ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Διπλωματική Εργασία

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ (E-BANKING): ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Της

ΣΤΑΥΡΟΥΛΑΣ Ν. ΜΑΓΓΟΥ

Επιβλέπουσα Καθηγήτρια: Ευγενία Αλεξανδροπούλου - Αιγυπτιάδου

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του μεταπτυχιακού διπλώματος ειδίκευσης στα Πληροφοριακά Συστήματα

Φεβρουάριος 2014

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτριά μου, κα Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου, για την κατανόηση και τη βοήθεια που μου προσέφερε ώστε να ολοκληρωθεί η παρούσα εργασία.

Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους καθηγητές του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών στα Πληροφοριακά Συστήματα του Πανεπιστημίου Μακεδονίας, για τις πολύτιμες γνώσεις που μου προσέφεραν καθ' όλη τη διάρκεια των σπουδών.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξη που μου παρέχει σε όλα τα βήματα της ζωής μου.

ΠΕΡΙΛΗΨΗ

Με την παρούσα εργασία επιχειρείται μια προσέγγιση στην ασφάλεια των προσωπικών δεδομένων, τα οποία διακινούνται μέσα σε πληροφοριακά συστήματα ηλεκτρονικής τραπεζικής.

Αρχικά, παρουσιάζονται οι έννοιες των πληροφοριακών συστημάτων και ειδικότερα των τραπεζικών πληροφοριακών συστημάτων, η εξέλιξή και η διείσδυση τους στον επιχειρηματικό κλάδο και δη στον τραπεζικό. Έπειτα παρουσιάζεται η ηλεκτρονική τραπεζική, οι υπηρεσίες που προσφέρει στους όλο και αυξανόμενους χρήστες της, καθώς και τα πλεονεκτήματα και μειονεκτήματα της ηλεκτρονικής τραπεζικής τόσο για τους χρήστες, όσο και για τα ίδια τα τραπεζικά ιδρύματα.

Στη συνέχεια, παρουσιάζονται οι κίνδυνοι που ελλοχεύουν στα συστήματα της ηλεκτρονικής τραπεζική και οι μέθοδοι εξαπάτησης των χρηστών. Ακολουθεί αναφορά στους μηχανισμούς ασφάλειας των τραπεζικών πληροφοριακών συστημάτων και μια σύντομη αναφορά στην συστήματα ηλεκτρονικής τραπεζικής στην Ελλάδα.

Έπειτα, γίνεται μια προσπάθεια παρουσίασης την νομοθετικής δραστηριότητας σε ευρωπαϊκό αλλά και εθνικό επίπεδο αναφορικά με το ζήτημα της προστασίας των προσωπικών δεδομένων. Στη συνέχεια παρουσιάζονται κάποιες αποφάσεις της Αρχής Προστασίας των Προσωπικών Δεδομένων που αφορούν στον τραπεζικό κλάδο.

Η παρούσα εργασία ολοκληρώνεται με συμπερασματικές παρατηρήσεις σχετικά με το νομοθετικό πλαίσιο της προστασία των προσωπικών δεδομένων καθώς και προτάσεις για μελλοντική διερεύνηση του τομέα των τραπεζικών πληροφοριακών συστημάτων.

Πίνακας Περιεχομένων

ΚΕΦΑΛΑΙΟ Ι
ΕΙΣΑΓΩΓΗ

Το διαδίκτυο αποτελεί τον πιο διαδεδομένο τρόπο πρόσβασης σε κάθε είδους πληροφορία. Σήμερα, οι περισσότεροι άνθρωποι έχουν πρόσβαση στο διαδίκτυο είτε μέσω ευρυζωνικού δικτύου είτε μέσω του κινητού τηλεφώνου τους, γεγονός που καθιστά το διαδίκτυο ένα εύκολο, μαζικό και πλέον οικονομικό μέσο πρόσβασης. Η αλματώδης εξέλιξη της τεχνολογίας και του διαδικτύου, δεν μπορούσε να αφήσει αδιάφορες τις επιχειρήσεις, καθώς κρίθηκε επιτακτική η ανάγκη εκσυγχρονισμού των διαδικασιών και λειτουργιών τους προκειμένου να γίνουν ανταγωνιστικές και να επιτύχουν κέρδος. Από αυτόν τον εκσυγχρονισμό δεν θα μπορούσαν να απέχουν τα χρηματοπιστωτικά ιδρύματα.

Οι τραπεζικοί όμιλοι, έχουν εισάγει στις καθημερινές τους εργασίες τα πληροφοριακά συστήματα εδώ και αρκετές δεκαετίες. Η ηλεκτρονική τραπεζική ή e-banking μετρά ήδη 15 χρόνια ζωής στον ελληνικό τραπεζικό κλάδο και φαίνεται να κερδίζει διαρκώς έδαφος. Οι χρήστες της ηλεκτρονικής τραπεζικής αυξάνονται συνεχώς, αφού ανακαλύπτουν τα πλεονεκτήματα και την ευκολία που προσφέρουν οι υπηρεσίες της, με αποτέλεσμα σιγά σιγά ο παραδοσιακός τρόπος συναλλαγών των πελατών με την τράπεζα να υποκαθίσταται από τις τραπεζικές ηλεκτρονικές εφαρμογές.

Η τεχνολογική εξέλιξη εκτός από οφέλη δημιούργησε και περισσότερους κινδύνους για τα πληροφοριακά συστήματα. Έτσι, βασική προϋπόθεση για την αύξηση των χρηστών της ηλεκτρονικής τραπεζικής αποτελεί η εμπιστοσύνη προς την τράπεζα και κυρίως στα μέτρα ασφάλειας των πληροφοριακών της συστημάτων. Οι τράπεζες επενδύουν μεγάλα χρηματικά ποσά στο κομμάτι της ασφάλειας, προκειμένου να καταστήσουν τα πληροφορικά τους συστήματα άτρωτα σε επιθέσεις και απειλές.

Επιπλέον, επιτακτική καθίσταται η δημιουργία κατάλληλου νομικού πλαισίου για την προστασία των προσωπικών δεδομένων. Η λήψη μέτρων για την προστασία

της ιδιωτικότητας αποτελεί θετικό παράγοντα για την για την ανάπτυξη της ηλεκτρονικής τραπεζικής και αυξάνει την εμπιστοσύνη των χρηστών.

ΚΕΦΑΛΑΙΟ ΙΙ

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ.

2.1 Πληροφοριακά Συστήματα: Ορισμός και Βασικές Έννοιες.

Η σημερινή εποχή χαρακτηρίζεται από τη ολοένα αυξανόμενη χρήση της πληροφορικής τεχνολογίας. Ιδιαίτερα τα πληροφοριακά συστήματα, αποτελούν σημαντικό εργαλείο στον επιχειρηματικό κλάδο, καθώς υποστηρίζουν όλες τις λειτουργικές και παραγωγικές διαδικασίες που λαμβάνουν χώρο σε μια επιχείρηση ή έναν οργανισμό.

Αν εξετάσουμε μια επιχείρηση ή ένα οργανισμό ως σύστημα μπορούμε να θεωρήσουμε ότι αποτελείται από τρία διαφορετικά υποσυστήματα (Ε. Κιουντούζης, 1995)

1. *Το φυσικό σύστημα παραγωγής*, το οποίο μετασχηματίζει την πρώτη ύλη που εισέρχεται στο σύστημα σε προϊόν, σύμφωνα με τις εντολές που παίρνει από το σύστημα διοίκησης.
2. *Το σύστημα διοίκησης/ λήψης αποφάσεων*, το οποίο παραλαμβάνει πληροφορίες και δεδομένα από το πληροφοριακό σύστημα και παράγει εντολές προς το φυσικό σύστημα παραγωγής και οδηγίες για τις προσδοκίες και επιδιώξεις της διοίκησης, που επιθυμεί να επιτευχθούν.
3. *Το πληροφοριακό σύστημα*, το οποίο συνδέει το φυσικό σύστημα παραγωγής με το σύστημα διοίκησης και λήψης αποφάσεων. Μετασχηματίζει τα δεδομένα που υπάρχουν στο φυσικό σύστημα διοίκησης και σχετίζονται με την απόδοση της παραγωγικής διαδικασίας σε πληροφορίες που απαιτεί το σύστημα της διοίκησης για να πάρει αποφάσεις. Επιπλέον μετασχηματίζει τις εντολές του συστήματος σε κατάλληλες οδηγίες για το φυσικό σύστημα παραγωγής.

Από τα παραπάνω συμπεραίνουμε ότι τα τρία προαναφερθέντα υποσυστήματα αποτελούν μια ενιαία ενότητα για μια επιχείρηση ή έναν οργανισμό.

Τι εννοούμε όμως αναφερόμενοι στον όρο πληροφοριακό σύστημα; Στη βιβλιογραφία δεν υπάρχει ένας ξεκάθαρος ορισμός, με τον οποίο να συμφωνούν όλοι. Έτσι έχουν αποδοθεί αρκετοί ορισμοί, οι οποίοι αξίζει να αναφερθούν παρακάτω.

Σύμφωνα με τους Davies και Olson (1985) Πληροφοριακό Σύστημα είναι μια συλλογή ανθρώπων, επεξεργασιών, δεδομένων, μοντέλων, τεχνολογίας και μερικώς τυποποιημένης γλώσσας που συνθέτει μια ενιαία δομή, η οποία εξυπηρετεί ένα οργανωσιακό σκοπό ή μια λειτουργία.

Σύμφωνα με τους K. C. Laudon και J.P. Laudon, ένα πληροφοριακό σύστημα μπορεί να ορισθεί ως ένα σύνολο αλληλοσυσχετιζόμενων συνιστωσών που συλλέγουν, (ή ανακαλούν), επεξεργάζονται, αποθηκεύουν και διανέμουν πληροφορίες για την υποστήριξη της λήψης αποφάσεων, του συντονισμού και του ελέγχου σε ένα οργανισμό.

Ένας τρίτος ορισμός που έχει αποδοθεί από τον Ε. Κιουντούζη (1995), ορίζει το πληροφοριακό σύστημα ως ένα οργανωμένο σύνολο από πέντε στοιχεία, το οποίο επεξεργάζεται δεδομένα και παράγει πληροφορίες για λογαριασμό μιας επιχείρησης ή ενός οργανισμού, Οι πέντε συνιστώσες ενός πληροφοριακού συστήματος που χρησιμοποιεί ηλεκτρονικούς υπολογιστές είναι οι άνθρωποι, τα δεδομένα, το λογισμικό, ο υλικός εξοπλισμός και οι διαδικασίες.

Η σημασία και η σπουδαιότητα που παίζει ένα πληροφοριακό σύστημα σε μια επιχείρηση ή έναν οργανισμό πηγάζει από το γεγονός ότι αυτό παρέχει υπηρεσίες όπως η επεξεργασία δεδομένων για λογαριασμό της επιχείρησης, υποστήριξη των παραγωγικών και λειτουργικών διαδικασιών που λαμβάνουν χώρα μέσα στην επιχείρηση, δημιουργία και διαβίβαση πληροφοριών καθώς και παροχή βοήθειας στη διοίκηση της επιχείρησης ώστε να ασκεί έλεγχο και να λαμβάνει αποφάσεις (Ε. Κιουντούζης 1995).

2.2 Ιστορική Εξέλιξη Πληροφοριακών Συστημάτων

Η ιστορία των πληροφοριακών συστημάτων ξεκινάει τη δεκαετία του ’50. Οι πρώτες εφαρμογές πληροφοριακών συστημάτων, αναπτύχθηκαν με σκοπό να απλοποιήσουν επαναλαμβανόμενες διαδικασίες των επιχειρήσεων, όπως η μισθοδοσία και η τιμολόγηση προϊόντων. Η ανάγκη λοιπόν, ήταν κυρίως να απλουστευτούν οι λογιστικές κατά βάση, γραφειοκρατικές διαδικασίες των επιχειρήσεων της εποχής (http://el.wikipedia.org/).

Τη δεκαετία του ’60, τα πληροφοριακά συστήματα γίνονται εργαλείο των ανώτερων στελεχών των επιχειρήσεων. Οι εφαρμογές που αναπτύσσονται, βοηθούν τα στελέχη στη συγκέντρωση στοιχείων, τα οποία αξιοποιούνται με σκοπό την υποβοήθηση της παραγωγικής διαδικασίας και τον προσδιορισμό των αναγκών των επιχειρήσεων (Π. Αναστασιάδης, 2008).

Στη συνέχεια, τη δεκαετία του ’70, τα πληροφοριακά συστήματα εξελίσσονται ακόμα περισσότερο, μια και η χρήση τους συμβάλει στην επίλυση εξειδικευμένων διοικητικών προβλημάτων των επιχειρήσεων. Καθίστανται απαραίτητα για τη διαχείριση πληροφοριακών αποθεμάτων, με στόχο να βελτιώσουν τις διαδικασίες διαμόρφωσης και λήψης αποφάσεων (Π. Αναστασιάδης, 2008).

Η τεχνολογία της εποχής βοηθά στην περαιτέρω εξέλιξη των δυνατοτήτων των πληροφοριακών συστημάτων, όταν τη δεκαετία του ’80 αποτελούν ένα από τα πιο αποτελεσματικά εργαλεία της επιχείρησης. Η παραγωγή και η διαχείριση είναι άμεσα συνδεδεμένα με τη χρήση τους και αποτελούν το πλέον ανταγωνιστικό πλεονέκτημα των επιχειρήσεων (Π. Αναστασιάδης, 2008).

Φτάνοντας στη δεκαετία του ’90, τα πληροφοριακά συστήματα είναι αναπόσπαστο κομμάτι της επιχείρησης, αφού αποτελούν μια στρατηγική πλατφόρμα η οποία έχει ως στόχο την άμεση λήψη αποφάσεων με μακροχρόνιο ορίζοντα (Π. Αναστασιάδης, 2008).

Σήμερα τα πληροφοριακά συστήματα αποτελούν το κύριο εργαλείο των επιχειρήσεων και οργανισμών. Παρέχουν πληροφορίες που είναι απαραίτητες, για να διαχειρίζονται οι οργανισμοί αποδοτικά και αποτελεσματικά τα δεδομένα που έχουν στη διάθεσή τους, χρησιμοποιούν την τεχνολογία των δικτύων για να παρέχουν εφαρμογές καθώς και για την αποθήκευση δεδομένων ανεξαρτήτως διάταξης χώρου, τοποθεσίας , φύσης ή υλικού. Μαζί με την τεχνολογία των κινητών τηλεφώνων και των ασύρματων δικτύων οδήγησαν σε ένα νέο επίπεδο κινητικότητας στο οποίο οι διαχειριστές έχουν πρόσβαση σχεδόν από παντού με τη βοήθεια των φορητών υπολογιστών (http://el.wikipedia.org/).

2.3 Ασφάλεια Πληροφοριακών Συστημάτων

Το πρόβλημα της ασφάλειας των Πληροφοριακών συστημάτων είναι ιδιαίτερα έντονο στις μέρες μας. Η συνεχώς αυξανόμενη χρήση των τεχνολογιών, βασισμένων σε βάσεις δεδομένων και δίκτυα, καθώς και ο σημαντικός ρόλος των πληροφοριακών συστημάτων σε μια επιχείρηση, καθιστούν απαραίτητη τη λήψη μέτρων ασφάλειας για την προστασία των πληροφοριών τους.

Η έννοια της ασφάλειας των πληροφοριακών συστημάτων σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Σύμφωνα με τον παραπάνω ορισμό η ασφάλεια σχετίζεται με:

- *Την πρόληψη*, που περιλαμβάνει μέτρα ώστε να προληφθούν ενδεχόμενες φθορές στα συστατικά μέρη ενός πληροφοριακού συστήματος.
- *Την ανίχνευση*, που περιλαμβάνει την αναζήτηση του πότε, πως και από ποιόν προκλήθηκε φθορά σε ένα συστατικό ενός πληροφοριακού συστήματος.
- *Την αντίδραση*, που περιλαμβάνει την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Η πληροφορική ξεκίνησε να ασχολείται με την ασφάλεια των πληροφοριακών συστημάτων, στις αρχές της δεκαετίας του 1970. Η πρώτη σχετική δημοσίευση, από την Ομάδα Εργασίας του Συμβουλίου Αμυντικής Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, εξέτασε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως (μέσω τερματικών). Προηγουμένως, η πρόσβαση στους υπολογιστικούς πόρους προϋπέθετε την φυσική παρουσία και πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή. Η προσέγγιση στην λύση των προβλημάτων ασφάλειας μέχρι τότε βασιζόταν στην φυσική απομόνωση και προστασία του κεντρικού υπολογιστή καθώς και στον έλεγχο πρόσβασης σε αυτόν. Ένα από τα συμπεράσματα στην αναφορά της Ομάδας Εργασίας ήταν ότι ο χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικό πρόσβασης, μια πρόταση που ποτέ δεν υιοθετήθηκε ευρέως. Άλλες καινοτόμες ιδέες που εκφράστηκαν στην ανάλυση είχαν μεγαλύτερη απήχηση. Για παράδειγμα, αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει θεμέλιος λίθος στη δημιουργία πολιτικών ασφάλειας. Ο πρώτος ιός, ο Creeper, εμφανίστηκε επίσης στις αρχές της δεκαετίας του 1970, και το πρώτο δικτυακό "σκουλήκι" (worm), το σκουλήκι Morris, κυκλοφόρησε το 1998. Εκτιμάται ότι 6.000 συστήματα προσβλήθηκαν από το "σκουλήκι". Αξίζει να σημειωθεί ότι το 2007 ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί, γεγονός που κάνει επιτακτική την ανάγκη προστασίας των πληροφοριακών συστημάτων. (http://www.wikipedia.org).

Η έννοια της ασφαλείας των πληροφοριακών συστημάτων συνδέεται στενά με τρεις θεμελιώδεις έννοιες (Γ. Πάγκαλος & Ι. Μαυρίδης 2002):

1. Εμπιστευτικότητα (Confidentiality),
2. Ακεραιότητα (Integrity) και
3. Διαθεσιμότητα(Availability).

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Αυτό σημαίνει ότι τα δεδομένα που υπάρχουν σε ένα υπολογιστικό σύστημα, καθώς και τα δεδομένα τα οποία διακινούνται θα πρέπει να αποκαλύπτονται μόνο σε άτομα τα οποία είναι εξουσιοδοτημένα. Όλα τα παραπάνω, καταλήγουν στο ότι τα δεδομένα

δεν θα πρέπει απλά να προστατεύονται από τη μη εξουσιοδοτημένη ανάγνωση, αλλά και από την πληροφόρηση ότι αυτά τα δεδομένα υπάρχουν. Από τα παραπάνω εύκολα συμπεραίνουμε ότι η εμπιστευτικότητα έχει και άλλες πτυχές, όπως είναι η ιδιωτικότητα και η μυστικότητα. (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Η ακεραιότητα μπορεί να οριστεί, ως απαίτηση να είναι τα πράγματα όπως πρέπει να είναι, δηλαδή πρόληψη από μη εξουσιοδοτημένη μεταβολή δεδομένων, όπως εγγραφή, διαγραφή ή και δημιουργία δεδομένων. (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Η Διαθεσιμότητα αφορά στην ιδιότητα του πληροφοριακού συστήματος, όπου όλες οι υπηρεσίες του είναι προσπελάσιμες, χωρίς αδικαιολόγητη καθυστέρηση, όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Η Διαθεσιμότητα, αποτελεί, έναν από τους πιο σημαντικούς παράγοντες της καλής λειτουργίας ενός συστήματος και είναι καταλυτικός παράγοντας για την αντιμετώπιση του προβλήματος άρνησης εξυπηρέτησης (denial of service), όταν εξουσιοδοτημένοι χρήστες επιθυμούν να προσπελάσουν τους πόρους του (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Εκτός από τις παραπάνω θεμελιώδεις έννοιες υπάρχουν και μερικές ακόμη δευτερεύουσες άλλα εξίσου σημαντικές έννοιες ασφάλειας πληροφοριακών συστημάτων όπως (Γ. Πάγκαλος & Ι. Μαυρίδης 2002):

- *Εξουσιοδοτημένη χρήση (authorized use)*. Μόνο εξουσιοδοτημένα άτομα μπορούν να χρησιμοποιούν το πληροφοριακό σύστημα, πάντα σύμφωνα με τον προκαθορισμένο τρόπο.
- *Αυθεντικοποίηση μηνυμάτων (message authentication)*. Η βεβαιότητα ότι το άτομο που φέρεται να έστειλε το μήνυμα, σύμφωνα με το σύστημα, το έχει όντως στείλει.
- *Μη απάρνηση (non repudiation)*. Η βεβαιότητα ότι το μήνυμα έχει βρει τον παραλήπτη του.
- *Απόδοση ευθυνών (accountability)*. Οι χρήστες θα πρέπει να είναι υπεύθυνοι για τις πράξεις τους.

- *Αξιοπιστία (reliability) και Σιγουριά (safety)*: Οι δύο αυτές έννοιες θέτουν ως προϋπόθεση ότι τα συστήματα θα πρέπει να λειτουργούν κανονικά ακόμη και σε αντίξοες συνθήκες.

Όμως, κάθε πληροφοριακό σύστημα είναι ευάλωτο σε ευπάθειες. Με τον όρο ευπάθεια εννοούμε μια αδυναμία ή ένα ευάλωτο σημείο στο σύστημα ασφάλειας, το ο οποίο μπορεί να γίνει αντικείμενο επίθεσης για το σύστημα. Μία κατηγοριοποίηση των ευπαθειών περιλαμβάνει τα εξής: φυσικές ευπάθειες (Physical), εκ φύσεως (Natural), υλικού και λογισμικού (Hardware and Software), ευπάθειες μέσων (Media), ευπάθειες εκπομπών (Emanation), ευπάθειες επικοινωνιών (Communications) , καθώς και ανθρώπινες (Human) (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Η απειλή για ένα πληροφοριακό σύστημα αποτελεί οποιαδήποτε κατάσταση μπορεί να προκαλέσει ζημιά ή απώλεια, όπως ανθρώπινη επίθεση ή ακούσια ανθρώπινα λάθη, φυσική καταστροφή ή ακόμα και εσωτερική ατέλεια του εξοπλισμού ή του λογισμικού. Τα είδη των απειλών για τους πόρους του πληροφοριακού συστήματος σε σχέση με το υλικό, το λογισμικό και τα δεδομένα είναι: η υποκλοπή (interception), μεταβολή (modification), πλαστογραφία (fabrication) και η διακοπή (interruption). (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Για να περιοριστούν οι ευπάθειες και οι απειλές σε ένα πληροφοριακό σύστημα θα πρέπει να προβλεφθούν και να εφαρμοστούν μέτρα προστασίας (controls). Τα μέτρα προστασίας ή αντίμετρα (countermeasures) είναι οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός πληροφοριακού συστήματος. Τα διαφορετικά ειδή αντιμέτρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφαλείας των πληροφοριακών συστημάτων στις συνιστώσες της φυσικής ασφάλειας συστήματος (physical security), ασφάλειας υπολογιστικού συστήματος (computer security), ασφάλειας βάσεων δεδομένων (database security) και της ασφάλειας δικτύων επικοινωνιών (network security) (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Υπάρχουν διάφοροι τύποι μέτρων προστασίας για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος. Οι πιο χαρακτηριστικοί είναι, η κρυπτογραφία (encryption), τα μέτρα λογισμικού (software controls), τα μέτρα υλικού (hardware controls), τα φυσικά μέτρα υλικού (physical controls) και οι πολιτικές ασφαλείας (security policies) (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Για τα παραπάνω θα γίνει εκτενής αναφορά σε παρακάτω κεφάλαια της παρούσας εργασίας.

2.4 Τραπεζικά Πληροφοριακά Συστήματα

Η ανάπτυξη των πληροφοριακών συστημάτων, δεν θα μπορούσε να μην επηρεάσει τον χρηματοπιστωτικό κλάδο. Σήμερα, σχεδόν για όλες τις διαδικασίες που διεκπεραιώνει μια τράπεζα, χρησιμοποιούνται τεχνολογίες πληροφορικής. Οι ατέλειωτες ουρές που σχηματίζονταν στα γκισέ της τράπεζας ολοένα και μειώνονται καθώς οι τράπεζες λειτουργούν σε Online σύνδεση αν όχι όλο, μεγάλο μέρος των εφαρμογών τους.

Για να κατανοήσουμε το πλήθος και την πολυπλοκότητα των τραπεζικών πληροφοριακών συστημάτων θα αναφερθούμε στις αντιπροσωπευτικότερες εφαρμογές που υποστηρίζει και λειτουργεί μια τυπική τράπεζα είναι (Αλεξανδρής et al 2005).

- *Εφαρμογές Online Τραπεζικού Δικτύου Συναλλαγών*:

1. ATM
2. Καταθέσεις
3. Χορηγήσεις
4. Κίνηση Κεφαλαίων
5. Αγοραπωλησία Συναλλάγματος
6. Undrewriting
7. Τίτλοι Δημοσίου, όπως ομόλογα ή/και γραμμάτια
8. Εισαγωγές
9. Εξαγωγές

10. Κάρτες (πιστωτικές, χρεωστικές)

- *Ευρύτερα Διεθνή Δίκτυα Τραπεζικών Εφαρμογών*.

Το πιο γνωστό και ευρύτατα χρησιμοποιούμενο δίκτυο είναι το SWIFT (Society for Worldwide Interbank Telecommunication), το οποίο χρησιμοποιείται από τις περισσότερες ελληνικές τράπεζες, αν και έχει υψηλό κόστος και απαιτεί εξειδικευμένη απασχόληση για την υποστήριξή του. Το δίκτυο SWIFT εμπεριέχει πολύ υψηλές προδιαγραφές ασφάλειας, με τη οποία εξασφαλίζεται απόλυτα η ορθότητα και η εμπιστευτικότητα των μηνυμάτων.

Άλλα διεθνή δίκτυα είναι αυτά που παρέχουν οικονομικές πληροφορίες και έχουν αναπτυχθεί από μεγάλες τράπεζας του εξωτερικού ή ανεξάρτητους οργανισμούς παροχής πληροφοριών όπως είναι το REUTERS.

- *Εφαρμογές επικοινωνίας Ελληνικών Τραπεζών σε Εθνικό επίπεδο*.

Οι Ελληνικές Τράπεζες έχουν αναπτύξει και εφαρμογές επικοινωνίας σε Εθνικό επίπεδο. Πολλές τράπεζες χρησιμοποιούν μισθωμένες γραμμές ή ακόμα και διεπιλεγμένες γραμμές και αναπτύσσουν εφαρμογές για την αποστολή ή λήψη στοιχείων από και προς άλλους οργανισμούς (ΔΙΑΣ, Τράπεζα Ελλάδος, ΚΕ.Π.Υ.Ο, ΔΕΗ, ΟΤΕ). Καθίσταται αυτονόητο ότι οι εφαρμογές αυτές θα πρέπει να δημιουργούνται με γνώμονα έναν ασφαλή σχεδιασμό δικτύου.

- *Batch Τραπεζικές Εφαρμογές*.

Πολλές τραπεζικές εφαρμογές τρέχουν όταν είναι κλειστή η Τράπεζα. Οι εφαρμογές αυτές για να μπορέσουν να «τρέξουν» έχουν την ανάγκη κάποιας batch επεξεργασίας (ενημέρωση λογαριασμών, έκδοση τόκων, εκτυπώσεις extraits). Άλλες τραπεζικές εφαρμογές λόγω της μικρής συχνότητας παραγωγής τους είναι σχεδιασμένες να τρέχουν σε μορφή Batch και συνήθως παράλληλα με τα online συστήματα ή τον εφεδρικό ηλεκτρονικό υπολογιστή της Τράπεζας, ώστε να μην επηρεάζουν την απόκριση του δικτύου. Αυτές οι εφαρμογές μπορεί να είναι, η Γενική Λογιστική, οι μισθοδοσίες, συντάξεις, επιταγές, τα γραμμάτια κτλ. Οι batch εφαρμογές αφορούν καθαρά οικονομικά στοιχεία ιδιωτών ή υπαλλήλων (γραμμάτια, μισθοδοσία, συντάξεις) και απαιτούν ιδιαίτερη μεταχείριση από την πλευρά της ασφάλειας. Πέρα από τις μεθόδους εξασφάλισης της ακεραιότητας των αρχείων και

των προγραμμάτων που χρησιμοποιούν, απαιτούν ιδιαίτερες διαδικασίες ελέγχου κατά τη διάρκεια της προετοιμασίας των ενημερωτικών καταστάσεων, μεταβολών των προγραμμάτων ή οποιοδήποτε άλλων παρόμοιων διαδικασιών.

