπηρεσιών μέσα από το ηλεκτρονικό τους κατάστημα. Βεβαίως μέσα στους όρους συμφωνίας τους, διαβεβαιώνεται πως, όποτε γίνεται η ανάθεση υπηρεσιών υποστήριξης από τις εν λόγω τρίτες εταιρείες, τα ηλεκτρονικά καταστήματα απαιτούν και προσπαθούν να δεσμεύσουν προς την συμμόρφωση με τις αρχές της εχεμύθειας ως προς τα προσωπικά δεδομένα που καλούνται να επεξεργαστούν. Σε κάθε περίπτωση πάντως, για την όποια εμπορική επικοινωνία με τους πελάτες, χρειάζεται προηγουμένως η συγκατάθεσή τους η οποία δηλώνεται ως επί των πλείστον στην φόρμα συλλογής των στοιχείων κατά την εγγραφή τους στο ηλεκτρονικό κατάστημα. Το σίγουρο είναι πως δεν γίνεται κατάχρηση της δυνατότητας της επικοινωνίας με τους καταναλωτές του, εφόσον παράλληλα δίνεται η ανά πάσα στιγμή δυνατότητα διακοπής της λήψης του οποιουδήποτε μηνύματος.

Ένα δεύτερο πρόβλημα ελάσσονος σημασίας είναι μια τεχνολογική παρέμβαση που γίνεται εν αγνοία του καταναλωτή στον υπολογιστή του. Συνήθως εγκαθίσταται κάποια cookies, ανάλυση που έγινε σε άλλο κομμάτι της παρούσας εργασίας, όπου αφορούν αποκλειστικά είτε την συλλογή στατιστικών στοιχείων σχετικά με την επισκεψιμότητα στην ιστοσελίδα του καταστήματος, είτε βοηθούν στην λειτουργία του ηλεκτρονικού καλαθιού αγορών και ισχύουν μόνο κατά το χρονικό διάστημα που είναι ο καταναλωτής συνδεδεμένος στην ιστοσελίδα.

Παρόλα αυτά τα ψεγάδια, τα παραπάνω ηλεκτρονικά καταστήματα που αναφέρθηκαν, θεωρούνται συνεπή ως προς την ελληνική νομοθεσία καθώς ενημερώνουν ορθώς όλους τους καταναλωτές τους για οποιοδήποτε θέμα εμπεριέχεται στην σφαίρα της προστασίας των προσωπικών δεδομένων. [27]-[30]

### **Ιδιαίτερη Πολιτική Προστασίας Καταναλωτών**

Ωστόσο, παρά την γενικότερη διάθεση της πλειοψηφίας των ηλεκτρονικών καταστημάτων να εναρμονιστούν προς το συμφέρον όλων, υπάρχουν και ηλεκτρονικά καταστήματα που ακολουθούν ιδιαίτερη πολιτική προστασίας ειδικά σε ότι αφορά το κομμάτι των παροχών μετά την πώληση του προϊόντος/υπηρεσίας. Το Ηλεκτρονικό





#### 4.6 ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΟΛΙΤΙΚΗΣ ΠΡΟΣΤΑΣΙΑΣ ΚΑΤΑΝΑΛΩΤΩΝ ΣΕ ΙΣΤΟΣΕΛΙΔΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ.

Οι ιστοσελίδες κοινωνικής δικτύωσης (facebook, twitter κλπ) αποτελούν επίσης πεδίο εξαπάτησης καταναλωτών, όπως και τα ηλεκτρονικά καταστήματα.

Η εταιρεία safeline έλαβε συνολικά 1807 καταγγελίες παράνομου περιεχομένου στο Διαδίκτυο κατά τη διάρκεια του εξαμήνου Ιανουάριος - Ιούνιος 2011 και ανάμεσα σε αυτές, ιδιαίτερα αυξημένος θεωρείται ο αριθμός των καταγγελιών που αφορά στα κοινωνικά δίκτυα. Συγκεκριμένα, οι 565 καταγγελίες που έλαβε η εταιρεία safeline και αφορούσε στο facebook σχετιζόνταν με παραβίαση προσωπικών δεδομένων, υποκλοπή κωδικών πρόσβασης, δημιουργία ομάδων μίσους, περιπτώσεις εξύβρισης και συκοφαντικής δυσφήμισης, σεξουαλικής παρενόχλησης και τέλος απειλής.

