ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ
ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας

Τμήμα λογιστικής

Θέμα:
Τεχνολογίες ταυτοποίησης χρηστών με βάση την ιδιωτικότητα - προστασία προσωπικών δεδομένων

Παπούλια, Ηλίανα
Καριτζη Ευαγγελία
Σουλτάνης Χρήστος

Επιβλέπων καθηγητής: Φωτεινόπουλος Μιχαήλ

ΠΑΤΡΑ-2017

Περιεχόμενα

Πίνακας εικόνων

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία ολοκληρώθηκε στο πλαίσιο ολοκλήρωσης των σπουδών μας στο ΤΕΙ Δυτικής Ελλάδας, στο τμήμα λογιστικής. Η εργασία πραγματεύεται το ζήτημα της ιδιωτικότητας και της προστασία των προσωπικών δεδομένων σε ένα περιβάλλον που με την είσοδο του διαδικτύου στην ζωή μας δείχνει να είναι πιο ευάλωτα από ποτέ. Η τεχνολογία και η πρόοδος της έχει συντελέσει τόσο στην εύκολη υποκλοπή τέτοιων στοιχείων αλλά και στην αποθήκευση τεράστιων δεδομένων που μπορούν να επεξεργαστούν και να προσπελαστούν με τεράστιες ταχύτητες. Δυνατότητες που κάνουν την ιδιωτικότητα και τα προσωπικά δεδομένα ευάλωτα σε κακόβουλους χρηστές και λογισμικά. Από την άλλη όμως η τεχνολογία προσφέρει και δυνατότητες προστασίας αυτών των στοιχείων μέσο της απαίτησης προσωπικών κωδικών για κάποιον χρηστή ώστε να έχει πρόσβαση σε τέτοια στοιχεία, μέσω βιομετρικών χαρακτηριστικών κλπ.

ABSTRACT

This work was completed within the framework of the completion of our studies at the TEI of Western Greece, in the accounting department. The work deals with the issue of privacy and the protection of personal data in an environment that is more vulnerable than ever before with the advent of the internet. Technology and its progress has contributed to both the easy interception of such data and the storage of huge data that can be processed and accessed at enormous speeds. Features that make privacy and personal data vulnerable to malicious users and software. On the other hand, technology also offers protection for these elements by requiring personal passwords for a user to access such data through biometric features et.al.

ΕΙΣΑΓΩΓΗ

Στην παρούσα εργασία παρουσιάζονται οι τεχνολογίες που είναι αναγκαίες για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων. Σε μια εποχή που το διαδίκτυο και τα πληροφορικά συστήματα αποτελούν αναπόσπαστο στοιχειό της καθημερινής ζωής ενός ατόμου. Οι τεχνολογίες αυτές στοχεύουν στην προστασία και την ασφάλεια της ιδιωτικότητα και των προσωπικών δεδομένων. Οι εργασία αναπτύσσεται σε τρεις ενότητες σε μια προσπάθεια κάλυψης αυτών των μεγάλων σε έκταση και πολυπλοκότητα ζητημάτων.

Στην πρώτη ενότητα προσδιορίζεται αρχικά η έννοια της ιδιωτικότητας και των προσωπικών δεδομένων. Ακολούθως περιγράφονται ιστορικά στοιχεία μέσα από διεθνείς αποφάσεις και κατοχυρώσεις των δικαιωμάτων για την προστασία των προσωπικών δεδομένων. Στην συνέχεια προσδιορίζονται το ειδή που απειλούν την ιδιωτικότητα και τα προσωπικά δεδομένα στην σύγχρονη πραγματικότητα και η ενότητα ολοκληρώνεται με την παρουσίαση των ηλεκτρονικών μέσων και την σχέση τους με τα προσωπικά δεδομένα κυρίως από τις τεχνολογίες πιστοποίησης και προστασία των προσωπικών δεδομένων.

Στην επομένη ενότητα κρίθηκε αναγκαίο να προσδιοριστεί το νομικό πλαίσιο που προστατεύει τα προσωπικά δεδομένα τόσο σε διεθνές όσο και ευρωπαϊκό επίπεδο και να υπολογίζεται το ποσοστό ενσωμάτωσης των ευρωπαϊκών κανονισμών και οδηγιών στην ελληνική νομοθεσία για την προστασία των προσωπικών δεδομένων. Ακολούθως παρουσιάζονται οι τρόποι προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων. Στην συνέχεια παρουσιάζονται και αναλύονται τα συστήματα συλλογής και προστασίας των προσωπικών δεδομένων και στοιχείων. Τέλος η ενότητα ολοκληρώνεται με την παρουσίαση των πλεονεκτημάτων και των μειονεκτημάτων που διέπουν αυτές τις προσπάθειες.

Και η εργασία ολοκληρώνεται με τις προοπτικές που φαίνεται να προδιαγράφονται για τα προσωπικά δεδομένα και την ιδιωτικότητα. Στην συνέχεια παρουσιάζονται και αναλύονται τεχνολογικές και ανακαλύψεις πάνω στο ζήτημα της ιδιωτικότητας. Ακολούθως προσδιορίζεται οι αρχές που μελλοντικά θα διέπουν το σχεδιασμό των συστημάτων ταυτοποίησης και η εργασία ολοκληρώνεται με την παρουσίαση των μελλοντικών απαιτήσεων ασφάλειας.

ΚΕΦΑΛΑΙΟ_1: Προσδιοριστικά στοιχεία(ιδιωτικότητα, προσωπικά δεδομένα).

1.1 Ορισμοί ιδιωτικότητα, προσωπικά δεδομένα.

1.1.1 Ιδιωτητικότητα

Η πρώτη αναφορά που σχετίζεται με την αξία της ιδιωτικότητας υπάρχει το 1890 (Brandeis & Warre, 1980) όπου η ιδιωτικότητα συνδέεται με «*το δικαίωμα να μείνει κανείς μόνος του*» και προσδιορίζεται η αναγκαιότητα η έννοια να τεθεί υπό συνταγματική κατοχύρωση. Το 1948, το Γενικό Συμβούλιο των Ηνωμένων Εθνών στην «Παγκόσμια Δήλωση των Ανθρωπίνων Δικαιωμάτων» γίνεται μια γενική αφορά για το ζήτημα θέμα της ιδιωτικότητας και το 1950 η Ευρωπαϊκή Επιτροπή των Ανθρωπίνων Δικαιωμάτων διενεργεί καταστάσεις θεσμοθετήσεις του δικαιώματος σεβασμού της ιδιωτικής ζωής των ατόμων της. Η έννοια της ιδιωτικότητας, στην βάση του είδους και πλαίσιο των πληροφοριών, μπορεί να αποτελείται από την ακόλουθες μορφές (Rosenberg, 1992) :

- *Ιδιωτικότητα Πληροφοριών*: Που σχετίζεται με τον έλεγχο τους και πώς τα προσωπικά δεδομένα ενός προσώπου είναι δυνατόν να συληθούν, να αποθηκευτούν, να επεξεργαστούν ή να δημοσιοποιηθούν επιλεκτικά.
- *Εδαφική Ιδιωτικότητα*: Που σχετίζεται με την προστασία της στενής φυσικής περιοχής που περιβάλλει ένα άτομο, δηλαδή οικιακά και άλλα περιβάλλοντα, όπως για παράδειγμα ο εργασιακός ή ο δημόσιος χώρος.

- *Σωματική Ιδιωτικότητα*: Που σχετίζεται με την προστασία ενός ατόμου από αναίτια παρέμβαση, όπως ο σωματικός έλεγχος, η υποχρεωτική υποβολή σε εξέταση, πληροφορίες που παραβιάζουν την ηθική αίσθηση ενός ατόμου.

- *Ιδιωτικότητα Επικοινωνίας*: Σχετίζεται με τη προστασία της επικοινωνίας ενός προσώπου από μη εξουσιοδοτημένη παρακολούθηση.

Από τότε έχουν προταθεί και προκύψει πολλές κατηγοριοποιήσεις και αναδιατυπωσεις της έννοιας της ιδιωτικότητας στην βάση του πλαίσιου των πληροφοριών. Τα δεδομένα αναδείχθηκαν, σημασιοδοτήθηκαν και καθιερώθηκαν ως «ξεχωριστός» όρος και σε συνδυασμό με την επεξεργασία δεδομένων και κυρίως με την ανάπτυξη της αυτοματοποιημένης επεξεργασίας δεδομένων. Η συσχέτιση προσδιορίζει το “δεδομένο” ως τεχνικό όρο και τμήμα ενός συστήματος επεξεργασίας, και συμβάλει στον προσδιορισμό των “δεδομένων” ως στοιχείων μιας “επεξεργασμένης” πληροφορίας, ως στοιχεία της πληροφορίας που αποτέλεσε αντικείμενο αυτοματοποιημένης επεξεργασίας.

Στα περιβάλλοντα Ηλεκτρονικής Διακυβέρνησης, η συζήτηση για την ιδιωτικότητα και την προάσπισή της περιστρέφεται κυρίως γύρω από την ιδιωτικότητα των πληροφοριών και την ιδιωτικότητα της επικοινωνίας, καθώς δεν προκύπτουν ζητήματα άμεσα η εδαφική και σωματική ακεραιότητα (Auerbach, 2004).

Η επιτυχημένη παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης σχετίζεται σε μεγάλο βαθμό με τη διασφάλιση προάσπισης της ιδιωτικότητας των δεδομένων και πληροφοριών που χρησιμοποιούνται και αξιοποιούνται για την ολοκλήρωσή τους. Τα προσωπικά δεδομένα και πιο συγκεκριμένα η επεξεργασία τους χαρακτηρίζεται παράλληλα σε έναν από τους σημαντικότερους παράγοντες λήψης αποφάσεων στο πλαίσιο της άσκησης κρατικών καθηκόντων και αρμοδιοτήτων αλλά και γενικότερα της δραστηριότητας του Δημόσιου τομέα (Μήτρου, 2006).

Οι απειλές που προκύπτουν σχετίζονται με την χρήση του διαδικτύου ως μέσου επικοινωνίας, είτε αφορούν σε εδικότερα ζητήματα, όπως είναι η χρήση αναγνωριστικών χρηστών και η διασύνδεση δεδομένων και πληροφοριών (Ιγγλεζάκης, 2007).

1.1.2 Προσωπικά δεδομένα

Με βάση τα προσδιοριστικά χαρακτηριστικά της Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), στα προσωπικά εντάσσεται κάθε πληροφορία που προσδιορίζει και ταυτοποιεί ένα φυσικό πρόσωπο, όπως για παράδειγμα το όνομα, τη διεύθυνση, το τηλέφωνο, τα ενδιαφέροντα, οι φωτογραφίες και οι προσωπικές απόψεις. Ορισμένα προσωπικά δεδομένα προσδιορίζουν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής ζωής ενός ατόμου, όπως το θρήσκευμα, οι πολιτικές πεποιθήσεις, η κατάσταση της υγείας του ή η ερωτική ζωή του.

Στην Ελλάδα, στα "απλά" προσωπικά δεδομένα συμπεριλαμβάνονται:

- Το όνομα
- Το επώνυμο
- Η κατοικία
- Το επάγγελμα
- Το μορφωτικό επίπεδο
- Το εισόδημα
- Οι τραπεζικοί λογαριασμοί
- Οι καταναλωτικές συνήθειες
- Η ταξιδιωτική δραστηριότητα
- Η οικογενειακή κατάσταση
- Η περιουσιακή κατάσταση

Από την άλλη πλευρά, στα "ευαίσθητα" προσωπικά δεδομένα συγκαταλέγονται στοιχεία που σχετίζονται με τον "σκληρό πυρήνα" της ιδιωτικής ζωής του καθενός. Σε κάθε χώρα η έννοια της ιδιωτικής ζωής ή αλλιώς της ιδιωτικότητας, είναι διαφορετική. Στη Ελλάδα, τα ευαίσθητα προσωπικά δεδομένα προσδιορίζουν:

- Την φυλετική ή εθνική καταγωγή.
- Τις θρησκευτικά ή φιλοσοφικά πιστεύω.
- Τη συνδικαλιστική συμμέτοχη.
- Την υγεία.
- Τα πολιτικά φρονήματα.

Την κοινωνική πρόνοια

- Τις ποινικές διώξεις ή τα αδικήματα που έχει διαπράξει το άτομο όπως για παράδειγμα το ποινικό μητρώο.
- Τη συμμετοχή σε ενώσεις προσώπων που σχετίζονται με ευαίσθητα προσωπικά δεδομένα για παράδειγμα το σωματείο ομοφυλόφιλων).
- Την ερωτική ζωή.
- Τα μητρώα και αρχεία της Εθνικής Αρχής Ιατρικώς Υποβοηθούμενης Αναπαραγωγής.
- Τις δηλώσεις και τα στοιχεία ατόμων που ζητούν πολιτικό άσυλο.
- Τα δεδομένα των ληπτών και δωρητών ανθρωπίνων ιστών και οργάνων.
- Τα γενετικά στοιχεία.

Ουσιαστικά ο διαχωρισμός των προσωπικών δεδομένων σε απλά και ευαίσθητα αφορά τη διαδικασία συλλογής και επεξεργασίας αυτών, καθώς για τη νόμιμη επεξεργασία των απλών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου και η γνωστοποίηση στην αρμόδια Αρχή (Αρχή Προστασίας Προσωπικών Δεδομένων – ΑΠΔΠΧ). Από την άλλη πλευρά, για τα ευαίσθητα δεδομένα υπάρχει η γενική απαγόρευση της επεξεργασίας τους. Κατ' εξαίρεση επιτρέπεται η συλλογή και επεξεργασία τους καθώς και η τήρηση σχετικού αρχείου, μετά από την λήψης σχετικής άδειας από την ΑΠΔΧ (Αλεξανδροπούλου – Αιγυπτιάδου 2007).

Για τη λήψη άδειας από την ΑΠΔΧ, επιβάλλεται να υπάρχουν ειδική λόγοι (αρ.7 ν. 2472/1997), όπως:

- Η γραπτή συγκατάθεση του υποκειμένου των δεδομένων.
- Η διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- Η αναγκαιότητα αναγνώρισης, άσκησης ή υπεράσπισης δικαιώματος ενώπιων δικαστηρίου ή πειθαρχικού οργάνου (αρ.22 ν.3471/2006).
- Η ιατρική πρόληψη, διάγνωση, περίθαλψη ή διαχείριση υπηρεσιών υγείας (αρ.34 ν.2915/2001).
- Η εθνική ασφάλεια, η διακρίβωση εγκλημάτων, ποινικών καταδίκων ή η λήψη μέτρων ασφάλειας.
- Η προστασία της δημόσιας υγείας, η άσκηση δημόσιου φορολογικού ελέγχου

ή δημόσιου ελέγχου κοινωνικών παροχών (αρ.34 ν.2915/2001).

- Η πραγματοποίηση επιστημονικής έρευνας ενώ προβλέπεται και η διενέργεια προληπτικού ελέγχου τήρησης των δεδομένων αυτών (ν.2472/1997).

1.2 Ιστορική ανάδρομη ιδιωτικότητας και προσωπικών δεδομένων.

Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) της Ρώμης στις 4 Νοεμβρίου το 1950 μεταξύ των κρατών μελών του Συμβουλίου της Ευρώπης και άρχισε να ισχύει τον Σεπτέμβριο του 1953. Προσδιόριζε ανάμεσα στα αλλά την θέσπιση κανόνων για την προστασία των δικαιωμάτων που περιγράφονται στην Σχετική Οικουμενική Διακήρυξη, που είχε ψηφίσει το έτος 1948 η Γενική Συνέλευση των Ηνωμένων Εθνών. Μέσα από αυτές της διαδικασίες προέκυψε, η δημιουργία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου και προβλέπεται η προσφυγή σε αυτό, αφού προηγουμένως έχουν εξαντληθεί τα ένδικα μέσα στα εθνικά δικαστήρια. Η σύμβαση αυτή ακυρώθηκε από το Ελληνικό κράτος με το Ν.2329/1953 και ξεκίνησαν να ισχύουν με το Ν.Δ.53/1974, και από τότε είναι μέρος της Ελληνικής νομοθεσίας, με υπερέχουσα ισχύ απέναντι στους κοινούς νόμους, ως διεθνής σύμβαση(αρθρ.8§1τουΣ).

Η τεχνολογική πρόοδος της πληροφορικής και των τηλεπικοινωνιών και η επίδρασης τους στην διαμόρφωση της ιδιωτικής ζωής, έθεσες σημαντικά ζητήματα στα κράτη μέλη του Συμβουλίου της Ευρώπης στην υπογραφή της 108/28.1.1981 Σύμβασης του Συμβουλίου της Ευρώπης για τη προστασία των προσώπων όσων αφορά το ζητάμα της αυτοματοποιημένης επεξεργασίας των δεδομένων που αφορούν τα προσωπικά χαρακτήρα που ενστερνίστηκαν όλα τα κράτη μέλη της Ε.Ε. Η Σύμβαση περιλάμβανε τόσο τον δημόσιο όσο και στον ιδιωτικό τομέα. Το έτος 1977 με Κοινή Δήλωση το Συμβούλιο, το Κοινοβούλιο και η Επιτροπή διακήρυξαν πανηγυρικά ότι υποχρεούνται όταν ασκούν τα καθήκοντα τους να σέβονται τα ανθρώπινα δικαιώματα, όπως περιγράφονται στα εθνικά συντάγματα των κρατών μελών και στην ΕΣΔΑ. Στις 24/10/1995 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο θέσπισαν την Οδηγία 95/46 για την προστασία των ατόμων απέναντι στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (http//e-trial.blogspot.com).

Το κείμενο αυτό περιγράφεται ως ένα από τα πληρέστερα σε παγκόσμιο επίπεδο για την προστασία προσωπικών δεδομένων, το οποίο αποτελεί δεσμεύσει από τα κράτη μέλη της Ε.Ε. να εισαγάγουν και να δρουν με βάση το συγκεκριμένη νομική κατεύθυνση που απορεί από αυτό. Στην βάση του Συντάγματος του 1975 ώστε να προάσπιση την ιδιωτική και την οικογενειακή ζωή, δεν περιλαμαβεν όμως μεριμνά για την προστασία των προσωπικών δεδομένων. Είχε, όμως, κριθεί αυτό από το ΣτΕ ότι στην ιδιωτική ζωή περιλαμβάνονταν, ανάμεσα στα αλλά και προστατεύονταν κάθε τι που αφορά την υγεία του προσώπου, τις θρησκευτικές του πεποιθήσεις, την οικογενειακή συμπεριφορά του και τις ερωτικές του προτιμήσεις.