- *Εφαρμογές σε Pc's ή αυτόνομα συστήματα ή πολλαπλών χρηστών.*

Οι εφαρμογές σε PC ή αυτόνομα συστήματα πολλαπλών χρηστών περιλαμβάνουν κυρίως διοικητικής φύσης εργασίες (παρουσίες, άδειες, πρωτόκολλα, έγγραφα) και αντιμετωπίζονται με πακέτα της αγοράς ή με μικρά πληροφοριακά συστήματα που αναπτύσσονται από το προσωπικό της Τράπεζας. Τα πιο διαδεδομένα, είναι τα πακέτα λογιστικών φύλλων .Επίσης, μεγάλη χρήση γίνεται σε εκδοτικά πακέτα για την προετοιμασία εγγράφων, εγκυκλίων, ανακοινώσεων, καθώς και σε ειδικά πακέτα για το σχεδιασμό παρουσιάσεων. Αρκετές Τράπεζες έχουν αξιοποιήσει μικροϋπολογιστές αυτόνομους ή σε δίκτυα για την εγκατάσταση ειδικών εφαρμογών κλειδαρίθμου, οπτικής ανάγνωσης και επεξεργασίας επιταγών. Μεγάλη είναι και η χρήση πακέτων για CAD/CAM εφαρμογές, στατιστικές και οικονομετρικές εφαρμογές, νομικών ή άλλων βιβλιοθηκών και γραμματειακής υποστήριξης διοικήσεων με διευκολύνσεις αυτοματισμού γραφείου

2.5 Ασφάλεια Τραπεζικών Πληροφοριακών Συστημάτων

Η ασφάλεια τραπεζικών πληροφοριακών συστημάτων είναι η ικανότητα ενός Τραπεζικού Ιδρύματος να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες κάθε στιγμή αναζήτησης. Για αυτό το σκοπό πρέπει να ληφθούν μέτρα που εξασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και τη συνεχή και ανεμπόδιστη λειτουργία του κέντρου πληροφορικής(Αλεξανδρής et al 1995).

Η ασφάλεια αποτελεί αναγκαία συνθήκη έτσι ώστε σε συνεργασία με τις άλλες βασικές προϋποθέσεις λειτουργίας ενός οργανισμού να εξασφαλιστεί η εύρυθμη λειτουργία του. Η ασφάλεια είναι από τη φύση της δυναμική παράμετρος και όχι στατική. Συνεπώς, η πολιτική ασφαλείας θα πρέπει να επανεξετάζεται συνεχώς και να διορθώνεται όπου αυτό κρίνεται απαραίτητο.

Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων διακρίνεται σε δύο κατηγορίες:

1. την ασφάλεια σε περίπτωση έκτακτης ανάγκης και
2. την ασφάλεια στις καθημερινές διεργασίες.

Οι συνηθέστερες δυσλειτουργίες που μπορούν να συμβούν σε περιπτώσεις έκτακτης ανάγκης περιλαμβάνουν, διακοπές ηλεκτρικής ενέργειας, προσωρινές βλάβες από πυρκαγιά ή πλημμύρα, απώλεια γραμμών επικοινωνίας και διακοπή λειτουργίας μέρους του εξοπλισμού και του κεντρικού υπολογιστή. Για την αντιμετώπιση των παραπάνω δυσλειτουργιών γίνεται μετάπτωση στο εφεδρικό σύστημα (disaster recovery facility, D.R.F.) που υπάρχει στις περισσότερες Τράπεζες. Αν αυτό δεν είναι εφικτό, τότε σταματά η λειτουργία, έως ότου αποκατασταθεί η βλάβη και επανέρθει η πλήρης λειτουργία του συστήματος. Αυτό που μπορούμε να πούμε με σιγουριά, είναι ότι ένα λεπτομερές Σχέδιο Έκτακτης Ανάγκης θα πρέπει να συντάσσεται, να ελέγχεται αλλά και να αναθεωρείται, σε τακτά χρονικά διαστήματα (Αλεξανδρής et al 1995).

Από τη άλλη η ασφάλεια των καθημερινών λειτουργιών των πληροφοριακών συστημάτων, θα πρέπει να καλύπτει τα κτήρια, τις εγκαταστάσεις, το μηχανογραφικό εξοπλισμό και το λογισμικό. Παράλληλα, θα πρέπει να μεριμνά για το ποιοι και πως αναπτύσσουν, συντηρούν ή χειρίζονται τα διάφορα πληροφοριακά συστήματα, ποιοι μπαίνουν σε χώρους όπου διακινούνται εμπιστευτικές πληροφορίες, καθώς και πόσες γενιές δεδομένων φυλάσσονται, από ποια δεδομένα και που (Αλεξανδρής et al 1995).

Η ασφάλεια των καθημερινών τραπεζικών εργασιών θα μπορούσε να διακριθεί σε τέσσερις κατηγορίες (Αλεξανδρής et al 1995):

1. Τη φυσική ασφάλεια των πληροφοριακών συστημάτων
2. Τη λογική ασφάλεια των πληροφοριακών συστημάτων
3. Την ασφάλεια δικτύων και του εξοπλισμού συναλλαγών
4. Την ασφάλεια λοιπών δικτύων, περιφερειακού και βοηθητικού εξοπλισμού

Τα μέτρα προστασίας που αφορούν στην φυσική ασφάλεια των πληροφοριακών συστημάτων είναι, η προστασία των χώρων του κέντρου πληροφορικής. Επίσης,

απαραίτητη είναι η προστασία του υλικού καθώς και η προστασία των εφεδρικών αντιγράφων (back-up). Επιπλέον θα ήταν απαραίτητη η εγκατάσταση ενός συστήματος αδιάλειπτου λειτουργίας (U.P.S) και ενός συστήματος πυρόσβεσης. Με τα παραπάνω μέτρα, μπορούν αν αποφευχθούν καταστροφή ή βλάβη του υλικού εξοπλισμού, απώλεια ή αλλοίωση δεδομένων.

Η Λογική Ασφάλεια περιλαμβάνει την προφύλαξη του λογισμικού και των δεδομένων, ώστε να αποφευχθούν αλλοιώσεις στις παραμέτρους του συστήματος, απώλεια δίσκων, κλοπή συνθηματικών η ακόμα και ενεργοποίηση κακόβουλων λογισμικών.

Σε σχέση με την Ασφάλεια Δικτύου και εξοπλισμού συναλλαγών, εξετάζεται το δίκτυο των online συναλλαγών της Τράπεζας. Τα μηνύματα που μεταφέρονται στις τραπεζικές συναλλαγές είναι σημαντικά, επομένως είναι απαραίτητη η προστασία των μηνυμάτων, η οποία επιτυγχάνεται με την κρυπτογραφία και με άλλες μεθόδους αυθεντικοποίησης και πιστοποίησης. Έτσι, τα μέτρα που πρέπει να εφαρμοστούν για να επιτευχθεί η ασφάλεια στο On-Line δίκτυο συναλλαγών είναι: η κρυπτογραφία κατά τη μεταφορά των δεδομένων, οι αποκλειστικές και εναλλακτικές τηλεφωνικές γραμμές, διαδικασίες restart/recovery καθώς και μέτρα για τη φυσική προστασία της εγκατάστασης. Εάν δεν τηρηθούν αυτά τα μέτρα, μπορεί να προκληθεί υποκλοπή και τροποποίηση μηνυμάτων από παγίδευση γραμμών, υποκλοπή παραμέτρων αυθεντικοποίησης, λανθασμένη δρομολόγηση εξόδων και διασταυρούμενη επικοινωνία .

Σε ότι αφορά στην ασφάλεια λοιπών δικτύων, περιφερειακού και μηχανολογικού εξοπλισμού εξετάζονται οι παράμετροι ασφαλείας που ισχύουν για τον λοιπό «μηχανογραφικό» εξοπλισμό και υποστηρίζει τις υπηρεσίες της Τράπεζας που είναι που συνδεδεμένες με κάποιας μορφής δίκτυο είτε είναι αυτόνομοι μικροϋπολογιστές. Αυτά τα μέτρα είναι, η συστηματική λήψη ασφαλείας, εγκατάσταση και χρησιμοποίηση προγραμμάτων ανίχνευσης ιών (antiirus), εκπαίδευση των χρηστών στις τεχνικές προστασίας, φύλαξη των εμπιστευτικών αρχείων σε δισκέτες ή CD-ROM σε ασφαλή χώρο και η φυσική προστασία του χώρου του προσωπικού υπολογιστή, των περιφερειακών και βοηθητικών συσκευών. Οι κίνδυνοι που μπορεί να προκύψουν από την μη τήρηση των ανωτέρω μέτρων είναι

η μορφοποίηση δίσκου (formatting) ή το σβήσιμο αρχείων και προγραμμάτων, επίσης, μπορεί να τροποποιηθούν πεδία, με τα τοπικά δίκτυα (LAN) να διατρέχουν άμεσο κίνδυνο. Οι πλημμελείς διαδικασίες εφεδρικών αντιγράφων (back-up) ή αποθήκευσης, τα ξεχασμένα κλειδιά (passwords) ή μη εξουσιοδοτημένη προσπέλαση, μπορούν να δημιουργήσουν πρόβλημα.

ΚΕΦΑΛΑΙΟ ΙΙΙ

ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ (E- Banking)

Τα τραπεζικά ιδρύματα, αναζητούν διαρκώς νέους τρόπους προσέγγισης και αύξησης των πελατών τους. Στην εποχή της τεχνολογίας και του διαδικτύο, οι τραπεζικοί οργανισμοί δεν θα μπορούσαν να είναι απλά παρατηρητές, αλλά πρωτοπόροι. Έτσι, δραστηριοποιήθηκαν μέσω διαδικτύου, με σκοπό να προωθήσουν τα προϊόντα τους και να προσφέρουν στου πελάτες τους τη δυνατότητα της 24ωρης εξυπηρέτησης και επικοινωνίας μαζί τους. Αποτέλεσμα όλων τα παραπάνω είναι η ανάπτυξη της Ηλεκτρονικής Τραπεζικής ή e-banking.

3.1 Ιστορική Εξέλιξη

Η πρώτη μορφή της ηλεκτρονικής τραπεζικής είναι τα Αυτόματα Ταμειολογιστικά Μηχανήματα ή ATM τα οποία εμφανίστηκαν τη δεκαετία του ‘60. Το πρώτο μηχάνημα, προπομπός του σημερινού ATM, τοποθετήθηκε στην Αμερική από την City Bank of New York το 1961, αλλά αποσύρθηκε μετά από 6 μήνες, λόγω έλλειψης εμπιστοσύνης από τους πελάτες της τράπεζας. Έπειτα από πολλές βελτιώσεις το πρώτο σύγχρονο ATM, εγκαταστάθηκε στο Essex της Αγγλίας, από την Τράπεζα “Lloyd Bank” το 1972 (http://en.wikipedia.org, 27.12.2013).

Η εμφάνιση ηλεκτρονικής τραπεζικής, e-banking, με τη σημερινή μορφή της μετράει κιόλας 19 χρόνια. Η πρώτη ηλεκτρονική τράπεζα, η Security First Network Bank (SFNB), ιδρύθηκε στο Κεντάκυ της Αμερικής τον Οκτώβριο του 1995. Η SFNB, χωρίς να διαθέτει δίκτυο καταστημάτων, εξυπηρετούσε την πελατεία της μόνο μέσα από το διαδίκτυο. Η νέα αυτή τράπεζα σχεδιάστηκε και αναπτύχθηκε από ένα

μικρό σχετικά χρηματοοικονομικό οργανισμό, την Cardinal Bancshares, ο οποίος στη συνέχεια χρηματοδοτήθηκε με 2,4 εκατομμύρια δολάρια από δύο αμερικανικές τράπεζες την Huntington Bancshares και την Wachovia Corporation(Α. Τσάμης 2003).

Ο λόγος που οι δύο αυτές τράπεζες επένδυσαν τόσα χρήματα είναι ότι αυτές πρώτες διέκριναν, ότι πολλοί πελάτες των τραπεζών είχαν την ανάγκη να πραγματοποιούν τις συναλλαγές τους με απλό τρόπο, καθ' όλη τη διάρκεια της ημέρας, συνεχώς όλο το χρόνο και χωρίς γεωγραφικό περιορισμό. Επιπλέον αναγνώρισαν το μεγάλο πλεονέκτημα της Cardinal Bancshares να έχει σχεδιάσει την πιο προηγμένη αρχιτεκτονική ασφαλείας πληροφοριακών συστημάτων της εποχής, αρχιτεκτονική η οποία αποτελεί προϋπόθεση για την αποδοχή της ηλεκτρονικής τραπεζικής από τους πελάτες (Α. Τσάμης 2003).

Στα τέλη της δεκαετίας του '90 καταγράφηκε σημαντική αύξηση στην ίδρυση και λειτουργία διαδικτυακών τραπεζών, έτσι οι παραδοσιακές τράπεζες, οι οποίες προωθούσαν προϊόντα και υπηρεσίες και εξυπηρετούσαν τις συναλλαγές των πελατών τους μέσα από τα καταστήματά, ένιωσαν να απειλούνται, καθώς διαπίστωναν ότι ποσοστό των πελατών τους άρχιζε να στρέφεται προς τις τράπεζες νέας μορφής. Έτσι, αναγκάστηκαν να ακολουθήσουν την τάση της ηλεκτρονικής τραπεζικής, και σε αρκετές περιπτώσεις, αναγκάστηκαν να αναθεωρήσουν τα πληροφοριακά συστήματα και ορισμένων επιχειρησιακών λειτουργιών τους, ώστε να ανταποκρίνονται στα αιτήματα των πελατών που τους διαβιβάζονταν ηλεκτρονικά (Α. Τσάμης 2003).

Τελικά, οι παραδοσιακές τράπεζες άρχισαν να ενσωματώνουν τον τρόπο λειτουργίας των ηλεκτρονικών τραπεζών, δίνοντας περισσότερη έμφαση στη συνέργια ανάμεσα στα δίκτυα του φυσικού και του ηλεκτρονικού κόσμου, καθώς αναγνωρίστηκε ότι η μία μορφή συμπληρώνει την άλλη και αντίστροφα. Έτσι, τα ηλεκτρονικά δίκτυα μπορούν να εξυπηρετήσουν επαναλαμβανόμενες τραπεζικές και χρηματοοικονομικές εργασίες, να πληροφορήσουν, να ειδοποιήσουν τον πελάτη και να τον διευκολύνουν στην προσωπική του χρηματοοικονομική διαχείριση, ενώ παράλληλα το δίκτυο καταστημάτων εξυπηρετεί τον πελάτη σε ζητήματα όπως, στην

ανάλυση των αναγκών του, στην επεξήγηση πολύπλοκων προϊόντων, στην εκπαίδευση της πελατείας σε νέα προϊόντα και δίκτυα, καθώς και στην εξυπηρέτηση όσων συναλλαγών απαιτούν ακόμα τη φυσική παρουσία του πελάτη στο κατάστημα (Α. Τσάμης 2003).

Στη χώρα μας, την ηλεκτρονική τραπεζική εισήγαγε η «ΕΓΝΑΤΙΑ Τράπεζα» το 1997, και περιελάμβανε πληροφορίες συναλλαγών, όπως ερώτηση υπολοίπου και μεταφορές κεφαλαίων εντός Τράπεζας. Η πρώτη ολοκληρωμένη πλατφόρμα ηλεκτρονικών υπηρεσιών, εισήχθη στην Ελλάδα από τη Τράπεζα Πειραιώς το 2000, με το brand name «WINBANK» (Β. Αγγέλης 2005). Σήμερα, σχεδόν όλα τα χρηματοπιστωτικά ιδρύματα της χώρας μας διαθέτουν υπηρεσίες ηλεκτρονικής τραπεζικής και παρέχουν πλήθος τραπεζικών υπηρεσιών , όπως μεταφορά χρημάτων, πληρωμή λογαριασμών, παρακολούθηση κινήσεων λογαριασμών, κατάθεση αιτήσεων για κάρτα ή ακόμα και δάνειο, εντός και εκτός συνόρων.

Από τα παραπάνω, μπορούμε να συμπεράνουμε ότι η ηλεκτρονική τραπεζική αποτελεί στόχο για βελτιστοποίηση των επιχειρησιακών λειτουργιών στις παραδοσιακές τράπεζες, οι οποίες αναγκαστικά πλέον, ακολουθούν τα πρότυπα της ηλεκτρονικής τραπεζικής

3.2 Ορισμός Ηλεκτρονικής Τραπεζικής (e-banking)

Με τον όρο ηλεκτρονική τραπεζική ή e-banking εννοούμε τις υπηρεσίες που παρέχουν οι τράπεζες χωρίς τη φυσική παρουσία του πελάτη στο υποκατάστημα μιας τράπεζας αλλά μέσω του Διαδικτύου.

Η ηλεκτρονική τραπεζική, σύμφωνα με την Ένωση Ελληνικών Τραπεζών, περιλαμβάνει οποιαδήποτε εμπορική συναλλαγή που διεξάγεται μεταξύ της τράπεζας και των πελατών της, διαμέσου ηλεκτρονικών δικτύων και βοηθάει ή οδηγεί στην πώληση τραπεζικών προϊόντων και υπηρεσιών.

Ανάλογα με το κανάλι που χρησιμοποιείται ώστε να διανεμηθούν οι τραπεζικές υπηρεσίες, διακρίνουμε το e-Banking στις τρεις παρακάτω κατηγορίες:

- Mobile Banking, όπου η πρόσβαση στις συναλλαγές πραγματοποιείται μέσω κινητού τηλεφώνου
- Phone Banking, όπου χρησιμοποιείται το τηλέφωνο.
- Internet Banking όπου ως μέσο διεξαγωγής τραπεζικών συναλλαγών χρησιμοποιείται το Internet.

3.2.1 Mobile banking.

Το mobile banking δεν έχει καταφέρει να διεισδύσει στην ελληνική ηλεκτρονική τραπεζική. Το γεγονός όμως ότι η κινητή τηλεφωνία αναπτύσσεται διαρκώς και τυγχάνει μεγάλης αποδοχής στην χώρας μας, αποτελεί καλό οιωνό για την πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω κινητού τηλεφώνου (Α. Σινανιώτη – Μαυρούδη & Δ. Φαρσαρώτας, 2005).

Παρόλα αυτά, οι υπηρεσίες που προσφέρει το mobile banking στους χρήστες του είναι, η παρακολούθηση υπολοίπου και χαρτοφυλακίου, η μεταφορά χρημάτων, η πληρωμή λογαριασμών και καρτών, καθώς και η υποβολή αίτησης για χορήγηση τραπεζικών προϊόντων.

3.2.2 Phone Banking.

Με το phone banking, η τράπεζα γίνεται προσιτή στον πελάτη χωρίς γεωγραφικούς περιορισμούς, απλά με τη χρήση του τηλεφώνου. Οι υπηρεσίες που προσφέρει το phone banking, μπορούν να κατηγοριοποιηθούν ως εξής (Β. Αγγελής, 2005):

- Διεκπεραίωση συναλλαγών μέσω τηλεφωνικού κέντρου. Σε αυτή την περίπτωση ο πελάτης επικοινωνεί με κάποιον εκπρόσωπο της τράπεζας και υποβάλλει τα αιτήματά του, τα οποία ικανοποιούνται εφόσον έχουν ταυτοποιηθεί τα στοιχεία του πελάτη, ώστε να εξασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα.

- Διεκπεραίωση συναλλαγών μέσω αυτόματων συστημάτων. Σε αυτή την περίπτωση αυτή, ακολουθούνται και πάλι οι διαδικασίες εξασφάλισης της ακεραιότητας και εμπιστευτικότητας, αλλά ο πελάτης της τράπεζας δεν συνομιλεί με κάποιον εκπρόσωπο, αλλά απαντά στα αυτοματοποιημένα μηνύματα.

3.2.3 Internet Banking.

Το κανάλι επικοινωνίας που χρησιμοποιείται στο Internet banking είναι το διαδίκτυο. Για τη χρήση του Internet banking, ο πελάτης της τράπεζας θα πρέπει να έχει ένα ηλεκτρονικό υπολογιστή και μία σύνδεση στο internet. Στο Internet banking ο πελάτης μπορεί να διεκπεραιώνει κάθε είδους συναλλαγές με την τράπεζα και να εξασφαλίσει τη ενημέρωσή του για τραπεζικά προϊόντα ανά πάσα στιγμή το επιθυμήσει (Β. Αγγέλης 2005).

3.3 Προσφερόμενες Υπηρεσίες Μέσω Ηλεκτρονικής Τραπεζικής.

Οι τραπεζικές συναλλαγές που προσφέρονται μέσω της ηλεκτρονικής τραπεζικής χωρίζονται σε τέσσερις βασικές κατηγορίες, ως εξής(Β. Αγγέλης 2005):

- Οικονομικές συναλλαγές
- Πληροφοριακές Συναλλαγές
- Αιτήσεις
- Άλλες Υπηρεσίες

3.3.1 Οικονομικές Συναλλαγές

Οι οικονομικές συναλλαγές περιλαμβάνουν όλες τις συναλλαγές που θα μπορούσε να κάνει ο πελάτης της τράπεζας εάν βρισκόταν μπροστά από το ταμείο της. Οι συναλλαγές αυτές αφορούν ενδοτραπεζικές συναλλαγές, όπως μεταφορές κεφαλαίων, πληρωμή καρτών και δανείων, ακόμα και συναλλαγές που υλοποιούνται

ύστερα από συμφωνία της τράπεζας με Τρίτο Οργανισμό , όπως πληρωμές λογαριασμών εταιριών σταθερής και κινητής τηλεφωνίας.

Επιπλέον, μέσω της ηλεκτρονικής τραπεζικής διενεργούνται και συναλλαγές στα πλαίσια των διατραπεζικών συστημάτων, κυρίως του ΔΙΑΣ ΑΕ.

Η εταιρία ΔΙΑΣ ιδρύθηκε το 1989 με πρωτοβουλία της Ελληνικής Ένωσης Τραπεζών. Σκοπός της είναι η ανάπτυξη και λειτουργία υπηρεσιών πληροφορικής προς όφελος του ελληνικού τραπεζικού συστήματος. Το σύστημα πληρωμών της ΔΙΑΣ αποτελείται από μεταφορές πίστωσης, άμεσες χρεώσεις, επιταγές, συναλλαγές σε ΑΤΜ, πληρωμές με κάρτες, κ.λπ. (http://www.dias.com.gr)

Στις οικονομικές συναλλαγές, μπορούμε να συμπεριλάβουμε συνοπτικά τις παρακάτω:

- ✓ Μεταφορές εντός τράπεζας, είτε σε λογαριασμό του ίδιου του δικαιούχου, είτε σε λογαριασμό τρίτου.
- ✓ Εμβάσματα εσωτερικού
- ✓ Εμβάσματα εξωτερικού
- ✓ Πληρωμές δανείων
- ✓ Πληρωμές πιστωτικών καρτών
- ✓ Πληρωμές δημοσίου
- ✓ Πληρωμές λογαριασμών ΔΕΚΟ
- ✓ Πληρωμές κινητής και σταθερής τηλεφωνίας
- ✓ Πληρωμές τρίτων
- ✓ Μαζικές πληρωμές – Μισθοδοσία υπαλλήλων

3.3.2 Πληροφοριακές Συναλλαγές

Οι πληροφοριακές συναλλαγές, παρέχουν την δυνατότητα στους πελάτες της τράπεζας να ενημερώνονται για όλα τα προϊόντα της, ανά πάσα στιγμή και διακρίνονται στις ακόλουθες κατηγορίες:

- ✓ Πληροφορίες λογαριασμών

- ✓ Πληροφορίες καρτών
- ✓ Πληροφορίες επιταγών
- ✓ Πληροφορίες για πληρωμές δανείων

3.3.3. Αιτήσεις

Η συγκεκριμένη εφαρμογή της ηλεκτρονικής τραπεζικής δημιουργήθηκε με σκοπό να διευκολύνει τους πελάτες να κάνουν ορισμένες συναλλαγές που απαιτούν αίτηση. Έτσι, οι πελάτες μπορούν να υποβάλλουν αίτηση για τη συναλλαγή που επιθυμούν, συμπληρώνοντας σε μια ηλεκτρονική φόρμα. Με αυτό τον τρόπο ο πελάτης γνωρίζει εκ των προτέρων, ότι σε μερικές ημέρες θα υλοποιηθεί το αίτημά του, ή σε περίπτωση μη υλοποίησης, θα ενημερωθεί από την εκάστοτε τράπεζα για την κατάσταση της αίτησης, ώστε να βρεθεί λύση. Ορισμένες μορφές τέτοιων αιτήσεων, είναι οι ακόλουθες:

- ✓ Αίτηση ανοίγματος λογαριασμού
- ✓ Αίτηση για δάνειο
- ✓ Αίτηση για παραγγελία συναλλάγματος
- ✓ Αίτηση παραγγελίας μπλοκ επιταγών.

3.3.4. Άλλες υπηρεσίες

Οι τράπεζες μέσω της ηλεκτρονικής τραπεζικής παρέχουν την δυνατότητα στους πελάτες τους, να ενημερώνονται για διάφορα θέματα γενικού περιεχομένου όπως:

- ✓ Τον υπολογισμό του IBAN
- ✓ Μετατροπή νομισμάτων
- ✓ Υπολογισμός δόσεων δανείων

3.4 Πλεονεκτήματα Χρήσης Ηλεκτρονικής Τραπεζικής.

Από τα παραπάνω μπορούμε εύκολα να συμπεράνουμε ότι η εμφάνιση της ηλεκτρονικής τραπεζικής έχει διευκολύνει σε μεγάλο βαθμό την καθημερινές συναλλαγές μας με την τράπεζα. Ας δούμε όμως, πέρα από τα προφανή, ποια είναι τα πλεονεκτήματα - οφέλη που απορρέουν από την χρήση της ηλεκτρονικής τραπεζικής, τόσο για τους πελάτες της τράπεζας, είτε είναι ιδιώτες είτε είναι επιχειρήσεις, όσο και για την ίδια την τράπεζα.

3.4.1 Πλεονεκτήματα – Οφέλη για τον Ιδιώτη

Παρακάτω αναλύονται τα πλεονεκτήματα – οφέλη που προσφέρει η ηλεκτρονική τραπεζική σε πελάτες της που είναι ιδιώτες (Β. Αγγέλης, 2005).

Ίσως το πιο σημαντικό και άμεσο πλεονέκτημα της ηλεκτρονικής τραπεζικής είναι η διαθεσιμότητα των τραπεζικών υπηρεσιών 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα. Ο πελάτης μπορεί να έχει πρόσβαση και να εξυπηρετηθεί οποιαδήποτε στιγμή εκείνος επιθυμεί και σε σημαντικά ελάχιστο χρόνο, χωρίς να περιμένει σε χρονοβόρες ουρές. Για να κατανοήσει κάποιος τη τεράστια διαφορά του χρόνου εξυπηρέτησης, ας αναλογιστεί ότι τα τραπεζικά καταστήματα είναι στη διάθεση των πελατών 6,5 ώρες την ημέρα και μόνο τις πέντε εργάσιμες ημέρες της εβδομάδας.

Ο πελάτης δε χρειάζεται να περιμένει στην αναμονή κάποιου ταμείου τράπεζας ή σε κάποιο ATM για να εξυπηρετηθεί. Εύκολα και άμεσα εκτελεί την συναλλαγή που επιθυμεί, καθώς μέσω της ηλεκτρονικής τραπεζικής εξαλείφεται η ανάγκη φυσικής παρουσίας του πελάτη σε κατάστημα της τράπεζας.