Ο αριθμός αυτός των καταγγελιών περιλαμβάνει διάφορες κατηγορίες περιεχομένου

- Spam-phishing (27%)
- προσωπικά δεδομένα (15%)
- απόρρητο των επικοινωνιών (14%)
- εξύβριση/ συκοφαντική δυσφήμιση (13%)
- οικονομικές απάτες (13%)
- ρατσισμός/ ξενοφοβία (6%)
- παιδική πορνογραφία (5%)
- απειλή (5%)
- πνευματική ιδιοκτησία (2%)

Για να μπορέσει να ανταποκριθεί στις απαιτήσεις των καταγγελιών αυτών, η safeline βρίσκεται σε άμεση επικοινωνία με τους διαχειριστές του facebook, κάτι που έχει επιτευχθεί μέσω του παγκόσμιου συνδέσμου ανοιχτών γραμμών inhone, με σκοπό την αντιμετώπιση παράνομων δραστηριοτήτων.

Αξίζει να σημειωθεί ότι όλες οι καταγγελίες που αφορούσαν σε περιεχόμενο παιδικής πορνογραφίας προωθήθηκαν, μέσω της κοινής βάσης δεδομένων (URL database) του inhone, σε αντίστοιχες ανοιχτές γραμμές καταγγελιών άλλων χωρών. Στη

βάση αυτή καταγράφονται όλες οι καταγγελίες, των οποίων το περιεχόμενο σχετίζεται με εικόνες παιδικής σεξουαλικής κακοποίησης.

Σημαντικό είναι επίσης το γεγονός ότι πολλές από τις αγγελίες που αφορούσαν σε παράνομο περιεχόμενο προωθήθηκαν στη μονάδα δίωξης ηλεκτρονικού εγκλήματος της ελληνικής αστυνομίας με την οποία η safeline έχει ειδικό συμφωνητικό συνεργασίας.

### Εξηγήσεις από το facebook ζήτησαν οι Σκανδιναβοί

Οι υπηρεσίες πληροφορικής των σκανδιναβικών χωρών- Νορβηγία, Σουηδία, Δανία και Φιλανδία- ανακοίνωσαν ότι ζήτησαν απαντήσεις από τον ιστοχώρο facebook σχετικά με την διαχείριση των προσωπικών δεδομένων των χρηστών του. Οι τέσσερις εθνικές υπηρεσίες συνέταξαν έναν κατάλογο με 45 ερωτήσεις στις οποίες ζητούν από το facebook να απαντήσει 'με τη μεγαλύτερη δυνατή ακρίβεια' πριν από το τέλος του Αυγούστου. Για παράδειγμα, οι παραπάνω χώρες ζητούν από το facebook να τους διευκρινίσει ποιές πληροφορίες των λογαριασμών των χρηστών του μοιράζετε με άλλες επιχειρήσεις. Η χρήση από τρίτους των δημοσιεύσεων των χρηστών στο τοίχο τους, των φωτογραφιών τους, των πληροφοριών για το θρήσκευμα ή τις σεξουαλικές τους προτιμήσεις, καθώς και η πιθανότητα οι διαχειριστές των εφαρμογών να αλλάζουν τις παραμέτρους εμπιστευτικότητας των χρηστών είναι κάποια από τα θέματα που περιλαμβάνονται στο ερωτηματολόγιο των αρχών προς το facebook.

### Αναφορά προσβολής/παρενόγλησης/απαράδεκτου υλικού στο facebook.

Στο σύνδεσμο « αναφορά (report)» μπορεί να αναφέρει κανείς τυχόν προσβλητικό ή απαράδεκτο υλικό που μπορεί να υποπέσει στην αντίληψη του κατά την περιήγηση του στο facebook. Ο σύνδεσμος αυτός προωθεί τον χρήστη σε μια φόρμα όπου μπορεί εκεί να συγκεκριμενοποιήσει τον τύπο της προσβολής και να κάνει αναλυτική αναφορά. Όλες οι αναφορές είναι εμπιστευτικές:

- αναφορά προφίλ
- αναφορά φωτογραφίας
- αναφορά ενός εισερχόμενου μηνύματος

- αναφορά group ή γεγονόςτος
- αναφορά μιας σελίδας

επίσης εάν κάποιος βρει υλικό που παρακινεί σε τρομοκρατική συμπεριφορά ή συλλέγει χρήματα για τρομοκρατικές οργανώσεις, μπορεί να το αναφέρει άμεσα στη διεύθυνση [www.facebook.com/help/contact.php?show\\_form=terrorist\\_content](http://www.facebook.com/help/contact.php?show_form=terrorist_content).