Το έτος 1995 με την προώθηση της Οδηγία 95/46 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου προς τα κράτη της Ε.Ε. που σχετιζόταν με την προστασία των φυσικών προσώπων απέναντι στην επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, η οποία και τα υποχρέωνε στην εφαρμογή των απαραίτητων νομοθετικών κανονιστικών και διοικητικών διατάξεων που σχετίζονταν με την εφαρμογή της προαναφερθείσας οδηγίας. Το Ελληνικό κράτος συμμορφώθηκε με τις παραπάνω επιταγές και εξέδωσε τον Ν.2472/1997 που αφορούσε την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα κάτι που έγινε ποιο δίακριτών μέσα από την δημιουργία της ανεξάρτητη Αρχή Προστασίας Προσωπικών Δεδομένων με σκοπό την εποπτεία και έλεγχο των εν λόγω νομοθετικών διατάξεων, καθώς και άλλων αποφάσεων όπως αυτών του Ν.2774/1999 για τις δημόσιες τηλεπικοινωνίες, καθώς και τον σχετικά πρόσφατο ν.3471/2006 όπως ακόμα και με την άσκηση των αρμοδιοτήτων που ανά περίπτωση τους ανατίθενται.

Με το ψήφισμα της Ζ΄ Αναθεωρητικής Βουλής των Ελλήνων στις 6/4/2001 στο Σύνταγμα προστέθηκε η διάταξη του άρθρου 9Α με την οποία η προστασία των προσωπικών δεδομένων στην χώρας μας προσδιορίζεται και ως συνταγματικό δικαίωμα. Στην βάση του άρθρο 286 της Συνθήκης για την ΕΚ, η Κοινότητα αυτοδεσμεύεται να εφαρμόζει και η ίδια την οδηγία (http//e-trial.blogspot.com).

1.3 Ειδή απειλών ιδιωτικότητας και προσωπικών δεδομένων.

Για την ολοκλήρωση μιας διαδικαστικής συναλλαγής με κάποια δημοσία υπηρεσία, συνήθως είναι απαραίτητο να υπάρχει η φυσική παρουσία του ατόμου

ενώπιων ενός δημόσιου υπαλλήλου. Η διαδικασία της ταυτοποίησης γίνεται σε συνδυασμό με τη φυσική παρουσία του ατόμου, ενώ η διαδικασία της αυθεντικοποίησης ολοκληρώνεται με την παρουσίαση ενός έγγραφου που μέσα από αυτό μπορεί να γίνει η ταυτοποίηση, ανάλογα με το είδος της συναλλαγής και τη Δημόσια Υπηρεσία, μπορεί αυτό το έγγραφο να είναι διαφορετικό. Για παράδειγμα, για την έκδοση Αποδεικτικού Φορολογικής Ενημερότητας (Α.Φ.Ε.) ή για την υποβολή Δήλωσης Φορολογίας Εισοδήματος απαιτείται η φυσική παρουσία του πολίτη σε μία Δημόσια Οικονομική Υπηρεσία (Δ.Ο.Υ.), προκειμένου αυτός να ταυτοποιηθεί, και στην συνέχεια είναι αναγκαία η επίδειξη εγγράφου από στο οποίο διακρίνεται ο Αριθμός Δελτίου Ταυτότητας (Α.Δ.Τ.) ή ο Αριθμός Διαβατηρίου (Α.Δ.) προκειμένου να αυθεντικοποιηθεί. Άρα, πρώτα ο πολίτης ταυτοποιείται και ακολούθως αυθεντικοποιείται με την χρήση του κατάλληλου εγγράφου. Μέσα από αυτήν την διαδικασία διασφαλίζεται ότι μία οντότητα δεν μπορεί να υποδυθεί μία άλλη. Ο τρόπος παράκαμψης αυτών των διαδικασιών θα συμπεριλάμβανε είτε τη χρήση πλαστών στοιχείων από τον ενδιαφερόμενο είτε την απουσία ορθού ελέγχου από την μεριά του δημοσίου λειτουργού.

Οι διαδικασίες αυτές πραγματοποιούνται σε πραγματικότητα, σε περιπτώσεις ηλεκτρονικής διακυβέρνησης ένας πιθανός κακόβουλος χρήστης δεν θα προσπαθήσει μόνο να επωφεληθεί από τις αδυναμίες του συστήματος, ανάλογες με αυτές που έχουν αναφερθεί στις υπηρεσίες που προσφέρει το διαδικτύου, αλλά και στις διαδικασίες που προσδιορίζουν την εγγραφή, την ταυτοποίηση και την αυθεντικοποίησης, ανεξαρτήτως με της μορφής με τον όποιες αυτές εκτελούνται, ηλεκτρονικά ή μη (Ramaraj & Mukerji, 2012).

Ειδικότερα, ο κακόβουλος χρήστης επιδιώκει την επίτευξη ενός από τους ακόλουθους σκοπούς:

- Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες ή σε προσφερόμενη υπηρεσία.
- Αντιποίηση αρχής εξουσιοδοτημένου χρήστη ή υπηρεσίας.
- Παραβίαση της ιδιωτικότητας και μη εξουσιοδοτημένη πρόσβαση ή χρήση των δεδομένων που χαρακτηρίζονται προσωπικού χαρακτήρα.
- Άρνηση παροχής υπηρεσίας.

Στην περίπτωση ενός ατόμου που επιθυμεί να υποβάλλει Δήλωση Φορολογίας Εισοδήματος με ηλεκτρονικό τρόπο, επιβάλλεται να εξασφαλίσουν το περιβάλλον ανάλογο με αυτές που ακολουθούνται στη συνήθη διαδικασία υποβολής σε μια Δ.Ο.Υ., αυτές οι διαδικασίες στοχεύουν να ελαχιστοποιήσουν της πιθανότητας οι εμπλεκόμενες οντότητες να έχουν κακόβουλη δράση, εκμεταλλευόμενες κάποια σημεία ευπάθειας του συστήματος. Στην συνέχεια πραγματοποιείται μια προσπάθεια λεπτομερής παρουσίασης των απειλών αυτών που είναι πιθανό να προκύψουν σε επιθέσεις, ώστε να επιτύχει ο κακόβουλος χρήστης κάποιον από σκοπούς που αναφέρθηκαν στην προηγούμενη παράγραφο.

1.3.1 Απειλές Διακριτικών Αυθεντικοποίησης

Ένα σημαντικό σύνολο κίνδυνων στα Πληροφορικά Συστήματα στο οποία επαφίεται η διαχείριση ευαίσθητων πληροφοριών, προκύπτουν από τη μη ορθή διαχείριση των διακριτικών αυθεντικοποίησης τόσο από τους χρήστες όσο και από την υπηρεσία που τα προσφέρει. Σε αυτές τις καταστάσεις, ο επιτιθέμενος καταβάλει προσπάθεια να αυθεντικοποιηθεί ως νόμιμος χρήστης και να επιτύχει πρόσβαση σε πόρους του εξουσιοδοτημένου χρήστη μια πράξη που χαρακτηρίζεται ως αντιποίηση αρχής, κάνοντας αξιοποίηση κάποιου διακριτικού αυθεντικοποίησης του νόμιμου χρήστη, χωρίς αυτό να έχει γίνει αντιληπτό από τον άτομο που δέχεται επίθεση στα προσωπικά του στοιχειά. Οι απειλές για τα διακριτικά αυθεντικοποίησης διακρίνονται σε κατηγορίες στην βάση του τύπου του διακριτικού όπως αναφέρονται στην συνέχεια:

- Ένα στοιχείο που είναι γνωστό στον νόμιμο χρήστη είναι δυνατόν να υποκλαπεί από τον επιτιθέμενο. Όπως για παράδειγμα, ο επιτιθέμενος είναι πιθανόν να ανακαλύψει τον προσωπικό μυστικό κωδικό (Pin) ενός χρήστη κάνοντας επίθεση εξαντλητικής αναζήτησης. Οι πιο διαδομένοι τρόποι επίθεσης (Ferguson & Schneier, 2003) (Books LLC , 2010) στα συστήματα αυθεντικοποίησης με συνθηματικά είναι οι ακόλουθη:

    - Επιθέσεις αξιοποίησης λεξικών.
    - Επιθέσεις εξαντλητικής αναζήτησης.

- Επιθέσεις μες την χρήση τυχαίων δοκιμών.
- Υποκλοπή κατά τη μετάδοση των διαπιστευτηρίων.
- Κοινωνική Μηχανική.

- Ένα στοιχείο που κατέχει ο νόμιμος χρήστης είναι δυνατόν να κλαπεί από τον επιτιθέμενο, να αντιγραφεί ή και να γίνει χρήση του σε κάποια δοσοληψία, και ο νόμιμος χρήστης να έχει άγνοια. Για παράδειγμα, ο επιτιθέμενος είναι δυνατόν να κάνει χρήση κατάλληλου λογισμικού να υποκλέψει από το σύστημα του νόμιμου χρήστη το μυστικό διακριτικό που φυλήσετε στο σκληρό δίσκο του χρήστη όπως είναι το ιδιωτικό του κλειδί.

1.3.2 Απειλές στα Πρωτόκολλα Αυθεντικοποίησης και στις Παρεχόμενες Υπηρεσίες

Ένα σύνολο από τις γνωστότερες απειλές είναι δυνατό να προκύψουν στα πρωτόκολλα αυθεντικοποίησης και στις προσφερόμενες ηλεκτρονικά υπηρεσίες. (Καμπουράκης, et al., 2006) οι οποίες παρουσιάζονται στην συνέχεια και διαχωρίζονται ως ενεργές ή παθητικές με βάση την ενεργή ή παθητική συμμετοχή του κακόβουλου χρηστή (Καμπουράκης, Κρίτζαλης & Κάτσικας, 2006).

- *Υποκλοπή επικοινωνίας-δεδομένων*: Ο επιτιθέμενος στην εν' λόγο περίπτωση παρακολουθεί το δίκτυο, και καταγράφει τα μεταδιδόμενα δεδομένα, με δύο σκοπούς:
  - Την υποκλοπή δεδομένων: Για παράδειγμα ο επιτιθέμενος είναι δυνατόν να υποκλέψει δεδομένα συνομιλίας, μηνύματα ηλεκτρονικού ταχυδρομείου, κωδικούς κ.α.

  - Την ανάλυση των δεδομένων και την αξιοποίησή τους σε μια πιθανή επίθεση σε μελλοντικό χρόνο: Σε περιπτώσεις όπου τα δεδομένα που έχουν καταγραφεί είναι κρυπτογραφημένα, ο επιτιθέμενος είναι πιθανόν να καταβάλει προσπάθειες να αποκαλύψει το κλειδί κρυπτογράφησης, μέσα από την αξιοποίηση για παράδειγμα της εξαντλητικής αναζήτησης κλειδιού. Η ανάλυση των δεδομένων, σε

κάθε περίπτωση, διακρίνεται από διαφορετική στόχευση με βάση το σκοπό του επιτιθέμενου, όπως εμφάνιση του μυστικού κλειδιού ή εμπιστευτικών πληροφοριών και δεδομένων.

- *Επιθέσεις ενδιάμεσου*: Ο κακόβουλος χρήστης σε αυτήν την περίπτωση δρα ως μεσάζον, μεταβαλλόντας έντεχνα τα αποστελλόμενα μηνύματα, προωθώντας τα ακολούθως στα πιθανα θύματα του, χωρίς να γίνεται αντιληπτό. Οι μεταβολές των μηνυμάτων μπορούν να γίνουν και σε πραγματικό χρόνο είτε αξιοποιούνται σε μελλοντική χρονική στιγμή για την πραγματοποίηση κάποιας επίθεσης αυτής της κατηγορίας.
- *Υποκλοπή Συνόδου*: Ο επιτιθέμενος σε αυτή την περίπτωση κάνει χρήση και αξιοποίηση των δεδομένων από προηγούμενης έγκυρης συνοδό ανάμεσα σε δύο οντοτήτων για τη μη εξουσιοδοτημένη πρόσβαση στους παρεχόμενους υπολογιστικούς πόρους και υπηρεσίες.
- *Επιθέσεις επανάληψης*: Ο κακόβουλος χρηστής στην ελ' λόγο περίπτωση, αφού έχει υποκλέψει έναν μέρος από τα δεδομένα αυθεντικοποίησης, κάνει χρήση και αξιοποίηση τους σε μεταγενέστερο χρόνο, για να επιτύχει πρόσβαση ως νόμιμος χρήστης, χωρίς βεβαίως να γίνεται αντιληπτός ότι δεν είναι πράγματι ο νόμιμος χρήστης.
- *Επιθέσεις πλαστοπροσωπίας*: Σε αυτές συνυπολογίζονται και οι περιπτώσεις όπου ο επιτιθέμενος έχει επιτύχει μη εξουσιοδοτημένη πρόσβαση σε κάποιο από τα διακριτικά αυθεντικοποίησης του νόμιμου χρήστη.

- *Επιθέσεις πλημμύρας*: Ο επιτιθέμενος προσπαθεί να φτιάξει ένα σημαντικό υπολογιστικό φόρτο, κυρίως εξαιτίας των αυξημένων απαιτήσεων υπολογιστικών μεθόδων που αξιοποιούν τα πρωτόκολλα αυθεντικό-ποίησης και της μη σωστής διαχείρισης των υπολογιστικών πόρων του συστήματος που προσφέρει την ηλεκτρονική υπηρεσία, με σκοπό την ουσιαστικά αναίτια κατανάλωση των υπολογιστικών πόρων του συστήματος για να προκαλέσει άρνηση παροχής υπηρεσίας.
- *Επιθέσεις τροποποίησης δεδομένων:* Σε αυτή την περίπτωση γίνεται είτε επίθεση ενδιάμεσου, είτε περιλαμβάνεται η έγχυση κακόβουλου κώδικα στα μεταδιδόμενα δεδομένα για τη μη εξουσιοδοτημένη τροποποίηση των αποθηκευμένων δεδομένων του συστήματος. Αντιπροσωπευτική επίθεση της

τελευταίας περίπτωσης είναι η έγχυση SQL κώδικα στα δεδομένα που αποστέλλει στην υπηρεσία με σκοπό την μεταβολή ορισμένων αποθηκευμένων δεδομένων.

- *Επιθέσεις απόκρυψης ταυτότητας*: Ο επιτιθέμενος δημιουργεί μια κάλυψη για την πραγματική του ταυτότητα, κάνοντας χρήση μιας άλλης ταυτότητας άλλης εξουσιοδοτημένης οντότητας. Ειδικότερα, ο επιτιθέμενος κάνει χρήση μιας πλαστής IP διεύθυνση, δεν έχει σημασία αν είναι υπαρκτή ή όχι, η οποία δεν αντιπροσωπεύει την πραγματική διεύθυνση των πακέτων που αποστέλλονται, με σκοπό την απόκρυψη της αρχικής πηγής της επίθεσης ή για να επιτύχει πρόσβαση σε μη εξουσιοδοτημένους πόρους.

Ολοκληρώνοντας αυτήν την ενότητα θα πρέπει να σημειωθεί ότι οι επιθέσεις-απειλές αυτές, μεταβάλλονται στη διαδικασία εκτέλεσής τους, με βάση την υπηρεσία ή το πρωτόκολλο αυθεντικοποίησης εναντίον των οποίων γίνεται η επίθεση.

1.3.3 Απειλές κατά τη διαδικασία εγγραφής τελικού χρήστη

Οι πιο γνωστές απειλές προκύπτουν κατά τη διαδικασία της εγγραφής και είναι η ακόλουθές (Burr et al., 2011):

- *Πλαστοπροσωπία:* Σε αυτή την περίπτωση ο αιτών προσπαθεί ψευδώς να αναπαραστήσει μια κάποια άλλη οντότητα και παράσχει ψευδή δικαιολογητικά με σκοπό να τεκμηριώσει τον ισχυρισμό του.

- *Αποποίηση Εγγραφής*: Ο αιτών προσπαθεί να αποφύγει την πεπραγμένη διαδικασία εγγραφής και τα συνθηματικά, ψηφιακά πιστοποιητικά που εκδόθηκαν ως συνέχεια αυτής.

1.3.4 Άλλες απειλές

Πέραν των απειλών που προκύπτουν και περιγράφηκαν στις προηγούμενες ενότητες, τα υπολογιστικά συστήματα είναι πιθανόν να βρεθούν αντιμέτωπα και με τις ακόλουθες απειλές (Vivo et al., 1998):

Ιομορφικό λογισμικό: Το ιομορφικό λογισμικό περιλαμβάνει προγράμματα που κατασκευάζονται με στόχο την εξουδετέρωση κακόβουλου κώδικα σε έναν υπολογιστικό σύστημα, χωρίς αυτό να γίνεται άμεσα αντιληπτό στο διαχειριστή του συστήματος, με σκοπό την εκδήλωση μιας επίθεσης. Το ιομορφικό λογισμικό με βάση τις ιδιότητές του διαφοροποιείται ως εξής:

- *Ιός*: Ένας ιός είναι ένα πρόγραμμα το οποίο έχει τη ικανότητα να προστίθεται και να συνυπάρχει σε άλλο λογικό αντικείμενο, ενώ αναπαράγεται μέσω της ενεργοποίησης του λογικού αντικειμένου.

- *Δούρειος Ίππος*: Ένας δούρειος ίππος είναι πρόγραμμα που διαθέτει κρυφές λειτουργίες, οι οποίες, στην περίπτωση που ξεκινήσουν την δράση τους, αξιοποιούν τα δικαιώματα του χρήστη που εκτελεί το δούρειο ίππο, και τις οποίες εκμεταλλεύονται οι επιτιθέμενοι, για να διενεργήσουν μια επίθεση.

- *Σκουλήκια*: Ένα σκουλήκι αποτελεί ένα πρόγραμμα ιομορφικού λογισμικού, το οποίο έχει την ικανότητα να διαδίδεται και να αυτοαναπαράγεται.

Η μετάδοση του ιομορφικού λογισμικού σε κάποιο υπολογιστικό σύστημα έχει την δυνατότητα να πραγματοποιηθεί είτε με την αποθήκευσή του σε κάποιο μέσο αποθήκευσης είτε δικτυακά.

- *Υπερχειλίσεις προσωρινών χώρων*: Στις επιθέσεις υπερχείλισης προσωρινών χώρων, ο επιτιθέμενος βρίσκει ευκαιρία και εκμεταλλεύεται τον ελλιπή έλεγχο όταν γίνεται η αποθήκευση των δεδομένων στους αντίστοιχους καταχωρητές, έτσι προκύπτει η τροποποίηση της ροής εκτέλεσης της εφαρμογής στην οποία λαμβάνει χώρα η επίθεση, με στόχο την εκτέλεση του κώδικα που θέλει να πραγματοποιήσει ο επιτιθέμενος.

- *Μη εξουσιοδοτημένη είσοδος στο λειτουργικό σύστημα*. Ελλιπή συστήματα ελέγχου πρόσβασης στο λειτουργικό σύστημα πιθανόν να παράσχουν την δυνατότητα σε ένα μη εξουσιοδοτημένο χρήστη, πρόσβαση σε εμπιστευτικά στοιχεία και εξουσιοδότηση για εκτέλεση δράσεων οι οποίες υπ' κανονικές συνθήκες δε θα έπρεπε να πραγματοποιηθούν.