1. *Εξοικονόμηση χρόνου:* Ο χρήστης του e-banking κερδίζει χρόνο, αφού δεν είναι απαραίτητο να φύγει από εκεί που βρίσκεται για να μεταβεί σε κάποιο από τα καταστήματα της τράπεζας, προκειμένου να εκτελέσει την συναλλαγή που θέλει.
2. On-line παρακολούθηση τραπεζικών προϊόντων: Οι λογαριασμοί, οι κάρτες, οι επιταγές, τα δάνεια και γενικότερα οποιοδήποτε τραπεζικό προϊόν κατέχει ένας πελάτης της τράπεζας, είναι προσβάσιμο on-line. Ο χρήστης μέσα από λίγες οθόνες ή

κλήσεις ενημερώνεται εύκολα και γρήγορα για τα υπόλοιπα των λογαριασμών του, τις κινήσεις ιστορικού του, τις εντολές του, κ.λπ.

3. On-line μεταφορά κεφαλαίων: Ο χρήσης ηλεκτρονικής τραπεζικής μπορεί με συνοπτικές διαδικασίες να μεταφέρει κεφάλαια, τόσο εντός της τράπεζάς του, όσο και σε άλλες τράπεζες, ελέγχοντας πλήρως τις οφειλές και τις υποχρεώσεις του.

4. Μείωση χρήσης χαρτιού: Μέσω της ηλεκτρονικής τραπεζικής, τα statement των λογαριασμών, οι κινήσεις τους, οι κινήσεις καρτών, οι δόσεις δανείων, η κατάσταση των επιταγών και άλλα, είναι πλέον διαθέσιμα στην οθόνη του υπολογιστή, κατά συνέπεια ο χρήστης μπορεί να εκτυπώσει μόνο την πληροφορία που επιθυμεί, και όχι μεγάλο όγκο χαρτιού, όπως συνέβαινε παλαιότερα.

5. Εύκολη πρόσβαση από οποιοδήποτε σημείο του κόσμου: Ο πελάτης που είναι εγγεγραμμένος στο site του e-banking, μπορεί ανά πάσα στιγμή, ακόμη κι αν βρίσκεται στο εξωτερικό, να ελέγξει το χαρτοφυλάκιό του ή να εκτελέσει τις συναλλαγές που επιθυμεί, πληκτρολογώντας μόνο ορισμένα προσωπικά στοιχεία από τον χώρο του.

6. Μεγάλη γκάμα εξόφλησης λογαριασμών Επιχειρήσεων και Οργανισμών: Οι πελάτες βρίσκουν πλέον μία συνεχώς αυξανόμενη γκάμα επιχειρήσεων για να εξοφλήσουν τις οφειλές και τους λογαριασμούς τους από ένα σημείο πρόσβασης, με αποτέλεσμα να έχουν συγκεντρωτική ενημέρωση αλλά και να κάνουν καλύτερο προγραμματισμό των υποχρεώσεών τους.

7. Δυνατότητα επενδυτικών συναλλαγών: Οι χρήστες υπηρεσιών e-banking έχουν την δυνατότητα να εκτελούν επενδυτικές συναλλαγές (χρηματιστήριο) και να ελέγχουν οι ίδιοι τις εντολές τους, τα χαρτοφυλάκιά τους και την αποτίμηση αυτών.

8. Μικρότερο κόστος συναλλαγών: Όλο το εύρος των τραπεζικών συναλλαγών παρέχεται με μικρότερο κόστος τους πελάτες του e-banking, ενώ πολλές από αυτές παρέχονται και εντελώς δωρεάν.

9. Εύκολες συναλλαγές για άτομα με ειδικές ανάγκες: Οι άνθρωποι με κινητικά κυρίως προβλήματα, έχουν την δυνατότητα μέσω της ηλεκτρονικής τραπεζικής, να συναλλάσσονται εύκολα και γρήγορα με την τράπεζά τους, χωρίς να απαιτείται η μετακίνηση αυτών των ατόμων σε κατάστημα της τράπεζας.

10. Γνωριμία με νέες τεχνολογίες: Η διενέργεια συναλλαγών μέσω e-banking φέρνει αντιμέτωπο τον πελάτη της τράπεζας με νέες τεχνολογίες. Πολλοί είναι εκείνοι που παλαιότερα δεν είχαν καμία σχέση με τις νέες τεχνολογίες και πόσο μάλλον με το

internet banking, και τώρα, αναγνωρίζοντας τα οφέλη που προσφέρουν αυτές οι υπηρεσίες, έχουν εξοικειωθεί και κάνουν πλέον τις συναλλαγές τους αποκλειστικά μέσω του διαδικτύου.

3.4.1 Πλεονεκτήματα – Οφέλη για τις Επιχειρήσεις

Έχει αποδειχθεί ότι η εφαρμογή της ηλεκτρονικής τραπεζικής έχει γίνει αποδεκτή και πολύ χρήσιμη, ακόμη και για ορισμένες εταιρίες ή και Οργανισμούς. Πολλοί από αυτούς έχουν συνάψει συμφωνία με κάποια τράπεζα, ώστε μέσω του ebanking να μπορούν να εξυπηρετούνται εύκολα, αφενός εκείνοι και αφετέρου οι άνθρωποι που έχουν άμεση σχέση με αυτήν (εργαζόμενοι, πελάτες, προμηθευτές).

Συνεπώς, τα πλεονεκτήματα που απολαμβάνουν οι διάφορες εταιρίες-Οργανισμοί χρήστες του e-banking είναι τα ακόλουθα (Β. Αγγέλης, 2005):
1. Οργανωμένα πακέτα υπηρεσιών πληρωμών για επιχειρήσεις: Μία εταιρία έχει ένα ολοκληρωμένο περιβάλλον πληρωμών, τόσο των οφειλών της στο Δημόσιο (ΦΠΑ, εργοδοτικές εισφορές ΙΚΑ, τέλη κυκλοφορίας), όσο και των οφειλών της σε ΔΕΚΟ και οργανισμούς.
2. Εύκολη ενημέρωση των μηχανογραφικών συστημάτων της εταιρίας: Μέσω της ευκολίας του downloading που προσφέρουν οι τράπεζες μέσω της ηλεκτρονικής τραπεζικής, οι επιχειρήσεις μπορούν εύκολα και άμεσα να ενημερώνουν τα μηχανογραφικά και λογιστικά τους συστήματα με τις κινήσεις των λογαριασμών της εταιρίας.
3. Εκτέλεση μισθοδοσίας προσωπικού ή μαζικών πληρωμών προμηθευτών: η επιχείρηση έχει τη δυνατότητα, με πολύ συνοπτική διαδικασία να εκτελεί τη μισθοδοσία του προσωπικού της, ή να πληρώνει τους προμηθευτές της και να παρακολουθεί on-line την κατάσταση των πληρωμών της.
4. Διαφορετικά δικαιώματα χρήσης και πρόσβασης: Η εταιρία έχει τη δυνατότητα να επιλέξει ποιοι υπάλληλοί της θα χρησιμοποιούν ηλεκτρονικές τραπεζικές υπηρεσίες και τι δικαιώματα θα έχουν, τόσο σε επίπεδο πρόσβασης σε λογαριασμούς και κάρτες, όσο και σε επίπεδο τέλεσης συναλλαγών. Στους εταιρικούς πελάτες δίνεται και η δυνατότητα της έγκρισης συναλλαγών, δηλαδή άλλος χρήστης να καταχωρεί τις

εντολές και διαφορετικός χρήστης να δίνει την έγκριση για την εκτέλεσή τους.

5. Δημιουργία εναλλακτικού δικτύου εξόφλησης λογαριασμών: Πολλές εταιρίες μπορούν να εκμεταλλευτούν την ηλεκτρονική τραπεζική, ως ένα επιπλέον δίκτυο είσπραξης των υποχρεώσεων των πελατών της. Ήδη, αρκετές εταιρίες χρησιμοποιούν πλέον το διατραπεζικό σύστημα DIASDEBIT σε συνεργασία με τράπεζες του εσωτερικού, για την εξόφληση των λογαριασμών τους από τους πελάτες.

6. Δημιουργία εναλλακτικού δικτύου πώλησης προϊόντων και υπηρεσιών: Οι εταιρίες προσφέρουν σε όλους τους πελάτες τους έναν εναλλακτικό, ασφαλή και εξ ποστάσεως τρόπο αγορών και πληρωμής των οφειλών τους, με συνεργασίες στο χώρο του e-Commerce και των Payments.

3.4.1 Πλεονεκτήματα – Οφέλη για τις Τράπεζες

Σύμφωνα με έρευνες, παρατηρήθηκε ότι οι τράπεζες έχουν σημαντικά οφέλη από την δημιουργία εφαρμογών ηλεκτρονικής τραπεζικής. Συγκεκριμένα, τα οφέλη αυτά, απαριθμούνται παρακάτω ως εξής (Β. Αγγέλης, 2005):

1. *Καλύτερη διαχείριση πληροφοριών:* Οι συναλλαγές που εκτελούνται μέσω των ηλεκτρονικών καναλιών, ιδιαίτερα του internet, παρέχουν πληροφορίες σχετικά με την καταναλωτική συμπεριφορά των πελατών, οι οποίες βοηθούν τις τράπεζες να κατανοήσουν τις ανάγκες των πελατών τους, ώστε να δημιουργήσουν εξειδικευμένα προϊόντα και υπηρεσίες, προσαρμοσμένα στις ανάγκες του κάθε πελάτη.

2. *Η διείσδυση του internet:* Ήδη το διαδίκτυο έχει παίξει σημαντικό ρόλο στη διάδοση των ηλεκτρονικών συναλλαγών. Το διαδίκτυο, ως μέσο, αναμένεται να διαδοθεί πολύ περισσότερο σε όλες τις χώρες, ενώ ραγδαία είναι και η διάδοση του mobile banking σε Ελλάδα και Ιταλία, λόγω της έντονης διάδοσης της κινητής τηλεφωνίας.

3. *Ευκολία, διαφάνεια, εξυπηρέτηση:* Οι πελάτες των τραπεζών είναι καλύτερα ενημερωμένοι για τα παρεχόμενα προϊόντα και υπηρεσίες. Η χρήση των υπηρεσιών e-banking δημιουργεί επιπλέον κανάλι συναλλαγής του πελάτη με την τράπεζα σε 24ωρη βάση, στο οποίο και αναμένεται να επικρατήσεις μεγαλύτερη διαφάνεια, αφού

οι πελάτες θα γνωρίζουν τα προϊόντα και τις υπηρεσίες κάθε τράπεζας, χωρίς να χρειάζεται να την επισκέπτονται.

4. *Πίεση περιθωρίων κέρδους, μείωση λειτουργικού κόστους:* Η εξ αποστάσεως παροχή υπηρεσιών έχει ως αποτέλεσμα την πίεση του περιθωρίου κέρδους των προϊόντων-υπηρεσιών των τραπεζών, με συνέπεια οι τράπεζες, για να συσφίξουν τις πελατειακές τους σχέσεις, εστιάζουν στην όλο και καλύτερη εξυπηρέτηση των πελατών τους. Έτσι, τα τραπεζικά καταστήματα αναβαθμίζονται και εξελίσσονται σε σημεία πώλησης και παροχής συμβουλευτικών υπηρεσιών. Επιπλέον, θα αυξηθεί η ταχύτητα εξυπηρέτησης των συναλλαγών, καθώς δεν θα δημιουργούνται καθυστερήσεις για απλές συναλλαγές στα ταμεία, και αυτό φέρνει και μείωση του λειτουργικού κόστους των τραπεζών.

5. *Βελτίωση των B2B και B2C συναλλαγών:* διαδραματίζοντας σημαντικό ρόλο στο ηλεκτρονικό εμπόριο και έχοντας καλλιεργήσει σχέσης αμοιβαίας εμπιστοσύνης και ασφάλειας, οι τράπεζες διευκολύνουν σημαντικά την διεκπεραίωση των συναλλαγών μεταξύ πελατών και εμπόρων, καθώς και μεταξύ των εμπόρων.

3.5 Μειονεκτήματα Χρήσης Ηλεκτρονικής Τραπεζικής.

Σε σχέση με τα πολυάριθμα προαναφερθέντα πλεονεκτήματα της ηλεκτρονικής τραπεζικής, τα φερόμενα ως μειονεκτήματα είναι σαφώς λιγότερα. Παρόλα αυτά αξίζει να αναφερθούν παρακάτω.

3.5.1 Μειονεκτήματα για τον Πελάτη

Ως μειονέκτημα θα μπορούσε να θεωρηθεί η διαδικασία εγγραφής του πελάτη στο πληροφοριακό σύστημα της ηλεκτρονικής τραπεζικής της τράπεζας. Για την εγγραφή του πελάτη - χρήστη, απαιτείται η φυσική παρουσία του στην τράπεζα, όπου θα πρέπει να προσκομίσει τα απαραίτητα για την εγγραφή του δικαιολογητικά και να υπογράψει τα απαραίτητα έγγραφα.

Επιπλέον, πολλοί πελάτες της τράπεζας δεν είναι εξοικειωμένοι με τις νέες τεχνολογίες. Έτσι, οι δικτυακοί τόποι των τραπεζών που προσφέρουν ηλεκτρονικές

υπηρεσίες, φαίνονται δύσχρηστοι, λόγω της αδυναμίας των πελατών να συμβαδίσουν με τις τεχνολογίες του internet.

Ένα άλλο σημαντικό πρόβλημα, είναι η δυσπιστία του πελάτη. Πολλοί πελάτες των τραπεζών δεν εμπιστεύονται την ηλεκτρονική τραπεζική, λόγω αμφιβολιών που τρέφουν στον τομέα της ασφάλεια των πληροφοριακών συστημάτων. Το θέμα της ασφάλεια είναι τεράστιο. Οι πελάτες εμφανίζονται δύσπιστοι ως προς την εξασφάλιση διαφάνειας των συναλλαγών τους.

Τέλος, ένα άλλο σοβαρό θέμα που ανακύπτει είναι συγκέντρωση πληροφοριών που σχετίζονται με την οικονομική ζωή των συναλλασσομένων, γεγονός που κάνει τους πελάτες να είναι ακόμη πιο δύσπιστοι στη χρήση της ηλεκτρονικής τραπεζικής.

3.5.2 Μειονεκτήματα για την Τράπεζα.

Το κύριο μειονέκτημα από την πλευρά των τραπεζών, είναι το κόστος εγκατάστασης και το λειτουργικό κόστος της ηλεκτρονικής τραπεζικής. Το κόστος αφορά στην εγκατάσταση του πληροφοριακού συστήματος της ηλεκτρονικής τραπεζικής, καθώς και στην δημιουργία της ιστοσελίδας, η οποία θα πρέπει να έχει συγκεκριμένες προδιαγραφές ασφάλειας. Ένα επιπλέον κόστος είναι αυτό της ασφάλειας του πληροφοριακού συστήματος της ηλεκτρονικής τραπεζικής, καθώς και οι ηλεκτρονικές επιθέσεις είναι συχνές και η ασφάλεια είναι από τα πιο σημαντικά θέματα που πρέπει να αντιμετωπίσει η τράπεζα. Το κόστος συντήρησης της ιστοσελίδας, μια και η τεχνολογία εξελίσσεται συνεχώς και εμφανίζονται νέοι κίνδυνοι υποκλοπής δεδομένων. Τέλος, το κόστος εκπαίδευσης και επιμόρφωσης του προσωπικού. Το προσωπικό της τράπεζας θα πρέπει να επιμορφώνεται και να είναι διαρκώς ενήμερο για κάθε εξέλιξη στο σύστημα της ηλεκτρονικής τραπεζικής ώστε να είναι σε θέση να επιλύσει οποιαδήποτε στιγμή τυχόν απορίες των χρηστών της.

ΚΕΦΑΛΑΙΟ IV

ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΡΑΠΕΖΙΚΗΣ.

Σύμφωνα με όσα αναπτύξαμε στο προηγούμενο κεφάλαιο, διαπιστώνουμε ότι η ηλεκτρονική τραπεζική ναι μεν διευκολύνει τις καθημερινές συναλλαγές των πελατών της τράπεζας, αλλά εγείρει θέματα ασφάλειας που σχετίζονται με τις συναλλαγές αλλά και τα δεδομένα, οικονομικά και προσωπικά, που διακινούνται στο διαδίκτυο. Τα ερωτήματα που προκύπτουν είναι, κατά πόσο είναι ασφαλή τα δεδομένα των πελατών της τράπεζας που αποθηκεύονται στα τραπεζικά πληροφοριακά συστήματα των τραπεζών, καθώς και με ποιον τρόπο διασφαλίζεται, από πλευράς της τράπεζας, η ασφάλεια αυτή.

4.1 Στόχοι Μηχανισμών Ασφάλειας Ηλεκτρονικής Τραπεζικής.

Το σύνολο των μηχανισμών ασφαλείας ενός συστήματος ηλεκτρονικής τραπεζικής, θεωρείται ότι έχουν επιτελέσει τον σκοπό τους, όταν έχουν επιτευχθεί οι παρακάτω στόχοι (http://www.ecb.europa.eu, 2003):

- ✓ *Η ακεραιότητα των περιουσιακών στοιχείων*. Ίσως αποτελεί τον πιο σημαντικό στόχο ασφάλειας, ότι τα χρήματα δεν πρέπει να αλλοιώνονται ούτε ως προς την ποσότητα, ούτε ως προς κάποιο άλλο χαρακτηριστικό τους, σε όποιο υποσύστημα και αν αποθηκευτούν.
- ✓ *Η εμπιστευτικότητα των δεδομένων*. Τα δεδομένα όλων των κατηγοριών που διακινούνται μέσα στο πληροφοριακό σύστημα πρέπει να γνωστοποιούνται αποκλειστικά και μόνο στους εξουσιοδοτημένους χρήστες. Οι καταναλωτές δεν μπορούν να γνωρίζουν τους κωδικούς πρόσβασης του διαχειριστή και ο διαχειριστής δεν πρέπει να γνωρίζει τα υπόλοιπα των λογαριασμών των καταναλωτών, εκτός από τις περιπτώσεις που αυτό προβλέπεται.
- ✓ *Η πιστοποίηση του ηλεκτρονικού χρήματος* που μετακινείται μεταξύ των υποσυστημάτων και η πιστοποίηση των υποσυστημάτων που ανταλλάσσουν δεδομένα μεταξύ τους.

- ✓ *Ο έλεγχος πρόσβασης στο πληροφοριακό σύστημα*. Κάθε χρήστης, καταναλωτής ή διαχειριστής, πρέπει να διαθέτει ένα σύνολο μοναδικών κωδικών, με σκοπό τον περιορισμό της πρόσβασης στα αντίστοιχα δεδομένα που τον αφορούν.
- ✓ *Η δέσμευση και η επιβεβαίωση της αξιοπιστίας των εκτελούμενων συναλλαγών*. Κάθε συναλλαγή αφορά συγκεκριμένο χρηματικό ποσό και συγκεκριμένα υποσυστήματα. Αν κάποιο από αυτά δεν μπορεί να καθοριστεί σαφώς, η συναλλαγή πρέπει να καθίσταται αδύνατη.
- ✓ *Η πραγματοποίηση ολοκληρωμένων συναλλαγών*. Εφόσον προκύψει κάποιο πρόβλημα πριν την τελική επιβεβαίωση, η συναλλαγή πρέπει να ακυρώνεται εξ ολοκλήρου. Απαγορεύεται η τμηματική πραγματοποίηση μιας συναλλαγής.
- ✓ *Η Τήρηση της ορθής σειράς των συναλλαγών και των διαδικασιών που προβλέπονται για κάθε συναλλαγή*. Η εκτέλεση μίας ή περισσότερων πράξεων σε λανθασμένη σειρά απαγορεύεται, καθώς μπορεί να προκαλέσει ανεπιθύμητες επιπλοκές ή απρόβλεπτες συνέπειες.
- ✓ *Η αποφυγή απώλειας μονάδων ηλεκτρονικού χρήματος*. Οι ποσότητες χρήματος που εισέρχονται στο πληροφοριακό σύστημα πρέπει να εκτελούν έναν πλήρη κύκλο ζωής. Με άλλα λόγια δεν πρέπει να προκύπτουν διαφορές στις συναλλαγές σε ένα ασφαλές πληροφοριακό συστήμα.
- ✓ *Η τήρηση των ορίων των χρηματικών ποσών*. Σε κάθε συναλλαγή υπάρχει ένα ανώτατο ποσό χρημάτων που μπορούν να διακινηθούν, είτε αυτό καθορίζεται από τους συναλλασσόμενους είτε έχει προκαθοριστεί κατά την κατασκευή του πληροφοριακού συστήματος.
- ✓ *Η ανιχνευσιμότητα των συναλλαγών*. Αυτός ο στόχος αφορά το διαχειριστή, καθώς πρέπει να είναι σε θέση να παρακολουθήσει όλα τα βήματα κατά την εκτέλεση μιας συναλλαγής, αλλά και τις νόμιμες τροποποιήσεις του πληροφοριακού συστήματος, οι οποίες είναι απαραίτητες για την ορθή και αποδοτική λειτουργία του.
- ✓ *Ο εντοπισμός κάθε μη φυσιολογικής ενέργειας* στο πληροφοριακό σύστημα, όπως η παράνομη πρόσβαση ή η προσπάθεια αλλοίωσης των δεδομένων.

- ✓ *Η αντίδραση του πληροφοριακού συστήματος σε κάθε απρόοπτη αλλαγή* της κατάστασής του, όπως η απότομη πτώση τάσης ή η διακοπή οποιασδήποτε προσπάθειας για παράνομη πρόσβαση.
- ✓ *Η χρήση εξελιγμένων πρωτοκόλλων κρυπτογράφησης* για προστασία των πληροφοριών.
- ✓ *Τα ασφαλή μέσα μεταφοράς δεδομένων και οι ασφαλείς χώροι* εγκατάστασης των μηχανημάτων, ώστε να μην είναι εύκολη η φυσική πρόσβαση σε σημαντικά μέρη του πληροφοριακού συστήματος.
- ✓ *Η ενημέρωση του λογισμικού ασφαλείας* με τις τελευταίες εκδόσεις για την καταπολέμηση κάθε νέας απειλής.
- ✓ *Η διαθεσιμότητα του πληροφοριακού συστήματος*, δηλαδή η δυνατότητα χρήσης του ακόμη και σε περιόδους συντήρησης ή βλάβης.

4.2 Κίνδυνοι Ηλεκτρονικής Τραπεζικής.

Οι κίνδυνοι που ελλοχεύουν στα συστήματα ηλεκτρονικής τραπεζικής, ολοένα και αυξάνονται. Οι περισσότερες ηλεκτρονικές απάτες, έχουν ως στόχο να εξαπατήσουν τον χρήστη υποκλέπτοντας τα στοιχεία εισόδου στις ηλεκτρονικές υπηρεσίες της τράπεζας.

Στη συνέχεια ακολουθούν οι πιο συχνά χρησιμοποιούμενες μέθοδοι εξαπάτησης των χρηστών της ηλεκτρονικής τραπεζικής.

4.2.1 Ηλεκτρονικό Ψάρεμα ή Phishing.

Όπως το ίδιο του όνομά του υπονοεί, πρόκειται για παραλλαγή του αγγλικού «fishing» δηλαδή του «ψαρέματος». Τον όρο phishing εννοούμε τη διαδικασία κατά την οποία ο επίδοξος υποκλοπέας προσπαθεί να αποσπάσει τα προσωπικά στοιχεία, οικονομικού συνήθως χαρακτήρα, που αφορούν τραπεζικούς λογαριασμούς και πιστωτικές κάρτες. Ως «δόλωμα» χρησιμοποιείται κάποιο ψεύτικο πρόσχημα.

Ο τρόπος με τον οποίο ο υποκλοπέας προσπαθεί να αποσπάσει τα προσωπικά στοιχεία του επίδοξου θύματος είναι συνήθως, με την αποστολή κάποιου spam e-

mail. Στο εν λόγω e-mail ο υποκλοπέας συστήνεται ως αξιόπιστο πρόσωπο που ανήκει σε κάποια εταιρία ή οργανισμό, πολλές φορές ακόμα και από την ίδια την υπηρεσία του e-mail, και ζητά από το θύμα κάποια προσωπικά στοιχεία.

Ο χρήστης, θεωρώντας ότι το e-mail προέρχεται όντως από τον ισχυριζόμενο αποστολέα, στέλνει τα προσωπικά του στοιχεία. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους υποκλοπείς για την πραγματοποίηση μη εξουσιοδοτημένων και παράνομων οικονομικών συναλλαγών.

Βασικό εργαλείο του phishing είναι οι αποπλανητικοί σύνδεσμοι (link manipulation). Ο χρήστης βρίσκεται σε μία ιστοσελίδα, e-mail ή άμεσο μήνυμα, παραπέμπεται σε έναν σύνδεσμο επιφανειακά αξιόπιστο, αλλά είναι φτιαγμένος έτσι ώστε να τον οδηγεί σε διαφορετική ιστοσελίδα από αυτή που προβλέπεται.

Αυτό είναι κάτι πολύ κρίσιμο αλλά ταυτόχρονα και πολύ εύκολο στη δημιουργία του, αφού σε έναν απλό HTML κώδικα δίνεται η δυνατότητα να μετατρέψει κανείς τον τίτλο του συνδέσμου όπως θέλει. Κάπως έτσι λειτουργούν και οι ψεύτικες ιστοσελίδες (fake websites), που μέσω παραπλανητικών συνδέσμων, οδηγούν τους χρήστες σε σελίδες οπτικά πανομοιότυπες με τις αυθεντικές ιστοσελίδες, αλλά ανήκουν στον server του υποκλοπέα. Σε κάποιες περιπτώσεις, η αναγραφή είναι τόσο καλή, που και ο ίδιος ο φυλλομετρητής «ξεγελιέται» και δείχνει στην γραμμή διευθύνσεων την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου σύντομου χρονικού διαστήματος, ο λογαριασμός του θα μπλοκαριστεί και δε θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητούνται, χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος.

Μία επιτυχημένη επίθεση phishing στηρίζεται σε τρεις βασικούς παράγοντες:

1. την έλλειψη γνώσεων του θύματος,
2. την έλλειψη προσοχής του θύματος και
3. την οπτική εξαπάτηση.

Ο μέσος άνθρωπος ξέρει να χειρίζεται τις βασικές λειτουργίες του υπολογιστή και του διαδικτύου χωρίς να γνωρίζει την διαδικασία με την οποία αυτό λειτουργεί. Ακόμα και σε περιπτώσεις που ο χρήστης έχει τις κατάλληλες γνώσεις για να ανιχνεύσει τα κακόβουλα στοιχεία, πολλές φορές δεν θα προσέξει τα σημάδια, αφού μπορεί να είναι αφηρημένος ή απασχολημένος με κάτι άλλο. Σύμφωνα με μία αναφορά της εταιρίας Symantec το 2006, οι επιθέσεις Phishing αυξήθηκαν κατά 30% σε σημαντικές μέρες όπως ήταν τα Χριστούγεννα, η Πρωτοχρονιά και το Κύπελλο του Ποδοσφαίρου. Έτσι ο χρήστης μπορεί είτε να μην δίνει αρκετή σημασία στις υπάρχουσες προειδοποιήσεις ασφάλειας ή στην έλλειψη αυτών.