#### 4.7 ΠΡΟΛΗΠΤΙΚΑ ΜΕΤΡΑ

Προληπτικά μέτρα προστασίας πρέπει πάντα να λαμβάνονται από τους χρήστες του Διαδικτύου, διότι οι κίνδυνοι από ιούς, παράνομες εισβολές και υπερβολικές χρεώσεις σε τηλεφωνικούς αριθμούς ήταν αρκετά συχνοί.

Κατά προτίμηση, ο χρήστης που εισέρχεται στο Διαδίκτυο από dial up σύνδεση θα πρέπει να δεσμεύει την γραμμή με έναν κωδικό που θα προμηθευτεί από τον ΟΤΕ τις εξερχόμενες διεθνείς κλήσεις, καθόσον υπάρχει ο κίνδυνος του dialer (πρόγραμμα που συνδέει τον υπολογιστή με άλλους υπολογιστές της αλλοδαπής με αποτέλεσμα την υπερβολική τηλεφωνική χρέωσή του). Τέτοιου είδους απειλές με τον καιρό έχουν εξαφανιστεί λόγω ανάπτυξης της τεχνολογίας. Πλέον οι συνδέσεις στο διαδίκτυο γίνονται με νεότερες τεχνολογίες από dial up, με αποτέλεσμα κι οι ταχύτητες σύνδεσης να είναι υψηλότερες αλλά και να αποφεύγεται ο κίνδυνος της «κρυφής» χρέωσης. Επίσης ένας προσεκτικός χρήστης, θα πρέπει να εγκαταστήσει προγράμματα για την προστασία από ιούς και ηλεκτρονικές επιθέσεις που αναφέρθηκε σε παραπάνω κεφάλαιο.

Θα αναφερθούν παρακάτω επιγραμματικά, κίνδυνοι και μέτρα προστασίας για την ίσως πιο ευπαθή ομάδα χρηστών, και κατ' επέκταση, καταναλωτών όπως είναι τα παιδιά (με την έννοια κάτω των 18 ετών).

##### Κίνδυνοι για τα παιδιά

1. Μπορούν να εκτεθούν σε ακατάλληλο πορνογραφικό ή προσβλητικό περιεχόμενο



2. Μπορούν να έρθουν σε διαδικτυακή επαφή με άγνωστους που μπορεί να τα βλάψουν
3. Υπόκεινται σε πιέσεις από τις έμμεσες αλλά επιβλητικές διαφημίσεις στο Διαδίκτυο
4. Μπορούν να εθιστούν στην χρήση του Διαδικτύου και έτσι να κινδυνεύουν να παραμελήσουν τις κοινωνικές τους δραστηριότητες, τις σχολικές τους υποχρεώσεις καθώς και τα παιχνίδια τους με φίλους.

### Συμβουλές για τα παιδιά

1. Οφείλουν να εξηγούν στους γονείς τους ή σε κάποιον ενήλικα για εικόνες ή κείμενα που βρίσκουν στο διαδίκτυο κι ίσως που τα ανησυχούν ή τα φοβίζουν
2. Να εξηγούν στους γονείς τους τις εμπειρίες κατά την περιπλάνησή τους στο Διαδίκτυο
3. Να διαφυλάσσουν τις προσωπικές τους πληροφορίες. Ποτέ δεν πρέπει να δίνουν το όνομά τους, τα στοιχεία του γενικότερα
4. Να κρατούν κωδικό εισόδου στον υπολογιστή τους, μυστικό
5. Μέχρι κάποια ηλικία, να επιτρέπεται η είσοδος στο Διαδίκτυο μόνο με την άδεια και την παρουσία των γονέων τους
6. Στις αμεσότερες διεπαφές όπως είναι τα chatrooms ή τα e-mails, θα πρέπει το περιεχόμενο της συνομιλίας να μην είναι προσβλητικό. Σε περίπτωση που το παιδί νιώσει άβολα, θα πρέπει να διακόπτεται η συζήτηση.
7. Να μην εμπιστεύονται, ως χρήστες, την όποια πληροφορία δέχεται η αντίληψή τους. Θα πρέπει να υπάρχει κριτική στάση απέναντι σε οποιαδήποτε πληροφορία.