1.3.5 **Πιθανές επιπτώσεις απειλών – κινδύνων**

Οι απειλές που αναλύθηκαν στις προηγούμενες ενότητες, προσδιορίζουν τις διαφορετικές επιπτώσεις στα άτομα και στους δημόσιους φορείς που παρέχουν τις υπηρεσίες ηλεκτρονικής διακυβέρνησης, στην περίπτωση που αξιοποιηθούν σε πιθανές επιθετικές ενεργείς. Στον πίνακα ακόλουθο (πινάκα1.1) ενδεικτικά προσδιορίζονται οι πιθανές επιπτώσεις που είναι δυνατόν να προκύψουν από αυτούς τους κίνδυνους, τόσο στους χρήστες όσο και στους δημόσιους φορείς σε σύγκριση με το επίπεδο εμπιστοσύνης που σχετίζεται η υπηρεσία. Είναι παραίτιο να επισημανθεί ότι ο πίνακας δεν αφορά μια εξαντλητικής αποτύπωσης των επιπτώσεων, καθώς αυτές μεταβαλλονται ανάλογα με την εκάστοτε υπηρεσία και τις πιθανές επιπρόσθετες νομικές, οικονομικές κ.λπ. επιπτώσεις που ενδέχεται να υποστεί ο φορέας.

Πινάκας 1.1: Πιθανές επιπτώσεις κίνδυνων

Κίνδυνος	Πιθανές Επιπτώσεις Τελικών Χρηστών	Πιθανές Επιπτώσεις Φορέων Παροχής Υπηρεσιών
Υποκλοπή Διακριτικών Αυθεντικοποίησης	Μη εξουσιοδοτημένη πρόσβαση παραβίαση ιδιωτικότητας υποβολή λανθασμένων στοιχείων	Επεξεργασία λανθασμένων στοιχείων
Επιθέσεις ενδιάμεσου	Παραβίαση ιδιωτικότητας υποβολή λανθασμένων στοιχείων	Επεξεργασία λανθασμένων στοιχείων αντιποίηση υπηρεσίας
Υποκλοπή Επικοινωνίας-Δεδομένων	Παραβίαση ιδιωτικότητας μη εξουσιοδοτημένη πρόσβαση	Δημοσίευση προσωπικών δεδομένων
Υποκλοπή Συνόδου	Μη εξουσιοδοτημένη πρόσβαση	Δημοσίευση προσωπικών δεδομένων
Επιθέσεις Επανάληψης	Μη εξουσιοδοτημένη πρόσβαση υποβολή λανθασμένων στοιχείων	Επεξεργασία λανθασμένων στοιχείων
Επιθέσεις Πλαστοπροσωπίας	Μη εξουσιοδοτημένη πρόσβαση	Επεξεργασία λανθασμένων στοιχείων
Επιθέσεις Πλημμύρας	Άρνηση πρόσβασης στην υπηρεσία	Μη παροχή υπηρεσίας
Επιθέσεις Τροποποίησης Δεδομένων	Υποβολή Λανθασμένων Στοιχείων	Επεξεργασία λανθασμένων στοιχείων
Ιομορφικό Λογισμικό	Άρνηση πρόσβασης στην υπηρεσία	Μη παροχή υπηρεσίας

1.3.6 Τρόποι Αντιμετώπισης και Ελαχιστοποίησης Απειλών και Κινδύνων

Για την ελαχιστοποίηση της πιθανότητας αναβάθμισης μιας απειλής σε κίνδυνο, επιβάλλεται τα μέτρα ασφάλειας τα οποία έχουν παρθεί να αντιμετωπίζουν

ικανοποιητικά τις απαιτούμενες μορφές ασφάλειας και σε περιπτώσεις που κρίνεται απαραίτητο περιλαμβάνουν, ανάμεσα στα άλλα, την παροχή υπηρεσιών ασφάλειας όπως:

- *Αυθεντικοποίηση*, η οποία αφορά το επίπεδο εμπιστοσύνης το οποίο οι συναλλασσόμενοι θα πρέπει να έχουν, σε σχέση με την ταυτότητα των εμπλεκομένων μερών.
- *Εξουσιοδότηση*, η οποία σχετίζεται με τα δικαιώματα που έχει κάθε οντότητα, στο πλαίσιο μιας συναλλαγής.
- *Ακεραιότητα* των δεδομένων, που σχετίζεται με την απαίτηση περί μη μεταβολής του περιεχομένου των μηνυμάτων στα πλαίσια μιας συναλλαγής.
- *Μη-αποποίηση* αποστολής και λήψης δεδομένων, που σχετίζεται με την παροχή δεδομενων, με βάση τα οποία μία οντότητα δε θα έχει την δυνατότητα, αρχικά, σε μεταγενέστερο χρόνο να αρνηθεί ότι έχει συμμετάσχει σε μία συγκεκριμένη ηλεκτρονική συναλλαγή.
- Υπηρεσίες εξασφάλισης της εμπιστευτικότητας των μηνυμάτων ανάμεσα στους χρηστές και γενικότερα της ιδιωτικότητας των εμπλεκομένων οντοτήτων σε μία ηλεκτρονική δραστηριότητα.

Ακολούθως αναφέρονται ενδεικτικές μέθοδοι για την αντιμετώπιση ή περιορισμό των κινδύνων στις οποίες αναφερθήκαμε αναλυτικά στο παρόν κεφαλαίο.

1.3.6.1

Οι απειλές των διακριτικών αυθεντικοποίησης, όπως αναφέρθηκαν σε προηγούμενη ενότητα 3.4.2, η κατηγοριοποίηση τους γίνεται με βάση τον τύπο του διακριτικού. Άρα για την ελαχιστοποίηση εμφάνισης αυτού του είδους των απειλών απαιτείται να ληφθούν τα αντίστοιχα μέτρα προστασία. Ειδικότερα, όσον αφορά στη διακύβευση των συνθηματικών του χρήστη, επιβάλλεται να ακολουθούντα οι ακόλουθες πρακτικές:

- Αξιοποίηση ασφαλών συνθηματικών.
- Ασφαλής αποθήκευσή τους και υπό την μορφή κρυπτογράφησης.

- Ασφαλής μετάδοση και μεταφορά των διαπιστευτηρίων κατά τη διάρκεια της διαδικασία αυθεντικοποίησης.
- Περιορισμός έγκυρων προσπαθειών υποβολής συνθηματικού.
- Συχνές μεταβολές του συνθηματικού από το χρήστη.

Αντίστοιχα οι χρήστες είναι υποχρεωμένοι να διατηρούν τα διακριτικά αυθεντικοποίησής τους σε μέρη με ασφαλή με στόχο την μη δυνατότητα η υποκλοπή τους από κακόβουλους χρήστες.

1.3.6.2 Ελαχιστοποίηση και τρόποι αντιμετώπισης απειλών στα πρωτόκολλα αυθεντικοποίησης και στις προσφερόμενες υπηρεσίες

Τα πρωτόκολλα αυθεντικοποίησης και οι ηλεκτρονικά παρεχόμενες υπηρεσίες προσδιορίζονται ως τα βασικότερα μέρη των υπηρεσιών ηλεκτρονικής διακυβέρνησης. Άρα, ο περιορισμος εμφάνισης των κινδύνων, αλλά και η πιθανή αντιμετώπισή τους, εξασφαλίζουν της ορθής λειτουργίας των συστημάτων αυτών (Evangelidis, 2004).

Έτσι για κάθε κίνδυνο που αναφέρθηκε πιο πάνω επιβάλλεται να λαμβάνονται τα αντίστοιχα μέτρα ελαχιστοποίησης και αντιμετώπισης, αναλυτικότερα:

- *Υποκλοπή επικοινωνίας-δεδομένων*: Τα πρωτόκολλα αυθεντικοποίησης και οι προσφερόμενες ηλεκτρονικά υπηρεσίες επιβάλλεται να διασφαλίζουν την εμπιστευτικότητα των σημαντικών δεδομένων όπως συνθηματικά, μυστικά κλειδιά που αφορούν τη διαδικασία αυθεντικοποίησης, και τα ευαίσθητα δεδομένα που ανταλλάσσονται, μεταφέρονται και επεξεργάζονται σε αυτές. Αυτό σημαίνει ότι ο επιτιθέμενος που καταγράφει υποκλέπτοντας την επικοινωνία, είναι αδύνατον να αποκαλύψει οποιοδήποτε πληροφορία που συμβάλει στη διακύβευση των εμπιστευτικών πληροφοριών, είτε αφορούν τα διαπιστευτήρια του χρήστη, είτε με ευαίσθητες πληροφορίες που σχετιζονται τον ίδιο. Έτσι τα δεδομένα που σχετίζονται με τα πρωτόκολλα αυθεντικοποίησης και τις υπηρεσίες, τουλάχιστον όσον αφορά στις απόρρητες πληροφορίες-δεδομένα, επιβάλλεται να μεταδίδονται σε καθαρή μη-κρυπτογραφημένη μορφή, αλλά είναι απαραίτητο να κάνουν χρήση

απαραιτήτων μηχανισμών ασφάλειας, ώστε να εξασφαλίζεται η εμπιστευτικότητά τους.

- *Επιθέσεις Ενδιάμεσου*: Η ελαχιστοποίηση της πιθανότητας της παρουσίας αυτού του είδους των επιθέσεων είναι δυνατόν να πραγματοποιηθεί μόνο με την χρήση μηχανισμών ασφάλειας, όπως για παράδειγμα το πρωτόκολλο SSL, το οποίο έχει στόχο την προστασία από τέτοιου είδους επιθέσεων ή άλλων εναλλακτικών συστημάτων αυθεντικοποίησης που έχει αποδειχθεί η ρωμαλεότητα τους σε επιθέσεις ενδιάμεσου. (Jun, et al., 2006). Παρά ταύτα είναι σημαντικό να σημειωθεί ότι, ακόμα και ανάλογες περιπτώσεις, υπάρχουν καταστάσεις που γίνονται τέτοιου είδους επιθέσεις (NZ eGov, 2009).

- *Επιθέσεις Επανάληψης και Υποκλοπής Συνόδων*: Για την αποτροπή τέτοιους είδους επιθέσεων, τα πρωτόκολλα αυθεντικοποίησης και οι προσφερόμενες υπηρεσίες επιβάλλεται να επεξεργάζονται δεδομένα που έχουν σχέση με προηγούμενες συνόδους και που είναι πιθανόν να επιδράσουν στην ορθή λειτουργία του συστήματος. Ακόμα, είναι αναγκαίο να τονιστεί ότι, όπως και στις περιπτώσεις υποκλοπών στοιχείων, τα δεδομένα που είναι δυνατόν να οδηγήσουν σε πιθανό κίνδυνο την ασφάλεια του συστήματος είτε με επίθεση επανάληψης είτε με υποκλοπή συνόδου, επιβάλλεται να μη αποστελονται σε μη κρυπτογραφημένη μορφή, αλλά είναι απαραίτητο να αξιοποιούνται και να γίνεται χρήση των κατάλληλων μηχανισμών ασφάλειας, ώστε να εξασφαλίζεται η εμπιστευτικότητα τους.

- *Επιθέσεις Πλαστοπροσωπίας*: Στις επιθέσεις πλαστοπροσωπίας ο επιτιθέμενος επιδιώκει να αποδείξει την κατοχή νόμιμων διαπιστευτηρίων. Έτσι, τα πρωτόκολλα αυθεντικοποίησης δε θα πρέπει να φανερώνουν δεδομένα που είναι δυνατόν να συμβάλουν στην επίτευξη επιθέσεων πλαστοπροσωπίας.
- *Επιθέσεις Πλημμύρας*: Οι επιθέσεις πλημμύρας, τόσο στα πρωτόκολλα αυθεντικοποίησης όσο και στις προσφερόμενες υπηρεσίες, είναι σχετικά δύσκολο να περιοριστούν, αλλά είναι δυνατόν ανιχνευθούν και να αντιμετωπισθούν στη συνέχεια με την αξιοποίηση και χρήση κατάλληλων μηχανισμών.

- *Επιθέσεις Τροποποίησης Δεδομένων*: Οι επιθέσεις τροποποίησης δεδομένων τόσο στα πρωτόκολλα αυθεντικοποίησης όσο και στις προσφερόμενες υπηρεσίες, είναι δυνατόν να αντιμετωπισθούν με την αξιοποίηση κατάλληλων μηχανισμών ακεραιότητας, όπως message authentication code ή message integrity checksum, H-MAC και ψηφιακές υπογραφές (Ferguson & Schneier, 2003).
- *Επιθέσεις Απόκρυψης Ταυτότητας*: Οι επιθέσεις αυτές είναι δυνατόν να ελαχιστοποιηθούν με την αξιοποίηση κατάλληλων μηχανισμών φιλτραρίσματος (Γκρίτζαλης et al., 2003),

  οι οποίοι δεν επιτρέπουν την κίνηση δεδομένων σε ορισμένα τμήματα ενός συγκεκριμένου δικτύου. Ο μηχανισμός είναι δυνατόν να εφαρμοστεί σε οποιοδήποτε ανάχωμα ασφαλείας (*Firewall*) επιπέδου δικτύου υλοποιεί τη μέθοδο που προσφέρεται στο RFC 2267.

1.3.6.3 Ελαχιστοποίηση και Μορφές Αντιμετώπισης των Απειλών με την Εγγραφής Τελικού Χρήστη

Σε αρκετές περιπτώσεις οι απειλές που αναφέρθηκαν σε προηγούμενες οντότητες οφείλονται στις επιθέσεις που μπορούν να προκύψουν κατά τη διαδικασία εγγραφής. Για το λόγο αυτό, η υπηρεσία εγγραφής επιβάλλεται να:

- Ταχτοποιεί και να αυθεντικοποιεί τις οντότητες που επιδιώκουν εγγραφής σε κάποια υπηρεσία.
- Είναι αυστηρή και ακριβής στην διάρκεια της ορθότητας των υποβληθέντων δικαιολογητικών και στοιχείων, ώστε να είναι δυνατός ο εντοπισμός των ψευδών δικαιολογητικών.
- Αξιοποιεί διαδικασίες καταγραφής όλων των ενεργειών που γίνονται από την υπηρεσία εγγραφής, ώστε να μην επιτρεπεται η αποποίηση εγγραφής σε κάποια υπηρεσία από μια οντότητα.

1.3.6.5 Ανάλυση Επικινδυνότητας και Αποτίμηση Κινδύνου

Τα περιουσιακά στοιχεία (*Assets*) ενός Π.Σ. Ηλεκτρονικής Διακυβέρνησης τα οποία επιβάλλεται να προστατεύονται είναι τα εξής:

- Υλικό (*Hardware*).

- Λογισμικό (*Software*),
- Πληροφορίες και Δεδομένα (*Information and Data*).
- Τεκμηρίωση διαδικασιών (*Procedure Documentation*).
- Προσωπικό (*Personne*l).
- Εγκαταστάσεις (*Facilities*).

Η αξία των αγαθών προσδιορίζεται με ανάλογο τρόπο και σε σχέση με τη φύση του αγαθού. Για παράδειγμα, η αξία του υλικού ή άλλου εξοπλισμού είναι δυνατόν να υπολογιστεί σε σύγκριση με το οικονομικό μέγεθος που είναι απαραίτητο για την αντικατάστασή της. Αντίθετα, η αξία των αγαθών είναι δυνατόν να υπολογιστεί σε σύγκριση με τις επιπτώσεις απώλειας της ασφάλειάς τους, δηλαδή σε σχέση με ενδεχόμενη παραβίαση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους καθώς και σε σχέση με τις επιπτώσεις από την παραβίαση αυτή. Απειλή αποτελεί οποιαδήποτε πράξη ή γεγονός που θα μπορούσε πιθανόν να έχει επιβλαβές αποτέλεσμα στο Π.Σ. παραδείγματα τέτοιων απειλών είναι:

- Απώλεια υπηρεσιών, (διακοπή ρεύματος).
- Καταστροφή δεδομένων.
- Τροποποίηση δεδομένων.
- Παρακολούθηση δεδομένων.
- Φυσικές απειλές, (πλημύρα).
- Φυσικές καταστροφές (σεισμός).
- Σφάλματα (σφάλμα εξυπηρετητή ή λογισμικού).
- Μη εξουσιοδοτημένες ενέργειες (μη εξουσιοδοτημένη χρήση εξοπλισμού).

Ως ευπάθεια χαρακτηρίζεται μια αδυναμία του Π.Σ., η ύπαρξη της οποίας είναι δυνατόν να επιτρέψει την πραγματοποίησης μιας απειλής. Ευπάθειες είναι:

- Ευπάθειες υλικού (έλλειψη ορθών πρακτικών απόσυρσης υλικού).
- Ευπάθειες λογισμικού (παράλειψη αποσύνδεσης χρηστών, μετά την ολοκλήρωση των εργασιών τους).
- Ευπάθειες δικτύου (μη κρυπτογραφημένη μετάδοση εμπιστευτικών πληροφοριών).

- Ευπάθειες προσωπικού (έλλειψη ενημερότητας ασφάλειας).
- Ευπάθειες διοίκησης (έλλειψη τεκμηριωμένων διαδικασιών).

Επίπτωση είναι το αποτέλεσμα της αποτυχίας να εξασφαλιστεί η ασφάλεια του Π.Σ., το αποτέλεσμα δηλαδή από μίας επιτυχημένη παραβίαση της ασφάλειάς του. Οι επιπτώσεις που είναι πιθανόν να προκύψουν από μία τέτοια παραβίαση κατηγοριοποιούνται σε τέσσερις βασικούς τύπους:

- Διαρροή.
- Τροποποίηση.
- Καταστροφή.
- Μη διαθεσιμότητα.

Μετά τον υπολογισμό της επικινδυνότητας ακολουθεί η επιλογή και εφαρμογή αντιμέτρων για τη εξασφάλιση και προστασία του Π.Σ. Ως αντίμετρο χαρακτηρίζεται ένας μηχανισμός ή μια διαδικασία που λειτουργεί στο περιβάλλον του Π.Σ. με στόχο να ελαττώσει ένα ή πε-περισσότερα από τα συστατικά της επικινδυνότητας στην οποία εκτίθεται. Τα πιθανά αντί-μετρά κατηγοριοποιούνται σε τέσσερις βασικούς τύπους:

- Φυσικά.
- Διαδικαστικά.
- Τεχνικά.
- Προσωπικού.

1.4 Ηλεκτρονικά μέσα και προσωπικά δεδομένα.

Η οπουδήποτε συναλλαγή που πραγματοποιείται εντός του διαδικτύου προϋποθέτει την συγκέντρωση πληροφοριών για τον χρήστη, ο οποίος αναγκαστικά αφήνει τα «ίχνη» του στο διαδίκτυο. Η συλλογή των προσωπικών δεδομένων του χρήστη, που πραγματοποιείται με εκούσιο, αλλά συχνότερα κατά ακούσιο τρόπο, είναι δυνατόν ο φορέας να δημιουργήσει αρχείο προσωπικών δεδομένων του και

εικόνα για το επάγγελμα, την υγεία, την οικονομική κατάσταση, τις αντιλήψεις και τις συνήθειες του χρήστη και στην ουσία να έχει ένα πλήρες προφίλ με τα χαρακτηριστικά της προσωπικότητας του.