Στόχος του hacker είναι να πείσει το θύμα για την αυθεντικότητα και την αξιοπιστία του. Αυτό το επιτυγχάνει με,

1. *Παραπλανητικό κείμενο*, που συνήθως είναι οι παραπλανητικοί σύνδεσμοι με λανθασμένη σύνταξη ή ορθογραφία (π.χ. www.fasebook.com), αναγραμματισμούς (π.χ. www.yutoube.com) ή να αντικαθιστά παρόμοια γράμματα όπως το αγγλικό μικρό l (L) με το κεφαλαίο I (i), κλπ.
2. *Παραπλανητικές εικόνες,* που μπορεί να είναι οι ίδιες οπτικά με τις εικόνες που χρησιμοποιεί κάποια ιστοσελίδα, για παράδειγμα το λογότυπό της αλλά όταν πατάς σε αυτές να σε οδηγούν αλλού.
3. *Παραπλανητικό design,* που ο υποκλοπέας μπορεί να φτιάξει μία ολόκληρη ιστοσελίδα με την ίδια ακριβώς σχεδίαση που έχει η αυθεντική.

Εάν ένα phishing website καταφέρει να συνδυάσει όλα τα παραπάνω, στις περισσότερες περιπτώσεις έχει κατά 90% επιτυχημένες επιθέσεις (http://el.wikipedia.org/, 28.12.2013).

4.2.2. Pharming

Το pharming είναι παρόμοια τεχνική εξαπάτησης με αυτή του phishing και έχει σαν στόχο την κλοπή των προσωπικών δεδομένων των χρηστών του διαδικτύου Το pharming θεωρείται πολύ επικίνδυνη μέθοδος εξαπάτησης του θύματος, καθώς ένα ειδικό πρόγραμμα που εκμεταλλεύεται κενά ασφαλείας του συστήματος. Οι χρήστες νομίζουν πως βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL, ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη. Οι απατεώνες καταφέρνουν να εκτρέψουν τη ροή των επισκεπτών σε άλλο ιστοχώρο, όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών. ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, ο συγκεκριμένος υπολογιστής τον "οδηγεί" μόνο σε πλαστές ιστοσελίδες. Ειδικότερα, αν πρόκειται για ιστοσελίδα τράπεζας, η προσπάθεια του θύματος να πραγματοποιήσει τις συναλλαγές του μέσω ηλεκτρονικής τραπεζικής καταλήγει στη μεταφορά των χρημάτων του στους υποκλοπείς. Λόγω του τρόπου λειτουργίας του, το pharming, βαθμιαία εξελίσσεται σε μία από τις σοβαρότερες μορφές εγκληματικότητας στο διαδίκτυο (http://el.wikipedia.org/, 28.12.2013).

4.2.3 Cross-Site Scripting (XSS).

Οι XSS (cross site scripting) είναι από τις πιο διαδεδομένες επιθέσεις στο διαδίκτυο. Εκμεταλλεύονται διάφορες ευπάθειες των υπολογιστικών συστημάτων για να πραγματοποιήσουν τις επιθέσεις τους. Οι επιθέσεις αυτές γίνονται από κάποιο κακόβουλο χρήστη που έχει ως στόχο: την κλοπή ταυτότητας, πρόσβαση σε ευαίσθητες ή εμπιστευτικές πληροφορίες, στην κατασκοπία πλοήγησης των χρηστών, στην ψεύτικη διαφήμιση (http://el.wikipedia.org/, 28.12.2013).

4.2.4 Scamming

Σε γενικές γραμμές οι απάτες που είναι γνωστές με τον όρο «scam» αφορούν κάποια συναλλαγή που για να ολοκληρωθεί χρειάζεται κάποια χρήματα από το υποψήφιο θύμα - παραλήπτη του παραπλανητικού μηνύματος. Ωστόσο, το θύμα δεν παραλαμβάνει ποτέ τα προσφερόμενα ανταλλάγματα.

Ο τρόπος προσέγγισης του υποψήφιου θύματος γίνται μέσω ηλεκτρονικού ταχυδρομείου. Αποστέλλεται μήνυμα, που ζητάει με συγκινησιακά φορτισμένο τόνο από τον παραλήπτη να βοηθήσει στην διεκπεραίωση κάποιας οικονομικής συναλλαγής, η οποία συνήθως αφορά ποσό πολλών εκατομμυρίων. Ως αποτέλεσμα της βοήθειάς του θα έχει προμήθεια ένα σημαντικό ποσοστό του ποσού αυτού.

Οι συναλλαγές που εμφανίζονται συχνότερα είναι: η διεκδίκηση ανύπαρκτων κληρονομιών, η αποδέσμευση χρημάτων από τραπεζικούς λογαριασμούς, η παραλαβή και αποθήκευση των χρημάτων του αποστολέα σε ασφαλές μέρος και η επένδυση των χρημάτων αυτών στη χώρα του θύματος. Η συντριπτική πλειοψηφία τέτοιων μηνυμάτων προέρχεται από τη Νιγηρία. Για το λόγο αυτό η πρακτική αυτή αποκαλείται «νιγηριανό scam» αλλά και «απάτη 419» από το άρθρο του ποινικού κώδικα της Νιγηρίας.

Για να πείσουν το θύμα, οι υποκλοπείς διατηρούν την επικοινωνία και στέλνουν μάλιστα και αποδεικτικά στοιχεία της ταυτότητάς τους (φυσικά πλαστά), ώστε το θύμα να μην έχει την παραμικρή αμφιβολία. Κάποια στιγμή ζητούν χρήματα από τον παραλήπτη για τα έξοδα της συναλλαγής, φόρους κ.λπ. Από τη στιγμή που θα παραλάβουν τα χρήματα, κάθε δίοδος επικοινωνίας διακόπτεται.

Άλλος τρόπος προσέγγισης είναι «διεθνή λαχεία», όπου στέλνονται e-mail, ανακοινώνοντας κέρδη. Στη συνέχεια ζητούν απ' αυτούς να καταβάλλουν χρήματα για διαδικαστικά έξοδα. Με αυτό τον τρόπο κατορθώνουν να αποσπούν σημαντικά χρηματικά ποσά. Στην ίδια λογική λειτουργούν και οι αποκαλούμενες δημοπρασίες. Σε μη αξιόπιστες ιστοσελίδες δημοπρασιών ενδέχεται να γίνεται πλειστηριασμός ανύπαρκτων αντικειμένων. Τα θύματα πληρώνουν προκαταβολές και διαδικαστικά έξοδα, και δεν παραλαμβάνουν ποτέ το αντικείμενο για το οποίο πλειοδότησαν.

Μια ακόμα μέθοδος scamming είναι η αποστολή στο θύμα ενός e-mail με ένα συνημμένο αρχείο ή πρόγραμμα. Μόλις το ανοίξει αρχίζει διαδικασία κρυπτογράφησης των αρχείων που είναι αποθηκευμένα στον υπολογιστή του. Ως συνέπεια, το θύμα δεν μπορεί να ανοίξει κανένα αρχείο του εκτός από το μήνυμα που

του άφησαν οι υποκλοπείς στο οποίο του εξηγούν ότι μόνο αφού πληρώσει ένα συγκεκριμένο ποσό θα του αποσταλεί ο κωδικός πρόσβασης (http://www.saferinternet.gr/, 28.12.2013).

4.2.5 Keyloggers.

Τα keyloggers είναι επιβλαβή προγράμματα που εκτελούνται σχεδόν αόρατα, καταγράφουν όλες τις πληροφορίες που πληκτρολογεί ο χρήστης και στη συνεχεία, στέλνουν πληροφορίες στον υποκλοπέα που έχει μολύνει το χρήστη με το keylogger.

Τα keyloggers είναι πολύ επικίνδυνα, καθώς μπορούν να υποκλέψουν τα προσωπικά στοιχεία του χρήστη, όπως ο αριθμός πιστωτικής κάρτας, καθώς και τους κωδικούς σας πρόσβασης. Ο χρήστης δεν μπορεί να αντιληφθεί ότι έχει μολυνθεί από keyloggers και ανυποψίαστος μπορεί χρησιμοποιήσει τον δικτυακό τόπο της ηλεκτρονικής τραπεζικής της τράπεζας του και να γνωστοποιήσει άθελά του τους προσωπικούς κωδικούς του.

4.2.6 Δούρειοι Ίπποι ή Trojan Horses.

Οι δούρειοι ίπποι, είναι προγράμματα με κρυφές λειτουργίες που δεν περιλαμβάνονται στην τεκμηρίωση που τα συνοδεύει. Οι δούρειοι ίπποι επικαλούνται ότι επιτελούν μια εργασία ενώ στην πραγματικότητα εκτελούν και/ή μια διαφορετική. Αυτή η διαφορετική λειτουργία είναι αυτή που εκτελεί συγκαλυμμένες ενέργειες, όπως για παράδειγμα η κλοπή συνθηματικών.

Υπάρχουν δούρειοι ίπποι οι οποίοι δεν επιτελούν τη λειτουργία την οποία ισχυρίζονται και όταν εκτελούνται προχωρούν στην καταστροφή των αρχείων και των πόρων του συστήματος. Από την άλλη υπάρχουν και οι δούρειοι ίπποι, οι οποίοι ναι μεν επιτελούν την λειτουργία που ισχυρίζονται, αλλά λειτουργούν συγχρόνων επιτελούν και μια δεύτερη λειτουργία χωρίς να προκαλούν υποψίες στον χρήστη. Έτσι δεν χρειάζεται να αναπαράγονται μόνοι τους, αλλά στην ουσία ο ίδιος ο χρήστης φροντίζει να βοηθά τους δούρειους ίππους να μολύνουν τα αρχεία και τους πόρους

του συστήματος.Η καλύτερη μέθοδος πρόληψης κατά των δούρειων ίππων είναι η ενημέρωση των χρηστών (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

4.3 Κρυπτογραφία.

Ο κυριότερος τρόπος αντιμετώπισης των κινδύνων από κακόβουλα λογισμικά, όπως αυτά που αναφέρθηκαν εκτενώς παραπάνω, είναι η κρυπτογραφία, η οποία εφαρμόζεται σήμερα σε όλα τα πληροφοριακά συστήματα που διακινούν σημαντικές πληροφορίες, όπως είναι τα τραπεζικά πληροφοριακά συστήματα της ηλεκτρονικής τραπεζικής.

Ο όρος κρυπτογραφία προέρχεται από τα λέξεις «κρύπτος» και «γράφος», που σημαίνει τη μελέτη της μυστικογραφίας, δηλαδή τη μελέτη, χρήση και ανάπτυξη τεχνικών κρυπτογράφησης και αποκρυπτογράφησης για την απόκρυψη των περιεχομένων των μηνυμάτων και την διευκόλυνση της ανίχνευσης κακόβουλων μετατροπών στα μηνύματα (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Παρακάτω, οφείλουμε να εξηγήσουμε κάποιες βασικές έννοιες της κρυπτογραφίας, που θα συναντήσουμε στη συνέχεια του κεφαλαίου (Γ. Πάγκαλος & Ι. Μαυρίδης 2002).

Κρυπτογράφηση, είναι η διαδικασία μετατροπής ενός μηνύματος σε μια ακατανόητη μορφή με τη χρήσης ενός κρυπτογραφικού αλγόριθμου, ώστε να μην είναι αναγνώσιμο από τρίτα μέρη.

Αποκρυπτογράφηση, είναι η αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή η διεργασία ανάκτησης τους αρχικού μηνύματος.

Αρχικό κείμενο, είναι το μήνυμα το οποίο κρυπτογραφείται.

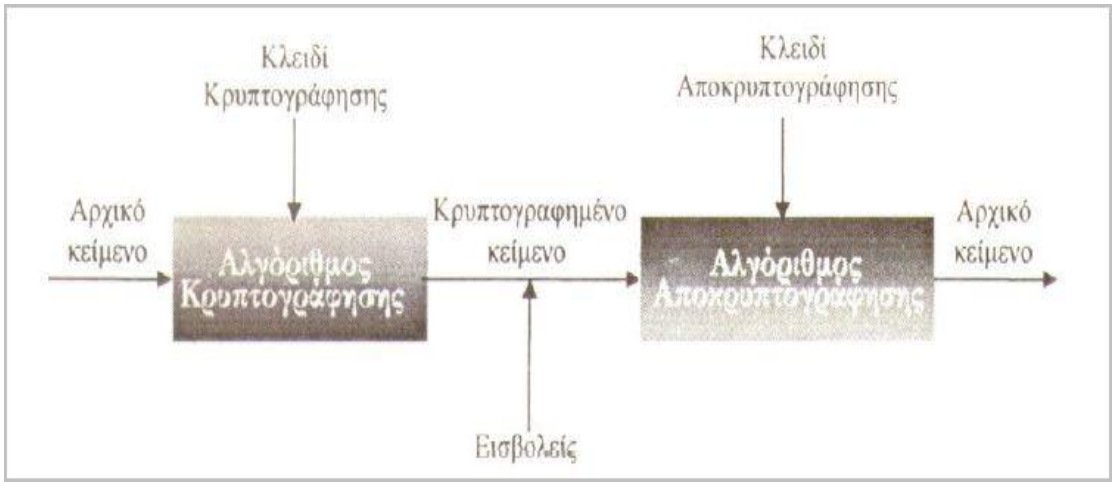
Κρυπτογραφημένο μήνυμα, είναι το αποτέλεσμα ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό μήνυμα.

Αλγόριθμος Κρυπτογράφησης, είναι η μέθοδος μετασχηματισμού δεδομένων σε μορφή που να μην επιτρέπει σε μη εξουσιοδοτημένα μέρη την αποκάλυψη του περιεχομένου τους.

Αλγόριθμος Αποκρυπτογράφησης, είναι η μέθοδος μετασχηματισμού του κρυπτογραφημένου μηνύματος στην αρχική του μορφή.
Κλειδί, είναι ένας αριθμός που χρησιμοποιείται σε συνδυασμό με τον αλγόριθμο κρυπτογράφησης/ αποκρυπτογράφησης, με σκοπό τη διατήρηση της μυστικότητας της πληροφορίας.

Η κρυπτογραφία είναι γνωστή από αρχαιοτάτων χρόνων και δείγματά της έχουν βρεθεί σε πολλά αρχαία κείμενα. Σήμερα η όλη διαδικασία είναι πιο σύνθετη και έχει αναχθεί σε ολόκληρο επιστημονικό κλάδο. Η κρυπτογραφία χρησιμοποιείται για την προστασία της μυστικότητας και της ακεραιότητας των δεδομένων καθώς και για την προστασία συναλλαγών σε ένα ανοιχτό δίκτυο όπως είναι το internet (Αλεξανδρής et al, 1995).

Σε ένα τυπικό σύστημα κρυπτογράφησης τα δεδομένα κρυπτογραφούνται και το παραγόμενο μήνυμα αποστέλλεται στον παραλήπτη και αποκρυπτογραφείται για να αναπαραχθεί το αρχικό μήνυμα. Στην παρακάτω εικόνα βλέπουμε ένα τυπικό σύστημα κρυπτογράφησης, στο οποίο μπορούμε να διακρίνουμε και τα τρωτά σημεία στα οποία μπορούν να επέμβουν οι πιθανοί εισβολείς.



Σχήμα 1*: Τυπικό σύστημα Κρυπτογράφησης (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).*

Όλες οι επικοινωνίες στο διαδίκτυο χρησιμοποιούν το πρωτόκολλο επικοινωνίας TCP/IP (Transmission Control Protocol/ /internet Protocol), το οποίο επιτρέπει να στέλνονται πληροφορίες από το έναν υπολογιστή στον άλλο μέσω

ενδιάμεσων υπολογιστών και δικτύων. Έτσι, τα τρίτα μέρη μπορούν να παρεμβαίνουν στην επικοινωνία είτε υποκλέπτοντας, είτε παραποιώντας είτε παραπλανώντας. Μια καλά σχεδιασμένη λύση στα παραπάνω προβλήματα είναι η εκτεταμένη χρήση της κρυπτογραφίας που επιτρέπει(Γ. Πάγκαλος & Ι. Μαυρίδης, 2002):

- ✓ Κρυπτογράφηση και αποκρυπτογράφηση
- ✓ Ανίχνευση αλλοιώσεων
- ✓ Αυθεντικοποίηση του αποστολέα
- ✓ Αδυναμία απάρνησης του αποστολέα

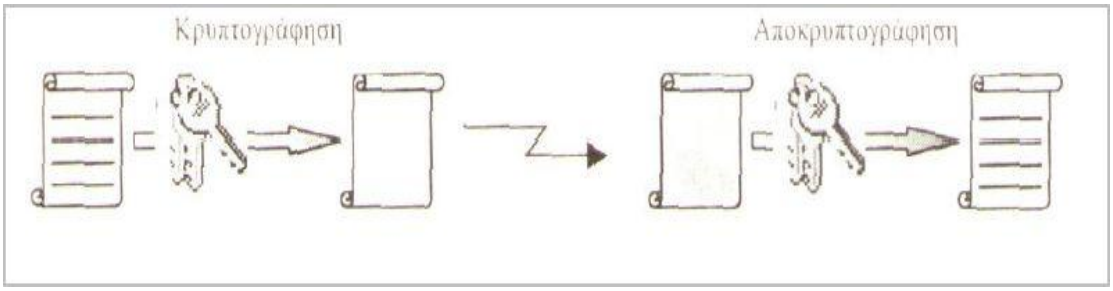
Για την αντιμετώπιση των παραπάνω θεμάτων ασφάλειας αναπτύχτηκε η τεχνολογία Υποδομής Δημοσίου Κλειδιών (ΥΔΚ). Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει τεχνολογίες όπως η κρυπτογράφηση δημοσίου κλειδιού, ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές.

Υπάρχουν διάφοροι τύποι κρυπτογραφικών αλγορίθμων, οι οποίοι ταξινομούνται ανάλογα με τα κλειδιά και τον τρόπο κρυπτογράφησης των μηνυμάτων. Αυτοί που θα μας απασχολήσουν είναι οι κρυπτογραφικοί αλγόριθμοι με βάση τα κλειδιά, οι οποίοι χωρίζονται στους(Γ. Πάγκαλος & Ι. Μαυρίδης, 2002):

- κρυπτογραφικούς αλγόριθμους *μυστικού ή συμμετρικού κλειδιού* και
- κρυπτογραφικούς αλγόριθμους *δημοσίου ή ασύμμετρου κλειδιού*.

4.3.1 Κρυπτογραφία Μυστικού Κλειδιού ή Συμμετρική Κρυπτογράφηση.

Οι αλγόριθμοι μυστικού κλειδιού ή συμμετρικής κρυπτογράφησης βασίζονται στη ύπαρξη ενός μυστικού κλειδιού που είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Το κλειδί αυτό χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση του μηνύματος.



***Σχήμα 2**: Κρυπτογράφηση Ιδιωτικού Κλειδιού (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).*

Ενώ η συμμετρική κρυπτογράφησης εγγυάται την εμπιστευτικότητα, αφού κρυπτογραφεί και αποκρυπτογραφεί το μήνυμα με ένα μυστικό κλειδί, δεν εγγυάται την εμπιστευτικότητα, αφού δεν μπορεί να εγγυηθεί για το πώς θα γίνει η ανταλλαγή του κλειδιού. Για να είναι ασφαλής η επικοινωνία θα πρέπει μέσω κάποιου ασφαλούς καναλιού επικοινωνίας να γίνει η ανταλλαγή του μυστικού κλειδιού. Ένα ακόμη πρόβλημα που ανακύπτει με την κρυπτογράφηση του μυστικού κλειδιού είναι η ταυτοποίηση. Πολλοί άνθρωποι μπορεί να έχουν πρόσβαση στο κοινό κλειδί, άρα να κάποιος λάβει ένα κρυπτογραφημένο μήνυμα δεν μπορεί να αποδείξει ποιος πραγματικά του το έστειλε (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

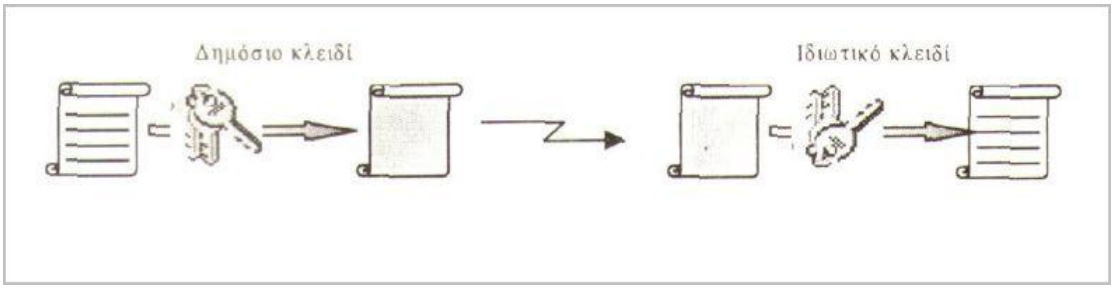
Πλεονέκτημα της συμμετρικής κρυπτογράφησης είναι η ταχύτητα της διαδικασίας, κρυπτογράφησης/ αποκρυπτογράφησης. Το θέμα της ασφάλειας της συμμετρικής κρυπτογράφησης όμως εξαρτάται από τη διαφύλαξη του μυστικού κλειδιού κρυπτογράφησης/ αποκρυπτογράφησης. Ο πιο γνωστός αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο DES και χρησιμοποιείται κυρίως στις εμπορικές εφαρμογές.

4.3.2 Κρυπτογραφία Δημοσίου Κλειδιού ή Ασύμμετρη Κρυπτογράφηση.

Η κρυπτογραφία δημοσίου κλειδιού εφευρέθηκε το 1970 από τους Diffie & Hellman και στηρίζεται στην βασική ιδέα ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται το ίδιο μυστικό κλειδί. Αντιθέτως, έχουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Η ασύμμετρη κρυπτογραφία εμφανίστηκε για να δώσει λύσεις στα προβλήματα που ανέκυπταν από τη συμμετρική κρυπτογράφηση, δηλαδή να εγγυηθεί για την ταυτότητα του αποστολέα καθώς και για την δύσκολη διανομή του μυστικού κλειδιού σε αποστολέα και παραλήπτη.

Η κρυπτογράφηση δημοσίου κλειδιού περιλαμβάνει τη χρήση δύο κλειδιών, ενός δημοσίου κλειδιού και ενός προσωπικού κλειδιού. Το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και όταν παραληφθούν από τον παραλήπτη αποκρυπτογραφούνται με το προσωπικό κλειδί του (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

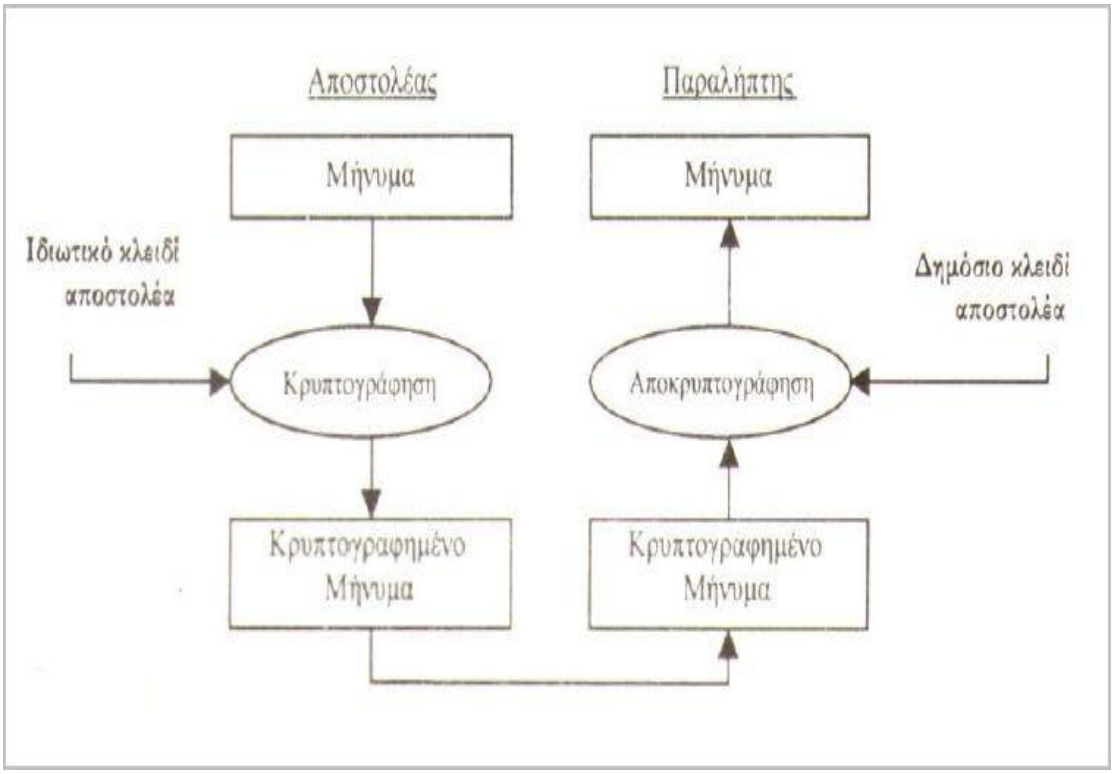


Σχήμα 3*: Κρυπτογράφηση Δημοσίου Κλειδιού (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).*

Τα δύο κλειδιά έχουν μαθηματική σχέση μεταξύ τους. Εάν το δημόσιο κλειδί χρησιμοποιηθεί για την κρυπτογράφηση της πληροφορίας το προσωπικό κλειδί θα χρησιμοποιηθεί για την αποκρυπτογράφηση και αντίστροφα. Στην παραπάνω διαδικασία, η γνώση του δημοσίου κλειδιού κρυπτογράφησης δεν επιτρέπει την ανακάλυψη του ιδιωτικού κλειδιού αποκρυπτογράφησης. Είναι υπολογιστικά αδύνατο να βρει κανείς το κλειδί της αποκρυπτογράφησης, μόνο από τη γνώση του κλειδιού κρυπτογράφησης και του αλγορίθμου που χρησιμοποιήθηκε (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

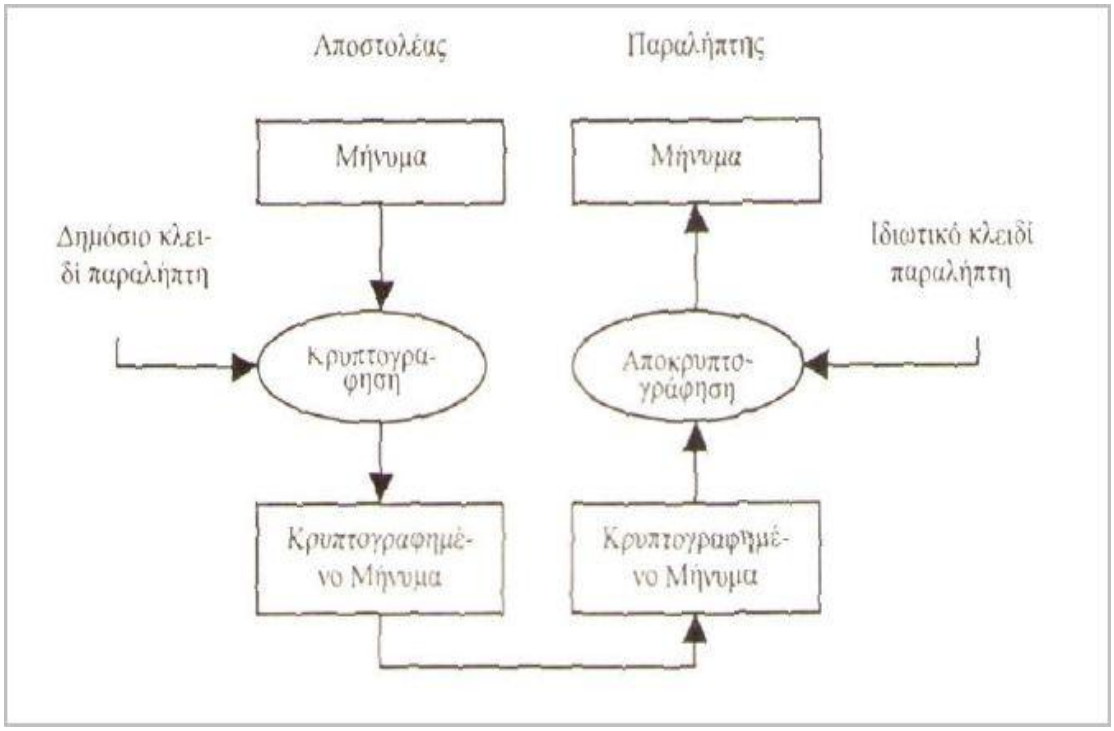
Η διαδικασία κρυπτογράφησης με τη χρήση ζεύγους κλειδιών μπορεί να γίνει με τρεις τρόπους. Ο πρώτος τρόπος εξασφαλίζει την ταυτότητα του αποστολέα, αφού για την κρυπτογράφηση χρησιμοποιείται από τον αποστολέα το ιδιωτικό του κλειδί. Η αποκρυπτογράφηση γίνεται με το δημόσιο κλειδί του αποστολέα, άρα ο παραλήπτης είναι σίγουρος για την ταυτότητα του αποστολέα. Σε αυτή την

περίπτωση όμως δεν εξασφαλίζεται η εμπιστευτικότητα, αφού το δημόσιο κλειδί του αποστολέα είναι γνωστό.