### Συμβουλές για τους γονείς

1. Καλό θα ήταν να τοποθετείται ο ηλεκτρονικός υπολογιστής σε χώρους όπως το σαλόνι κι όχι σε υπνοδωμάτια. Αν ο γονέας ασχοληθεί με το παιδί του ως προς την εξερεύνηση του Διαδικτύου, το παιδί θα γίνει καλύτερος ηλεκτρονικός καταναλωτής και θα γνωρίζει να αποφεύγει τις όποιες παγίδες των ηλεκτρονικών καταστημάτων

2. Θα πρέπει να ενημερώνουν τα παιδιά τους κατάλληλα, ειδικά όσον αφορά τον τομέα των άγνωστων ανθρώπων που τα προσεγγίζουν.
3. Σκόπιμο είναι να ενθαρρύνονται τα παιδιά ώστε να προτιμούν ιστοσελίδες που προτείνουν οι ίδιοι οι γονείς κι όχι δικές τους που έχουν ενημερωθεί από φίλους τους.
4. Θα πρέπει να εγκαταστήσουν στον υπολογιστή κάποιο λογισμικό φίλτρο που απαγορεύει την προσπέλαση συγκεκριμένων ιστοσελίδων κυρίως ανάρμοστου υλικού.
5. Η συζήτηση γονέων με παιδιά για τους κινδύνους που εγκυμονεί το Διαδίκτυο μπορεί να αποβεί σωτήρια. Χρειάζεται να δείχνεται ευαισθησία κι έγνοια έτσι ώστε να κατανοούν και τα ίδια τους κινδύνους

Περνώντας από τα γενικότερα προληπτικά μέτρα που καλείται ένα παιδί αλλά κι ένας γονέας να λάβει, στα μέτρα εκείνα που σχετίζονται άμεσα με τους τρόπους αντιμετώπισης κατά της ηλεκτρονικής εξαπάτησης. Σε γενικότερες γραμμές, η αγορά από το διαδίκτυο είναι ασφαλής, ιδιαίτερα όταν γίνεται από αναγνωρισμένα και μεγάλα ηλεκτρονικά καταστήματα. Υπάρχουν όμως και περιπτώσεις που εγκυμονούν κινδύνους για τους καταναλωτές. Οι κίνδυνοι αυτοί, όπως έχει αναφερθεί και παραπάνω στην παρούσα εργασία, σχετίζονται κυρίως με την αθέτηση των όρων της εμπορικής συμφωνίας (μη παράδοση των προϊόντων ή των υπηρεσιών, παράδοση ελαττωματικών αγαθών, χρέωση κρυφών εξόδων).

Συνοπτικά θα πρέπει ο καταναλωτής να είναι εν μέρει καχύποπτος και να προσέχει ιδιαίτερα, διαβάζοντας τους όρους της εμπορικής συναλλαγής και ελέγχοντας τη φερεγγυότητα του ηλεκτρονικού καταστήματος με το οποίο συναλλάσσεται. Υπάρχουν αρκετοί τρόποι για να προστατευθεί κανείς από την εξαπάτηση κατά τη διάρκεια εμπορικών συναλλαγών στο διαδίκτυο και οποιοσδήποτε συνδυασμός τους θα προστατεύσει επαρκώς τον καταναλωτή.

#### Ειδικότερα:

1. Προσοχή στους όρους συναλλαγής

2. Προσοχή στους όρους χρήστης της ιστοσελίδας του ηλεκτρονικού καταστήματος
3. Βεβαίωση φερεγγυότητας του ηλεκτρονικού καταστήματος με το οποίο συναλλάσσεται ο καταναλωτής
4. Έλεγχος στις πληροφορίες που αναγράφονται για το προϊόν, την τιμή του και το νόμισμα που θα γίνει η συναλλαγή καθώς και το τελικό κόστος συμπεριλαμβανομένων και των εξόδων αποστολής
5. Σαφή μελέτη της πολιτικής επιστροφών της εταιρείας
6. Προσεκτική μελέτη των όρων ασφαλείας πληρωμής της ιστοσελίδας
7. Εξακρίβωση του χρόνου παράδοσης του προϊόντος

Άλλοι τρόποι προστασίας, κάπως πιο εξειδικευμένων γνώσεων είναι οι εξής:

1. Εξοπλισμός του υπολογιστή του καταναλωτή με ειδικό λογισμικό ασφαλείας, που ανιχνεύει κακόβουλο λογισμικό στον υπολογιστή του
2. Όταν γίνεται η πληρωμή, θα πρέπει ο καταναλωτής να είναι σίγουρος για την ασφαλή και κρυπτογραφημένη σύνδεση του υπολογιστή του (εμφανίζεται είτε με την αλλαγή χρώματος της περιοχής που πληκτρολογεί την ηλεκτρονική διεύθυνση, είτε με ένα σύμβολο κάτω δεξιά στο πρόγραμμα πλοήγησης, είτε με την αλλαγή της διεύθυνσης από http σε https
3. Μη αποθήκευση προσωπικών κωδικών πρόσβασης στην μνήμη του υπολογιστή
4. Μη δημοσίευση προσωπικών κωδικών καταναλωτή σε τρίτα άτομα
5. Ο κωδικός ασφαλείας, προκειμένου να έχει μεγαλύτερη ασφάλεια, οφείλει να είναι πιο σύνθετος περιέχοντας γράμματα, αριθμούς και σύμβολα
6. Μη κοινοποίηση προσωπικών πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου καθώς η τεχνολογία είναι άνευ κρυπτογράφησης κι άρα μη ασφαλής υπηρεσία



7. Προτίμηση για αγορές προπληρωμένων διαδικτυακών υπηρεσιών, καθώς παρέχονται από εταιρείες φερέγγυες και σοβαρές που προσφέρουν αποζημίωση σε περίπτωση εξαπάτησης
8. Χρησιμοποίηση προπληρωμένων πιστωτικών καρτών

Ωστόσο μπορούν να παρθούν επιπρόσθετα μέτρα προστασίας κατά την διάρκεια της συναλλαγής όπως:

1. Αποθήκευση στον υπολογιστή την συναλλαγή που πραγματοποιείται
2. Βαθιά γνώση της πολιτικής της εταιρείας αναφορικά με την χρήση των προσωπικών στοιχείων του εκάστοτε καταναλωτή
3. Εκτύπωση και κράτηση της πολιτικής επιστροφών που αναγράφεται εκείνη την στιγμή στην ιστοσελίδα του ηλεκτρονικού καταστήματος

Μετά το πέρας της αγοράς ο καταναλωτής οφείλει να γνωρίζει πως:

1. Έχει τα ίδια δικαιώματα σαν να έκανε την αγορά του από ένα τυπικό κατάστημα που έχει φυσική υπόσταση
2. Να κρατά όλα τα στοιχεία επικοινωνίας
3. Να κρατά αντίγραφο των όρων και των προϋποθέσεων αγοράς
4. Σύμφωνα με την νομοθεσία της Ευρωπαϊκής Ένωσης, μπορεί να ακυρώσει μια υπηρεσία ή να επιστρέψει ένα προϊόν, μέσα σε συγκεκριμένο χρονικό διάστημα, συνήθως επτά ημερών, γνωστό κι ως "cooling – off period"
5. Σε περίπτωση επιστροφής όμως πληρώνει ο ίδιος ο καταναλωτής τα έξοδα αποστολής
6. Σε περίπτωση παράδοσης ελαττωματικού προϊόντος, μπορεί να προβεί σε άμεση καταγγελία στις αρμόδιες υπηρεσίες
7. Σε περίπτωση μη εκτέλεσης μιας υπηρεσίας, δικαιούται ο καταναλωτής την επιστροφή των χρημάτων του

## ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι επιχειρήσεις με το πέρασ των καιρών εξελίχθηκαν με τάχιστους ρυθμούς. Ολοένα και περισσότεροι επιχειρηματίες επιλέγουν την νέα αυτή μορφή της εικονικής επιχειρήσης. Έχοντας καλή γνώση της τεχνολογίας, οι ιδιοκτήτες αυτού του είδους επιχειρήσεων γίνονται ιδιαίτερα ανταγωνιστικοί σε σχέση με την κλασική μορφή επιχειρήσεων που συνάμα αντιμετωπίζει το κόστος της φυσικής παρουσίας. Όπως αναλύθηκε, οι λειτουργίες των εικονικών επιχειρήσεων ελάχιστα διαφέρουν από όσα γνωρίζουμε μέχρι σήμερα. Ταυτόχρονα όμως έχουν εμπλουτιστεί και με νέες παροχές προς τους καταναλωτές τους. Έτσι ενώ τα βασικά συστατικά έμειναν αναλλοίωτα, εν τούτοις έχουμε εξέλιξη κάποιων διαδικασιών όπως είναι οι τρόποι πληρωμής, η προστασία των καταναλωτών αλλά και 24ώρη παροχή των υπηρεσιών του καταστήματος χωρίς καμία διακοπή. Το ηλεκτρονικό εμπόριο αλλά και το ηλεκτρονικό επιχειρείν ανθοφορεί τα τελευταία χρόνια τόσο σε παγκόσμιο επίπεδο, αλλά και σε εγχώριο επίπεδο. Η παγκόσμια χρηματοπιστωτική κρίση έχει επιφέρει σειρά εμποδίων στο εμπόριο κι έτσι η μείωση του κόστους λόγω μη φυσικής παρουσίας, πλεονέκτημα ηλεκτρονικής επιχειρήσης, κάνει τους νέους Έλληνες επιχειρηματίες να τις προτιμούν. Σίγουρα υπάρχουν και μειονεκτήματα χρήσης αυτού του είδους τεχνολογίας, μα υπερκαλύπτονται από την πληθώρα πλεονεκτημάτων που αποδίδει μια τέτοια επιχειρηματική κίνηση. Έτσι δικαιολογείται άλλωστε, έρευνα της Ελληνικής Στατιστικής Εταιρείας (ΕΛ.ΣΤΑΤ.) που αποδίδει τα δέοντα στους χρήστες καταναλωτές μέσω διαδικτύου. Παρά την επιφυλακτικότητά τους, οι ηλεκτρονικές αγορές ανέρχονται σε ποσοστό 18,4 % για το περασμένο έτος.

Στον αντίποδα των πολυάριθμων θετικών συνεπειών που έχει για τους καταναλωτές μια ηλεκτρονική επιχείρηση βρίσκεται εμφανώς η απειλή ύπαρξης νέων αξιόποιων δραστηριοτήτων από επιτήδειους προκειμένου να εκμεταλλευτούν χρήστες διαδικτύου που αγοράζουν ηλεκτρονικά, υποκλέπτοντας προσωπικά τους δεδομένα. Με δεδομένο λοιπόν το μέγεθος των απειλών κατά της ασφάλειας, η ανάγκη αντιμετώπισης των απειλών του εγκλήματος στον κυβερνοχώρο έχει παγκόσμια διάσταση και μια χώρα όπως η Ελλάδα δεν θα μπορούσε να μην προβεί στην σύνθεση και λειτουργία νομοθεσίας προστασίας. Τα είδη της ηλεκτρονικής εξαπάτησης, όπως αναλύθηκε και παραπάνω, στοχεύει κυρίως στο να εκμαιεύσει κάποιος προσωπικά στοιχεία των καταναλωτών όπως είναι οι κωδικοί για πιστωτικές τους κυρίως κάρτες ή άλλα στοιχεία

που όμως έχουν ανταλλακτική αξία. Έτσι ο εγκληματίας θα τα χρησιμοποιήσει προς όφελός του χρεώνοντας τον ανυποψίαστο καταναλωτή εν αγνοία του. Σίγουρα υπάρχουν οργανισμοί που ενημερώνουν διαρκώς τους καταναλωτές για τον τρόπο ασφαλούς χρήσης αυτού του είδους των αγορών μα η προληπτική αυτοπροστασία ίσως αποτελεί την σημαντικότερη άμυνα προς αυτού του είδους τις απειλές.