Οι πληροφορίες για τα προσωπικά δεδομένα που συλλέγονται από διαδικτυακές δράσεις αποδεικνύονται πολύτιμες αποτελούν πολίτες πήγες πληροφόρησης των επιχειρήσεων, ενώ ο κίνδυνος «κατηγοριοποίησης», αλλά ακόμη και χειραγώγησης του χρήση μέσω της χρήση των στοιχείο από τις παραπάνω διαδικασίες, είναι ορατός.

Τα λεγόμενα «cookies» είναι αυτοεγκαθιστώμενα προγράμματα ανιχνευτές, που χρησιμεύουν στους κατόχους ιστοσελίδων ως «κατασκοπευτικό» λογισμικό, παρέχοντας σε αυτούς τη δυνατότητα να κατασκευής αρχείων που σχετίζονται με το ιστορικό των επισκέψεων σε μια ιστοσελίδα και τις πράξεις, που έγιναν μέσα σε αυτήν αυτής όπως για παράδειγμα αγορές, κατέβασμα αρχείων κ.σ. Στόχος της χρησιμοποίησης τους είναι καταρχήν η ταχύτερη πρόσβαση στην ιστοσελίδα την κάποια επόμενη φορά που ο χρήστης θα επισκεφθεί και είναι απαραίτητο της επαναπληκτρολόγησης του συνόλου πληροφοριών όπως για παράδειγμα προσωπικών κωδικών, αριθμών πιστωτικών κ.α προκειμένου να προβεί σε κάποια συναλλαγή. Έτσι όμως συγκεντρώνονται δεδομένα σχετικά με τα προσωπικά ενδιαφέροντα του χρήστη, για τα προϊόντα που αγοράζει, τις σύνηθες του κ.α. (Αλεξανδρίδου, 2004).

Τα «cookies» γίνονται δεκτά από το δίκαιο, υπό ορισμένες προϋποθέσεις επειδή συμβάλουν στην ταχύτερη ροή πληροφοριών στο διαδίκτυο και προσφέρουν ευχρηστία γενικότερα στις συναλλαγές. Το πρόβλημα εμφανίζεται, όταν οι παραπάνω φορείς παροχής υπηρεσιών δεν ενημερώνουν τους επισκέπτες των ιστοσελίδων τους, ότι συγκεντρώνουν τα δεδομένα αυτά με σκοπό την ανάλυση και διαχείριση τους με σκοπό την εξυπηρέτηση συμφερόντων των εταιριών τους και δεν έχουν πάρει τη συναίνεση τους. Μετά τη συγκέντρωση των εν λόγω δεδομένων, ο φορέας παροχής υπηρεσιών μπορεί πλέον να τα επεξεργαστεί και να χρησιμοποιήσει πληροφορίες, που αποτελούν το αποτέλεσμα αυτής της επεξεργασίας, για σκοπούς ποικίλους, που στις περισσότερες περιπτώσεις επιδιώκουν το εμπορικό κέρδος. Σε όλες τις παραπάνω περιπτώσεις υπάρχει σαφής προσβολή του δικαιώματος πληροφοριακού αυτοκαθορισμού, η οποία φτάνει πολλές φορές ως την προσβολή του δικαιώματος του ιδιωτικού βίου και ακολούθως έχει πρόσβαση στα προσωπικά δεδομένα του κάθε χρήστη.

Όσων αφορά την ελληνική νομοθεσία εθνικού δικαίου, το αρθρ. 9Α Συντάγματος Πρόκειται για διάταξη, που προστέθηκε μετά την τελευταία αναθεώρηση του 2001 και αποτελεί ρητή καθιέρωση του δικαιώματος πληροφοριακού αυτοκαθορισμού, το οποίο συναγόταν παλαιότερα από διάφορες διατάξεις του Συντάγματος και της ΕΣΔΑ. Η διάταξη αυτήν αναφέρει ότι «καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει». Εκτός από αυτό, σχετικές είναι και οι διατάξεις των αρθρ. 9 και 19 του Συντάγματος, που κατοχυρώνουν αντίστοιχα το απαραβίαστο της ιδιωτικής ζωής του ατόμου και το απαραβίαστο του απορρήτου των επικοινωνιών. Σε επίπεδο τυπικού νόμου ισχύουν κυρίως ο ν. 2472/97 ο ν. 2774/99 και ο 3471/2006. Σημαντικές για την πρακτική εφαρμογή της σχετικής νομοθεσίας είναι και οι αποφάσεις που απορρέουν από την Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, οι οποίες επιλύουν διάφορα ρυθμιστικά και ερμηνευτικά ζητήματα.

Στο πεδίο εφαρμογής του ν. 2472/97, που μετέφερε την οδηγία 95/46 ΕΚ, εμπίπτει και η συλλογή και επεξεργασία προσωπικών δεδομένων που αφορούν το διαδικτύου. Με το νόμο αυτό επεκτάθηκε η έννοια των παράνομων προσβολών της προσωπικότητας σε σχέση με αυτές, που μπορούσαν να υπαχθούν στη διάταξη του αρθρ. 57 ΑΚ και επικεντρώθηκε περισσότερο στην διαδικασία της πρόληψη των προσβολών με επιβολή περιορισμών και απαγορεύσεων στην πηγή των κινδύνων. Οι πράξεις συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα χαρακτηρίζονται ως πράξεις «διακινδύνευσης» του δικαιώματος στην προσωπικότητα. Δεν αποκλείεται βέβαια να προκύψουν στο πλαίσιο του διαδικτύου και πράξεις, οι οποίες που συνιστούν άμεση προσβολή του δικαιώματος στην προσωπικότητα και εμπίπτουν στο αρθρ. 57 ΑΚ.

Ο ν. 2472/97 αναφέρει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ιδίως σε περιπτώσεις που αυτά να συλλέγονται κατά τρόπο θεμιτό και νόμιμο και να υφίστανται νόμιμη επεξεργασία, να είναι ακριβή και να ενημερώνονται οι χρηστές, όταν χρειάζεται (αρθρ. 4 § 1). Ακόμα, το υποκείμενο των δεδομένων πρέπει να έχει δώσει τη συγκατάθεση του, εκτός και αν υπάρχουν προϋποθέσεις εξαιρέσεις, που προβλέπονται στο νόμο (βλ. αρθρ. 5 § 1 ν. 2472/97).

Αυστηρότερη προστασία επιβάλλεται, σε περιπτώσεις που αφορούν ευαίσθητα προσωπικά δεδομένα (αρθρ. 7 ν. 2472/97).

Ακόμα, καθιερώνεται δικαίωμα του υποκειμένου των δεδομένων, να ενημερώνεται με τρόπο απλό και σαφή για το σκοπό της επεξεργασίας, για τις κατηγορίες δεδομένων που είναι προς επεξεργασίας, για τους αποδέκτες των δεδομένων αυτών και για τα στοιχεία του υπευθύνου επεξεργασίας των δεδομένων. Μεγάλη σημασία έχει και η καθιέρωση του δικαιώματος του υποκειμένου της επεξεργασίας να έχει πρόσβαση σε όλα τα δεδομένα προσωπικού χαρακτήρα, που τον αφορούν και ακόμα, να πληροφορείται την πηγή προέλευσης τους.

Για την περίπτωση παράβασης των υποχρεώσεων τους, οι υπεύθυνοι επεξεργασίας έρχονται αντιμέτωποι με ποινικές και διοικητικές κυρώσεις. Ο νόμος προσδιορίζει την ευθύνη για αποζημίωση του προσώπου, που προκάλεσε περιουσιακή ή ηθική βλάβη στο υποκείμενο των προσωπικών δεδομένων (αρθρ. 21 επ. ν. 2472/97).

Το ισχύον νομοθετικό πλαίσιο στηριζόταν ακόμα στο ν. 2774/99 που αφορούσε τα προσωπικά δεδομένα και την προστασία τους, στον τηλεπικοινωνιακό τομέα. Με το νόμο αυτό το εθνικό δίκαιο εναρμονίστηκε προς την οδηγία 97/66/ΕΚ. Εκτός από την τηλεφωνία, συμβατική και κινητή, στη ρύθμιση του νόμου εντάσσονται ακόμα και οι υπηρεσίες, που παρέχονται μέσω του ISDN (Integrated Services Digital Network).

Μία από τις σημαντικότερες αρχές που προορίζει ο νόμος αυτός, ο οποίος εφαρμόζεται, ότι όταν πρόκειται γενικότερα για υπηρεσίες στο πλαίσιο του διαδικτύου, είναι αυτή που αφορά του απορρήτου των επικοινωνιών.

Ακόμα, προβλέπεται ότι η επεξεργασία των δεδομένων είναι δυνατή μόνον, αν υπάρχει συγκατάθεση του χρήστη ή όταν η επεξεργασία είναι αναγκαία για την εκτέλεση της σύμβασης (αρθρ. 4 § 2) Ο νόμος καθιερώνει αστική, αλλά και ποινική ευθύνη του παραβάτη, ο οποίος προκαλεί με τις ενέργειες του περιουσιακή ή ηθική βλάβη σε άλλο πρόσωπο (αρθρ. 12 επ. ν. 2774/99). Πλέον είναι σε ισχύει οΝ.3471/2006 είναι η Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στο σύνολο των ηλεκτρονικών επικοινωνιών και συναλλαγών.

Το ηλεκτρονικό ταχυδρομείο (e-mail) χαρακτηρίζεται ως νέα μορφή τηλεπικοινωνίας, ο κανόνας του απορρήτου των επικοινωνιών περιλαμβάνει και αυτό. Για την προστασία του απορρήτου της επικοινωνίας που λαμβάνει χώρα μέσω του διαδικτύου έχουν θεσπιστεί μάλιστα και ειδικές διατάξεις στον Ποινικό Κώδικα.

Πρόκειται για τα αρθρ. 370Β και 370Γ. που τιμωρεί την χωρίς δικαίωμα πρόσβαση-διείσδυση σε συστήματα υπολογιστών διαμέσου των δικτύων επικοινωνίας το δε αξιόποινο προκύπτει και όταν ακόμη η παραπάνω πρόσβαση γίνεται χωρίς την επισκοπού βλάβη.

Στο ίδιο πνεύμα κινείται και η ρύθμιση, που σχετίζεται με την πραγματοποίηση της άμεσης διαφήμισης. Εφόσον το ζητήσει ο καταναλωτής, το πρόσωπο που πραγματοποιεί την άμεση διαφήμιση, οφείλει να διακόψει αμέσως κάθε μορφή της εν λόγω διαφήμισης και να διαγράψει τα προσωπικά στοιχεία, που έχει συγκεντρώσει για τον εν λόγω καταναλωτή. Εξάλλου, όταν πραγματοποιείται άμεση διαφήμιση, ο νόμος επιτάσσει να γίνεται αυτή κατά τέτοιο τρόπο, ώστε να μην διαταράσσεται η ιδιωτική ζωή του καταναλωτή (άρθρ. 9 §§ 12, 13 ν. 2251/94).
Είναι δεδομένο ότι η διαρκής ανάπτυξη του διαδίκου έχουν συντέλεση στην δημιουργεί αρχών καλής συμπεριφοράς, βάση των οποίων οι οποίες συνέπειες ενός χρήστης δεν επιτρέπεται να γνωστοποιεί πληροφορίες προσωπικού περιεχομένου άλλου χρήστη, όπως για παράδειγμα την ηλεκτρονική του αλληλογραφία κ.α. Όσον αφορά στο ηλεκτρονικό ταχυδρομείο, επιβάλλεται να συνειδητοποιηθεί από τους χρήστες το γεγονός ότι το περιεχόμενο του είναι εύκολα προσβάσιμο από τρίτους και μάλιστα, χωρίς προκύπτουν ίχνη παραβίασης. Για το λόγο αυτό, όταν πρόκειται για εμπιστευτικές πληροφορίες πρέπει να μην επιλέγεται η διαβίβαση μέσω ηλεκτρονικού ταχυδρομείου.

Για την αντιμετώπιση ζητημάτων, που δημιουργούνται όσον αφορά στην εμπιστευτικότητα μεταδιδόμενων μέσω του διαδικτύου πληροφοριών, έχουν ανακαλυφθεί και γίνεται χρήση τους, και αφορά τις μεθόδους της κρυπτογραφίας. Μέσω της κρυπτογραφίας είναι δυνατόν και διασφαλιστεί ο εμπιστευτικός χαρακτήρα και η ασφαλή πιστοποίηση μεταδιδόμενων πληροφοριών (Αλεξανδρίδου, 2004).

1.5 Τεχνολογίες πιστοποιήσεις και προστασίας προσωπικών δεδομένων.

Με τον όρο αυθεντικοποίηση προσδιορίζεται η διεργασία της πιστοποίησης και επιβεβαίωσης της ταυτότητας ενός χρηστή, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που αυτός έχει στην κατοχή του. Εδικότερα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός

χρηστή ή κάποιων στοιχειών της. Σε καμία αντίθετη περίπτωσης δε θα πρέπει η αυθεντικοποίηση ενός χρήστη να συσχετίζεται με την παροχή εξουσιοδότησης στους πόρους του Π.Σ.

1.5.1 Μηχανισμοί Αυθεντικοποίησης

Τα συστήματα αυθεντικοποίησης είναι πιθανόν να διαχωριστούν στην βάση της μεθόδου, η οποία χρησιμοποιείται για την πιστοποίηση της ταυτότητας ενός χρήστη. Οι μέθοδοι αυτοί διαχωρίζονται (Burr et al., 2011) ως εξής:

- Κάτι που γνωρίζει ο χρήστης, για παράδειγμα ένα συνθηματικό.
- Κάτι που κατέχει ο χρήστης, όπως για παράδειγμα μία έξυπνη κάρτα.
- Κάποιο χαρακτηριστικό γνώρισμα, βιομετρικές μέθοδοι για παράδειγμα βιομετρικά στοιχεία.
- Συνδυασμός κάποιων από τα προηγούμενα χαρακτηριστικά γνωρίσματα.

Οι μηχανισμοί αυθεντικοποίησης, ανεξάρτητα από τα χαρακτηριστικά που χρησιμοποιούν, αξιοποιούν δύο ειδή κλειδιών:

- Μυστικά κλειδιά: Σε αυτά περιλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά.
- Ασύμμετρα κλειδιά: Σε αυτά περιλαμβάνονται τα ζεύγη κλειδιών, από τα οποία το ένα είναι δημόσια γνωστό (δημόσιο κλειδί), ενώ το άλλο παραμένει μυστικό (ιδιωτικό κλειδί) (Burr, 2011).

Τα συστήματα αυθεντικοποίησης είναι δυνατόν να προσδιοριστούν και ως μονοδιάστατα ή πολυδιάστατα, στην βάση των διαφορετικών χαρακτηριστικών που κάνουν χρήση, με σκοπό την εξασφάλιση του επιθυμητού επίπεδου βεβαιότητας για την ταυτότητα κάποιας ηλεκτρονικής οντότητας. Για παράδειγμα, η χρησιμοποίηση ενός ιδιωτικού κλειδιού ως διακριτικού αυθεντικοποίησης, που είναι προστατευμένο από το συνθηματικό του χρήστη, περιγράφει ένα παράδειγμα δισδιάστατου συστήματος αυθεντικοποίησης.

ΚΕΦΑΛΑΙΟ_2: Νομικό πλαίσιο και ανάγκη προστασίας προσωπικών δεδομένων.

2.1 Νομικό πλαίσιο και προστασία προσωπικών δεδομένων.

Το δικαίωμα στην προστασία της ιδιωτικής σφαίρας κάποιου ατόμου έναντι αυθαίρετων επεμβάσεων, και ειδικότερα του κράτους, κατοχυρώνεται σε διεθνές νομοθετική έκθεση για πρώτη φορά το 1948 στο άρθρο 12 της Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών για τα Ανθρώπινα Δικαιώματα, και σχετιζόταν με το σεβασμό της ιδιωτικής και ζωής εντός της οικογένειας. Η Οικουμενική Διακήρυξη επηρέασε και την θέσπιση νομοθετικών προτοβουλείων για τα ανθρώπινα δικαιώματα στην Ευρώπη (ΟΗΕ, 1948).

2.1.1 Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ)

Το Συμβούλιο της Ευρώπης τέθηκε σε λειτουργία λίγο μετά τον τερματισμό του Β' Παγκοσμίου Πολέμου με συνεργασία των ευρωπαϊκών κρατών με σκοπό την προαγωγή του κράτους δικαίου, της δημοκρατίας, τα ανθρώπινα δικαιωμάτων και γενικότερα την κοινωνική πρόοδο και ανάπτυξης. Έτσι στα πλαίσια της προώθησης αυτού του σκοπού, το 1950 έθεσε σε εφαρμογή την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία τέθηκε σε ισχύ το 1953.

Η συμμόρφωση προς την ΕΣΔΑ χαρακτηρίζεται ως διεθνή υποχρέωση των κρατών. Πλέον, όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης (ΣτΕ) έχουν εντάξει στην νομοθεσία τους την ΕΣΔΑ ώστε να προσδιορίζει την προστασία των ανθρωπίνων δικαιωμάτων και κατ' επέκταση των προσωπικών δικαιωμάτων. Έτσι δεσμεύονται να δρουν στο πλαίσιο αυτών των διατάξεων.

Το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) ιδρύθηκε στο Στρασβούργο της Γαλλίας το 1959, με στόχο την εξασφάλιση και τήρηση από τα συμβαλλόμενα μέρη των υποχρεώσεων που πηγάζουν από την ΕΣΔΑ. Το ΕΔΔΑ διασφαλίζει την τήρηση των προαναφερθέντων υποχρεώσεων από τα κράτη μελετώντας προσφυγές φυσικών προσώπων, ενώσεων προσώπων, ΜΚΟ ή νομικών προσώπων που εμφανίζεται να παρουσιάζουν παραβιάσεις της ΕΣΔΑ. Το 2013, το Συμβούλιο της Ευρώπης αποτελείτο από 47 κράτη μέλη, 28 εκ των οποίων είναι όλα και κράτη μέλη της ΕΕ, τότε. Τα άτομα που ζητούν την συνδρομή της ΕΔΔΑ δεν είναι αναγκαίο να είναι πολίτες κράτους μέλους του ΣτΕ. Το ΕΔΔΑ θέτει υπό μελέτη επίσης διακρατικές προσφυγές, οι οποίες γίνονται από ένα ή περισσότερα κράτη μέλη του ΣτΕ κατά άλλου κράτους μέλους.

Το δικαίωμα στην προστασία των προσωπικών δεδομένων είναι τμήμα των δικαιωμάτων του άρθρου 8 ΕΣΔΑ, το οποίο αποτελεί εγγύηση των δικαιωμάτων που αφορούν το σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και προσδιορίζει τους κανόνες υπό τις οποίες επιτρέπονται περιορισμοί στα προαναφερθέντα δικαιώματα.