***Σχήμα 4**: Αυθεντικότητα αλλά όχι εμπιστευτικότητα (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).*

Ο δεύτερος τρόπος, χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για την κρυπτογράφηση και το ιδιωτικό κλειδί του αποστολέα για την αποκρυπτογράφηση. Με αυτόν τον τρόπο εξασφαλίζεται η εμπιστευτικότητα, αφού μόνο ο παραλήπτης μπορεί να διαβάσει τον μήνυμα με το ιδιωτικό του κλειδί, αλλά δεν εξασφαλίζεται η ταυτότητα του αποστολέα.



Σχήμα 5*: Εμπιστευτικότητα αλλά όχι αυθεντικότητα (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).*

Ο τρίτος τρόπος συνδυάζει τους δύο προαναφερθέντες τρόπους και τελικά εξασφαλίζει και την εμπιστευτικότητα αλλά και την ταυτότητα του εμπλεκόμενων μερών στην επικοινωνία. Σε αυτή την περίπτωση ο αποστολέας κρυπτογραφεί τα δεδομένα με το ιδιωτικό του κλειδί και στη συνέχεια με το δημόσιο κλειδί του παραλήπτη. Έτσι όταν ο παραλήπτης λάβει το μήνυμα, αποκρυπτογραφεί με το ιδιωτικό του κλειδί και έτσι εξασφαλίζεται η εμπιστευτικότητα και στη συνέχεια αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, όπου και τον ταυτοποιεί (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

Το πρώτο σύστημα δημοσίου κλειδιού αναπτύχθηκε από τους Rivest, Shamir και Adleman στα τέλη της δεκαετίας του ’70 και έχει το όνομα RSA, από τα αρχικά των κατασκευαστών του. Η ασφάλειά του βασίζεται στη δυσκολία εύρεσης ων κοινών παραγόντων πολύ μεγάλων αριθμών.

Η κρυπτογράφηση του δημοσίου κλειδιού έχει το πλεονέκτημα ότι το δημόσιο κλειδί διανέμεται ελεύθερα. Αυτό διευκολύνει την επικοινωνία απομακρυσμένων

χρηστών. Από τη άλλη η ασύμμετρη κρυπτογράφηση είναι πιο αργή σε σχέση με την συμμετρική γιατί απαιτεί περισσότερους υπολογισμούς.

4.4 Ψηφιακές Υπογραφές.

Όπως αναφέρθηκε και παραπάνω, σε περίπτωση που απαιτείται μόνο η αυθεντικοποίηση του αποστολέα με την κρυπτογράφηση ασύμμετρου κλειδιού, τότε το μήνυμα δεν έχει παρά να κρυπτογραφηθεί με το ιδιωτικό κλειδί του αποστολέα και να αποκρυπτογραφηθεί με το δημόσιο κλειδί του αποστολέα από τον παραλήπτη. Έτσι όλο το κρυπτογραφημένο μήνυμα αποτελεί μια ψηφιακή υπογραφή του αποστολέα. Κατά αυτόν τον τρόπο εξασφαλίζεται και η αυθεντικοποίηση του αποστολέα αλλά και η ακεραιότητα του μηνύματος, αφού χωρίς το ιδιωτικό κλειδί του αποστολέα δεν μπορεί να γίνει καμία παραποίηση στο μήνυμα (Κάτσικας et al, 2003).

Ένα πρόβλημα που ανακύπτει σε αυτή την περίπτωση είναι οι απαιτήσεις σε χώρο αποθήκευση, αφού κάθε μήνυμα πρέπει να είναι αποθηκευμένο σε μη κρυπτογραφημένη μορφή για πρακτικούς λόγους και πρέπει να φυλάσσεται ένα αντίγραφο ασφαλείας σε κρυπτογραφημένη μορφή, ώστε τα περιεχόμενά του να μπορούν αν προσδιοριστούν εύκολα σε περίπτωση διαφωνίας. Για την επίλυση των παραπάνω προβλημάτων, κρυπτογραφείται ένα μικρό τμήμα από bits, το οποίο θα αποτελεί συνάρτηση του κειμένου και ονομάζεται αυθεντικοποιητής. Αν ο αυθεντικοποιητής κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα , τότε χαρακτηρίζεται ως ψηφιακή υπογραφή. Για τη δημιουργία ψηφιακής υπογραφής ενός κειμένου από μία οντότητα, συνήθως κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα η σύνοψη του μηνύματος (Κάτσικας et al, 2003).

Η ψηφιακή υπογραφή δεν προσφέρει εμπιστευτικότητα στο μήνυμα, αλλά αποτελεί υπηρεσία που ικανοποιεί απαιτήσεις ακεραιότητας μηνύματος, αυθεντικοποίησης αποστολέα και μη αποποίησης αποστολής μηνύματος.

4.5 Ψηφιακά Πιστοποιητικά.

Τα δημόσια κλειδιά της ασύμμετρης κρυπτογραφίας για να είναι αποτελεσματικά πρέπει να είναι γνωστά σε όσους ενδιαφέρονται. Για την αντιστοίχιση και δέσμευση όμως ενός δημοσίου κλειδιού σε ένα άτομο, οργανισμό ή άλλη οντότητα απαιτείται η διαδικασία της πιστοποίησης. Για αυτό το σκοπό χρησιμοποιούνται τα ψηφιακά πιστοποιητικά, τα οποία αποτελούν το μέσο με το οποίο μεταδίδονται με ασφαλή τρόπο οι τιμές των δημοσίων κλειδιών και οι πληροφορίες του κατόχου ου σχετίζονται με αυτά. Η πιστοποίηση αποτελεί βασική λειτουργία όλων των Υποδομών Δημοσίου Κλειδιού (Κάτσικας et al, 2003).

Η απόκτηση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση σε μια Αρχή Πιστοποίησης (ΑΠ), η οποία επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό. Το πιστοποιητικό περιλαμβάνει (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002):

- ✓ το όνομα και πληροφορίες αναγνώρισης του χρήστη στον οποίο αναφέρεται το πιστοποιητικό,
- ✓ το δημόσιο κλειδί του χρήστη,
- ✓ την ημερομηνία λήξης του πιστοποιητικού,
- ✓ το όνομα και την υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε,
- ✓ Ένα σειριακό αριθμό πιστοποιητικού

Τα πιστοποιητικά χαρακτηρίζονται ακόμα και από το είδος της πληροφορίας που περιέχουν. Έτσι υπάρχουν πιστοποιητικά ταυτότητα, που ταυτοποιούν μια οντότητα και πιστοποιητικά χαρακτηριστικών, που περιγράφουν τις ιδιότητες μιας οντότητας Το πρότυπο X.509 είναι το πλέον διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών και η έκδοσή του X.509 v3 θεωρείται από τις πιο επιτυχημένες.

4.6. Πρωτόκολλο Secure Socket Layer (SSL).

Το Secure Socket Layer (SSL), είναι ένα πρωτόκολλο για τη μεταφορά δεδομένων μεταξύ δύο συσκευών, που αναπτύχθηκε για να παρέχει ιδιωτικότητα και

ακεραιότητα πληροφοριών στο Internet. Το SSL διαχειρίζεται την εμπιστευτικότητα και την ακεραιότητα του καναλιού μετάδοσης, καθώς και την αυθεντικοποίηση του εξυπηρετητή, αλλά και του πελάτη όταν είναι απαραίτητο.

Το SSL, σχεδιάστηκε από την NETSCAPE, για να παρέχει ασφάλεια κατά τη μετάδοση ευαίσθητων πληροφοριών με βάση το πρωτόκολλο TCP/IP και παρέχει υπηρεσίες όπως είναι η κρυπτογράφηση δεδομένων, η αυθεντικοποίηση εξυπηρετητή και η ακεραιότητα των μηνυμάτων που μεταδίδονται στο διαδίκτυο. Ένα άλλο πρωτόκολλο για την ασφαλή μετάδοση δεδομένων στο διαδίκτυο είναι το Secure HTTP (S-HTTP), το οποίο σχεδιάστηκε για τη μυστική μετάδοση μεμονωμένων μηνυμάτων. Τα δύο αυτά πρωτόκολλά είναι συμπληρωματικά (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

Ο τρόπος λειτουργίας του πρωτοκόλλου SSL εξασφαλίζει τη ασφαλή μετάδοση, χρησιμοποιώντας την κρυπτογράφηση RSA δημόσιου κλειδιού. Όταν ένας φυλλομετρητής συνδεθεί με μια SSL προστατευμένη σελίδα, ο SSL εξυπηρετητής στέλνει μια αίτηση για την έναρξη μιας SSL συνόδου. Αν υποστηρίζει το ίδιο πρωτόκολλο SSL, ενημερώνει τον εξυπηρετητή για την ταυτότητα της συνόδου, τους αλγορίθμους κρυπτογράφησης και τις μεθόδους συμπίεσης που υποστηρίζει. Ο εξυπηρετητής κάνει τις αντίστοιχες επιλογές και έτσι ξεκινά η επικοινωνία. Στην αρχή της επικοινωνίας γίνεται η ανταλλαγή ψηφιακών πιστοποιητικών. Έπειτα ο πελάτης καθορίζει ένα κλειδί συνόδου, το οποίο είναι κατάλληλο για τον αλγόριθμο κρυπτογράφησης που επιλέχθηκε. Τέλος, ο πελάτης με το δημόσιο κλειδί του εξυπηρετητή, κρυπτογραφεί το κλειδί συνόδου και ο εξυπηρετητής με το ιδιωτικό του κλειδί αποκρυπτογραφεί και αποκτά το κλειδί συνόδου (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

4.7 Firewalls.

Ένα σύστημα firewall, ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετείται ανάμεσα στο διαδίκτυο και το υπό προστασία δίκτυο. Το λογισμικό αυτό επιτρέπει την προσπέλαση δεδομένων των εξωτερικών χρηστών στο

προστατευμένο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά, όπως ονόματα χρηστών και συνθηματικά, διευθύνσεις IP ή ακόμα και domain names (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

Σκοπός της εγκατάστασης ενός firewall είναι να προστατευτούν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντας τα δικαιώματά τους στο δίκτυο. Τα firewalls προστατεύουν από απειλές όπως η μη εξουσιοδοτημένη προσπέλαση των δικτυακών πόρων, η άρνηση εξυπηρέτησης και η προσποίηση (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

Τα πλεονεκτήματα που προσφέρουν σε ένα δίκτυο τα firewalls είναι πολλά. Επιτρέπουν αποτελεσματικά την επιβολή ασφάλειας που θέλουμε να εφαρμόσουμε στο σύστημά μας. Μέσω παραμετροποιήσεων μας επιτρέπουν να ορίσουμε ποιος χρήστης θα έχει πρόσβαση σε ποιο πόρο. Προστατεύουν από ευπαθείς υπηρεσίες δικτύων, καθώς είναι γνωστό ότι τα πρωτόκολλα παρουσιάζουν εγγενή προβλήματα ασφάλειας. Επιπλέον αποτελούν μέσο καταγραφής για τη χρήση και συναγερμού για την παράνομη χρήση του δικτύου και επιβάλλουν ελεγχόμενη πρόσβαση στο εσωτερικό δίκτυο (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

Παρά τα παραπάνω πλεονεκτήματα τα firewalls δεν πρέπει να θεωρούνται πανάκεια για τα προβλήματα ασφάλειας, καθώς δεν προστατεύουν από εσωτερικούς χρήστες, όπως για παράδειγμα τους υπαλλήλους του οργανισμού. Επίσης μπορούν να προστατεύουν ένα περιβάλλον, μόνο όταν το ελέγχουν πλήρως, άρα δεν θα πρέπει να υπάρχουν συνδέσεις που να μην διοχετεύονται μέσω firewall. Αποτελούν το πιο ορατό σημείο του οργανισμού προς τον έξω κόσμο, άρα είναι και ο πιο ελκυστικός στόχος επίθεσης. Τέλος δεν θα πρέπει να αμελούμε το γεγονός ότι χρειάζονται σωστή εγκατάσταση, προσεκτικές ρυθμίσεις και συνεχείς ενημερώσεις, αλλιώς δεν έχουν τα αναμενόμενα αποτελέσματα και το πιο σημαντικό από όλα είναι ότι τα firewalls δεν είναι άτρωτα (Γ. Πάγκαλος & Ι. Μαυρίδης, 2002).

4.8. Μέτρα Προστασίας Από την Πλευρά του Χρήστη.

Παραπάνω αναφέρθηκαν διάφοροι τρόποι προστασία των ηλεκτρονικών πληροφοριακών συστημάτων τους οποίους οι τράπεζες φροντίζουν να τηρούν και να λαμβάνουν εκτεταμένα μέτρα για να προστατεύσουν τις πληροφορίες που μεταβιβάζονται και διεκπεραιώνονται κατά τη διενέργεια τραπεζικών συναλλαγών στο διαδίκτυο.

Παρόλα αυτά οι Τράπεζες δεν είναι σε θέση να ασκήσουν έλεγχο στα συστήματα που χρησιμοποιούν οι πελάτες τους για τις τραπεζικές τους συναλλαγές στο διαδίκτυο. Θα πρέπει και οι ίδιοι οι χρήστες να φροντίσουν για την ασφάλεια των προσωπικών τους συστημάτων και γι' αυτό τον σκοπό η Ένωση Ελληνικών Τραπεζών παραθέτει «10 κανόνες» προς τους χρήστες των ηλεκτρονικών τραπεζικών πληροφοριακών συστημάτων με σκοπό να ενισχυθεί η ασφάλεια των υπολογιστών που χρησιμοποιούν για την πρόσβασή τους στο διαδίκτυο και να περιοριστούν οι κίνδυνοι στο ελάχιστο, Οι «10 κανόνες» προτρέπουν τους χρήστες της ηλεκτρονικής τραπεζικής να φροντίσουν για τα παρακάτω:

- ✓ Προστατεύστε τα απόρρητα προσωπικά δεδομένα που στέλνετε μέσω διαδικτύου.
- ✓ Βεβαιωθείτε με ποιον έχετε να κάνετε.
- ✓ Προσοχή με απόρρητα προσωπικά δεδομένα και μέσα πρόσβασης.
- ✓ Επιλέξτε ασφαλή κωδικό πρόσβασης.
- ✓ Χρησιμοποιείτε προγράμματα μόνο από αξιόπιστες πηγές.
- ✓ Χρησιμοποιείτε ενημερωμένες εκδόσεις προγραμμάτων.
- ✓ Εκτελέστε έλεγχο ασφαλείας στον υπολογιστή σας
- ✓ Ενεργοποιείστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησης.
- ✓ Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο λογισμικό ασφαλείας.
- ✓ Να δημιουργείτε τακτικά αντίγραφα ασφαλείας.

ΚΕΦΑΛΑΙΟ V

Η ΗΛΕΚΤΡΟΝΙΚΗ ΤΡΑΠΕΖΙΚΗ ΣΤΗΝ ΕΛΛΑΔΑ.

Όπως αναφέρθηκε και προηγούμενα, η ηλεκτρονική τραπεζική στην Ελλάδα εμφανίστηκε το 1997 από την «ΕΓΝΑΤΙΑ Τράπεζα». Από τότε οι εξελίξεις στο χώρο των ηλεκτρονικών συναλλαγών ήταν ραγδαίες. Ο αριθμός των ηλεκτρονικών χρηστών έχει αυξηθεί με και σύμφωνα με στοιχεία την Ελληνική Ένωσης Τραπεζών, οι χρήστες το 2010 ανέρχονταν σε 1.929.688, φυσικά και νομικά πρόσωπα με ρυθμό ετήσιας αύξησης 12%.

Η αύξηση αυτή θεωρείται αναμενόμενη, αφού όλο και περισσότεροι χρήστες ανακαλύπτουν τις υπηρεσίες της ηλεκτρονικής τραπεζικής και τολμούν να ωφεληθούν από τα πλεονεκτήματα που προσφέρει και έχουν αναφερθεί εκτενώς σε προηγούμενο κεφάλαιο.

Χαρακτηριστικά είναι τα αποτελέσματα της μελέτης του Εργαστηρίου Ηλεκτρονικού Επιχειρείν και Εμπορίου ELTRUN του Τμήματος Διοικητικής Επιστήμης και Τεχνολογίας του Οικονομικού Πανεπιστημίου Αθηνών για λογαριασμό της Τράπεζας Πειραιώς, που παρουσίασε ο αναπληρωτής γενικός διευθυντής της Τράπεζας Πειραιώς, Σωτήρης Συρμακέζης, σε πρόσφατο banking forum της ΕΕΔΕ. Το 72% του δείγματος που χρησιμοποιήθηκε ήταν μεταξύ 25-35 ετών. Ανάμεσα στα πολύ ενδιαφέροντα αποτελέσματα που εξήγαγε η παραπάνω έρευνα, ήταν ότι το 97% των ερωτηθέντων θεωρεί ότι η χρήση ηλεκτρονικών καναλιών είναι πιο παραγωγική και βολική και το 64% να εκτιμά ότι η χρήση των ηλεκτρονικών καναλιών μειώνει τον κίνδυνο στις συναλλαγές.

Στην ίδια έρευνα εκτός από προφανή οφέλη, δηλαδή την 24ωρη εξυπηρέτηση, την εξοικονόμηση χρόνου, την ευκολία ενημέρωσης και διεκπεραίωσης των συναλλαγών, αναδείχθηκαν και άλλα οφέλη, όπως ότι η εξοικονόμηση χρημάτων σε όσους χρησιμοποιούν την ηλεκτρονική τραπεζική μπορεί να φθάσει τα 464 ευρώ σε ετήσια βάση και να εξοικονομήσει 30 ώρες από τον χρόνο του καταναλωτή. Επιπλέον, σε μια εποχή όπου το «μότο» όλων των τραπεζικών ομίλων είναι οι

«πράσινες συναλλαγές», σημειώνεται και αποφυγή 40 τόνων CO_2 (έργο απορρόφησης 3.000 δέντρων).

Ας δούμε παρακάτω ποιες ελληνικές τράπεζες προσφέρουν υπηρεσίες ηλεκτρονικής τραπεζικής στους πελάτες τους, τι δυνατότητες προσφέρουν και πώς διασφαλίζουν την ασφάλεια των συναλλαγών.

5.1 Alpha Bank

Η εγγραφή στην υπηρεσία της ηλεκτρονικής τραπεζικής στον όμιλο της Alpha Bank προσφέρεται δωρεάν. Ο χρήστης, εφόσον ολοκληρώσει την εγγραφή του στο πληροφοριακό σύστημα της ηλεκτρονικής τραπεζικής έχει τη δυνατότητα να εκτελέσει πλήθος ενεργειών, όπως λογαριασμούς Alpha Bank και άλλων Τραπεζών στην Ελλάδα και το Εξωτερικό, πληρωμή των οφειλών, δυνατότητα πραγματοποίησης ερωτήσεων για την κατάσταση των συναλλαγών, ενημέρωση μέσω e-mail ή sms για τις εντολές μεταφοράς ή πληρωμής που δεν έχουν εκτελεστεί, όπως επίσης και ενημέρωση για τις κινήσεις και τα υπόλοιπα των λογαριασμών καταθέσεων, των καρτών και των δανείων. Παράλληλα, ο χρήστης μπορεί να έχει πλήρη πληροφόρηση για το μεγαλύτερο μέρος των στοιχείων και χαρακτηριστικών των υπηρεσιών που προσφέρει η τράπεζα.

Η ηλεκτρονική τραπεζική της Alpha Bank λαμβάνει όλα τα απαραίτητα μέτρα για την προστασία των συναλλαγών. Χρησιμοποιεί κρυπτογράφηση SSL 128 bits σε κάθε συναλλαγή και χρησιμοποιεί επιπρόσθετα συστήματα ασφαλείας (Firewalls), τα οποία ελέγχουν και καταγράφουν την πρόσβαση στα συστήματά της.

Για την είσοδο στην υπηρεσία, ο χρήστης πρέπει να χρησιμοποιεί τους προσωπικούς του κωδικούς ασφαλείας. Σε περίπτωση που πληκτρολογηθεί πέντε συνεχόμενες φορές λάθος ο κωδικός, κλειδώνει αυτόματα την υπηρεσία και δεν μπορεί να χρησιμοποιηθεί, παρά μόνο εάν ο πελάτης πραγματοποιήσει γραπτή αίτηση σε κάποιο κατάστημα της Τράπεζας. Δίνει όμως τη δυνατότητα στον πελάτη να μεταβάλλει τους κωδικούς του όσο συχνά θέλει.

Επιπρόσθετα, διαθέτει όριο 30 λεπτών για την ολοκλήρωση των συναλλαγών. Μετά τη λήξη των 30 λεπτών, το σύστημα αποσυνδέει τον πελάτη αυτόματα. Αν μετά την σύνδεση του πελάτη δεν εκτελεστεί καμία συναλλαγή μέσα σε διάστημα 20 λεπτών, τότε πάλι το σύστημα αποσυνδέεται αυτόματα. Έχει θεσπίσει ανώτατο όριο μεταφοράς σε μη προδηλωμένους λογαριασμούς, όπως και η πληρωμή καρτών άλλης Τράπεζας περιορίζεται από την επιλογή του ανώτατου ορίου μεταφοράς. Τέλος, παρέχει στους χρήστες τη συσκευή πρόσθετου κωδικού ασφάλειας (6-ψήφιος κωδικός) για την εισαγωγή πρόσθετων κωδικών ασφαλείας. Η διαδικτυακή ταυτότητα της Τράπεζας επιβεβαιώνεται από την εταιρία VeriSign.

5.2 Eurobank

Οι υπηρεσίες e-Banking της τράπεζας Eurobank επιτρέπουν στους χρήστες της την διεκπεραίωση τόσο των τραπεζικών όσο και των χρηματιστηριακών τους συναλλαγών εύκολα. Οι ιδιώτες αλλά και οι επιχειρήσεις έχουν τη δυνατότητα να διεκπεραιώσουν συναλλαγές όπως, πληρωμή πιστωτικής κάρτας ή/και δανείου, εξόφληση λογαριασμών κοινή ωφέλειας, αλλά και καταβολή ΦΠΑ και υποχρεώσεων προς το ΙΚΑ, αγορά και πώληση μετοχών σε πραγματικό χρόνο, ενημέρωση online για τα υπόλοιπα και τις κινήσεις των λογαριασμών, μεταφορά ποσών σε Ελλάδα και εξωτερικό με προνομιακούς όρους σε σχέση με τα υποκαταστήματα, ενημέρωση μέσω e-mail και sms για κινήσεις λογαριασμών και καρτών, καθώς και ομαδικές πληρωμές προμηθευτών ή μισθοδοσίας υπαλλήλων. Μια δυνατότητα ακόμα που προσφέρει στις επιχειρήσεις, είναι ο ορισμών χρηστών που θα εκτελούν και εγκρίνουν συναλλαγές. Έτσι, κάθε στέλεχος μπορεί να έχει συγκεκριμένες λειτουργίες στο σύστημα, αντίστοιχες με τη θέση και τις αρμοδιότητές του στην επιχείρηση.

Τα μέτρα προστασίας που λαμβάνει η τράπεζα Eurobank για την προστασία των συναλλαγών είναι, η εισαγωγή των προσωπικών κωδικών του χρήστη για την είσοδο στη υπηρεσία. Αν οι προσπάθειες εισόδου στο σύστημα υπερβούν τις τρεις λανθασμένες, οι προσωπικοί κωδικοί χρήστη μπλοκάρονται.

Η Ταυτοποίηση της Τράπεζας από την εταιρία VeriSign, και για τη μεταφορά των δεδομένων η Τράπεζα χρησιμοποιεί κρυπτογράφηση στα 128bit με το πρωτόκολλο επικοινωνίας SSL. Επιπλέον προστασία παρέχεται από την τεχνολογία Firewall.

Για την ολοκλήρωση των συναλλαγών προς τρίτους, η Τράπεζα εφαρμόζει και το μέτρο ασφαλείας της αποστολής Κωδικών μιας Χρήσης, οι οποίοι στέλνονται με sms στο κινητό τηλέφωνο του χρήστη. Οι κωδικοί έχουν σύντομη διάρκεια ζωής και μπορούν να χρησιμοποιηθούν για μια και μόνο συναλλαγή. Η ολοκλήρωση μίας συναλλαγής επιτρέπεται μέσα σε ένα συγκεκριμένο χρονικό όριο δεκαπέντε λεπτών, μετά τη λήξη του οποίου το σύστημα αποσυνδέει το χρήστη αυτόματα.

Αξίζει να αναφερθεί ότι για τη διενέργεια συναλλαγών στις οποίες ο παραλήπτης δεν είναι γνωστός και είναι πιθανό να εμπεριέχουν ρίσκο (μεταφορές σε τρίτους, εμβάσματα), η Τράπεζα απαιτεί τη χρήση της Ψηφιακής Πιστοποίησης. Το ψηφιακό πιστοποιητικό (digital certificate) αποτελεί το μέσο που παρέχει τη δυνατότητα στον κάτοχό του να υπογράφει ψηφιακά όλες τις ηλεκτρονικές συναλλαγές που εκτελεί μέσω του e-Banking. Η Eurobank σημειώνει, πως είναι η μόνη Τράπεζα πάροχος ψηφιακών πιστοποιητικών εγγεγραμμένη στα μητρώα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

5.3 Τράπεζα Πειραιώς

Οι υπηρεσίες ηλεκτρονικής τραπεζικής της τράπεζας Πειραιώς φέρουν φέρουν το όνομα Winbank.. Μέσω του πληροφοριακού συστήματος ηλεκτρονικής τραπεζικής ο πελάτης μπορεί να απολαμβάνει σχεδόν όλες τις Τραπεζικές Υπηρεσίες. Οι παρεχόμενες υπηρεσίες περιλαμβάνουν τη διαχείρισης λογαριασμών, επιταγών, πιστωτικών καρτών, προπληρωμένη Κάρτα – WEBUY, διαχείριση δανείων, πληρωμές – μεταφορές, winbank alerts.

Η Τράπεζα Πειραιώς για να προστατέψει το σύστημα της Ηλεκτρονικής Τραπεζικής winbank εφαρμόζει μέτρα προστασίας όπως, συνεργασία με την εταιρία

VeriSign, χρήση κατά τη μεταφορά των δεδομένων του πρωτόκολλου κρυπτογράφησης SSL 128bit., έλεγχος από firewall.

Οι κωδικοί είναι απαραίτητοι για την αναγνώριση του χρήστη σε κάθε φορά στην υπηρεσία και την πρώτη φορά που θα χρησιμοποιηθεί η υπηρεσία, το σύστημα υποχρεώνει το χρήστη να μεταβάλει τα στοιχεία του. Η αλλαγή του προσωπικού Κωδικού Ασφαλείας είναι υποχρεωτική κάθε 2 με 6 μήνες. Εκτός της υποχρεωτικής αλλαγής, οι κωδικοί μπορούν να μεταβληθούν όσο συχνά επιθυμεί ο πελάτης. Εάν ο χρήστης εισάγει τρεις φορές λάθος τον Προσωπικό του Κωδικό Ασφαλείας, το σύστημα κλειδώνει τους κωδικούς και απαγορεύει την πρόσβαση στην υπηρεσία winbank. Για να ξεκλειδωθούν οι κωδικοί απαιτείται η επικοινωνία με το κέντρο εξυπηρέτησης πελατών της Τράπεζας Πειραιώς.