Αποτέλεσμα αυτού αποτελεί ότι η παραβατικότητα καθίσταται όλο και συχνότερο, πολυπλοκότερο και επικινδυνότερο φαινόμενο. Επιπρόσθετα αρνητικά λειτουργεί και ότι πλέον αυτού του είδους τα εγκλήματα μπορούν πλέον να πραγματοποιηθούν από τον καθένα αλλά και να πλήξουν τον καθένα. Παρόλα ταύτα το νομικό πλαίσιο που έχει αναπτυχθεί για ζητήματα ηλεκτρονικών επιχειρήσεων καλύπτει επαρκώς πολλά ζητήματα γύρω από αυτού του είδους τις επιχειρήσεις, από την σύστασή τους μέχρι και την ασφάλεια των καταναλωτών σε περίπτωση απάτης. Το νομικό αυτό πλαίσιο εντάσσεται σε μια ευρύτερη παγκόσμια προσπάθεια ανάπτυξης τέτοιου είδους επιχειρηματικών πρωτοβουλιών που όμως προστατεύονται από επιτήδειους εγκληματίες. Στον ελλαδικό χώρο, στο κομμάτι προστασίας των καταναλωτών, έχουν δημιουργηθεί Ανεξάρτητες Ρυθμιστικές Αρχές όπως η ΑΠΠΔ και η ΑΔΑΕ. Το μελανό σημείο στην παρούσα νομοθεσία αποτελεί πως δεν υπάρχει ταυτόχρονη εξέλιξη των νόμων συναρτήσει της ανάπτυξης της τεχνολογίας σε παγκόσμιο επίπεδο. Δεν είναι τυχαίο άλλωστε που χαρακτηριστικά, τα επίπεδα προστατίμων αναγράφονται ακόμα σε ισοτιμία δραχμής αντί για ευρώ. Πάντως, σε Ευρωπαϊκό Επίπεδο, οι κινήσεις για πλήρη ρύθμιση και προστασία των ηλεκτρονικών συναλλαγών, είναι σε πολύ υψηλά επίπεδα λόγω της πρωτοβουλίας i2010.

Κλείνοντας, θα ήταν άξιο να αναφερθεί η εσφαλμένη φιλολογία γύρω από την μη ασφάλεια του διαδικτύου στο κομμάτι των ηλεκτρονικών επιχειρήσεων. Κίνδυνοι σαφώς υπάρχουν παντού, σε οποιαδήποτε συναλλαγή, ακόμα και στις φυσικές αγορές ενός καταναλωτή. Το σημαντικό είναι πως θα πρέπει ο εκάστοτε καταναλωτής να είναι συνετός και πλήρως ενημερωμένος για τις ηλεκτρονικές συναλλαγές. Θα πρέπει να δρα με λογική και σύνεση, απαγκιστρωμένος από φόβο και άρνηση, ώστε να προβεί σε μια επιτυχή αγορά. Η ασφάλεια, σε τεχνολογικό επίπεδο, είναι άκρως ανεπτυγμένη και παρουσιάζει συνεχώς εξελίξεις αλλά και καινοτόμες διαδικασίες προστασίας. Χαρακτηριστική θεωρία αποτελεί η κρυπτογράφηση που ολοένα και μετουσιώνεται σε



πολύπλοκο και διαιδαλώδες σύστημα, το οποίο μετατρέπει τους τυχόν εγκληματίες ανάξιους στην ρήξη του. Διακρίνονται πλέον αυτά τα προγράμματα από πλήρη ακεραιότητα, με σχεδόν μηδενικά «παραθυράκια» προσπέλασης στο λογισμικό τους έτσι ώστε οι ηλεκτρονικές συναλλαγές μέσω πιστωτικών καρτών, να αποτελεί πλέον το ασφαλέστερο μέσω αγοράς ενός προϊόντος ή μιας υπηρεσίας. Προληπτικά μέτρα πάντως είναι σημαντικό να παρθούν τόσο από τους καταναλωτές γενικότερα αλλά και από γονείς με την μορφή ενημέρωσης προς τα παιδιά τους, που αποτελούν φυσικά τους μελλοντικούς ηλεκτρονικούς καταναλωτές.