Συνολικότερα η νομολογία του, το ΕΔΔΑ κάλυψε ένα πολύ μεγάλο σύνολο πολλών υποθέσεων στις οποίες προέκυπταν ζητήματα προστασίας των προσωπικών δεδομένων. Οι σημαντικότερες από αυτές αφορούσαν υποκλοπή επικοινωνιών, διαφορές μορφές παρακολούθησης και προστασία έναντι της διατήρησης προσωπικών δεδομένων από δημόσιες αρχές (ΣτΕ, 1950).

2.1.2 Σύμβαση 108 του Συμβουλίου της Ευρώπης

Η είσοδος της πληροφορικής τη δεκαετία του 1960, προσδιόρισε μια νέα δυναμική και πραγματικότητα, δηλαδή μια αυξανομένη ανάγκη θέσπισης λεπτομερέστερων κανόνων για υπεράσπισης των δικαιωμάτων του ανθρώπου μέσα από την προστασία των προσωπικών δεδομένων του. Έως τα μέσα της δεκαετίας του ‘70, η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης ενέταξε στο οπλοστάσιο της ποικίλα ψηφίσματα που αφορούσαν την προστασία των προσωπικών δεδομένων, διά παραπομπής στο άρθρο 8 ΕΣΔΑ (ΕΔΔΑ, 2008).

Το 1981 άνοιξε η διαδικασία για υπογραφή της Σύμβαση για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων. Η Σύμβαση 108 ήταν και είναι η μοναδική νομικά δεσμευτική διεθνής σήμανση στον τομέα της προστασίας των προσωπικών δεδομένων (ΣτΕ, (ETS αριθ. 108) 1999).

Η Σύμβαση 108 βρίσκει εφαρμογή σε κάθε επεξεργασία προσωπικών δεδομένων που πηγάζει τόσο από τον ιδιωτικό όσο και τον δημόσιο τομέα, όπως για παράδειγμα η διεργασίες που προκύπτουν από δικαστικές αρχές και από αρχές επιβολής του νόμου. Η σύμβαση παρέχει προστασία στο άτομο από ενδεχόμενες καταχρηστικές ενέργειες κατά τη συλλογή και επεξεργασία προσωπικών δεδομένων και ταυτόχρονα επιδιώκει να ελέγξει και τη διασυνοριακή ροή προσωπικών δεδομένων. Όσον αφορά τη συγκέντρωση και επεξεργασία προσωπικών δεδομένων, οι αρχές που δημιουργούνται και σχετίζονται ιδίως τη θεμιτή και νόμιμη συλλογή και αυτοματοποιημένη επεξεργασία δεδομένων, τα οποία συγκεντρώνονται για συγκεκριμένους θεμιτούς σκοπούς και δεν χρησιμοποιούνται για σκοπούς ασύμβατους προς αυτούς, ούτε διατηρούνται για χρονικό διάστημα μεγαλύτερο του χρειαζούμενου. Αφορούν ακόμα την ποιότητα των δεδομένων, ιδίως στην βάση της πρόβλεψης ότι τα δεδομένα επιβάλλεται να είναι αναγκαία, πρόσφορα και όχι υπερβολικά όπως και ακριβή.

Η Σύμβαση, εκτός των εγγυήσεων που προσφέρει για τη συλλογή και την επεξεργασία προσωπικών δεδομένων, δεν επιτρέπει, ελλείψει κατάλληλων νομικών εγγυήσεων, την επεξεργασία «ευαίσθητων» δεδομένων, όπως των δεδομένων που αφορούν τη φυλή, τις πολιτικές πεποιθήσεις, την υγεία, τη θρησκεία, τη σεξουαλική ζωή και το ποινικό μητρώο του προσώπου.

Η Σύμβαση κατοχυρώνει ακόμα το δικαίωμα του προσώπου να έχει ειπούν του τι είδους στοιχεία διατηρούνται σχετικά με αυτό και, στην περίπτωση που είναι αναγκαίο, να επιδιώξει τη διόρθωσή τους. Περιορισμοί των δικαιωμάτων που κατοχυρώνονται με τη Σύμβαση είναι δυνατόν να τεθούν μόνον όταν διακυβεύεται υπέρτερο συμφέρον, όπως για παράδειγμα η εθνική ασφάλεια ή η εθνική άμυνα.

Η Σύμβαση προβλέπει μεν την ελεύθερη ροή προσωπικών δεδομένων μεταξύ των συμβαλλόμενων μερών, παρόλα αυτά επιβάλλει ένα σύνολο περιορισμών προς τα κράτη που η νομοθεσία των οποίων δεν παρέχει ισοδύναμη προστασία. Με σκοπό την περαιτέρω ανάπτυξη των γενικών αρχών και κανόνων που προκύπτουν μέσα από

την Σύμβαση 108, η Επιτροπή Υπουργών του ΣτΕ έχει εκδώσει πλήθος μη δεσμευτικών κανονισμών.

Το σύνολο των κρατών μελών της ΕΕ έχουν ενσωματώσει τη Σύμβαση 108. Το 1999, η Σύμβαση 108 τροποποιήθηκε ώστε να παρασχεθεί η δυνατότητα υιοθέτησης της από την ΕΕ. Το 2001 ενσωματώθηκε πρόσθετο πρωτόκολλο στη Σύμβαση 108, το οποίο προσδιορίζει τις διατάξεις που αφορούσαν τη διασυνοριακή ροή δεδομένων προς μη συμβαλλόμενα μέρη, τις αποκαλούμενες «τρίτες χώρες», και σχετικά με την δεσμευτική σύσταση εθνικών εποπτικών αρχών προστασίας των δεδομένων (ΣτΕ, 2001).

Η απόφαση για ανανέωση και εκσυγχρονισμό της Σύμβασης 108, μέσα από δημόσια διαβούλευση που έγινε το 2011,προσδιορίσε και επιβεβαίωσε δύο κεντρικοί στόχοι: από την μια την ενίσχυση της προστασίας της ιδιωτικότητας στον ψηφιακό χώρο και, από την άλλη, την ενίσχυση του μηχανισμού επόπτευσης της Σύμβασης.

Η Σύμβαση 108 είναι ανοικτή στην προσχώρηση και μη κρατών μελών του ΣτΕ, όπως και χωρών που δεν είναι στην Ευρώπη. Η δυνατότητα της Σύμβασης να τεθεί και ως οικουμενικό πρότυπο και ο μη περιοριστικός χαρακτήρας της θα ήταν δυνατόν να διατελέσει τη βάση για την προώθηση της προστασίας των δεδομένων σε διεθνές επίπεδο.

Μέχρι στιγμής, τα 45 από τα 46 συμβαλλόμενα μέρη στη Σύμβαση 108 είναι κράτη μέλη του ΣτΕ. Η πρώτη μη ευρωπαϊκή χώρα που μπήκε σε αυτήν ήταν η Ουρουγουάη, τον Αύγουστο 2013, το δε Μαρόκο που προσκλήθηκε να εισέρθει στη Σύμβαση 108 από την Επιτροπή Υπουργών και αναμένετε η διαδικασία επισημοποίησης της προσχώρησής του.

2.1.3 Ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Οι πρώτες συνθήκες των Ευρωπαϊκών Κοινοτήτων δεν εμπεριείχαν κάποια αναφορά στα ανθρώπινα δικαιώματα πόσο μάλλον σε πιθανή προστασία τους. Με την έναρξη όμως των διαδικασιών παρεμπόδισης τους ενώπιον και την έκθεση τέτοιων περιπτώσεων στο Δικαστήριο των Ευρωπαϊκών Κοινοτήτων (ΔΕΚ) που σχετίζονταν με πιθανές παραβιάσεις ανθρωπίνων δικαιωμάτων σε τομείς που σχετίζονταν με το πεδίο εφαρμογής του ενωσιακού δικαίου, ξεκίνησε η ανάπτυξη

μιας καινούριας προσέγγισης. Για την παροχή προστασίας στο άτομο, τα θεμελιώδη δικαιώματα υιοθετήθηκαν στις αναφερόμενες «γενικές αρχές» του ευρωπαϊκού δικαίου. Με βάσει το Δικαστήριο, οι εν λόγω γενικές αρχές περιγράφουν το περιεχόμενο της προστασίας των ανθρωπίνων δικαιωμάτων που προβλέπεται στα εθνικά συντάγματα και στις συνθήκες για τα δικαιώματα του ανθρώπου, ιδίως στην ΕΣΔΑ. Το Δικαστήριο προσδιόρισε ότι θα διασφαλίσει τη συμμόρφωση του ενωσιακού δικαίου προς τις εν λόγω αρχές.

Με την προϋπόθεση ότι οι πολιτικές πιθανόν να έχουν επίδραση στα ανθρώπινα δικαιώματα και σε μια στόχευση της ΕΕ να κάνει τους πολίτες να την νοιώθουν «πιο κοντά» στην ΕΕ. Το 2000 η ΕΕ προέβη σε διακήρυξη του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτη»). Ο Χάρτης ενσωματώνει το σύνολο των ατομικών, πολιτικών, οικονομικών και κοινωνικών δικαιωμάτων των ευρωπαίων πολιτών, σε μία σύνθεση των κοινών συνταγματικών εθίμων και των κοινών διεθνών υποχρεώσεων των κρατών μελών. Τα δικαιώματα που προσδιορίζονται στον Χάρτη χωρίζονται σε 6 κεφάλαια: αξιοπρέπεια, ελευθερίες, ισότητα, αλληλεγγύη, δικαιώματα των πολιτών και δικαιοσύνη. Παρότι στην αρχη ο Χάρτης αποτελούσε αποκλειστικά πολιτικό έγγραφο, κατέστη νομικά δεσμευτικός ως πρωτογενές ενωσιακό δίκαιο με το να ξεκίνα να ισχύει με την Συνθήκη της Λισαβόνας την 1η Δεκεμβρίου 2009 (Συνθήκης για την Ευρωπαϊκή Ένωση, Ευρωπαϊκές Κοινότητες (2012).

Το πρωτογενές ενωσιακό δίκαιο αναφέρεται ακόμα στη γενική αρμοδιότητα της ΕΕ να νομοθετεί σε θέματα προστασίας των δεδομένων. Ο Χάρτης αναφέρατε αποκλειστικά στο μόνο τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, αλλά κατοχυρώνει και το δικαίωμα στην προστασία των δεδομένων, αναβαθμίζοντας ρητά την προσφερόμενη προστασία σε επίπεδο θεμελιώδους δικαιώματος στο ενωσιακό δίκαιο. Τα θεσμικά όργανα της ΕΕ και τα κράτη μέλη είναι υποχρεωμένα να σέβονται και να εγγυώνται το εν λόγω δικαίωμα, αναγκαιότητα η οποία ισχύει και για τα κράτη μέλη όταν εφαρμόζουν το δίκαιο της Ένωσης. Το άρθρο 8 του Χάρτη, το οποίο δημιουργήθηκε αρκετά χρόνια μετά την Οδηγία για την προστασία των προσωπικών δεδομένων, πρέπει να προσδιορίζεται ως ενσωμάτωση του προϋπάρχοντος ενωσιακού δικαίου στον ζητήμα αυτό. Ως εκ τούτου, ο Χάρτης δεν περιλαμβάνει απλώς ρητή αναφορά στο δικαίωμα.

Τον Ιανουάριο 2012, η Ευρωπαϊκή Επιτροπή πρότεινε ένα σύνολο μέτρων για τον επαναπροσδιορισμό της προστασίας των προσωπικών δεδομένων, δηλώνοντας ότι οι υπάρχοντες κανόνες είναι δεδομένο και επιβάλλεται να συνταχθούν με την εποχή στο πλαίσιο των ραγδαίων τεχνολογικών εξελίξεων και της παγκοσμιοποίησης. Η μεταρρυθμιστική δέσμη είναι από πρόταση Γενικού Κανονισμού για την προστασία των προσωπικών δεδομένων ο οποίος θα αντικαταστήσει την Οδηγία για την προστασία των προσωπικών δεδομένων, καθώς και από καινούργια Οδηγία για την προστασία των προσωπικών δεδομένων η οποία θα προσδιορίζει τους τομείς της αστυνομικής και της δικαστικής συνεργασίας σε ποινικές υποθέσεις. Κατά τον χρόνο έκδοσης του παρόντος εγχειριδίου, η συζήτηση σχετικά με τη μεταρρυθμιστική δέσμη είναι σε διαβούλευσης (Ευρωπαϊκή Επιτροπή, 2012).

2.1.4 **Προσδιορισμός δικαιωμάτων**.

`Το δικαίωμα στην προστασία των δεδομένων δεν χαρακτηρίζεται ως απόλυτο. Είναι υποχρεωτικό να σταθμίζεται σε σχέση με τα υπόλοιπο άλλα δικαιώματα. Το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που κατοχυρώνεται στο άρθρο 8 του Χάρτη «δεν είναι πάντως απόλυτο, αλλά επιβάλλεται να λαμβάνεται υπόψη σε σχέση με τον ρόλο που επιτελεί στην κοινωνία».
Εξάλλου, το άρθρο 52 του Χάρτη περιγράφει ότι επιτρέπεται ο προσδιορισμός περιορισμών στην άσκηση δικαιωμάτων, όπως των άρθρων 7 και 8 αυτού, υπό την προϋπόθεση ότι οι περιορισμοί αυτοί περιγράφονται από τον νόμο, ώστε να βασίζονται στο βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών και, στηρίζονται στην αρχή της αναλογικότητας, είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε σκοπούς γενικού συμφέροντος που καθορίζει η Ευρωπαϊκή Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών τρίτων.

Ως εκ τούτου, κατά πάγια νομολογία τόσο του ΕΔΔΑ όσο και του ΔΕΕ, επιβάλλεται να γίνεται ορθή στάθμιση δικαιωμάτων στην εφαρμογή και την ερμηνεία του άρθρου 8 ΕΣΔΑ και του άρθρου 8 του Χάρτη (ΔΕΕ, 2010).

2.1.5 **Πρόσβαση σε έγγραφα**

Η ελευθερία της πληροφόρησης στην βάση του με το άρθρο 11 του Χάρτη και το άρθρο 10 της ΕΣΔΑ προσφέρει προστασία στο δικαίωμα όχι μόνο της μετάδοσης αλλά και της λήψης δεδομένων. Η πιστοποίηση της σημασίας της κρατικής διαφάνειας στην προώθηση και λειτουργία της μιας δημοκρατικής κοινωνίας αυξάνεται συνεχώς. Ως εκ τούτου, τις 2 τελευταίες δέκατες το δικαίωμα πρόσβασης σε έγγραφα που υπάρχουν στα αρχεία των δημόσιων αρχών, προσδιορίστηκαν ως σημαντικά δικαίωματα κάθε πολίτη της Ευρωπαϊκής Ένωσης και κάθε φυσικού ή νομικού προσώπου που διαμένει ή έχει την έδρα του σε κράτος μέλος.

Στο πλαίσιο του δικαίου του ΣτΕ, είναι πιθανόν να προκύψει αναφορά στις αρχές που προσδιορίζονται στη σύσταση σχετικά με την προσβασιμότητα σε επίσημα έγγραφα, η οποία αποτέλεσε την πηγή έμπνευσης των συντακτών της Σύμβασης για την πρόσβαση σε επίσημα έγγραφα (*Σύμβαση 205*) (ΔΕΕ, 2010).

Στο πλαίσιο του δικαίου της ΕΕ, το δικαίωμα πρόσβασης σε έγγραφα προσδιορίζεται από τον Κανονισμό 1049/2001 για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής. Με το άρθρο 42 του Χάρτη και το άρθρο 15 παράγραφος 3 ΣΛΕΕ, το δικαίωμα πρόσβασης επεκτάθηκε «σε έγγραφα των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, ανεξαρτήτως υποθέματος». Σύμφωνα με το άρθρο 52 παράγραφος 2 του Χάρτη, το δικαίωμα πρόσβασης σε δημόσια έγγραφα ασκείται ακόμα υπό τους όρους και εντός των ορίων που προσδιορίζονται στο άρθρο 15 παράγραφος 3 ΣΛΕΕ. Το δικαίωμα αυτό δεν αποκλείεται περιέλθει σε σύγκρουση με το δικαίωμα στην προστασία των προσωπικών δεδομένων εάν η πρόσβαση αυτή συντελεί σε αποκάλυψη προσωπικών δεδομένων τρίτου. Παρόλα αυτά, τα αιτήματα πρόσβασης σε έγγραφα ή πληροφορίες που είναι στην κατοχή δημόσιων αρχών πιθανόν να είναι υποχρεωτικό να πρέπει να σταθμίζονται με το δικαίωμα προστασίας των προσώπων, τα δεδομένα των οποίων συμπεριλαμβάνονται στα απαιτουμενα έγγραφα. Στην βάση αυτής της απόφασης, για οποιοδήποτε περιορισμό στο δικαίωμα προστασίας των προσωπικών δεδομένων σε σχέση προς την πρόσβαση σε έγγραφα απαιτείται να προκύπτει ειδικός και θεμιτός λόγος. Το δικαίωμα πρόσβασης σε έγγραφα δεν είναι

δυνατόν να προσδιορίζονται αυτόματα το προβάδισμα έναντι του δικαιώματος προστασίας των δεδομένων (ΕΔΔΑ, 2013).

2.2 Τρόποι προστασίας ιδιωτικότητα και προσωπικών δεδομένων.

Στην προσπάθεια προσδιορισμού των τρόπων για την προστασία των προσωπικών δεδομένων είναι αναγκαίο να ορισθεί η έννοια της ιδιωτικότητας και με αυτό ξεκινά το αυτή η ενότητα. Και ακολουθεί ο προσδιορισμός της έννοια αυτής σε συνδυασμό με την πληροφοριακή της διάσταση.

2.2.1Τι είναι η ιδιωτικότητα

Στην προσπάθεια προσδιορισμού της ιδιωτικότητας, διακρίνεται η δυσκολία να προσφερθεί μια έννοια που να την καθορίζει συνολικά, από την άλλη όμως είναι εμφανής η ευκολία στην υπεράσπιση της. Είναι αρκετά γνωστή η συνηγορία των αμερικανών δικαστών Warren και Brandeis (1896) υπέρ του δικαιώματος του ατόμου σε μία ανεμπόδιστη ιδιωτική ζωή, είναι τόσο συνήθης όσο και, πλέον, ανεπαρκής για τον ορισμό ή ακριβέστερα τον προσδιορισμό της ιδιωτικότητας. Έναν αιώνα και πλέον υπό την σημαντικότατη επίδραση της τεχνολογικής επανάστασης, η «κλασική» αντίληψη της ιδιωτικότητας έχει ενσωματώσει και επιπλέον στοιχεία με επιμέρους δικαιώματα, όπως για παράδειγμα το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο πλήρης έλεγχος της πρόσβασης στον ιδιωτικό χώρο (κατοικίας), η ελαχιστοποίηση των «παρεμβάσεων», η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της υπό στενή έννοια ιδιωτικότητας , της ανωνυμίας και της απόσυρσης (Παπαδημητρίου, 2004).