Εάν δεν υπάρξει καμία δραστηριότητα για δέκα λεπτά γίνεται αυτόματη αποσύνδεση από την υπηρεσία. Η Τράπεζα χρησιμοποιεί και το μέτρο ασφαλείας των πρόσθετων κωδικών extraPIN. Ο Κωδικός extraPIN ζητείται μετά την είσοδο στην υπηρεσία winbank και χρησιμοποιείται για μεταφορές σε τρίτους, πληρωμές πιστωτικών καρτών άλλης Τράπεζας, φόρτιση της κάρτας Webuy, μαζικές πληρωμές και εμβάσματα, μισθοδοσίες, εξαίρεση λογαριασμών, αίτηση ανοίγματος καταθετικού λογαριασμού, διαχείριση αιτήσεων, αλλαγή των προσωπικών στοιχείων και για την υπηρεσία Λεφτά στο Λεπτό. Οι κωδικοί extraPIN αποστέλλονται με sms στο κινητό του χρήστη, είναι μιας χρήσης, ισχύει για 60 δευτερόλεπτα και όταν καταχωρηθεί παύει να ισχύει.

5.4 Εθνική Τράπεζα

Η ηλεκτρονική τραπεζική της Εθνικής Τράπεζας ονομάζεται i-bank και απευθύνεται σε επιχειρήσεις και ιδιώτες παρέχοντας πληθώρα δυνατοτήτων. Το i-bank παρέχει μεγάλο εύρος συναλλαγών που εξασφαλίζουν την παρακολούθηση και διαχείριση των καταθετικών, δανειακών και επενδυτικών λογαριασμών των πελατών σε πραγματικό χρόνο. Δίνει τη δυνατότητα πληροφόρησης του πελάτη για τα υπόλοιπα και τις κινήσεις των λογαριασμών του και τις πληρωμές των πιστωτικών

του καρτών, καθώς και λογαριασμούς ΔΕΗ, ΟΤΕ, κινητής και σταθερής τηλεφωνίας, ασφαλιστήρια συμβόλαια κ.α. Ο πελάτης μπορεί να μεταφέρει ποσά σε λογαριασμούς δικούς του ή τρίτων στην Εθνική αλλά και σε άλλες τράπεζες, στην Ελλάδα και στο εξωτερικό.

Όπως και οι άλλες τράπεζες έτσι και η Εθνική Τράπεζα για την προστασία και την ασφάλεια της μεταφοράς των δεδομένων χρησιμοποιεί το πρωτόκολλο ασφαλούς επικοινωνίας SSL των 128 bit. Στα συστήματα της Τράπεζας εφαρμόζεται ελεγχόμενη πρόσβαση, με τη χρήση της τεχνολογίας Firewall. Η αυθεντικότητα της Τράπεζας εξασφαλίζεται με το πιστοποιητικό της VeriSign, έναν από τους μεγαλύτερους, διεθνούς κύρους οργανισμούς έκδοσης πιστοποιητικών στο Internet.

Η ταυτοποίηση του χρήστη και η πρόσβασή του στο Internet Banking πραγματοποιείται με τον κωδικό χρήστη (UserID) και το μυστικό κωδικό (password). Έπειτα από τέσσερις λανθασμένες προσπάθειες εισαγωγής στο σύστημα, υπάρχει η δυνατότητα μπλοκαρίσματος των υπηρεσιών και απαιτείται η έκδοση νέου. Ο χρήστης έχει τη δυνατότητα να αλλάζει / δεσμεύει το password και να κλειδώνει τη συσκευή i-code εάν την έχει χάσει. Για μεγαλύτερη ασφάλεια, το σύστημα ζητά αλλαγή password κάθε δύο μήνες.

Ο ηλεκτρονικός κλειδάριθμος (i-code) αποτελεί κομμάτι ασφαλείας του συστήματος i-bank και είναι απαραίτητος για την πραγματοποίηση συναλλαγών ασφαλείας, όπως οι μεταφορές χρημάτων. Το i-code είναι ένας εξαψήφιος για ιδιώτες και οκταψήφιος για επιχειρήσεις κωδικός, που παραμένει ενεργός για 32 δευτερόλεπτα και η εισαγωγή του επιβεβαιώνει την πρόθεση του χρήστη να πραγματοποιήσει μια συγκεκριμένη συναλλαγή. Μέσω του κωδικού αυτού επιβεβαιώνεται η ολοκλήρωση και η ορθότητα της συναλλαγής. Ο κωδικός επιβεβαίωσης i-code (check) είναι ένας τριψήφιος κωδικός που επιβεβαιώνει από την πλευρά της Τράπεζας την ολοκλήρωση της συναλλαγής. Το σύστημα αποσυνδέει τον χρήστη όταν παραμένει στο Internet Banking για χρόνο μεγαλύτερο των 10 λεπτών χωρίς να διεκπεραιώσει καμία συναλλαγή.

ΚΕΦΑΛΑΙΟ VI

ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΕ ΕΥΡΩΠΑΪΚΟ ΕΠΙΠΕΔΟ.

Η ανάγκη για την προστασία των προσωπικών δεδομένων κρίθηκε απαραίτητη από τη στιγμή που κατέστη αντιληπτή η ποιοτική διαφορά στις δυνατότητες συλλογής και επεξεργασίας των πληροφοριών που δημιούργησαν τα πληροφοριακά συστήματα σε σχέση με τις παραδοσιακές μεθόδους. Κρίθηκε επιτακτική η ανάγκη να βρεθεί ένας τρόπος ώστε να μπορεί να προστατευθεί η ιδιωτικότητα του ατόμου, παράλληλα με τη ραγδαία τεχνολογική εξέλιξη. Στόχος των σχετικών νομοθεσιών της προστασίας των προσωπικών δεδομένων είναι η διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων και ιδίως της ιδιωτικής ζωής.

6.1. Νομοθετήματα «Πρώτης Γενιάς».

Η προστασία των προσωπικών δεδομένων αντιμετωπίσθηκε αρχικά τη δεκαετία του ’70 με τα νομοθετήματα της «πρώτης γενιάς». Από τα ευρωπαϊκά κράτη, εκείνο που ανταποκρίθηκε πρώτο στις προκλήσεις για την προστασία από την επεξεργασία προσωπικών δεδομένων ήταν το ομόσπονδο γερμανικό κρατίδιο της Έσσης με την έκδοση σχετικού Νόμου. Έπειτα ακολούθησαν οι εθνικές νομοθεσίες των Σκανδιναβικών χωρών, της τότε Ομοσπονδιακής Δημοκρατίας της Γερμανίας, της Αυστρίας, της Γαλλίας και του Λουξεμβούργου.

Λίγα χρόνια αργότερα, το 1980 ο Οργανισμός για Οικονομική Συνεργασία και Ανάπτυξη (Ο.Ο.Σ.Α), υιοθέτησε ένα κείμενο με τίτλο «αρχές διέπουσες την προστασία της ιδιωτικής σφαίρας του ανθρώπου και τις διασυνοριακές ροές προσωπικών στοιχείων», προσκαλώντας προς τα κράτη-μέλη να συμβάλλουν στην κατοχύρωση των αρχών προστασίας . Το κείμενο του Ο.Ο.Σ.Α μπορεί να θεωρηθεί ένα καλό παράδειγμα δικαίου, με την έννοια ότι η ύπαρξη του θεμελιώνει τη συναίνεση των δυτικών χωρών ως προς τον τρόπο αντιμετώπισης των προβλημάτων που ανακύπτουν από τη χρήση της πληροφορικής, την άσκηση των ελευθεριών και τη διεθνή ανταλλαγή ονομαστικών δεδομένων (Τ. Μαρίνος 1991).

Κοινό χαρακτηριστικό των νομοθετημάτων της «πρώτης γενιάς» είναι η δυσπιστία και ο φόβος της κοινωνίας, εξαιτίας της εξέλιξης της πληροφορικής τεχνολογίας. Αποτέλεσμα αυτής της δυσπιστίας ήταν η θεσμοθέτηση νόμων με άκαμπτες ρήτρες, αυστηρό και κατασταλτικό έλεγχος και εξοντωτικές κυρώσεις (Ε. Αλεξανδροπούλου- Αιγυπτιάδου 2007).

6.2 Νομοθετήματα «Δεύτερης Γενιάς».

Η «δεύτερη γενιά» νομοθετημάτων οριοθετείται στις αρχές της δεκαετίας του ’80. Η νομοθεσία φαίνεται να αναγνωρίζει τα οφέλη από την χρήση των ηλεκτρονικών υπολογιστών και συνειδητοποιεί την αξία τους. Αποτέλεσμα είναι η αλλαγή του χαρακτήρα των νομοθεσιών, οι οποίες είναι πιο εύκαμπτες ανάλογα με το είδος των επεξεργαζόμενων στοιχείων ενώ παράλληλα παρατηρείται περιορισμός των γενικών αφορισμών και απαγορεύσεων (Γ. Λουκέρης, 1997).

Το 1981, υπεγράφη στο Στρασβούργο στα πλαίσια του Συμβουλίου της Ευρώπης, η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα. Η Σύμβαση 108/28.1.1981 κωδικοποίησε τις αρχές που αποτελούσαν το «σκληρό πυρήνα» της προστασίας δεδομένων προσωπικού χαρακτήρα, αποτελώντας την αφετηρία μιας δεύτερης περιόδου για την προστασία από την επεξεργασία προσωπικών δεδομένων. Η Σύμβαση 108, όπως είναι γνωστή, αποτέλεσε ισχυρό κίνητρο για την ψήφιση ειδικών νόμων από αρκετές χώρες, ενώ άλλες τροποποίησαν τις νομοθεσίες τους αναθεωρώντας τις αντιλήψεις των νομοθετημάτων της «πρώτης γενιάς» (Μ. Αυγουστιανάκης, 2001).

Κάποια χρόνια αργότερα, το 1985, η Γαλλία, η Γερμανία, το Βέλγιο, Οι Κάτω Χώρες και το Λουξεμβούργο σύναψαν τη Συμφωνία του Σένγκεν, η οποία προέβλεπε σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα των χωρών. Η Σύμβαση εφαρμογής της Συμφωνίας Σένγκεν υπογράφηκε το 1990 και προσχώρησαν η Ιταλία, η Ισπανία και Πορτογαλία το 1991 και η Ελλάδα το 1992. Μέχρι το 1996 είχαν προσχωρήσει η Αυστρία, Η Δανία, η Σουηδία η Νορβηγία, η Ισλανδία και η Φιλανδία. Προκειμένου να εξασφαλιστεί η ασφάλεια, η οποία θα ήταν τρωτή λόγω

της ελεύθερης κυκλοφορίας προσώπων και αγαθών δημιουργήθηκε ένα σύστημα ανταλλαγής πληροφοριών, στηριζόμενο στην πληροφορική τεχνολογία, μεταξύ των συμβαλλομένων κρατών της Συνθήκης Σένγκεν. Υποχρέωση κάθε συμβαλλόμενου κράτους στην Συνθήκη Σένγκεν ήταν να θεσπίσει την αναγκαία νομοθεσία, ώστε να εξασφαλιστεί η προστασία των προσωπικών δεδομένων που διακινούνταν μεταξύ των κρατών (Α. Παπαδόπουλος, 1999).

6.3 Νομοθετήματα «Τρίτης Γενιάς».

Τα νομοθετήματα «τρίτης γενιάς» εμφανίστηκαν τη δεκαετία του 1990 και εξακολουθούν να ισχύουν μέχρι και σήμερα. Λόγω της ραγδαίας εξέλιξης της πληροφορικής τεχνολογίας, τα νομοθετήματα αυτά αντανακλούν τη προσπάθεια του νομοθέτη να ανταποκριθεί στην ανάγκη ρύθμισης της επεξεργασίας των προσωπικών δεδομένων.

Ορόσημο για την προστασία των προσωπικών δεδομένων υπήρξε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου «Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων και την ελεύθερη κυκλοφορία αυτών». Στόχος της εν λόγω Οδηγίας ήταν η εναρμόνιση των νομοθεσιών των κρατών- μελών της Ευρωπαϊκή Ένωσης, ώστε να διασφαλίζεται η προστασία των προσώπων, αλλά και η ελεύθερη κυκλοφορία των δεδομένων για την εγκαθίδρυση και λειτουργία της εσωτερικής αγοράς (Ε. Αλεξανδροπούλου-Αιγυπτιάδου, 2007). Η Ελλάδα ενσωμάτωσε την Οδηγία 95/46/ΕΚ στην ελληνική νομοθεσία το 1997 με τον νόμο 2472, ο οποίος αναλύεται σε επόμενο κεφάλαιο. Με την Οδηγία 95/46/ΕΚ, η Ευρωπαϊκή Κοινότητα την πρώτη σημαντική προσπάθεια να ρυθμιστεί κατά τρόπο ενιαίο εκ μέρους των κρατών μελών, η προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς και η ελεύθερη κυκλοφορία των δεδομένων αυτών.

Με τον Κανονισμό 45/2001 του Ευρωπαϊκού Κοινοβουλίου επιδιώκεται η διασφάλιση από τα όργανα και τους οργανισμούς της Κοινότητας των κανόνων προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των προσώπων, καθώς και την ελεύθερη κυκλοφορία των προσωπικών δεδομένων μεταξύ των κρατών- μελών

και των οργάνων και Οργανισμών της Κοινότητας. Με τον Κανονισμό 45/2001 εισάγεται ο θεσμός του Ευρωπαίου Επόπτη Προστασίας Δεδομένων. Απαρχή μιας τέτοιας πρωτοβουλίας, στάθηκε η διάταξη του άρθρου 286 της Συνθήκης ΕΚ, σύμφωνα με την οποία από 1/1/1999 οι κοινοτικές πράξεις για την προστασία του ατόμου από την επεξεργασία και την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εφαρμόζονται στα όργανα και οργανισμούς που έχουν ιδρυθεί από τη Συνθήκη ΕΚ ή βάσει αυτής, ενώ προβλέπεται και η *σύσταση ανεξάρτητου εποπτικού οργάνου* που επιφορτίζεται με την παρακολούθηση της εφαρμογής των κοινοτικών πράξεων στα όργανα και τους οργανισμούς της Κοινότητας (Ν. Σκανδάμης, 1997).

Σημαντική είναι η οδηγία 1999/93/ΕΚ, στην οποία ορίζεται η ηλεκτρονική υπογραφή και καθιερώνεται η νομική ισχύς της. Η Οδηγία αυτή εκδόθηκε αφού ήδη ορισμένες χώρες, όπως η Γερμανία και η Ιταλία είχαν αρχίσει να θεσπίζουν σε εθνικό επίπεδο νομοθεσία περί ψηφιακών υπογραφών. Η Οδηγία 1999/93/ΕΚ συνιστά μια ενιαία νομοθετική βάση, κοινή για όλες τις χώρες της Ευρωπαϊκής Ένωσης, η οποία περιγράφει τα σχετικά με ηλεκτρονικές υπογραφές, ψηφιακά πιστοποιητικά και παροχή υπηρεσιών πιστοποίησης και θέτει τα ελάχιστα απαιτούμενα επίπεδα ασφάλειας, ενώ παράλληλα φροντίζει να διασφαλίσει την ελεύθερη διακίνηση των σχετικών προϊόντων και υπηρεσιών στην ενιαία αγορά (Κ. Χριστοδούλου, 2001). Η Ελλάδα ενσωμάτωσε την Κοινοτική Οδηγία με την έκδοση του Προεδρικού Διατάγματος 150/2001 «Προσαρμογή στην Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».

6.4 Δικαίωμα «Πληροφοριακού Αυτοκαθορισμού».

Η επεξεργασία των προσωπικών δεδομένων στηρίζεται στη συστηματική καταγραφή όλων των πλευρών της προσωπικότητας του πολίτη, πράγμα που κάνει φανερή τη στενή σύνδεση της προστασίας των προσωπικών δεδομένων με τα ατομικά δικαιώματα, και ιδίως με αυτά της προστασίας της ιδιωτικής ζωής και της προσωπικότητας. Συγκεκριμένα, η προστασία των πληροφοριών που αφορούν το άτομο θεμελιώνεται στην προστασία της ιδιωτικής ζωής, στην προστασία της

ανθρώπινης αξιοπρέπειας, στο δικαίωμα της ελεύθερης ανάπτυξης της προσωπικότητας και στην προστασία της επικοινωνίας. Τα θεμελιώδη αυτά δικαιώματα, οδηγούν στην αναγνώριση του επιτρεπτού της επεξεργασίας προσωπικών δεδομένων ως ζητήματος συνταγματικής τάξης.

Ειδική εκδήλωση των δικαιωμάτων αυτών, και κυρίως του δικαιώματος ελεύθερης ανάπτυξης της προσωπικότητας, αποτελεί το δικαίωμα πληροφοριακού αυτοκαθορισμού των πολιτών ή αλλιώς δικαίωμα αυτοδιάθεσης των πληροφοριών, στο οποίο στηρίχθηκε η προστασία του ατόμου από την αθέμιτη επεξεργασία των προσωπικών του δεδομένων. Το δικαίωμα αυτό συνίσταται στο δικαίωμα του ατόμου να καθορίζει στα νόμιμα πλαίσια την επεξεργασία των πληροφοριών που τον αφορούν και αναγνωρίστηκε αρχικά από την νομολογία του γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου που στην ιστορική του πλέον απόφαση της 15.12.1983 (Α. Γέροντας, 1997).

Το περιεχόμενο του πληροφοριακού αυτοπροσδιορισμού, έχει δύο σκέλη. Το πρώτο έχει να κάνει με την προστασία της ανθρώπινης αξιοπρέπειας, έτσι ώστε να μην καθίσταται κανείς αντικείμενο επεξεργασίας των προσωπικών του πληροφοριών ενώ το δεύτερο αναφέρεται στην προστασία της ελεύθερης ανάπτυξης της προσωπικότητας στην κοινωνία της πληροφορίας (Λ. Μήτρου, 2001). Εάν ο πολίτης δεν είναι σε θέση να γνωρίζει ποιος, πότε, και γιατί συλλέγει και επεξεργάζεται δεδομένα που τον αφορούν προσβάλλονται όχι μόνο οι δυνατότητες ανάπτυξης της προσωπικότητας του αλλά και το γενικό συμφέρον, γιατί η αυτονομία αποτελεί θεμελιώδη προϋπόθεση λειτουργίας μιας ελεύθερης και δημοκρατικής πολιτείας που στηρίζεται στην δυνατότητα δράσης και συμμετοχής των πολιτών της (Α. Γέροντας, 1997).

Το δικαίωμα του πληροφοριακού αυτοκαθορισμού σε σχέση με τις νέες τεχνολογίες της πληροφορίας μας οδηγεί στο συμπέρασμα ότι πρόκειται για δικαίωμα της νέας εποχής, εντασσόμενο στη λεγόμενη «τρίτη γενιά» θεμελιωδών δικαιωμάτων.

ΚΕΦΑΛΑΙΟ VII

ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΛΛΑΔΑ.

7.1 Νόμος 2472/1997: «Προστασία Του Ατόμου Από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα».

Το νομοθετικό κείμενο το οποίο αποτέλεσε «σταθμό» για την προστασία των προσωπικών δεδομένων σε κοινοτικό επίπεδο είναι η Οδηγία 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», με την οποία η Ευρωπαϊκή Κοινότητα θέλησε να θέσει ένα υψηλό επίπεδο προστασίας για όλα τα κράτη- μέλη. Με βάση αυτή την Οδηγία η ελληνική νομοθεσία ψήφισε τον Νόμο 2472/1997 για την «Προστασία του Ατόμου Από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα».

Τα προσωπικά δεδομένα αποτελούν ένα ιδιαίτερο σημαντικό κομμάτι της ηλεκτρονικής τραπεζικής, καθώς οι ηλεκτρονικές συναλλαγές των χρηστών περιέχουν πληροφορίες σχετικά με δεδομένα προσωπικού χαρακτήρα, όπως η οικονομική κατάσταση των χρηστών, οι οικονομικές τους εκκρεμότητες, το εισόδημά τους ή η ακίνητη περιουσία τους.

7.1.1 Ορισμοί και Έννοιες

Για να γίνει κατανοητή η ανάλυση του πλαισίου προστασίας των προσωπικών δεδομένων, είναι απαραίτητο να διευκρινιστούν οι κυριότεροι ορισμοί, τους οποίους εισάγει ο Ν. 2472/97.

Ο Ν . 2472/1997 δε δίνει έναν αυστηρό ορισμό των προσωπικών δεδομένων, αλλά επιτρέπει την απόδοση του όρου σε διαφορετικά δεδομένα, ανάλογα με την περίπτωση και τη δυνατότητα να προσδιοριστούν με βάση τα δεδομένα τα πρόσωπα, στα οποία αυτά αναφέρονται.

Η Αρχή Προστασίας των Προσωπικών δεδομένων ορίζει τα δεδομένα προσωπικού χαρακτήρα ή διαφορετικά, προσωπικά δεδομένα, κάθε πληροφορία που αναφέρεται σε ένα φυσικό πρόσωπο και το περιγράφει όπως για παράδειγμα στοιχεία αναγνώρισης, φυσικά χαρακτηριστικά, εκπαίδευση, εργασία, οικονομική κατάσταση, ενδιαφέροντα, δραστηριότητες, συνήθειες.

Από τον παραπάνω ορισμό προκύπτει ότι ως προσωπικό δεδομένο νοείται οποιαδήποτε πληροφορία που αναφέρεται σε συγκεκριμένο άτομο, από την πιο «απλή» μέχρι την πιο «ευαίσθητη». Εξαιρούνται από την προστασία του Ν. 2472/97 δεδομένα που συγκεντρώνονται για στατιστικές μελέτες, μια και σε περιπτώσεις στατιστικών μελετών δεν ενδιαφέρουν αποτελέσματα που προκύπτουν από ξεχωριστά άτομα, αλλά τα αθροιστικά αποτελέσματα, τα οποία είναι και στατιστικά αξιοποιήσιμα.

Τα προσωπικά δεδομένα διαχωρίζονται σε δύο κατηγορίες, στα «απλά προσωπικά δεδομένα» και τα «ευαίσθητα προσωπικά δεδομένα». Ο διαχωρισμός έχει να κάνει με το είδος της πληροφορίας που περιέχουν τα δεδομένα.

Σύμφωνα με το άρθρο 2 του Νόμου 2472/1997 περί Προστασίας του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα, ευαίσθητα προσωπικά δεδομένα αποτελούν τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα απλά προσωπικά δεδομένα αφορούν σε κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

Η ουσιαστική διαφορά ανάμεσα στα απλά και τα ευαίσθητα προσωπικά δεδομένα βρίσκεται στην ενισχυμένη νομική προστασία των δεύτερων. Για την

νόμιμη επεξεργασία των ευαίσθητων δεδομένων απαιτείται η γραπτή συγκατάθεση του υποκειμένου που υφίσταται την επεξεργασία των προσωπικών του δεδομένων, καθώς και η λήψη άδειας από την Αρχή Προστασία Προσωπικών Δεδομένων, η οποία αποτελεί ανεξάρτητη δημόσια αρχή, ενώ για την επεξεργασία των απλών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου και απλή γνωστοποίηση της επεξεργασίας στην Αρχή.

Άλλοι σημαντικοί ορισμοί είναι αυτοί των εμπλεκομένων στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ως υποκείμενο ορίζεται το πρόσωπο στο οποίο αναφέρονται τα δεδομένα και με κατάλληλη επεξεργασία μπορούν να αποκαλύψουν την ταυτότητά του. Ο υπεύθυνος επεξεργασίας των δεδομένων είναι αυτός που ορίζει το σκοπό και τον τρόπο με τον οποίο γίνεται η επεξεργασία, είτε πρόκειται για φυσικό είτε για νομικό πρόσωπο. Ανάλογη νομική υπόσταση μπορεί να έχει και το πρόσωπο που ορίζει ο υπεύθυνος ως εκτελούντα την επεξεργασία. Συνήθως είναι κάποιο φυσικό πρόσωπο καταρτισμένο στη χρήση τεχνολογικών μέσων για την επεξεργασία των δεδομένων ή εταιρεία ή οργανισμός με την κατάλληλη τεχνογνωσία, με την αυστηρή προϋπόθεση ότι εκτελούν την επεξεργασία για λογαριασμό και με τρόπο που υποδεικνύει ο υπεύθυνος. Επίσης ο νόμος ορίζει τον αποδέκτη των δεδομένων, στον οποίο γνωστοποιούνται με οποιονδήποτε τρόπο τα δεδομένα, όπως μία δημόσια υπηρεσία ή ιδιωτικός οργανισμός ή άλλο πρόσωπο.

Τα δεδομένα προσωπικού χαρακτήρα μπορούν να υποστούν επεξεργασία κατά διάφορους τρόπους. Σε αυτούς περιλαμβάνεται η συλλογή, η καταχώριση και οργάνωση σε βάσεις δεδομένων, η τροποποίησή τους, η διάδοση με οποιοδήποτε μέσο, το κλείδωμα ή η διαγραφή τους. Τέτοιου είδους επεξεργασία υφίστανται δεδομένα των πελατών των ιδρυμάτων ηλεκτρονικού χρήματος κατά την καταχώρησή τους σε πελατολόγια ή κατά την αξιοποίηση των πελατολογίων για διάφορους σκοπούς. Γενικά τα δεδομένα που συγκεντρώνονται αποθηκεύονται σε αρχεία όπως οι βάσεις δεδομένων. Πολλές φορές συσχετίζονται μεταξύ τους αρχεία που τηρούνται για διαφορετικούς σκοπούς είτε για στατιστική αξιοποίησή τους είτε για προώθηση νέων προϊόντων και υπηρεσιών.

Τέλος πρέπει να αναφερθεί ότι ο νόμος 2472/1997 περιλαμβάνει τόσο τη μερικώς ή πλήρως αυτοματοποιημένη επεξεργασία όσο και τη μη αυτοματοποιημένη, εφόσον γίνεται για επαγγελματικούς ή άλλους δημόσιου χαρακτήρα σκοπούς. Επομένως αποκλείονται οι περιπτώσεις επεξεργασίας στα πλαίσια προσωπικών ή κατ' οίκον δραστηριοτήτων.

7.1.2 Βασικές Αρχές Επεξεργασίας των Προσωπικών Δεδομένων

Η επεξεργασία των προσωπικών δεδομένων για είναι νόμιμη, πρέπει να τηρεί κάποιες αρχές όπως αυτές ορίζονται στο άρθρο 4 του Ν. 2472/1997. Σκοπός των αρχών αυτών είναι, η μείωση του κινδύνου προσβολής της προσωπικότητας του υποκειμένου όπου υφίσταται την επεξεργασία των προσωπικών του δεδομένων, καθώς και η διασφάλιση διαρκούς ελέγχου της επεξεργασίας από την πλευρά του υποκειμένου και από την πλευρά του κράτους.

- *Αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας.*

Σύμφωνα με την αρχή της νομιμότητας του σκοπού και του τρόπου επεξεργασίας τα προσωπικά δεδομένα θα πρέπει να συλλέγονται κατά τρόπο θεμιτό και νόμιμο και να υφίστανται νόμιμη επεξεργασία για καθορισμένους, σαφείς και νόμιμους σκοπούς. Η αρχή αυτή προκύπτει από το άρθρο 4, παράγραφος 1α του Ν. 2472/1997 το οποίο επισημαίνει ότι η επεξεργασία των δεδομένων, πρέπει να εξυπηρετεί κάποιον σκοπό και δεν μπορεί να γίνεται δίχως λόγο, έστω και με την πρόθεση μελλοντικού προσδιορισμού του σκοπού. Επιπλέον, η επεξεργασία πρέπει να εξυπηρετεί νόμιμο και συγκεκριμένο σκοπό και να μην υπερβαίνει το σκοπό της. Ο σκοπός της επεξεργασίας προσωπικών δεδομένων θα πρέπει να θα πρέπει να δηλώνεται στην Αρχή προστασία των Προσωπικών Δεδομένων. Σε περίπτωση που ο υπεύθυνος επεξεργασίας θελήσει να επεξεργασθεί τα ίδια δεδομένα για διαφορετικό σκοπό πρέπει αν τον δηλώσει εκ νέου στην Αρχή (Ε. Αλεξανδροπούλου- Αιγυπτιάδου, 2007).