Εν κατακλείδι, οι ηλεκτρονικές επιχειρήσεις αποτελούν σοφή επιλογή λόγω μειωμένου κόστους, μα αυτό αντισταθμίζεται οικονομικά από τα επίπεδα τεχνογνωσίας και προστασίας που καλείται να έχει το ηλεκτρονικό κατάστημα ως προς τους καταναλωτές του. Μια τέτοια συνεχή εγρήγορση αποτελεί ένα κοστοβόρο έξοδο της επιχείρησης, μα αναγκαίο για την λειτουργία της. Τα πλεονεκτήματα μια τέτοιας επιλογής δεν σταματούν στα χρηματοοικονομικά μεγέθη, αφού και οι καταναλωτές κερδίζουν σε χρόνο και χρήμα είτε από την «γρήγορη» επίσκεψη πολλών καταστημάτων από την οθόνη του υπολογιστή τους, είναι από την σύγκριση τιμών. Μηδενίζεται λοιπόν το κόστος μετάβασης των καταναλωτών. Οι προβλέψεις των ακαδημαϊκών κλάδων διαβλέπουν ολοένα και μεγαλύτερη διάδοση αυτών των επιχειρήσεων. Ο χρόνος τελικά θα δείξει το αποτέλεσμα.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Γ. Δουκίδης, Β. Θεμιστοκλέους, Β. Δράκος, Ν. Παπαζεφειροπούλου, «Ηλεκτρονικό Εμπόριο», Εκδόσεις Νέων Τεχνολογιών
2. Ε. Αλεξανδρίδου, Καθηγήτριας στο Α.Π.Θ., "Το δίκαιο του Ηλεκτρονικού Εμπορίου", Εκδόσεις Σάκκουλα Α.Ε
3. Τ.Ε. Συνοδινού, Δ.Ν. Δικηγόρου, "Η Νομική Προστασία των Βάσεων Δεδομένων", Εκδόσεις Σάκκουλα Α.Ε
4. Μ. Γκιούρδας, «Ηλεκτρονικό Εμπόριο», Εκδόσεις Γκιούρδα
5. Αρ. Πασχόπουλος & Π. Σκάλτσας, «Ηλεκτρονικό Εμπόριο. Νέο περιβάλλον, νέα εργαλεία, νέοι ηγέτες», Εκδόσεις Κλειδάριθμος
6. D. Chaffey, «E-Business and E-Commerce Management», Εκδόσεις Pearson Education
7. K. Laudon & C. Traver, «E-Commerce», Εκδόσεις Pearson Education
8. Χ. Τσουραμάνης, «Οικονομία & Εγκληματικότητα», Εκδόσεις Β. Κατσαρού
9. <http://www.tanea.gr//Article.aspx?d=20070628&nid=5098841&sn=ΟΙΚΟΝΟΜΙΑ&spid=631>
10. [www.worldgmc.com/greece](http://www.worldgmc.com/greece)
11. [www.statistics.gr](http://www.statistics.gr)
12. [www.e-crime.gr](http://www.e-crime.gr)
13. [www.kathimerini.gr](http://www.kathimerini.gr)
14. [www.safeline.gr](http://www.safeline.gr)
15. <http://diktiakovima.blogspot.com/2010/04/ebay.html>
16. [http://www.cybercrimelaw.net/documents/cybercrime\\_history.pdf](http://www.cybercrimelaw.net/documents/cybercrime_history.pdf)

.(The 3rd Interpol Symposium on International Fraud, Saint-Cloud, Paris, France, December 11-13, 1979)

17. [www.inka.gr](http://www.inka.gr)
18. [www.newinka.gr](http://www.newinka.gr)
19. [www.saferinternet.gr](http://www.saferinternet.gr)
20. [www.gge.gr](http://www.gge.gr)
21. [http://ec.europa.eu/youreurope/business/starting-business/setting-up/greece/index\\_el.htm](http://ec.europa.eu/youreurope/business/starting-business/setting-up/greece/index_el.htm)
22. [www.dpa.gr](http://www.dpa.gr)
23. [www.adae.gr](http://www.adae.gr)
24. [http://europa.eu.int/information\\_society/eeurope/index\\_en.htm](http://europa.eu.int/information_society/eeurope/index_en.htm)
25. <http://webcache.googleusercontent.com/search?q=cache:X2hRrkPz1vgJ:eur-lex.europa.eu/LexUriServ/LexUriServ.do%3Furi%3DCELEX:32000L0031:EL:HTML+2000/31/%CE%95%CE%9A&cd=1&hl=el&ct=clnk&gl=gr&source=www.google.gr>
26. [www.dart.gov.gr/NewsInner.aspx?new\\_id=201&nwc\\_id=21](http://www.dart.gov.gr/NewsInner.aspx?new_id=201&nwc_id=21)
27. <http://www.multirama.gr/legal/usage>
28. <http://www.multirama.gr/legal/security>
29. <http://www.e-germanos.gr/e-germanos/login/userPrivacy.eg>
30. <http://www.mediamarkt.gr/?langId=&layer=privacy>
31. [http://zizanio.de/eshop.php?action=news\\_detail&news\\_id=36&PHPSESSID\\_gre\\_ekshops\\_esales=b5a5t77g9g46m6opd1q231vof4](http://zizanio.de/eshop.php?action=news_detail&news_id=36&PHPSESSID_gre_ekshops_esales=b5a5t77g9g46m6opd1q231vof4)