2.2.2 Η ιδιωτικότητα στην πληροφοριακή.

Ο χρόνος δείχνει τα σημάδια τους στην έννοια της ιδιωτικότητας σε συνδυασμό με την τεχνολογία και την γενικότερη εξέλιξη των κοινωνιών. Εστί μέσα σε αυτό το πλαίσιο γίνεται όλο και περισσότερο αντιληπτό ότι η ιδιωτικότητα ως αξίωση σεβασμού του απόρρητου προσφέρει αναγκαία μεν, ανεπαρκή παρόλα αυτά προστασία στο άτομο. Η διεύρυνση της ιδιωτικότητας αλλά και η αναγκαιότητα

προσδιορισμού και οριοθέτησης των στοιχείων που επιβάλλεται να την διέπουν έναντι των προσβολών πρόεκυψε ως επιτακτικότερη, όταν κατέστη αντιληπτή η ποιοτική διαφορά στις δυνατότητες συγκέντρωσης, επεξεργασίας, διάχυσης, συσχετισμού των πληροφοριών που κατασκεύαζαν τα πληροφοριακά και επικοινωνιακά συστήματα και κυρίως η δυνατότητα χρησιμοποίησης τους, ανταλλαγής και συσχετισμού των δεδομένων που έχουν συγκεντρωθεί για πολλαπλούς και διαφορετικούς από τους αρχικούς σκοπούς.

Η τεχνολογική ανάπτυξη και η αναγκαστική είσοδου στη ζωή και στην επικοινωνία του ατόμου, στην προσωπικότητα και στις συνήθειες του προσδιόρισε την ποιοτική διάσταση των κινδύνων που σχετίζονται με την αναδυόμενη Κοινωνία της Πληροφορίας, καθώς ήδη η ποσοτική αύξηση προσδιόριζε την αύξηση της έντασης, του βαθμού προσβολής των δικαιωμάτων. Από τις αρχές του ‘70 που οι ηλεκτρονικοί υπολογιστές έκαναν τα πρώτα τους βήματα σε επίπεδο φιλοσοφικό, πολιτικό και νομικό. Πρόεκυψαν ζητήματα που αναφέρονταν στο δικαίωμα στην πληροφοριακή πλέον ιδιωτικότητα και αργότερα τέθηκαν στο επίκεντρο μιας διαβούλευσης που υπέθετε στην τεχνολογία της πληροφορικής τους κινδύνους ενός καινουργίου «Πανοπτικού», το οποίο, σε αντίθεση με το Panopticon του Bentham, δεν περιοριζόταν σε κλειστές επιτηρούμενες κοινότητες αλλά θα σχετιζόταν προοπτικά το σύνολο των ατόμων και των δραστηριοτήτων τους (Bentham, 1995).

Η «διαφανής κοινωνία» ή ο «διαφανής πολίτης», συνήθεις εκφράσεις κυρίως στα κείμενα των δεκαετιών του ’70 ακόμα και του ’ 80, δεν είναι ακριβώς μόνο το αποτέλεσμα μιας συγκεντρωτικής κρατικής εξουσίας που αυξάνει το σύνολο της συλλογής της στοιχείων, η εκπλήρωση της κασσάνδρειας προφητείας του Orwell (1948), αλλά, πολύ περισσότερο, συνέπεια της διάχυσης της επεξεργασίας της πληροφορίας στο κράτος, την οικονομία και την κοινωνία. Κατέστη ακόμα προφανής ότι η όλο και μεγαλύτερη αύξηση των ικανότητων επεξεργασίας της προσωπικής πληροφορίας προσδιοριζόταν από σχέση αντιστρόφως ανάλογη προς την ικανότητα του προσώπου να έχει υπό έλεγχο του τη χρήση των πληροφοριών που το αφορούν. Το διακυβευόμενο αγαθό δεν είναι πια πλέον η προστασία της αξίωσης για ανενόχλητη ιδιωτική σφαίρα αλλά αφορά την απώλεια ελέγχου επί των στοιχείων που αφορούν προσωπικές πληροφορίες. Στην βάση μάλιστα του «κλασικού» ορισμό του Westin, η ίδια η έννοια της ιδιωτικότητας περιγράφεται ακριβώς ως η αξίωση των

ατόμων, ομάδων ή θεσμών να προσδιορίζουν οι ίδιοι πότε, πως και σε ποιο επίπεδο οι πληροφορίες που τους αφορούν θα γίνονται γνωστές στους άλλους (Westin, 1967).

Η θεωρία του ελέγχου, όπως προσδιορίστηκε στις ΗΠΑ, εξελίχθηκε με την έμφαση στη σχέση ιδιωτικότητας και ελευθερίας, η ιδιωτικότητα αναφέρεται στην ικανότητα των προσώπων να διαμορφώνουν άποψη για τη ζωή τους και να ζουν στην βάση αυτής. Η σχετική αμερικανική θεωρία διαμορφώνεται, χωρίς να ταυτίζεται, με την κυρίαρχη ευρωπαϊκή προσέγγιση, όπως αυτή προκύπτει τόσο από τη θεωρία όσο και από τη νομολογία. Η προστασία της ιδιωτικότητας χαρακτηρίζει την αυτονομία του ανθρώπου, τη συμμετοχή στην κοινωνική ζωή και την επικοινωνία του με τον περίγυρο του. Όπως χαρακτηριστικά επισημαίνει το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου, το άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου που προσδιορίζει την προστασία του ιδιωτικού βίου και αποσκοπεί κατά κύριο λόγο στην εξασφάλιση της ανάπτυξης, χωρίς εξωτερική παρέμβαση, της προσωπικότητας κάθε ατόμου στη σχέση του με τον κοινωνικό περίγυρο (Gaskin,1989).

Η προσέγγιση αυτή διακρίνεται να επικρατεί στη νομική θεωρία και τη νομολογία των δικαστηρίων, τόσο υπερεθνικών όσο και εθνικών. Το γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο, αναφερόμενο στο δικαίωμα του πληροφοριακού αυτοπροσδιορισμού, συσχέτιζε την ανάπτυξη της προσωπικότητας στην κοινωνική συναναστροφή, τη διαμόρφωση ίδιας γνώμης, την ελευθερία απόφασης και τη συμμετοχή στον κοινωνικό και πολιτικό διάλογο από την ελευθερία του πολίτη να συναποφασίζει ποιες πληροφορίες που σχετίζονται με αυτόν θα μπορούν να γίνουν γνώστες στο περιβάλλον του και αφετέρου τη δυνατότητα να ελέγχει τον πληροφοριακό και αξιολογικό ορίζοντα αυτών με τους οποίους έρχεται σε επαφή. Η προστασία των επιλογών ζωής έναντι του δημόσιου ελέγχου σχετίζεται περαιτέρω με την ισότητα καθώς προστατεύει τα άτομα απέναντι στη κοινωνική δυσμένεια ή των διακρίσεων που είναι δυνατόν να συνεπάγεται η συχνά μη σύννομη ή/και μη εξουσιοδοτημένη γνώση μίας πληροφορίας (Laurie, 2002).

Στην ικανότητα των ατόμων για ελεύθερες αποφάσεις και επιλογές, χωρίς παρεμβάσεις, προσδιορίζεται ο έλεγχος, που σχετίζεται με τη λειτουργία μιας

κοινωνίας ελευθερίας. Η ελευθερία της απόφασης δεν χαρακτηρίζεται από την μόνο από την σημαντικότητα της σε σχέση με το άτομο, δεν συνιστά απλώς μέσο για την πραγμάτωση των αντιλήψεων και των στόχων του σύμφωνα με τις αντιλήψεις του. Η πληροφοριακή δηκτικότητα στοχεύει μέσα από την θεσμική της στο να γίνει εφικτό, το άτομο να συμμετέχει στις διαδικασίες της κοινωνίας. Καθιστά παράλληλα δυνατή την παροχή και άλλων ελευθεριών όπως, την απόλαυση άλλων ατομικών δικαιωμάτων, όπως η ελευθερία της έκφρασης, η συμμετοχή σε πολιτικές και συνδικαλιστικές ενώσεις την θρησκευτική ελευθερία κα.. Με κάθε τέτοια απόφαση εξασφαλίζεται το δημόσιο συμφέρον την τοποθέτηση των βάσεων για μια εξελίξιμη κοινωνία που βασίζεταιστη συμμετοχή των ατόμων στις κοινωνικές και πολιτικές διεργασίες, στον ελεύθερο δημόσιο διάλογο και την πολλαπλότητα (Δόνος, Μήτρου, Μίττλεττον, Παπακωνσταντίνου, 2002).

2.2.3 Προστασία προσωπικών δεδομένων

Έχει ήδη επισημανθεί, η αναγκαιότητά της προστασίας της ιδιωτικότητας προβάλλει, πιο έντονα όταν γίνεται κατανοητή η ποσοτική και ποιοτική διαφορά στις δυνατότητες συλλογής και επεξεργασίας πληροφοριών που προσέφεραν τα πληροφοριακά συστήματα. Τα οποία προσέφεραν την δυνατότητα την πολυλειτουργική χρήση και την «αποξένωση» της πληροφορίας από τον φορέα της, το αρχικό περιβάλλον και τους αρχικούς σκοπούς της συλλογής και επεξεργασίας της. Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η αποκέντρωση της επεξεργασίας, η διείσδυση της επεξεργασίας και της δικτύωσης στο πλαίσιο ενός συνολικόερου πεδίου της ανθρώπινης δραστηριότητας προσδιορίζουν και αλλάζουν με έντονο τρόπο το περιβάλλον χρήσης της προσωπικής πληροφορίας, αλλά και τα ζητήματα που προκύπτουν σε σύγκριση με την προστασία τους. Σε αυτό το πλαίσιο προκύπτει το αίτημα για προστασία προσωπικών δεδομένων. Σε αντίθεση με την ιδιωτικότητα υπό στενή έννοια, η προστασία προσωπικών δεδομένων προάγεται ως αίτημα που προκύπτει σε συνδυασμό με την τεχνολογική εξέλιξη, καθώς αξιολογείται πως οι υφιστάμενες ρυθμίσεις δεν παρέχουν επαρκή προστατευτική ασπίδα έναντι των το προβαλλόμενων κινδύνων (Samuelson, 2000).

Συνυπολογίζοντας τις ιδιαίτερες ικανότητες και επιδράσεις της ηλεκτρονικής επεξεργασίας προσωπικής πληροφορίας, η προστασία προσωπικών δεδομένων δεν πρέπει να προσδιορίζεται από τη ρύθμιση και την προστασία της πληροφορίας που το άτομο χαρακτηρίζει ως ιδιωτική και ευαίσθητη και για τον λόγο αυτό επιθυμεί να απαγορεύσει ή να περιορίσει τη συλλογή, χρήση και διάδοσή της. Αφορά οποιαδήποτε πληροφορία που σχετίζεται με ένα φυσικό πρόσωπο, καθώς η πληροφοριακή αξία ακόμη και μίας καταρχήν «αβλαβούς» πληροφορίας προσδιορίζεται εν τέλει από την επεξεργασία της, τον συνδυασμό της με άλλα στοιχεία, από το περιβάλλον εντός του οποίου γίνεται χρήση και αξιολογείται (Hustinx, 2005).

Στο πλαίσιο της προστασίας προσωπικών δεδομένων ο πληροφοριακός αυτοκαθορισμός δεν καθορίζεται στην αξίωση για παρεμπόδιση της μη εξουσιοδοτημένης χρήσης ή της αποκάλυψης σε τρίτους. συναποτελείται και προσδιορίζεται από ένα σύνολο αρχών, δικαιωμάτων και εγγυήσεων. Ως δίκαιο προστασίας προσωπικών δεδομένων που αναφέρεται στο σύνολο των κανόνων, προϋποθέσεων, όρων, εξουσιών και απαγορεύσεων συγκριτικά με τη συλλογή και επεξεργασία προσωπικών δεδομένων, καθώς και τις ρυθμίσεις που αφορούν με τις διαδικασίες, θεσμικούς ελέγχους, εγγυήσεις και αντίβαρα των περιορισμών των δικαιωμάτων προστασίας των προσωπικών δεδομένων των ατόμων (Solove, 2008).

2.2.4 Ιδιωτικότητα-ασφάλεια-απόρρητο

Η «κλασική» προσέγγιση της ιδιωτικότητας ως refugium παραπέμπει στον προσδιορισμό καταφυγίου, και αναφέρεται σε στοιχεία ταύτισης ή και σύγχυσης με την έννοια που προσδιορίζει το και την εμπιστευτικότητας. Οι όροι αυτοί, αν και συνήθως προσδιορίζονται και χρησιμοποιούνται ως ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται. Η έννοια του απόρρητου προσδιορίζεται είτε τη μη προσπελασιμότητα ορισμένων πληροφοριών που επαφίενται στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να εξασφαλίσουν πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης, είτε τις κατέχουν λόγω της θέσης και της αρμοδιότητάς τους. Εάν πρόκειται για

πληροφορία που σχετίζονται με δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη και εμπιστευτική η πληροφορία είναι αναγκαίο να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.α.(Solove, 2008).

Το "απόρρητο" εμποδίζει τους τρίτους από τη γνώση, τη χρήση και αξιοποίηση των πληροφοριών, εφόσον δεν προκύπτει κάποιος νόμιμος λόγος και η αντίστοιχη διαδικασία που περιλαμβανει την δυνατότητα της άρσης του απορρήτου. Αξίζει πάντως να σημειωθεί ότι σε ορισμένες χώρες, όπως για παράδειγμα στις ΗΠΑ, ήδη το γεγονός ότι ένα πρόσωπο εμπιστεύεται μία πληροφορία που το σχετίζεται με ένα άλλο πρόσωπο ή οργανισμό οδηγεί στη στέρηση της προστασίας που επιφυλάσσεται στην ιδιωτικότητα. Η άποψη αυτή συνδέεται με κρίσιμα για τα πρόσωπα αποτελέσματα, όπως για παράδειγμα το εύρος και τις προϋποθέσεις για περαιτέρω κοινοποίηση των πληροφοριών αυτών. Το Ανώτατο Δικαστήριο των ΗΠΑ (Supreme Court) αναφέρει ότι ένα πρόσωπο δεν έχει εύλογη προσδοκία ιδιωτικότητας, όσον αφορά πληροφορίες που αποκάλυψε με την συγκατάθεση του σε ένα τρίτο πρόσωπο ή οργανισμό και ακολούθως πέρασαν από αυτό σε μία δημόσια αρχή, ακόμη και εάν η πληροφορία προσφέρθηκε αρχικά με την υπόθεση ότι θα γίνει χρήση της για έναν περιορισμένο σκοπό. Στο σημείο αυτό διακρίνεται μία βασική απόκλιση της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης, η χρήση της εν τέλει δεν υπάρχει κατά τη στιγμή που η πληροφορία "παραδίδεται" σε κάποιον άλλον, "διαφεύγει" από το πρόσωπο που αφορά και παύει να προσδιορίζεται ως "μυστική" (Schwartz & Reidenberg)

Η ευρωπαϊκή προσέγγιση, που σχετίζεται με το απόρρητο χαρακτήρα των προσωπικών πληροφοριών δεν προσδιορίζεται αποκλειστικά και μόνο από τη φύση τους αλλά προβλέπεται και ρητά στο εν' λόγω κανονιστικό πλαίσιο. Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την προστασία προσωπικών δεδομένων προσφέρει μία ιδιότυπης αρνητικής διατύπωσης ρύθμιση για το απόρρητο, καθώς αναφέρει ότι όποιος επεξεργάζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας ή του εκτελούντος επεξεργασία πραγματοποιεί αυτή την εργασία μόνο έπειτα από εντολή του υπεύθυνου επεξεργασίας. Ο ελληνικός νόμος για την προστασία προσωπικών δεδομένων (ν. 2472/97) στο άρθρο 10 § 1 περιέχει μεν μία αντίστοιχη διατύπωση

αλλά παραλληλα προσδιορίζει συνολικά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως απόρρητη (Simitis 2006).

Το απόρρητο μέσα από τον προσδιορισμό της εμπιστευτικότητας σχετίζεται επισης με την ασφάλεια των πληροφοριών αλλά δεν ταυτίζεται με αυτή. Η ασφάλεια της πληροφορίας δεν εξυπηρετείται μόνο από την εγγύηση της εμπιστευτικότητας. Η εμπιστευτικότητα διακρίνεται ως μόνο μία από τις παραμέτρους που περιγράφουν την ασφάλεια των πληροφοριών, στην οποία συνυπολογίζεται η εγκυρότητα, η αυθεντικότητα, η ακεραιότητα και η διαθεσιμότητα. Η ασφάλεια χαρακτηρίζει ένα οργανωμένο σύνολο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που είναι απαραίτητα για να προστατευτούν τα στοιχεία ενός πληροφοριακού συστήματος και προφανώς δεν διασφαλίζει μόνο, ίσως ούτε καν κυρίως, τις νομικές διστάσεις (Γκρίτζαλη, 2004).

Σε κάθε περίπτωση, τόσο η κοινοτική όσο και η ελληνική νομολογία για την προστασία προσωπικών δεδομένων είναι τόσο δεδομένη όσο και αναγκαία η λήψη «κατάλληλων» μέτρων ασφάλειας, ώστε να παρέχεται προστασία στα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Ο νομοθέτης επάγει επίσης στον υπεύθυνο επεξεργασίας την υποχρέωση να εξασφαλίζει το επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των στοιχειών (Ν. 2472/97 & άρθρο 17 της Οδηγίας 95/46/ΕΚ).

2.3 **Τα προβλήματα προστασίας προσωπικών δεδομένων στο Διαδίκτυο.**

2.3.1 Η **φύση του Διαδικτύου**

Σαφώς και η χρήση του διαδικτύου προσφέρει καινούργιο πεδίο και νέα ζητήματα ως προς την επεξεργασία και την προστασία των προσωπικών δεδομένων. Προς αυτήν την κατεύθυνση αυτό επιβάλλεται να προσδιοριστούν τα χαρακτηριστικά που είναι μεν γνωστά αλλά χαρακτηρίζονται ως ιδιαίτερα κρίσιμα σε σύγκριση με τη λειτουργία του αλλά και την χρήση των προσωπικών δεδομένων. Το Διαδίκτυο

αποτελεί ένα εκρηκτικό νέο μέσο που αφορά το σύνολο των ανθρωπίνων δραστηριοτήτων. Το φαινόμενο αυτό έχει μεταβάλει ραγδαία και ριζικά τον τρόπο με τον οποίο διαβιούμε και λειτουργούμε ως άτομα, πολίτες, εργαζόμενοι, καταναλωτές κ.α.