- *Η αρχή της αναλογικότητας*.

Σύμφωνα με τη αρχή της αναλογικότητας τα υπό επεξεργασία προσωπικά δεδομένα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά χρειάζεται για τους σκοπούς της επεξεργασίας. Η παραπάνω αρχή χρησιμοποιεί ένα ποιοτικό και ένα ποσοτικό κριτήριο. Ελέγχεται δηλαδή, αν το συγκεκριμένο δεδομένο είναι συναφές με τον επιδιωκόμενο σκοπό και πρόσφορο να οδηγήσει στην επίτευξή του. Αν δεν τηρείται το παραπάνω ποιοτικό κριτήριο, τότε η επεξεργασία θεωρείται παράνομη. Σε περίπτωση που η επεξεργασία περάσει με επιτυχία τον έλεγχο νομιμότητας με βάση το ποιοτικό κριτήριο, ακολουθεί ο έλεγχος με βάση το ποσοτικό κριτήριο και να καταλήξει θετικός, η επεξεργασία είναι σύμφωνη με την αρχή της αναλογικότητας (Ε. Αλεξανδροπούλου- Αιγυπτιάδου, 2007).

- *Η αρχή της ακρίβειας*.

Σύμφωνα μα την αρχή της ακρίβειας, τα προσωπικών δεδομένων που υπόκεινται σε επεξεργασία πρέπει να ανταποκρίνονται την πραγματικότητα, να είναι επίκαιρα και ακριβή και εφόσον χρειάζεται να υποβάλλονται σε ενημέρωση (Α. Γεέροντας, 2002).

- *Η αρχή της χρονικής διάρκειας τήρησης των δεδομένων*.

Σύμφωνα με την αρχή της χρονικής τήρησης των δεδομένων, τα δεδομένα μπορούν να τηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων μόνο κατά τη διάρκεια της περιόδου που απαιτείται για την πραγματοποίηση των σκοπών της συλλογής και της επεξεργασίας τους. Έτσι, αν τα δεδομένα τηρούνται με τρόπο που δεν συνδέονται με το συγκεκριμένο πρόσωπο, δεν υπάρχει χρονικός περιορισμός στη διατήρησή τους. Αρμόδια για τον καθορισμό της διάρκειας τήρησης των δεδομένων είναι η Αρχή Προστασίας Προσωπικών Δεδομένων (Ε. Αλεξανδροπούλου- Αιγυπτιάδου, 2007).

Η τήρηση των αρχών επεξεργασίας αποτελεί υποχρέωση του υπεύθυνου επεξεργασίας . Σε περίπτωση που τα προσωπικά δεδομένα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά την παράβαση των ανωτέρω αρχών, καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας και η Αρχή επιβάλλει τη διακοπή της

επεξεργασίας και την καταστροφή των προσωπικών δεδομένων που έχουν ήδη υποστεί επεξεργασία.

7.1.3 Προϋποθέσεις Επεξεργασίας.

Ο Ν. 2472/1997, χρησιμοποιεί τον όρο «επεξεργασία» με ευρύτατο περιεχόμενο. Περιλαμβάνει κάθε εργασία, όπως συλλογή, καταχώρηση, οργάνωση, διατήρηση, αποθήκευση, διαβίβαση, διασύνδεση, διαγραφή, καταστροφή που εφαρμόζεται σε προσωπικά δεδομένα από το Δημόσιο, Νομικά Πρόσωπα Δημοσίου Δικαίου ή Νομικά Πρόσωπα Ιδιωτικού Δικαίου, ένωση προσώπων ή φυσικό πρόσωπο.

Για να γίνει η επεξεργασία δεδομένων προσωπικού χαρακτήρα, θα πρέπει να πληρούνται δύο προϋποθέσεις. Πρώτη προϋπόθεση είναι η συγκατάθεση επεξεργασίας από το υποκείμενο των δεδομένων, εφόσον η απόφαση ληφθεί ρητά και ελεύθερα και αφού προηγουμένως γίνει πλήρης ενημέρωση σχετικά με το σκοπό της επεξεργασίας, τα στοιχεία του υπεύθυνου επεξεργασίας και του ή των αποδεκτών της, ενώ σε περίπτωση που το υποκείμενο αδυνατεί νομικά να δηλώσει τη βούλησή του, αυτό γίνεται από νόμιμο εκπρόσωπο. Κατ' εξαίρεση η επεξεργασία χωρίς συγκατάθεση, μπορεί να επιτραπεί μόνο αν η επεξεργασία είναι αναγκαία:
α) για την εκτέλεση σύμβασης, στην οποία το υποκείμενο είναι το συμβαλλόμενο μέρος.
β) για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας, οποία επιβάλλεται από τον νόμο.
γ) για τη διαφύλαξη του ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεση του
δ) για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημοσίας εξουσίας
ε) για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι δεν θίγονται οι θεμελιώδεις ελευθερίες.

Η άλλη προϋπόθεση είναι η γραπτή γνωστοποίηση στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της έναρξης της επεξεργασίας ή της τήρησης των αντίστοιχων αρχείων με τα προσωπικά δεδομένα. Αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να δηλώσει στην αρμόδια αρχή τα στοιχεία του, επωνυμία ή όνομα και διεύθυνση, το σκοπό της επεξεργασίας, τη χρονική της διάρκεια, το μέρος και τον εξοπλισμό που θα χρησιμοποιηθεί για την αποθήκευση των αρχείων με τα δεδομένα, τους αποδέκτες, ενδεχόμενη διαβίβαση μέρους ή όλου του αρχείου εκτός συνόρων και τα μέτρα ασφαλείας για την προστασία των δεδομένων. Η Αρχή τηρεί αυτά τα δεδομένα σε ειδικά Μητρώα Επεξεργασίας και τα ενημερώνει για τυχόν αλλαγές, οι οποίες πρέπει να γνωστοποιηθούν σε αυτή άμεσα από τον υπεύθυνο επεξεργασίας.

Ο Ν. 2472/1997 εφαρμόζεται σε κάθε επεξεργασία, εφόσον αυτή εκτελείται εντός Ελληνικής επικράτειας ή σε τόπο όπου βάσει δημοσίου διεθνούς δικαίου εφαρμόζεται το ελληνικό δίκαιο.

7.1.4 Διασύνδεση Αρχείων.

Η διασύνδεση αρχείων συνίσταται στη δυνατότητα συσχέτισης των δεδομένων ενός αρχείου με δεδομένα αρχείου ή αρχείων που τηρούνται από τον ίδιο υπεύθυνο επεξεργασίας για άλλο σκοπό ή από άλλον ή άλλους υπεύθυνους επεξεργασίας. Η διασύνδεση αρχείων αποτελεί σύνηθες φαινόμενο της οικονομικής ζωής, κυρίως στα πλαίσια της αύξησης του μεριδίου αγοράς. Ο νόμος θέτει όρους, οι οποίοι πρέπει να τηρούνται υποχρεωτικά προκειμένου η διασύνδεση να θεωρείται νόμιμη. Ο βασικός όρος είναι ότι οποιαδήποτε διασύνδεση πρέπει να γνωστοποιείται στην Αρχή Προστασίας. Εάν γίνεται διασύνδεση μεταξύ αρχείων για τα οποία έχουν δηλωθεί διαφορετικοί υπεύθυνοι, τότε η δήλωση πρέπει να γίνεται από κοινού από όλους τους εμπλεκόμενους υπευθύνους.

Στην περίπτωση που κάποιο από τα αρχεία περιέχει ευαίσθητα δεδομένα ή η διασύνδεση οδηγεί στην αποκάλυψή τους, τότε ο νόμος προβλέπει τη χορήγηση ειδικής άδειας διασύνδεσης μετά από ακρόαση των υπευθύνων. Η άδεια περιλαμβάνει το σκοπό της διασύνδεσης, το είδος των δεδομένων των αρχείων, το χρονικό διάστημα ισχύος της διασύνδεσης και όποια άλλη προϋπόθεση θεωρηθεί απαραίτητη, ώστε να προστατευθούν τα δικαιώματα των υποκειμένων. Η Αρχή

Προστασίας τηρεί ειδικό μητρώο διασυνδέσεων για να παρακολουθεί την τήρηση των παραπάνω διατάξεων, στο οποίο καταχωρεί τις δηλώσεις των υπευθύνων και αντίγραφα των αδειών (Ε. Αλεξανδροπούλου- Αιγυπτιάδου, 2007).

7.1.5 Διασυνοριακή Ροή Δεδομένων.

Αρκετές φορές είναι απαραίτητη η μεταφορά δεδομένων εκτός συνόρων, προκειμένου να εκτελεστεί επιτυχώς η επεξεργασία τους, είτε γιατί κάποιο μέρος του εξοπλισμού για την επεξεργασία είναι εγκατεστημένο σε χώρα του εξωτερικού είτε επειδή κάποια αρχεία ή ακόμη και υποκείμενα δεδομένων βρίσκονται εκεί. Βέβαια η πιο συνηθισμένη αιτία είναι η παγκόσμια φύση της σύγχρονης οικονομίας, καθώς δεν είναι σπάνιες οι συναλλαγές μεταξύ Ελλήνων καταναλωτών και εμπόρων ή άλλων εταιρειών του εξωτερικού. Ακόμη η απελευθέρωση της τραπεζικής αγοράς σήμανε την άρση πολλών από τους περιορισμούς, προκειμένου κάποια τράπεζα του εξωτερικού να ανοίξει υποκαταστήματα ή θυγατρικές στην Ελλάδα και το αντίστροφο. Πολλές φορές το κριτήριο «διεθνοποίησης» μίας τράπεζας είναι και φορολογικής φύσεως, κάτι που δεν αλλάζει τίποτα στο τελικό αποτέλεσμα και τη διαδικασία επεξεργασίας προσωπικών δεδομένων.

Η διαβίβαση αρχείων προσωπικών δεδομένων σε χώρες εντός της Ευρωπαϊκή Ένωσης γίνεται ελεύθερα. Σε διαφορετική περίπτωση, απαραίτητη είναι η λήψη ειδικής άδειας από την Αρχή Προστασίας. Η Αρχή παρέχει άδεια μόνο όταν διασφαλιστεί ότι η εν λόγω χώρα εξασφαλίζει το απαραίτητο επίπεδο προστασίας και για τον σκοπό αυτό συνεκτιμά τη φύση των δεδομένων, τους σκοπούς της επεξεργασίας, τη διάρκεια της επεξεργασίας, τους γενικούς και ειδικούς κανόνες δικαίου που διέπουν τη συγκεκριμένη χώρα, τα μέτρα ασφάλειας των προσωπικών δεδομένων καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων. Υπάρχουν όμως και χώρες, οι οποίες παρόλο που δεν ανήκουν στην Ευρωπαϊκή Ένωση, επιτρέπεται σύμφωνα με απόφαση της Αρχής η διαβίβαση δεδομένων διότι εξασφαλίζουν ικανοποιητικό επίπεδο ασφάλειας. Τέτοιες χώρες είναι η Ελβετία και ο Καναδάς (Γ. Γιαννόπουλος, 2001; Θ. Σιδηρόπουλος, 2003).

Η Αρχή κατ΄ εξαίρεση επιτρέπει την διαβίβαση δεδομένων σε χώρες που δεν ανήκουν στην Ευρωπαϊκή Ένωση και δεν έχουν κριθεί ότι εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας, εφόσον συντρέχουν οι παρακάτω προϋποθέσεις:

1. Το υποκείμενο έδωσε τη συγκατάθεσή του για διαβίβαση των δεδομένων, η οποία έχει παραχωρηθεί με νόμιμο τρόπο.
2. Όταν η διαβίβαση κρίνεται απαραίτητη για τη διασφάλιση του ζωτικού συμφέροντος του υποκειμένου των δεδομένων και το ίδιο το υποκείμενο αδυνατεί λόγω φυσικής ή νομικής αδυναμίας να δώσει τη συγκατάθεσή του, ή για την εκτέλεση σύμβασης ή για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί ύστερα από αίτηση του υποκειμένου των δεδομένων.
3. Η διαβίβαση είναι απαραίτητη για τη αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημοσίου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες Αρχές της άλλης χώρας.
4. Όταν η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.
5. Όταν η διαβίβαση πραγματοποιείται από δημόσιο μητρώο.
6. Όταν ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων.

Σε κάθε περίπτωση η Αρχή ενημερώνει την Ευρωπαϊκή Επιτροπή και τις αντίστοιχες αρχές άλλων κρατών όταν θεωρεί ότι μια χώρα δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, καθώς και για τις άδειες τις οποίες χορηγεί όταν κρίνει όταν υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις. Σε αντίθετη περίπτωση η Αρχή δεν χορηγεί άδεια.

7.1.6 Απόρρητο και Ασφάλεια Επεξεργασίας.

Ο Ν. 2472/1997 ορίζει ρητά στο άρθρο 10, ότι η επεξεργασία των προσωπικών δεδομένων είναι απόρρητη και διεξάγεται μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο κατ’ εντολή του.

Προκειμένου να διεξαχθεί η επεξεργασία, ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου.

Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.

7.1.7 Δικαιώματα του Υποκειμένου Επεξεργασίας των Δεδομένων.

Ο νομοθέτης περιέλαβε στο Ν. 2472/97 ορισμένες διατάξεις, οι οποίες κατοχυρώνουν τα δικαιώματα του υποκειμένου, ώστε να εξασφαλίζεται ο πληρέστερος έλεγχος, η διαφάνεια και το σύνορο της επεξεργασίας που πραγματοποιείται. Τα δικαιώματα που έχει το υποκείμενο κατά την επεξεργασία των προσωπικών του δεδομένων είναι αυτό της ενημέρωσης, της πρόσβασης και της αντίρρησης και της προσωρινής δικαστικής προστασίας. Τα παραπάνω δικαιώματα του υποκειμένου αποτελούν αντίβαρο στον πληροφοριακό συγκεντρωτισμό. Η παροχή δικαιωμάτων προβλέπεται όχι μόνο στο Ν. 2472/1997 αλλά και στο Ν. 2774/1999, ο οποίος εξειδίκευσε και συμπλήρωσε τον Ν. 2472/1997 στο πεδίο των τηλεπικοινωνιών.

7.1.7.1. Δικαίωμα Ενημέρωσης.

Το δικαίωμα ενημέρωσης κατέχει εξέχουσα θέση μεταξύ τω δικαιωμάτων του υποκειμένου, επειδή βάση αυτού εξασφαλίζεται η διαφανής και σύννομη επεξεργασία

των προσωπικών δεδομένων και διευκολύνεται η άσκηση των δικαιωμάτων πρόσβασης και αντίρρησης. Το δικαίωμα της ενημέρωσης του υποκειμένου συνίσταται στη υποχρέωση του υπευθύνου επεξεργασίας να ενημερώνει το υποκείμενο κατά τρόπο πρόσφορο και σαφή. Το δικαίωμα της ενημέρωσης πηγάζει από το δικαίωμα της πληροφοριακής αυτοδιάθεσης του ατόμου. Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο των δεδομένων είτε το υποκείμενο έχει δώσει τη συγκατάθεσή του , είτε όχι (Α. Σινανιώτη – Μαυρούδη & Δ. Φαρσαρώτας, 2005).

Το περιεχόμενο της ενημέρωσης από τον υπεύθυνο επεξεργασίας περιλαμβάνει την ταυτότητα του υπευθύνου επεξεργασίας, τον σκοπό της επεξεργασίας, τους αποδέκτες των δεδομένων κατά τρόπο αποκλειστικό και όχι ενδεικτικό, καθώς και την ενημέρωση για την ύπαρξη δικαιώματος πρόσβασης. Επιπλέον αν ο υπεύθυνος τη επεξεργασίας ζητά τη συνδρομή του υποκειμένου, οφείλει να το ενημερώσει ειδικώς και εγγράφως για τα παραπάνω στοιχεία καθώς και για το δικαίωμα της αντίρρησης. Σε περίπτωση που τα δεδομένα επεξεργασίας ανακοινώνονται σε τρίτους, το υποκείμενο πρέπει να ενημερώνεται πριν την ανακοίνωση, καθώς και για το ποιοι είναι οι τρίτοι.

Ο χρόνος ενημέρωσης του υποκειμένου διαφέρει στην περίπτωση που η συλλογή γίνεται απευθείας από το υποκείμενο. Τότε η συλλογή και η ενημέρωση γίνονται ταυτόχρονα. Στην περίπτωση που η συλλογή γίνεται από τρίτο πρόσωπο, το υποκείμενο πρέπει να ενημερωθεί αμέσως μετά τη συλλογή και σε κάθε περίπτωση πριν από οποιαδήποτε χρήση ή άλλη επεξεργασία των δεδομένων. Η υποχρέωση ενημέρωσης δεν υφίσταται όταν η συλλογή γίνεται καθαρά για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα, το οποία εξακολουθούν να διατηρούν το δικαίωμα πρόσβασης και αντίρρησης.

7.1.7.2 Δικαίωμα Πρόσβασης.

Ο καθένας έχει δικαίωμα να γνωρίζει εάν τα προσωπικά του δεδομένα αποτέλεσαν ή αποτελούν αντικείμενο επεξεργασίας σύμφωνα με το άρθρο 12 του Ν.

2472/1997. Το υποκείμενο των δεδομένων έχει δικαίωμα να ζητά και να λαμβάνει από τον υπεύθυνο επεξεργασίας, όλα τα προσωπικά δεδομένα που υφίστανται επεξεργασία και το αφορούν, καθώς και την προέλευσή τους, τους σκοπούς της επεξεργασίας, τους αποδέκτες, τη εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση ή πληροφόρησή του, τη λογική της αυτοματοποιημένης επεξεργασίας, καθώς και τη διόρθωση, τη διαγραφή ή τη δέσμευση των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του νόμου. Επιπλέον μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας την κοινοποίηση σε τρίτους, στους οποίους έχουν ανακοινωθεί τα δεδομένα, καθώς και κάθε διόρθωση, διαγραφή ή δέσμευση εφόσον αυτό είναι εφικτό Ε. Αλεξανδροπούλου- Αιγυπτιάδου, 2007).

Το δικαίωμα πρόσβασης ασκείται εγγράφως και ο υπεύθυνος επεξεργασίας πρέπει να απατήσει εγγράφως εντός 15 ημερών. Εάν η απάντησή του δεν είναι ικανοποιητική, το υποκείμενο των δεδομένων έχει το δικαίωμα να προσφύγει στην Αρχή. το δικαίωμα πρόσβασης μπορεί να αποκλεισθεί για λόγους εθνικής ασφάλειας ή για τη διακρίβωση σοβαρών εγκλημάτων.

7.1.7.3 Δικαίωμα Αντίρρησης.

Το δικαίωμα αντίρρησης συνίσταται στην προβολή αντιρρήσεων εκ μέρους του υποκειμένου επεξεργασίας για τα προσωπικά του δεδομένα και αποτελεί το κατ' εξοχήν δυναμικό δικαίωμα του υποκειμένου.

Κάθε πρόσωπο έχει δικαίωμα να δηλώσει εγγράφως στην Αρχή, η οποία τον καταχωρεί σε ειδικά μητρώα, ότι δεν επιθυμεί να αποτελέσουν τα προσωπικά του δεδομένα αντικείμενο επεξεργασίας από οποιονδήποτε, είτε για λόγους προώθησης πωλήσεων είτα για λόγους παροχής υπηρεσιών. Ουσιαστικά πρόκειται για μια εκ των προτέρων άρνηση χορήγησης της συγκατάθεσης επεξεργασίας των προσωπικών δεδομένων και ονομάζεται δικαίωμα γενικής αντίρρησης. Τα μητρώα της Αρχής πρέπει να συμβουλεύονται οι υπεύθυνοι επεξεργασίας δεδομένων, προκειμένου να μην περιλαμβάνουν τα συγκεκριμένα πρόσωπα στα αρχεία τους

Μια δεύτερη διάκριση του δικαιώματος αντίρρησης είναι το δικαίωμα σχετικής αντίρρησης, όπου το υποκείμενο απευθύνεται εγγράφως σε συγκεκριμένο υπεύθυνο επεξεργασίας για συγκεκριμένα προσωπικά δεδομένα και ζητά εγγράφως συγκεκριμένες ενέργειες στις οποίες οφείλει να προβεί ο υπεύθυνος επεξεργασίας. Ο νόμος προβλέπει κάποιες ενδεικτικές ενέργειες, αλλά μπορεί να ζητηθούν και άλλες ενέργειες.

Ο υπεύθυνος είναι υποχρεωμένος να απαντήσει γραπτώς, ρητώς και τεκμηριωμένα εντός δεκαπέντε ημερών, ενώ σε περίπτωση που αρνηθεί, κοινοποιεί την απάντησή του στην Αρχή Προστασίας. Εφόσον το υποκείμενο δεν ικανοποιηθεί ή δε λάβει απάντηση, μπορεί να προσφύγει στην Αρχή, η οποία δικαιούται να επέμβει στην επεξεργασία, εφόσον κριθεί σκόπιμο.

7.1.7.4 Δικαίωμα Προσωρινής Δικαστικής Προστασίας.

Καθένας έχει δικαίωμα να ζητήσει από το αρμόδιο δικαστήριο την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει. Έτσι ο νόμος καθιερώνει το δικαίωμα προσωρινής δικαστικής προστασίας του υποκειμένου των δεδομένων, ενώπιον του αρμόδιου δικαστηρίου σε περίπτωση που αποφάσεις διοικητικών αρχών οι οποίες το αφορούν στηρίζονται σε αξιολόγηση πτυχών της προσωπικότητάς του και λαμβάνονται αποκλειστικά με αυτοματοποιημένη επεξεργασία των στοιχείων.

7.2 Νόμος 3471/2006 «Προστασία Δεδομένων Προσωπικού Χαρακτήρα και της Ιδιωτικής Ζωής στον Τομέα των Ηλεκτρονικών Επικοινωνιών και τροποποίηση του ν. 2472/1997».

Οι διαρκώς εξελισσόμενες τεχνολογίες στα δημόσια δίκτυα επικοινωνίας επέβαλλαν την προσαρμογή των νομοθετικών ρυθμίσεων, με σκοπό την πληρέστερη διασφάλιση της προστασίας των προσωπικών δεδομένων που χρησιμοποιούν τις προσφερόμενες υπηρεσίες ηλεκτρονικής επικοινωνίας (Α. Αλεξανδρίδου, 2004).

Η Ευρωπαϊκή Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, η οποία αντικατέστησε την Οδηγία 97/66/ΕΚ, θέλησε να προσαρμόσει τη νομοθεσία στις εξελίξεις της αγορά και των τεχνολογιών, ώστε να παρέχεται σε όλους τους χρήστες το ίδιο επίπεδο προστασίας, ανεξάρτητα από τις χρησιμοποιούμενες τεχνολογίες. Η παραπάνω Οδηγία θεσμοθετήθηκε στα ελληνικά πλαίσια με τον Ν. 3471/2006.

Οι διατάξεις του ν. 3471/2006, αποτελούν συμπλήρωση και εξειδίκευση του ν. 2472/1997. Οι ρυθμίσεις του ν. 3471/2006 εφαρμόζονται μόνο δημόσια δίκτυα επικοινωνίας και στις διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικής επικοινωνίας. Ο ν. 3471/2006 διασφαλίζει το απόρρητο των επικοινωνιών φυσικών και νομικών προσώπων, τα εξωτερικά στοιχεία της επικοινωνίας, τα δεδομένα κίνησης και τα δεδομένα θέσης. Επιπλέον περιλαμβάνονται λεπτομερείς ρυθμίσεις για την αναλυτική χρέωση των παρεχόμενων υπηρεσιών, για την ένδειξη ταυτότητας και περιορισμό αναγνώρισης καλούσαν και συνδεδεμένης γραμμής, για τις προϋποθέσεις νόμιμης αυτόματης προώθησης κλήσεων, για τους δημόσιους καταλόγους συνδρομητών σε έντυπη ή ηλεκτρονική μορφή, για τις μη ζητηθείσες επικοινωνίες με σκοπό την άμεση προώθηση προϊόντων ή υπηρεσιών ή τη διαφήμιση, για την ασφάλεια των υπό επεξεργασία δεδομένων. Επίσης ορίζει την Αρχή Προστασίας Προσωπικών Δεδομένων και την Αρχή Διασφάλισης του Απορρήτου και των Επικοινωνιών στην εποπτεία εφαρμογής του νόμου.

7.3 Αρχή Προστασίας των Προσωπικών Δεδομένων.

Η Αρχή Προστασίας Προσωπικών Δεδομένων, αποτελεί ανεξάρτητη αρχή, η οποία λειτουργεί από το Νοέμβριο του 1997, υπάγεται στον Υπουργό Δικαιοσύνης και εδρεύει στην Αθήνα. Η Αρχή δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο και η αποστολή της είναι η εποπτεία της εφαρμογής του Ν. 2472/1997. Κατά την άσκηση των καθηκόντων τους τα μέλη της Αρχής απολαύουν προσωπικής και λειτουργικής ανεξαρτησίας (άρθρο 15§2). Ο Πρόεδρος και τα μέλη της Αρχής διορίζονται με ορισμένη θητεία, η οποία είναι τετραετής και μπορεί να ανανεωθεί

μόνο μία φορά . Η σύνθεση των έξι μελών, ανανεώνεται κατά το ήμισυ ανά διετία. Μετά τη δεύτερη συγκρότηση της Αρχής γίνεται κλήρωση μεταξύ των έξι τακτικών μελών της, ώστε τρία να έχουν τετραετή θητεία και τρία διετή. Με σκοπό τη διασφάλιση της ανανέωσης και της αναγκαίας συνέχειας της Αρχής, τα μέλη δεν μπορούν , κατά τη διάρκεια της θητείας, να απομακρυνθούν παρά μόνο για σοβαρή αιτία.

Οι αρμοδιότητες της Αρχής είναι ευρύτατες (άρθρο 19) και συνοψίζονται κυρίως στις εξής:

- ✓ στη συνδρομή για την κατάρτιση Κωδίκων δεοντολογίας από τις ενδιαφερόμενες ενώσεις φυσικών ή νομικών προσώπων ή τα διάφορα επαγγελματικά σωματεία,
- ✓ στη διεξαγωγή διοικητικών εξετάσεων και ελέγχων. Οι έλεγχοι διενεργούνται είτε αυτεπαγγέλτως, είτε κατόπιν καταγγελίας σε οποιοδήποτε αρχείο, χωρίς να μπορεί να αντιταχθεί στην Αρχή κανενός είδους απόρρητο, με μόνη εξαίρεση τα στοιχεία ταυτότητας συνεργατών που περιέχονται σε αρχεία που τηρούνται για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.
- ✓ στην επιβολή κυρώσεων, σύμφωνα με το άρθρο 21,
- ✓ στην έκδοση κανονιστικών πράξεων για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων στα οποία αναφέρεται ο νόμος,
- ✓ στην έκδοση οδηγιών, ώστε να καταστεί ευκολότερη και σαφέστερη η εφαρμογή των επιταγών του νόμου, με σκοπό την αποτελεσματικότερη προστασία των προσωπικών δεδομένων, μέσω της ενιαίας εφαρμογής της χρήσης αυτών των τελευταίων σε διάφορους τομείς,
- ✓ σε συστάσεις που αυτή απευθύνει στους υπεύθυνους επεξεργασίας και δίδει κατά την κρίση της περαιτέρω δημοσιότητα σε αυτές,
- ✓ στη χορήγηση αδειών που προβλέπονται από τις σχετικές διατάξεις του νόμου και καθορίζει το ύψος των σχετικών παραβόλων,
- ✓ στη γνωμοδότηση για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία των προσωπικών δεδομένων,
- ✓ στην εξέταση παραπόνων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων,

- ✓ στη συνεργασία με αντίστοιχες αρχές άλλων κρατών μελών της Ε.Ε και του Συμβουλίου της Ευρώπης σε ζητήματα σχετικά με την άσκηση των αρμοδιοτήτων της,
- ✓ στην καταγγελία των παραβάσεων των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές,
- ✓ στην ανακοίνωση στη Βουλή τυχόν παραβάσεων των ρυθμίσεων για την προστασία του προσώπου από την επεξεργασία προσωπικών δεδομένων και
- ✓ στην υποβολή στον Πρόεδρο της Βουλής και τον Πρωθυπουργό ετήσιας έκθεσης για τη δράση της και την κατάσταση προστασίας προσωπικών δεδομένων.