Τα τεχνικά εργαλεία είναι νέα όπως για παράδειγμα το browsing software εξελίσσονται με ταχύτατους ρυθμούς. Οι υπηρεσίες που προσφέρονται μέσω αυτής της υποδομής παρέχουν νέες δυνατότητες που σχετίζονται ιδιαίτερα τη διανομή πληροφορίας που περιλαμβάνει προσωπικές πληροφορίες. Το Διαδίκτυο δίνει την δυνατότητα της ταχύτατος διαβίβασης δεδομένων σε κάθε σύστημα, την δυνατότητα διασύνδεσης μεταξύ πληροφοριών που υπάρχουν σε διαφορετικούς χώρους και προσφέρονται για διαφορετικούς σκοπούς. Στην περίπτωση του Διαδικτύου εμπλέκονται αρκετές και διαφορετικές κατηγορίες συμμετεχόντων, οι οποίοι είναι αναρίθμητοι.

Το διαδίκτυο σαφώς και αποτελεί έναν σχετικά καινούργιο πεδίο έκφρασης, ένα διεθνές πεδίο που δεν έχει συνοριακούς περιορισμούς, ένα πεδίο αποκεντρωμένο που κανένας ιδιώτης και κανένα κράτος δεν έχει την δυνατότητα να μπορέσει να το θέση υπό πλήρη τουλάχιστον έλεγχο, ένα πεδίο ετερογενές όπου ο καθένας έχει την δυνατότητας να ενεργήσει, να εκφραστεί και να εργαστεί. Συμβολίζει και ενσωματώνει την παγκοσμιοποίηση της οικονομίας, της κοινωνίας, της ανθρώπινης επικοινωνίας. Η ουσία της μεταβολής προκύπτει στη δημιουργία ενός “ολοκληρωμένου περιβάλλοντος επικοινωνίας”, στο οποίο σε κάθε άτομο παρεχεται η δυνατότητα να επικοινωνήσει με κάθε άτομο κάνοντας χρήση οποιοδήποτε μέσου. Το διαδίκτυο συνυπολογίζει τέλος στα υπέρ του το στοιχείο της αποπλάνησης, της γοητείας που εμπεριέχει αυτή η αμφίδρομη σχέση, στην οποία είναι δύσκολο να αντισταθεί κανείς, η ταχύτητα, η ευκολία της πρόσβασης, η εργονομία της θέσης εργασίας, η χαμηλή τιμή πρόσβασης, ο διάλογος, και οι ποικίλες προσφορές.

Θα πρέπει ολοκληρώνοντας να επισημανθεί μία βασική μεταλλαγή που διενεργήθηκε τα τελευταία χρόνια στη λειτουργία και στο κέντρο βάρους του διαδικτύου. Το διαδίκτυο αρχισε πραγματικά να λειτουργεί ως ένα forum, μία αγορά υπό την έννοια της αρχικής και κυριολεκτικής σημασίας της λέξης, της ελεύθερης ανταλλαγής απόψεων. Όσο όμως στο διαδίκτυο γίνεται χρήση όλο και περισσότερο για μορφές επιχειρηματικής δραστηριότητας και αποτελεί το πεδίο του ηλεκτρονικού

εμπορίου και είναι ευδιάκριτο ότι συμβάλει σε μία μεταβολής της φύσης του και από “αγορά” γίνεται “παζάρι”.

2.3.2 Η επεξεργασία προσωπικών δεδομένων στο Διαδίκτυο

Οι νέες αυτές δυνατότητες υπηρετούν και συμβάλουν τις τάσεις αξιοποίησης και αναπόφευκτα την “εμπορευματοποίησης” των πληροφοριών και ειδικότερα οι προσωπικες πληροφορίες (προτιμήσεις, αγοραστικές σύνηθες, καθημερινότητα κ.α) αποτελούν σημαντικότατα στοιχεία για τις επιχειρήσεις. Η χρήση προσωπικών δεδομένων επιβάλλεται να αποτελούν πρωταρχική προτεραιότητα κατά την χρήση των υπηρεσιών του Διαδικτύου.

Ένα χαρακτηριστικό των δικτύων τηλεπικοινωνιών και ιδιαίτερα του Διαδικτύου είναι η δυνατότητα παραγωγής, μεταφοράς και αποθήκευσης τεράστιας ποσότητας δεδομένων που προκύπτουν ώστε να εξασφαλίσουν τις σωστές διασυνδέσεις. Ένας αριθμός δεδομένων είναι αναγκαίος για την δημιουργία της σύνδεσης, τη διαβίβαση δεδομένων και την χρέωσή της. Τα δεδομένα (δια)σύνδεσης σχετίζονται με τις τεχνικές στις οποίες χρησιμοποιούνται για την αποκατάσταση της σύνδεσης. Πρόκειται αφενός για τις διευθύνσεις των μηχανών του δικτύου (IP) και αφετέρου για τη ιστοσελίδα που επιθυμεί να επισκεφθεί ο “πλοηγός” ή το μήνυμα. Η χρησιμοποίηση του διαδικτύου παράγει προσωπικές πληροφορίες για τους χρήστες. Σε σχέση με το διαδίκτυο προσδιορίζονται καινούργιες μορφές απειλών κατά της ιδιωτικότητας. Οι μορφές αυτές είναι εφικτό να διαχωριστούν σε συστηματικούς και λειτουργικούς λόγους σε δύο μεγάλες κατηγορίες α) την εμφανή συλλογή δεδομένων και β) τη συλλογή δεδομένων εν αγνοία του υποκειμένου-χρήστη των υπηρεσιών του Διαδικτύου.

2.3.2.1 «Εμφανής» συλλογή

Η χαρακτηριζόμενη ως φανερή συλλογή δεδομένων γίνεται είτε με τις πρακτικές που παρατηρούνται στα discussion forums, είτε μέσω της αξιοποίησης και εκμετάλλευσης των ηλεκτρονικών μηνυμάτων είτε μέσω καταλόγων.

Ως προς τα discussion groups/ forums έχει δημιουργηθεί ένα λογισμικό που δίνει την δυνατότητα στον εντοπισμό των ηλεκτρονικών διευθύνσεων και το σύνολο των θεμάτων στα οποία το άτομο έχει λάβει μέρος. Σε αρκετές περιπτώσεις των λεγόμενων news groups η ηλεκτρονική διεύθυνση του ατόμου που λαμβάνει μέρος δημοσιοποιείται συνδυαστικά με το όνομα ή το ψευδώνυμο του. Η καταγραφή είναι δυνατόν να οδηγήσει σε περαιτέρω χρήση των δεδομένων από τον ISP και θα μπορούσε να συνδυαστεί με περισσότερες λεπτομέρειες για το πρόσωπο που συλλέγεται on-line στα chat rooms. Δύο από τους βασικούς στόχους χρήσης αυτών των δεδομένων αποτελούν:

- Ο έλεγχος των χαρακτηριστικών και των στοιχείων του περιεχομένου
- Η διαμόρφωση των καταλόγων προσωπικών δεδομένων.

Ως προς τις περισσότερες επικοινωνίες με ηλεκτρονικό ταχυδρομείο είναι εφικτός ο προσδιορισμός του αποστολέα είτε διαμέσου της διεύθυνσης του ηλεκτρονικού ταχυδρομείου είτε μέσω του πρωτοκόλλου διαδικτύου (IP). Τις πληροφορίες αυτές στις περισσότερες περιπτώσεις τις διαθέτει τόσο ο παραλήπτης του ηλεκτρονικού ταχυδρομείου όσο και οι εταιρίες που παρέχουν την πρόσβαση και τις υπηρεσίες ηλεκτρονικού ταχυδρομείου.

Η συλλογή προσωπικών δεδομένων είναι εφικτή και μέσων των καταλόγων που δημιουργούνται στο διαδίκτυο. Πρόκειται για σελίδες αφορούν εν μέρει ή εξ ολοκλήρου στη διάδοση μέσω του Διαδικτύου καταλόγων μελών, συνδρομητών κ.α. οι οποίοι κατά κύριο λόγο βρίσκονται ήδη και σε άλλη μορφή, γραπτή ή τηλεματική. Είναι απαραίτητο να διευκρινιστεί ότι η δυνατότητα της ελεύθερης υφαρπαγής των πληροφοριών που υπάρχουν στο διαδίκτυο που πηγάζει μέσα από την δυσκολία έως την πλήρη αδυναμία ελέγχου της χρήσης που μπορεί να πραγματοποιηθεί σε αυτά τα δεδομένα από τρίτους. Οι δημοσιεύσεις και οι κατάλογοι είναι στις περισσότερες των περιπτώσεων διαθέσιμοι στο Διαδίκτυο υπό τη μορφή της βάσης δεδομένων που παρέχει κριτήρια αναζήτησης προκειμένου να λάβει ένα άτομο μια πληροφορία για ένα ή περισσότερα υποκείμενα. Είναι σχετικά απλό να συνδυάσει κάποιος δημόσια πληροφορίες που υπάρχουν στο διαδίκτυο και να μπορέσει να διαμορφώσει ένα προφίλ της κατάστασης ή της συμπεριφοράς ενός ατόμου. Η εξέλιξη της αυτοματοποίησης συμβάλει ιδιαίτερα τις τεχνικές του data mining και data

warehousing. Σχετίζεται με τεχνικές «σκαψίματος» σε «τόνους» από δεδομένα με σκοπό τον συνδυασμό, την αποκάλυψη σχέσεων κλπ. Σε σχέση με τους καταλόγους είναι αναγκαίο να αναφερθεί ότι το υποκείμενο όταν δίνει τη συγκατάθεσή του να αποτελέσει μέρος σε ενός κατάλογου δεν είναι δυνατόν να γνωρίζει την ύπαρξη τεχνικών ανάστροφης αναζήτησης.

Συλλογή δεδομένων είναι δυνατόν να προκύψει και με την συμβολή εντύπων που διαμορφώνονται σε ψηφιακούς ο πλοηγούς και σχετίζονται με πληροφορίες για τη διεύθυνση, την ταυτότητα καθώς και πληροφορίες κοινωνικό-οικονομικού χαρακτήρα (επάγγελμα, ηλικία, φύλο κ.α.). Αυτό προκύπτει ιδίως όταν ο συγκεκριμένος δικτυακός τόπος προσφέρει δωρεάν υπηρεσίες όπως για παράδειγμα υπηρεσίες ηλεκτρονικού ταχυδρομείου , φιλοξενία ιστοσελίδας κ.α. Στην περίπτωση αυτή η συλλογή προσωπικών δεδομένων είναι εμφανέστατη και χαρακτηρίζεται ως ένα είδος αντιπαροχής για τη δωρεάν πρόσφορα της συγκεκριμένης υπηρεσίας. Μία αρκετά μεγάλη ερευνά στις ΗΠΑ, την οποία διεξήγαγε το Electronic Privacy Information Center (EPIC) αναφέρει ότι περισσότερες από τις 100 πλέον πολυσύχναστες σελίδες στο διαδίκτυο έχουν δημιουργηθεί με αυτόν τον τρόπο το προφίλ των επισκεπτών τους. Ακόμα κατά τη συναλλακτική επαφή στο πλαίσιο των ηλεκτρονικών αγορών ο χρήστης δεν έχει τη δυνατότητα να είναι ανώνυμος ή να κάνει χρήση σε ψευδώνυμο αφού για την πραγματοποίηση της συναλλαγής επιβάλλεται να δηλώσει την πραγματική του διεύθυνση και τα στοιχεία της πιστωτικής του κάρτας για να προωθηθεί η πληρωμή του συμφωνηθέντος τιμήματος.

Η συλλογή προσωπικών δεδομένων που προσδιορίστηκε στην παρούσα ενότητα είναι σε μεγάλο βαθμό γνωστή στον χρήστη χωρίς αυτό να σημαίνει ότι υπάρχει συνολική συνειδητοποίηση, απαραίτητα της εμβέλειας και του εύρους των αποτελεσμάτων αυτής της πρακτικής. Οπωσδήποτε δε η διαδικασία της συλλογής και η περαιτέρω πορεία και κατάληξη των δεδομένων αυτών δεν είναι ούτε προφανής ούτε ιδιαίτερα διαφανής για τον απλό χρηστή.

2.3.2.2 **Οι "αόρατες" επεξεργασίες**

Διακρίνονται ακόμα όμως μορφές συλλογής, οι οποίες προσδιορίζονται από το στοιχειό της αδιαφάνειας, αν όχι της “δολιότητας”. Τα περίφημα cookies αποτελούν μια απ τις ποιο χαρακτηριστικές μορφές αυτών των όρων, στην ουσία τα αρχεία πληροφορίας που αποστέλλονται από τον web server στον υπολογιστή του χρήστη με στόχο τον μελλοντικό προσδιορισμό της ταυτότητας του υπολογιστή για την ευκολία του χρηστή σε μετέπειτα επισκέψεις στην ίδια σελίδα. Οι εμπνευστές και τα άτομα που κάνουν χρήση αυτής την τεχνολογία κάνουν επίκληση σε αυτήν την πρακτική ώστε να δικαιολογήσουν την δυνατότητα να επιτρέπετε στον υπεύθυνο αρχείου να μαρκάρει τις προγενέστερες επισκέψεις της σελίδας από τον “πλοηγό” προκειμένου είτε να διευκολύνει την διαδικασία της επίσκεψης, είτε αποφεύγοντας για παράδειγμα τη συμπλήρωση κάθε φορά των στοιχείων προσδιορισμού της ταυτότητας, είτε να προσαρμόσει τις σελίδες στο προφίλ του πλοηγού, όπως αυτό προκύπτει από τα “ίχνη” που παραμένουν από τις προγενέστερες επισκέψεις. Είναι ωστόσο ευδιάκριτο ότι αυτή η πρακτική προσβάλλει, σε σημαντικό βαθμό την ιδιωτική ζωή των χρηστών. Είναι ακόμα εμφανεστατο ότι η καταγραφή δεδομένων που η τεχνολογία αυτή επιτρέπει, εξυπηρετεί και άλλους, απωτέρους σκοπούς.

Πραγματικά τελευταία διακρίνεται μια όλο και διευρυνόμενη μία πραγματική αγορά, ένα «παζάρι» προσωπικών δεδομένων. Πρόκειται για δεδομένα που παράγονται από συναλλαγές, όπως ημερομηνία, ταυτότητα του αποδέκτη, φύση του προϊόντος που αγοράστηκε και στο οποίο διακρίνονται «πάνω» δεδομένα ταυτότητας όπως το όνομα, η διεύθυνση καθώς και δεδομένα που προσδιορίζονται ως δημογραφικά, όπως η ηλικία, η περιουσιακή κατάσταση, η κοινωνικο-επαγγελματική κατηγορία, δεδομένα που συλλέγονται μέσα δειγματοληψίες ερωτηματολογίων στο δίκτυο είτε πριν την πρώτη σύνδεση είτε πριν την συναλλαγή. Το φαινόμενο αυτό καταγράφει μια συνέχει αύξηση και βρίσκεται σε πλήρη συσχέτιση με το διαδίκτυο και καθίσταται προοδευτικά βασικό πεδίο εμπορικής δραστηριότητας όπου τα άτομα δεν θα αναζητούν αποκλειστικά πληροφορίες αλλά πραγματοποιούν εμπορικές συναλλαγές.

Σημαντικό είναι να γίνει κατανοητό ότι ακόμα και αν κάποιος δεν πραγματοποιεί συναλλαγές μέσω του Διαδικτύου τα προσωπικά του δεδομένα καταγράφονται. Είναι αρκετή και μια απλή παθητική πλοήγηση στους ηλεκτρονικούς τόπους του διαδικτύου. Η πλοήγηση στο διαδίκτυο είναι δεδομένο ότι αφήνει ηλεκτρονικά αποτυπώματα και ψηφιακά ίχνη. Σε αντίθεση το πέρασμα από τα ράφια

του σούπερ-μάρκετ, τις βιτρίνες ενός εμπορικού σημείου, σε μία βιβλιοθήκη ή σε ένα βιβλιοπωλείο δεν υπάρχει η δυνατότητα καταγράφει τους. Όπως και στην ενδοδικτυακή πλοήγηση, συχνά δεν υπάρχει πρόθεση αγοράς αλλά προσδιορισμός στοιχειών για τα προϊόντα που προσφέρονται και μια γενικότερη ερευνά αγοράς. Η σημαντικότερη διαφορά είναι ότι ενώ η επίσκεψη μιας βιβλιοθήκης, το διάβασμα μιας εφημερίδας, ακόμα και μια βόλτα στις βιτρίνες είναι δυνατόν να γίνει σχεδόν υπό πλήρη ανωνυμία, η πλοήγηση στο δίκτυο αφήνει ένα μόνιμο και αναγνωρίσιμο ψηφιακό ίχνος. Αυτές οι τεχνικές προσφέρουν την δυνατότητα δημιουργίας των λεγόμενων clikc trails σε σύγκριση με τον χρήστη του Διαδικτύου.

Τα clikc trails προσδιορίζουν πληροφορίες σε σχέση με την “συμπεριφορά” του χρήστη, την ταυτότητά του, τους ηλεκτρονικούς δρόμους και μονοπάτια που «περπατά» στο διαδίκτυο και τις προτιμήσεις και ενέργειες που πραγματοποιεί που όταν επισκέπτεται μία ιστοσελίδα. Εξαιτίας του γεγονότος ότι το διαδίκτυο είχε προσδιοριστεί από την αρχή ως ένα ανοιχτό δίκτυο υπάρχουν πλήθος στοιχείων πρωτοκόλλων επικοινωνίας, τα οποία, περισσότερο τυχαία παρά από σχεδιασμό, είναι δυνατόν να συντελέσουν σε προσβολή της ιδιωτικής ζωής.

Ο DNS Server δέχεται και διατηρεί τα ίχνη από όλα τα ονόματα των servers με τα οποίο ο χρήστης προσπάθησε να έρθεις σε επαφή. Η εντολή Ping δίνει την δυνατότητα σε οποιονδήποτε να εντοπίζει εάν ένας συγκεκριμένος υπολογιστής είναι σε λειτουργία και συνδεδεμένος στο δίκτυο. Λογισμικό όπως τα ET, Alexa, Radiate παρέχουν την δυνατότητα την καταγραφής των ψηφιακών ιχνών στην διαρκεία έρευνας και την αναζήτηση στο διαδίκτυο, Η Alexa για παράδειγμα στέλνει στον «ενδιαφερόμενο» στοιχεία κάθε φορά που ο χρήστης πραγματοποιεί μια αγορά ενώ το Radiate δινει ενημέρωση για τις διαφημίσεις που «επιλέγουν» οι χρήστες.