7.4 Αποφάσεις Αρχής.

Η εξέλιξη και διάδοση των νέων τεχνολογιών επεξεργασίας, και ειδικά το άνοιγμα των αγορών και η ανάγκη για αύξηση των πωλήσεων αποτελούν πλέον τις βασικές συνιστώσες της μαζικής συλλογής και επεξεργασίας από τον ιδιωτικό τομέα με κατεξοχήν σκοπό την επίτευξη κέρδους. Η Αρχή μέσα από τις αποφάσεις της προσπάθησε να δημιουργήσει ένα επαρκές ρυθμιστικό σύστημα ελέγχου, το οποίο θα καθιστά τις σχέσεις αυτές –ειδικά για τα υποκείμενα των δεδομένων– περισσότερο ισότιμες. Παρακάτω, παρατίθενται ενδεικτικά κάποιες αποφάσεις, οδηγίες και γνωμοδοτήσεις που έχει εκδώσει η Αρχή και αφορούν στην προστασία των προσωπικών δεδομένων στον τραπεζικό κλάδο.

- *Οδηγία 1/2005*.

Η Οδηγία 1/2005 της Αρχής αφορά στην ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας. Η οδηγία 1/2005 κατηγοριοποιεί τους τύπους των προσωπικών δεδομένων προς καταστροφή, ανάλογα με το μέσο που χρησιμοποιείται για την τήρηση και την περαιτέρω επεξεργασία τους. Έτσι, διακρίνει τα,

- ✓ προσωπικά δεδομένα σε έντυπη μορφή (έγγραφα),
- ✓ τα προσωπικά δεδομένα σε ηλεκτρονική μορφή που τηρούνται σε οποιοδήποτε φυσικό υπόστρωμα (σκληρούς δίσκους υπολογιστών, CD, DVD,

δισκέττες, κ.λ.π). Τα δεδομένα αυτά μπορεί να βρίσκονται είτε σε δομημένη μορφή (π.χ. βάση δεδομένων), είτε να αποτελούν ένα σύνολο επιμέρους ηλεκτρονικών αρχείων (π.χ. αρχεία κειμένου, εικόνες, κ.λ.π).

- ✓ Προσωπικά δεδομένα σε άλλη μορφή (π.χ. δεδομένα που τηρούνται σε βιντεοκασέτες, μικροφίλμ, κλπ).

Τα προσωπικά δεδομένα πρέπει να καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας αμέσως μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Το άρθρο 6 της οδηγία 1/2005, ορίζει την ασφαλή καταστροφή δεδομένων που τηρούνται σε ηλεκτρονική ή άλλη μορφή. Στο άρθρο αυτό, καθιστά σαφές ότι σε ότι αφορά στα ηλεκτρονικά αρχεία η ασφαλής καταστροφή δεν επαρκεί η απλή διαγραφή τους με την εντολή «DELETE», καθώς κατά τον τρόπο αυτό διαγράφεται μόνο η αναφορά στα δεδομένα, ενώ τα ίδια τα δεδομένα ενδέχεται να είναι ανακτήσιμα με χρήση ειδικών προγραμμάτων λογισμικού. Ο ενδεικνυόμενος τρόπος για την ασφαλή καταστροφή των δεδομένων που είναι αποθηκευμένα σε επανεγγράψιμα μέσα είναι η αλλοίωση των δεδομένων μέσω της αντικατάστασης τους με τυχαίους χαρακτήρες (overwrite). Στην περίπτωση της καθημερινής καταστροφής δεδομένων, ένας εναλλακτικός τρόπος καταστροφής είναι η μορφοποίηση του υλικού υποστρώματος (format), ενώ στην περίπτωση της προγραμματισμένης καταστροφής του συνόλου των δεδομένων, ένας εναλλακτικός τρόπος καταστροφής είναι και η φυσική καταστροφή του ίδιου του υλικού υποστρώματος. Η καταστροφή των δεδομένων περιλαμβάνει και την καταστροφή όλων των αντιγράφων ασφαλείας (back up) που τηρεί ο υπεύθυνος επεξεργασίας. Σε κάθε περίπτωση, η προγραμματισμένη καταστροφή των δεδομένων πρέπει να συνοδεύεται από πρωτόκολλο καταστροφής.

- *Απόφαση129/2012.*

Η παραπάνω απόφαση της Αρχής επέβαλλε πρόστιμο σε τράπεζα, λόγω παραβίασης του άρθρου 10 του Ν. 2472/1997. Συγκεκριμένα, παραδόθηκαν έγγραφα στην Αρχή, τα οποία ευρέθησαν έξω από τα καταστήματα της εν λόγω τράπεζας και περιελάμβαναν φωτοτυπίες δελτίων ταυτότητας, διαβατηρίου, αντίγραφα εκκαθαριστικών σημειωμάτων της εφορίας, στοιχεία σχετικά με δάνεια πελατών –

φυσικών προσώπων, φωτοτυπίες επιταγής πελάτη – φυσικού προσώπου, φωτοτυπία κάρτας παραμονής αλλοδαπού, στοιχεία σχετικά με λογαριασμούς καρτών πελατών – φυσικών προσώπων, λίστα ακάλυπτων επιταγών στοιχείων που περιλαμβάνονται στο αρχείο του Τειρεσία, επικοινωνία πελατών σχετικά με την υπηρεσία e-banking. Τα παραπάνω έγγραφα βρέθηκαν σε παραπάνω από ένα καταστήματα την Τράπεζας, γεγονός που υποδηλώνει ελλείψεις στα μέτρα ασφάλειας που εφαρμόζονται από τα καταστήματα της τράπεζας. Η Αρχή, εξετάζοντας τα παραπάνω στοιχεία επέβαλε πρόστιμο ύψους 50.000 ευρώ στην Τράπεζα και την κάλεσε να εφαρμόσει πλήρως τις διατάξεις της Οδηγίας 1/2005 της Αρχής σχετικά με την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού επεξεργασίας.

- *Απόφαση 1661/2000.*

Η απόφαση 1661/2000 της Αρχής κατέλυσε μια διαδεδομένη πρακτική η οποία επικρατούσε στον τραπεζικό χώρο και η οποία επέμενε να αγνοεί και να παραβιάζει θεμελιώδη δικαιώματα συνδιαλλασσομένων με τράπεζες, μέσω της παράνομης επεξεργασίας των προσωπικών τους δεδομένων. Σε αυτή την περίπτωση, τράπεζα έστειλε επιστολή σε δημόσια υπηρεσία ενημερώνοντάς την για τις οφειλές υπαλλήλων της, λόγω μη έγκαιρης αποπληρωμής δανείων τους. Οι τελευταίοι προσέφυγαν ενώπιον της Αρχής, δεν έχει ζητηθεί η συγκατάθεση τους για τη διαβίβαση που πραγματοποίησε η τράπεζα. Έτσι, σύμφωνα με την Αρχή, η τράπεζα έπρεπε να παύσει άμεσα τη διαβίβαση σε δημόσιες υπηρεσίες στοιχείων σχετικών με τις υποχρεώσεις και οφειλές πελατών της, χωρίς την προηγούμενη ενημέρωση και συγκατάθεση αυτών, σύμφωνα με τα άρθρα 11§3 και 5§1, αλλά και να λάβει τα κατάλληλα μέτρα, μέσω της πληροφόρησης του προσωπικού της, έτσι ώστε να αποφευχθούν παρόμοια φαινόμενα στο μέλλον.

- *Απόφαση 57/2013.*

Ύστερα από αίτηση στην Αρχή, ο πελάτης της τράπεζας παραπονείται για παράνομη επεξεργασία των προσωπικών του δεδομένων καθώς και για μη ικανοποίηση του δικαιώματος πρόσβασης που άσκησε προς την Τράπεζα. Πιο συγκεκριμένα, ο προσφεύγων ισχυρίζεται ότι υπήρξε αθέμιτη πρόσβαση στα στοιχεία που τον αφορούν και τηρούνται από την ΤΕΙΡΕΣΙΑΣ Α.Ε. τα οποία διαβιβάστηκαν

στη συνέχεια σε συγγενικό του μη δικαιούμενο πρόσωπο. Προκειμένου να ενημερωθεί για το ποιες οικονομικές μονάδες αναζήτησαν προσωπικά του δεδομένα, ο προσφεύγων υπέβαλε αίτηση προς τη «ΤΕΙΡΕΣΙΑΣ Τραπεζικά Συστήματα Πληροφοριών Α.Ε.», η οποία του γνωστοποίησε τα τραπεζικά καταστήματα από τα οποία έγιναν οι αναζητήσεις των οικονομικών του στοιχείων. Στη συνέχεια ο προσφεύγων απέστειλε εξώδικη επιστολή με την οποία ζητούσε να του γνωρίσει η τράπεζα ποιός είναι ο υπεύθυνος χειριστής επεξεργασίας και μετάδοσης των προσωπικών του δεδομένων, σε ποιόν τρίτο και μετά από ποια δική του ενυπόγραφη συγκατάθεση ανακοινώθηκαν προσωπικά οικονομικά του δεδομένα και για ποιό λόγο έλαβε χώρα επεξεργασία προσωπικών οικονομικών του δεδομένων, ενώ, όπως ισχυρίζεται ο ίδιος, ουδέποτε είχε οποιαδήποτε συναλλακτική σχέση με την τράπεζα, όμως δεν πήρε απάντηση από την τράπεζα στο ως άνω έγγραφο.

Η Αρχή αποφάνθηκε ότι σύμφωνα με το άρθρο 5 παρ. 1 του ν.2472/97, κάθε επεξεργασία προσωπικών δεδομένων, για να είναι νόμιμη, πρέπει να πραγματοποιείται με τη συγκατάθεση των υποκειμένων των δεδομένων, εν προκειμένω των συναλλασσομένων με την τράπεζα. Επίσης σύμφωνα με το άρθρο 12 του ν.2472/97, το υποκείμενο των δεδομένων έχει δικαίωμα να ζητεί και να λαμβάνει από τον υπεύθυνο επεξεργασίας, χωρίς καθυστέρηση και κατά τρόπο εύληπτο και σαφή, όλα τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, καθώς και την προέλευσή τους, τους σκοπούς της επεξεργασίας, τους αποδέκτες, την εξέλιξη και τη λογική της αυτοματοποιημένης επεξεργασίας. Η Αρχή επέβαλε στην Τράπεζα χρηματικό πρόστιμο δέκα χιλιάδων (10,000.00) ευρώ, από τα οποία επτά χιλιάδες για παράβαση του άρθρου 5 παρ.1 και 2 και τρεις χιλιάδες (3,000.00) για παράβαση του άρθρου 12 του ν.2472/97 και προειδοποίησε την Τράπεζα να εξετάσει και να λάβει μέτρα για την πρόληψη παρόμοιων περιστατικών.

7.5 Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου COM(2012) (Βρυξέλλες, 27.1.2012).

Οι ραγδαίες τεχνολογικές εξελίξεις δημιουργούν νέες προκλήσεις για την προστασία των

δεδομένων προσωπικού χαρακτήρα και η ευρωπαϊκή επιτροπή ήδη από το 2012 έχουν προτείνει Κανονισμό για την «προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Στόχος του Κανονισμού είναι η βελτίωσης της ασφάλειας των προσωπικών δεδομένων και επιχειρήσεις του τομέα να μην είναι υποχρεωμένες να εφαρμόζουν διαφορετικούς κανόνες σε κάθε ένα κράτος μέλος της Ένωσης. Ήδη τέσσερις συναρμόδιες επιτροπές του Ευρωπαϊκού Κοινοβουλίου έχουν εγκρίνει τις εισηγήσεις τους ενώ η τελική αποφασιστική ψηφοφορία στην ολομέλεια θα έχει πραγματοποιηθεί μέχρι τις ευρωεκλογές (http://www.europarl.europa.eu/sides/, 26.1.2014).

Κάποια από τα βασικά σημεία του Κανονισμού εστιάζουν σε ζητήματα που δεν έχουν απασχολήσει ξανά τη νομοθεσία. Αυτά είναι:

- *Το δικαίωμα στη «λήθη»*. Η Ευρωπαϊκή Επιτροπή προβλέπει ότι καθένας θα έχει το δικαίωμα να ζητήσει την απαλοιφή όλων των προσωπικών στοιχείων του από τις βάσεις δεδομένων των επιχειρήσεων που τα συλλέγουν ή στα οποία οι ίδιοι τα «ανεβάζουν».
- *Η υποχρέωση για συγκατάθεση*. Οι επιχειρήσεις θα μπορούν να επεξεργασθούν τα στοιχεία μόνον αφού λάβουν προς τούτο τη συγκατάθεση των χρηστών η συγκατάθεση θα ισχύει για συγκεκριμένη χρήση και θα πρέπει να ανανεώνεται για κάθε πρόσθετη «αξιοποίηση» των στοιχείων.
- *«Προφάιλινγκ»*. Η πρακτική της ανίχνευσης της πιθανής συμπεριφοράς ή επιδόσεων ενός ατόμου με βάση την οικονομική του κατάσταση, την υγεία, τις προτιμήσεις ή ακόμα την καταγεγραμμένη συμπεριφορά του μέσω αυτοματοποιημένης ανάλυσης στοιχείων που βρίσκονται στο διαδίκτυο. Στόχος είναι και η πρακτική αυτή να απαιτεί την συναίνεση του ατόμου που την υφίσταται.

Ο κανονισμός σημειώνει ότι κάθε επιχείρηση και δημόσιος φορέας θα πρέπει να παραθέτει αναλυτική εξήγηση των μέτρων προστασίας που εφαρμόζει για τα δεδομένα των πολιτών - καταναλωτών που και υπό ορισμένες συνθήκες να έχει ειδικό υπάλληλο επιφορτισμένο και υπεύθυνο για τέτοια ζητήματα. Μάλιστα έχει προτείνει ότι ένας τέτοιος υπάλληλος να είναι υποχρεωτικός σε επιχειρήσεις που έχουν

περισσότερους από 250 εργαζομένους. Για την εφαρμογή όλων των ανωτέρω προβλέπονται σημαντικά πρόστιμα που μπορούν να φθάνουν το 1 εκατομμύριο ευρώ ή το 2% του ετήσιου κύκλου εργασιών της επιχείρησης.

ΚΕΦΑΛΑΙΟ VIII

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ.

Η αλματώδης εξέλιξη της τεχνολογίας έφερε πρωτόγνωρες αλλαγές στις σύγχρονες συναλλαγές. Τα πληροφοριακά συστήματα τυγχάνουν ευρείας εφαρμογής και απήχησης στις καθημερινές δραστηριότητες. Οι σύγχρονες επιχειρήσεις έχουν οργανώσει τη λειτουργία τους με τη βοήθεια των πληροφοριακών συστημάτων, καθώς επιτελούν εργασίες που στο κοντινό παρελθόν έμοιαζαν χρονοβόρες και δυσεπίλυτες. Οι Τράπεζες ως σύγχρονες επιχειρήσεις εφαρμόζουν τα πληροφοριακά συστήματα στο σύνολο των καθημερινών τους εργασιών. Η ηλεκτρονική τραπεζική διευκόλυνε την απελευθέρωση των χρηματοοικονομικών συναλλαγών, παρέχοντας τη δυνατότητα διεκπεραίωσης πλήθος συναλλαγών εύκολα, γρήγορα, από οποιοδήποτε γεωγραφικό σημείο και ανά πάσα στιγμή μέσα στη διάρκεια του εικοσιτετραώρου.

Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων προσπαθεί να βρει μεθόδους και να αναπτύξει συστήματα, τα οποία θα είναι δύσκολο να προσπελαστούν από άτομα χωρίς εξουσιοδοτημένη πρόσβαση γιατί τα δεδομένα και οι πληροφορίες που διακινούνται μεταξύ των συστημάτων αυτών είναι σπουδαίας σημαντικότητας και οποιαδήποτε παράνομη εισβολή μπορεί να προκαλέσει ανεπανόρθωτες ζημίες, σε οικονομικό επίπεδο και επίπεδο φήμης και πελατείας σε έναν τραπεζικό όμιλο. Η ασφάλεια των τραπεζικών πληροφοριακών συστημάτων μπορεί να διασπαστεί από τυχαίες ενέργειες, αλλά και από ηθελημένες παράνομες ενέργειες. Κλειδί για την αποτελεσματική ασφάλεια των Τραπεζικών Πληροφοριακών Συστημάτων, αποτελεί ο ανθρώπινος παράγοντας αφού πλήθος ηλεκτρονικών απατών βασίζεται στην ανθρώπινη αδυναμία.

Οι ελληνικοί τραπεζικού όμιλοι εφαρμόζουν αρκετά αποτελεσματικά τα μέτρα ασφαλείας της ηλεκτρονική τραπεζικής, προσφέροντας ένα ασφαλές

περιβάλλον στις ηλεκτρονικές συναλλαγές των χρηστών τους. Για την άριστη απόδοση των μέτρων ασφάλειας στα πληροφοριακά συστήματα των τραπεζών θα πρέπει λάβει μέτρα και ο ίδιος ο χρήστης. Η σωστή αντίληψη και εκπαίδευση του χρήστη των ηλεκτρονικών υπηρεσιών, μπορεί να παίξει πρωταρχικό ρόλο στη ασφάλεια των ηλεκτρονικών συναλλαγών του γιατί στην πλειονότητα των ηλεκτρονικών επιθέσεων ο άμεσος στόχος δεν είναι η Τράπεζα αλλά ο πελάτης.

Ιδιαίτερη σημασία για την ηλεκτρονική τραπεζική έχει η προστασία των προσωπικών δεδομένων των χρηστών. Οι χρήστες της ηλεκτρονική τραπεζικής για να μπορέσουν να εμπιστευτούν την ηλεκτρονική τραπεζική και να επωμιστούν τα οφέλη που παρέχει θα πρέπει να είναι σίγουροι ότι δεν θα υποκλαπούν τα προσωπικά τους δεδομένα και δεν διοχετευθούν πουθενά χωρίς τη ρητή τους συγκατάθεση. Ο νόμος 2472/1997 και έπειτα ο συμπληρωματικός νόμος 3471/2006 εξασφαλίζουν τα νόμιμα δικαιώματα των χρηστών και διασφαλίζουν την νομιμότητα της επεξεργασίας των προσωπικών δεδομένων που διακινούνται μέσω των τραπεζικών πληροφοριακών συστημάτων. Άλλωστε είναι θεμελιώδες το δικαίωμα του κάθε ατόμου στον πληροφοριακό αυτοκαθορισμό.

Νέα κανάλια ηλεκτρονικών συναλλαγών όπως το mobile banking αρχίζουν να αναπτύσσονται με δυναμικούς ρυθμούς και οι μελέτες θα πρέπει να είναι προσανατολισμένες στην ασφάλεια των νέων συστήματα ηλεκτρονικών συναλλαγών, γιατί παρουσιάζονται εξαιρετικά ευάλωτα στις ηλεκτρονικές απειλές. Οι τράπεζες από την πλευρά τους θα πρέπει να εστιάσουν σε θέματα εκπαίδευσης των χρηστών της ηλεκτρονικής τραπεζικής καθώς και των υπαλλήλων των τραπεζών. Η επιστήμη των πληροφοριακών συστημάτων διαρκώς εξελίσσεται και θα πρέπει να συνεχισθούν οι τεχνικές και θεωρητικές έρευνες για τη δημιουργία πιο ασφαλών και αποδοτικών Πληροφοριακών Συστημάτων.

Μαζί με την τεχνολογική εξέλιξη θα πρέπει όμως να εκσυγχρονιστεί και η νομολογία, η οποία θα πρέπει να είναι στις επάλξεις και να «αντιδρά» ανά πάσα στιγμή σε θέματα που δεν καλύπτονται από τη ισχύουσα ελληνική νομοθεσία.

ΚΑΤΑΛΟΓΟΣ ΑΝΑΦΟΡΩΝ

1. Αγγέλης, Β. (2005), Η βίβλος του e-banking, Αθήνα: Εκδόσεις Νέων Τεχνολογιών ΕΠΕ.
2. Αλεξανδρής Ν., Γκρίτζαλης Δ., Κιουντούζης Ε. (1995), Μια προσέγγιση της κοινωνικά αποδεκτής αξιοποίησης της Πληροφορικής σε ΕΠΥ, Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα.
3. Αλεξανδρίδου, Ε. (2004), Το δίκαιο του ηλεκτρονικού εμπορίου, Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.
4. Αλεξανδροπούλου- Αιγυπτιάδου, Ε. (2007), Προσωπικά δεδομένα, Αθήνα-Κομοτηνή: Εκδόσεις Σάκκουλα.
5. Αναστασιάδης, Π. (2000), Στον Αιώνα της Πληροφορίας. Αθήνα, Εκδόσεις Λιβάνη**.**
6. Αραβαντινός, Γ. (1997), Η προστασία των στοιχείων προσωπικού χαρακτήρα από την αθέμιτη επεξεργασία τους με ηλεκτρονικό υπολογιστή, Αθήνα-Κομοτηνή: Εκδόσεις Σάκκουλα.
7. Αυγουστιανάκης, Μ., Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων. Προβλήματα και αντιμετώπιση από το δίκαιο, ΔτΑ `11(2001)**.**
8. Γέροντας, Α. (1991), Το δικαίωμα της αυτοδιάθεσης των πληροφοριών-Υπερβολή ή αναγκαιότητα.
9. Γέροντας, Α. (2002), Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, Αθήνα- Κομοτηνή: Εκδόσεις Σάκκουλα.
10. Γιαννόπουλος Γ. (2003), «Internet banking: Νομικά Ζητήματα Από τη Διεξαγωγή Τραπεζικών Συναλλαγών στο Διαδίκτυο», Δελτίο Ένωσης Ελληνικών Τραπεζών.
11. Κάτσικας Σωκράτης Κ., Γκριτζάλης Δ., Γκριτζάλης Σ. (2003), Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε Περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης, Αθήνα: Εκδόσεις Παπασωτηρίου.

12. Καρέκλης Π. (2003), «Επιπτώσεις του Internet στη λειτουργία και Κερδοφορία των Επιχειρήσεων. Οφέλη Από τη Χρήση Υπηρεσιών Ηλεκτρονικής Τραπεζικής», Δελτίο Ένωσης Ελληνικών Τραπεζών.
13. Κάτος Β.Α., Στεφανίδης Γ.Χ. (2003), Τεχικές Κρυπτογραφίας & Κρυπτανάλυσης, Θεσσαλονίκη, Εκδόσεις Ζυγός.
14. Κάτσικας Σωκράτης Κ., Γκριτζάλης Δ., Γκριτζάλης Σ. (2004), Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών.
15. Γκόρτσος Χρ., Τσάκος Κ. (2003), "Το ευρωπαϊκό κοινοτικό δίκαιο για την ηλεκτρονική τραπεζική", Δελτίο Ένωσης Ελληνικών Τραπεζών.
16. Λουκέρης, Γ., Εναρμόνιση του δικαίου προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση, NoB 45 (1997).
17. Μήτρου, Λ., (1999), Η Αρχή Προστασίας Προσωπικών Δεδομένων, Αθήνα-Κομοτηνή.
18. Μήτρου, Λ., Η νέα Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ΔιμΕΕ 1(2004).
19. Παγκάλος Γ. & Μαυρίδης Ι. (2002), Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων, Εκδόσεις Ανικούλα.
20. Παπαδόπουλος, Α.
21. Παπαθανασίου, Ε. (2008), ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ: Θεωρία και Εφαρμογές, Αθήνα: Εκδόσεις Γκιούρδας
22. Σινανιώτη – Μαρούδη Αριστέα, Φαρσαρώτας Ιωάννης Δ. (2005), Ηλεκτρονική Τραπεζική, Εκδόσεις Σάκκουλα.
23. Ν. Σκανδάμης ,(1997), Ευρωπαϊκό Δίκαιο –θεσμοί και έννομες τάξεις της ευρωπαϊκής Ένωσης, Εκδόσεις Σάκκουλα.
24. Ταβλαρίδης Κ.(2000), «Η προστασία των καταναλωτών στην ηλεκτρονική τραπεζική», Δελτίο Ένωσης Ελληνικών Τραπεζών.
25. Τσάμης, Α. (2003), "Εξελίξεις, διαπιστώσεις και διλήμματα στη σύγχρονη ηλεκτρονική τραπεζική", Δελτίο Ένωσης Ελληνικών Τραπεζών.
26. Χοχλιούρος Ι. (2006), Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών: Διασφάλιση του απορρήτου και νόμιμη παρακολούθηση των επικοινωνιών, Αθήνα: Εκδόσεις Σάκκουλα.

27. Κ. Χριστοδούλου, Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία, 2001
28. Claessens J., Dem V, De Cock D., Preneel B., Vandewalle J., "On the Security of Today's Online Elecrtonic Banking Systems", Coputers & Security, Vol 21, No 3, pp 257-269.
29. Davis, G.B., & Olson, M.H. (1985), Management Information Systems, conceptual foundation, structure and development, 2nd. New York, McGraw-Hill.
30. Denning E. D., & Denning J. D. (1979), "Data Security", Vol. 11, No. 3.
31. ELTRUN (2011), «Η Σημασία της Ηλεκτρονικής Τραπεζικής για τους Πολίτες και την Εθνική Οικονομία», Issue No. 65.
32. Essinger, J., (1999), *The Virtual Banking Revolution. The Customer the Bank and the Future*. International Thomson Publishing Company. London.
33. Laudon, K. C., & Laudon, J.P. (2009), Πληροφοριακά Συστήματα Διοίκησης, Εκδόσεις Κλειδάριθμος
34. Ziqi L., Michael T.C., (2002), "Internet- based e-banking and consumer attitudes an empirical study", Information & Management, Vol 39, pp 283-295

ΝΟΜΟΘΕΤΙΚΑ ΚΕΙΜΕΝΑ

1. Σύμβαση του Συμβουλίου της Ευρώπης "για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Πληροφοριών Προσωπικού Χαρακτήρα» **(Σύμβαση 108 της 28-1-1981).**
2. **Οδηγία 95/46/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» (L 282/23-11-1995).
3. 4. **Ν.2472/10-4-1997 (ΦΕΚ 50 Α')** "Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα".
4. Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (COM (2012 11 final) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)

ΙΣΤΟΣΕΛΙΔΕΣ

1. **http://www.alpha.gr/ (**προσπελάστηκε στις 15.12.2013**)**
2. **http://www.piraeusbank.gr/ (**προσπελάστηκε στις 15.12.2013**)**
3. **http://www.eurobank.gr/ (**προσπελάστηκε στις 15.12.2013**)**
4. **http://www.nbg.gr/ (**προσπελάστηκε στις 15.12.2013**)**
5. "Ηλεκτρονικές Απάτες» διαθέσιμο στο: **http://www.saferinternet.gr/index.php?parentobjId=Page2&objId=Category37&childobjId=Category116#Text358 (**προσπελάστηκε στις 11.1.2014).
6. **"**Phishing" διαθέσιμο στο: http://el.wikipedia.org/w/index.php?title=Phishing&veaction=edit (προσπελάστηκε στις 5.1.2014).