Ένας σημαντικός κίνδυνος για την ιδιωτικότητα των χρηστών του διαδικτύου προσδιορίζεται στη εφαρμογή ενός λογισμικού που έχει την ικανότητα να διερευνήσει το δίκτυο και να συλλέξει όλες τις προσφερόμενες πληροφορίες για ένα συγκεκριμένο άτομο. Μελέτες που έχουν πραγματοποιηθεί έχουν αποδείξει ότι είναι δυνατή η συρραφή της λεπτομερούς βιογραφίας ενός τυχαία επιλεγέντος ατόμου μέσα από την χρήση του εν’ λόγο λογισμικού και την εκμετάλλευση πληροφοριών από όλες τις ομάδες επαφών στις οποίες συμμετάσχει το συγκεκριμένο άτομο. Οι ίδιες έρευνες αναφέρουν ότι είναι δυνατή η εύρεση της διεύθυνσης και του αριθμού

του τηλεφώνου του τυχαία επιλεγμένου ατόμου, την ημερομηνία γεννήσεως, τον τόπο σπουδών, το επάγγελμα, τον τόπο εργασίας, όπως και πληροφορίες που σχετίζονται με το ενδιαφέρον του για ερασιτεχνικό θέατρο, ποια μπύρα πίνει, τι είδους διατροφή επιλεγεί και τόπους διακοπών, καθώς και τις προσεγγίσεις του για ζητήματα όπως πολιτική, οικονομία, περιβάλλον κ.α. Υπάρχουν ήδη ορισμένοι ηλεκτρονικοί τόποι στις Ηνωμένες Πολιτείες που παρέχουν, για εμπορικούς σκοπούς, τέτοιου είδους "διερευνητικές" υπηρεσίες.

Κοινός παρονομαστής του συνόλου μορφών συλλογής και επεξεργασίας στοιχείων, είναι η προσβολή της ιδιωτικότητα και η απώλεια της ανωνυμίας. Το πρόβλημα της προστασίας της ιδιωτικότητας, της προστασίας των προσωπικών δεδομένων δεν αποτελεί απόρροια της εμφάνισης ή της διάδοσης του διαδικτύου, υπήρχε ήδη σε και κατά την παραδοσιακή, χειρόγραφη επεξεργασία και ήταν έγινε ποιο εμφανής με την ανάπτυξη των τεχνολογιών της πληροφορικής και της επεξεργασίας δεδομένων. Οπωσδήποτε η ριζική μεταβολή του τρόπου επικοινωνίας δείχνει τις συνέπειες της ως ένα επίπεδο. Τα χαρακτηριστικά του διαδικτύου το καθιστούν μια ειδική περίπτωση. Παρά τις αντιλήψεις που διακρίνεται να προκύπτουν τα πρώτα χρόνια της έκρηξης του διαδικτύου, είναι αναγκαίο να γίνει σαφές ότι αυτό δεν αναπτύσσεται όμως σε ένα “νομικό κενό”. Ο κυβερνοχώρος δεν είναι “ελεύθερος δικαίου χώρος”. Η παραβατικότητα δεν προσδιορίζεται με διαφορετικό τρόπο στον on-line απ΄ ότι στον off-line πραγματικότητα. Αντίστοιχα η διαμόρφωση της πολιτικής που σχετίζεται με το Διαδίκτυο και τα επιμέρους αλλά μείζονα ζητήματα που αυτό θέτει δεν πραγματοποιείται "εν κενώ" αλλά στην βάση σαφώς προσδιοριζόμενων κανόνων, αρχών και αξιών. Το διαδυκτίο δεν αποτελεί ένα αναρχικό γκέτο στο οποίο δεν υπάρχουν οι κανόνες και δεν υπάρχει θέση για τα ανθρώπινα δικαιώματα. Βέβαια εξαιτίας της φύσης του διαδικτύου, το οποίο δεν υπόκεινται στις κλασικές κατηγοριοποιήσεις του χώρου και του χρόνου ως προς την εφαρμογή του δικαίου, δεν διακρίνεται εύκολος ούτε ο προσδιορισμός των νομικών κανόνων που επιβάλλεται να εφαρμοστούν ούτε η εφαρμογή τους (Καίσης, 2002).

2.4 Η Προστασία της Ιδιωτικότητας τώρα και στο μέλλον

Τα στοιχεία της έρευνας της EMC δείχνουν ότι πως χρόνο με το χρόνο η εμπιστοσύνη του κόσμου σε σχέση με το επίπεδο προστασίας της ιδιωτικότητάς του περιορίζεται. Σε διάστημα ενός και μόνο χρόνου, το 59% των ερωτηθέντων από όλες

τις χώρες αισθάνεται ότι τώρα η ιδιωτικότητά του προστατεύεται λιγότερο. Η Βραζιλία και οι Η.Π.Α. παρουσίζανουν το υψηλότερο ποσοστό ερωτηθέντων που αισθάνονται ότι η ιδιωτικότητά τους έχει περιοριστεί με ποσοστά 71% και 70% αντίστοιχα. Η Γαλλία είναι η μόνη χώρα στην οποία η πλειοψηφία με ποσοστό 56% διαφωνεί με τη δήλωση ότι φέτος η ιδιωτικότητά τους έχει περιοριστεί συγκριτικά με την προηγούμενη χρονιά. Σημαντικό είναι ακόμα και το ποσοστό του 81% των συμμετεχόντων που εκτιμά ότι η προστασία της ιδιωτικότητας θα μειωθεί μέσα στα επόμενα πέντε χρόνια.

Στις 25 Νοεμβρίου 2014 το θέμα της προστασίας της ιδιωτικότητας στο διαδίκτυο αποτέλεσε ζήτημα και στη συνεδρίαση του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ), οπού και συζητήθηκε εκτενώς και έκτοτε περιγράφεται ως ανθρώπινο δικαίωμα.

Μάλιστα, ο Οργανισμός Ηνωμένων Εθνών με ψήφισμά του, παροτρύνε τις χώρες- μέλη του να προστατέψουν το δικαίωμα της ιδιωτικής ζωής των πολιτών τους στον πεδιοτων ψηφιακών επικοινωνιών αλλά και να τους προσφέρουν λύσεις, αν νιώσουν ότι η ιδιωτική τους ζωή παραβιάζεται. Μέτρο, το οποίο έγινε αποδεκτό από τα περισσότερα μελή της Επιτροπής Ανθρωπίνων Δικαιωμάτων της Γενικής Συνέλευσης(http://www.nytimes.com/2014/11/26/world/un-urges-protection-of-privacy-in-digital-era.html?ref=technology&_r=5).

Το ψήφισμα μπορεί να υποστηρίχτηκε από 65 χώρες μέλη αλλά όχι από τις Ηνωμένες Πολιτείες, την Αυστραλία, τη Βρετανία, τον Καναδά και τη Νέα Ζηλανδία, χώρες οι οποίες άτυπα αποτελούν μια συμμαχία αντικατασκοπείας, γνωστή και ως FIVE EYES.

Το ψήφισμα αυτό συστήνει για πρώτη φορά στην ιστορία τις κυβερνήσεις να «παρέχουν στα άτομα, των οποίων το δικαίωμα στην ιδιωτική ζωή έχει παραβιαστεί παράνομα ή αυθαίρετα, την πρόσβαση σε αποτελεσματικά ένδικα μέσα». Μάλιστα, το κείμενο του ψηφίσματος για πρώτη φορά αναφέρει ρητά μια αναφορά που δεν περιορίζεται αποκλειστικά στο περιεχόμενο κάθε επικοινωνίας μέσω διαδικτύου αλλά επεκτείνει το όριο του τι ορίζεται ως «ηλεκτρονικά προσωπικά δεδομένα» και στη συλλογή των metadata, τα οποία περιλαμβάνουν την ημερομηνία και την ώρα που στάλθηκε ένα email ή τη διάρκεια τηλεφωνημάτων.

Ο Niels Ole Finnemann, καθηγητή και διευθυντή του NetLab της Δανίας, αναφέρει ότι οι χρήστες διακρίνονται σε δύο κατηγορίες, αυτούς που επιλέγουν την ευκολία

και αυτούς που προτιμούν την ιδιωτικότητα. Αρκετοί επιστήμονες και ερευνητές είναι πεπιεσμένοι πως μέχρι το 2025 οι πληροφορίες που σήμερα θεωρούνται ιδιωτικές, θα είναι ακόμα πιο διάχυτες και πιο ρευστές (http://www.pewinternet.org/2014/12/18/future-of-privacy/)

Για τις απειλές και τους κινδύνους της ρευστότητας των πληροφοριών αλλά και συνολικότερα της παραβίασης της ιδιωτικότητας, προειδοποίησε η Πρόεδρος της Ομοσπονδιακής Επιτροπής Εμπορίου των Η.Π.Α. κυρίως σε ό, τι σχετίζεται με τα έξυπνα gadgets και το Internet of Things (IoT) (http://www.lifo.gr/now/digital-life/58035).

Ένα μέλλον γεμάτο με συσκευές διαρκώς συνδεδεμένες στο διαδίκτυο, συγκεντρώνουν κάθε πιθανό προσωπικό δεδομένο και έχουν την δυνατότητα να σκιαγραφήσουν μια «βαθιά προσωπική» εικόνα για τον τρόπο ζωής του χρήστη τους. Κάθε κίνηση του χρήστη σε smartphones και tablets μεταβάλλεται σε ένα σημείο δεδομένων όπου είναι πολύ απλό να συλλεχθεί, να γίνει χρήση του και να διαμοιραστεί. Το σημαντικό είναι πως ο χρήστης είτε άμεσα είτε Εμέσα δίνει την συγκατάθεση του σε αυτή τη διαδικασία διαμοιρασμού κάθε φορά που προσφέρει την συγκατάθεση του με την πολιτική προστασίας οποιασδήποτε διαδικτυακής υπηρεσίας.

2.4.1 Εμπιστοσύνη και Ασφάλεια

Η εμπιστοσύνη είναι μια σύνθετη και πολυδιάστατη έννοια στοιχείο που δυσκολεύει τον προσδιορισμό της. Αποτελεί αναπόσπαστο μέρος της ιδιωτικής ζωής τόσο στη συμβατική της μορφή, την ανταλλαγή των υποσχέσεων που επιβάλλεται τα άτομα να εμπιστεύονται, όσο και στη θεσμική της μορφή, την εμπιστοσύνη δηλαδή που είναι απαραίτητη στην αποκάλυψη ιδιωτικών πληροφοριών σε αφηρημένες οντότητες προς εταιρείες, κυβέρνηση κ.α.

Με τη χρήση των νέων τεχνολογιών, όπου τα προσωπικά δεδομένα ανταλλάσσονται, μεταφέρονται και αποθηκεύονται με διαρκώς αυξανομένη ταχύτητα και σε διαφορετικά περιβάλλοντα, η εμπιστοσύνη των καταναλωτών σε προϊόντα και υπηρεσίες ζωτικής σημασίας συνιστά πολύ βασική παράμετρο για τη συνέχιση και την εξέλιξη της σχέσης τους με κάθε οργανισμό και επιχείρηση. Αρκετοί χρήστες

ενδέχεται να νοιώθουν ευχαριστημένοι ή δυσαρεστημένοι με το σύστημα, την επιχείρηση ή την κυβέρνηση, ωστόσο αρκετές φορές δεν θα μπορούσαν να μην δείξουν εμπιστοσύνη και να μη μείνουν αποξενωμένοι, αφού η εμπιστοσύνη είναι βασική προϋπόθεση για τη συνεργασία.

Η συνεργασία ανακινεί ζητήματα ασφάλειας σχετικά με τις πληροφορίες, το υλικό και το λογισμικό. Μέσα από την επιλογή και εφαρμογή των κατάλληλων εγγυήσεων, η ασφάλεια συμβάλει στην αποστολή του οργανισμού με την προστασία των φυσικών και οικονομικών πόρων του, τη φήμη, τη νομική θέση, τους εργαζόμενους, τους πελάτες και άλλα υλικά και άυλα περιουσιακά στοιχεία.

Ο στόχος ενός αξιόπιστου συστήματος του υπολογιστή είναι να προσδιορίζει την πρόσβαση των χρηστών σε δεδομένα. Αυτός ο έλεγχος προσδιορίζεται από ένα σύνολο γενικών σκοπών και στόχων που καλείται *πολιτική ασφάλειας* και βασίζεται σε τρεις βασικές ιδέες οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός συστήματος, και είναι οι εξής:

- **Ακεραιότητα**: Η ακεραιότητα σχετίζεται με τη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνώριμη κατάσταση χωρίς ανεπιθύμητες διαφοροποιήσεις, αφαιρέσεις ή προσθήκες από άτομα που έχουν την εξουσιοδότηση, καθώς και την αποτροπή της πρόσβασης ή και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα που δεν διαθέτουν την απαιτουμένη άδεια.
- **Διαθεσιμότητα:** Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων περιγράφει την διασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών οποιαδήποτε στιγμή ανακληθούν από τον χρήστη. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που στοχεύουν στο να θέσουν εκτός λειτουργίας τους στοχευόμενους πόρους, προσωρινά ή μόνιμα. Η άρνηση υπηρεσιών δεν είναι δυνατόν να προσδιοριστεί αναγκαία ως εχθρική επίθεση. Για παράδειγμα, το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με αποτέλεσμα εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας, σε αυτήν την περίπτωση προκύπτουν παρόμοια προβλήματα.

· ***Εμπιστευτικότητα:*** Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα πρέπει να διατεθέντα αλλά ούτε να εκτίθενται σε μη εξουσιοδοτημένα άτομα (Κάτσικας & Μήτρου 2002)

Διάγραμμα 2.1: Βασικές Αρχές Ασφάλειας

Πηγή: Κάτσικας & Μήτρου 2002.

2.3 Συστήματα συλλογής προσωπικών δεδομένων και στοιχείων.

Όπως αναφέρθηκε και ποιο πάνω η χρήση νέων τεχνολογιών και του Διαδικτύου επιβάλει στα άτομα πλέον την αποκάλυψη προσωπικών πληροφοριών, που είναι στις περισσότερες περιπτώσεις βασική προϋπόθεση για την πρόσβαση σε υπηρεσίες, για να κάνουν online αγορές ή για να προσωποποιηθούν σε αυτές τις υπηρεσίες (Metzger, 2006).

Έτσι στα ευρύτερα πλαίσια της κοινωνίας της πληροφορίας οι εξελίξεις τα τελευταία χρόνια στις νέες τεχνολογίες πληροφορικής και επικοινωνιών προσφέρουν τη δυνατότητα συλλογής και επεξεργασίας σημαντικού όγκου προσωπικών δεδομένων. Τέτοιες τεχνολογίες είναι η Ηλεκτρονική Μάθηση (e-learning), η Ηλεκτρονική Διακυβέρνηση (e-government), το Ηλεκτρονικό Επιχειρείν (e-business), το Ηλεκτρονικού Εμπορίου (e-commerce), η Ηλεκτρονική Εφοδιαστική (e-logistics), η Ιχνηλασιμότητα (traceability), η Ηλεκτρονική Ανταλλαγή Δεδομένων (Electronic Data Interchange), τα Συστήματα Υποστήριξης Αποφάσεων (Decision Support Systems) καθώς και τα Έμπειρα Συστήματα (Expert Systems).

Μια από τις πιο σημαντικές εξελίξεις των τελευταίων χρόνων είναι και η ανάπτυξη των τεχνολογιών του διάχυτου υπολογισμού, που ενσωματώνει τον υπολογισμό στο περιβάλλον, αφού διασυνδεδεμένοι υπολογιστές, σκορπισμένοι στον χώρο δεν είναι αντιληπτοί από ανθρώπους ή αντικείμενα και προσφέρουν εξατομικευμένες υπηρεσίες για κάθε χρήστη βάσει των χαρακτηριστικών του, της προσωπικότητάς του, του περιβάλλοντός του κλπ. Σύμφωνα με τους York και Pendharkar (2004) η πανταχού παρούσα υπολογιστική ορίζεται ως «μηχανές που ταιριάζουν με το ανθρώπινο περιβάλλον αντί το περιβάλλον να αναγκάζει τους ανθρώπους να εισάγουν τις δικές τους». Ο Weiser (1993), ο πατέρας του ubiquitous computing, αναφέρει ότι το ανώτατο ιδανικό του είναι να κάνει ένας υπολογιστής τόσο φυσική και εφαρμοσμένη δουλειά ώστε να γίνεται χρήση του χωρίς καν να το σκεφτούμε και έχει τοποθετήσει τις ρίζες της στην μετα-μοντερνισμό. Σε συνδυασμό με τεχνολογίες προσδιορισμού θέσης τα αντικείμενα με ενσωματωμένους αισθητήρες (sensors) έχουν τη δυνατότητα γνώσεις για το που βρίσκονται τα ίδια ή άλλα αντικείμενα και πρόσωπα στο περιβάλλον (European Commission, 2008).

2.3.1 RFID **ετικέτες**

Από τις σημαντικότερες εφαρμογές του διάχυτου υπολογισμού είναι η RFID (Radio Frequency Identification), που σε ελληνική προσεγγίσει του όρου χαρακτηρίζεται ως «ταυτοποίηση μέσω ραδιοσυχνοτήτων». Οι τεχνολογίες RFID, σύμφωνα με το Commission Staff Working Document (2008), προσφέρουν την δυνατότητα σε κάθε αντικείμενο να έχει το δικό του μοναδικό αναγνωριστικό, σε εξέλιξη των barcodes που έχουν έναν αριθμό ταυτότητας για κάθε τύπο προϊόντος.

Ακόμα, έχουν τη δυνατότητα να διαβάζονται εξ αποστάσεως, κάτι που προσφέρει την δυνατότητα αυτόματης αναγνώριση σε αληθινό χρόνο και την παρακολούθηση των προσωπικών αντικειμένων. Ακόμα, ο Brito (2005), αναφέρει ότι υπάρχει η δυνατότητα αποθήκευσης περισσότερων δεδομένων σε σύγκριση με τα barcodes και δεν διακρίνονται από το ανθρώπινο μάτι τα RFID tags μιας και για την αναγνώριση τους δεν είναι αναγκαίο κάποιο οπτικό μέσο. Η εφαρμογή τους είναι σημαντική στον εμπορικό τομέα, παρακολούθησης των εμπορευμάτων, σε συστήματα αγοραπωλησιων, ανίχνευσης αποσκευών από αεροπορικές εταιρείες, για αντικατάσταση εισιτηρίων επιβίβασης αεροπορικών εταιρειών, για παρακολούθηση αυτοκινήτων σε σιδηρόδρομους, δημόσια λεωφορεία και κάδους απορριμμάτων (Brito, 2005).

Η λειτουργία των συστημάτων RFID αναφέρατε ως απλή και βασίζεται στη δυναμική και αμφίδρομη επικοινωνία των ετικετών και των αναγνωστών. Όταν οι ετικέτες RFID εντοπιστούν από την κεραίας του αναγνώστη, η μονάδα ελέγχου επικοινωνεί με ραδιοκύματα με την κεραία των ετικετών RFID. Οι ετικέτες RFID μπαίνουν σε λειτουργία με τη σειρά τους και αναφέρουν τα αναζητούμενα δεδομένα στους αναγνώστες. Στην συνέχεια παρεμβαίνει ένα ενδιάμεσο λογισμικό, το οποίο αντιλαμβάνεται τις πληροφορίες, οι οποίες στέλνονται από τη μονάδα ελέγχου του αναγνώστη και ο αναγνώστης τις παραπέμπει στο αναλογό πληροφοριακό σύστημα.

Ωστόσο, δεν είναι λίγες και οι εντάσεις που προκαλούν οι RFID τεχνολογίες για την παραβίαση της ιδιωτικής ζωής. Σύμφωνα με τον Eckfeldt (2005) σημαντικές εταιρείες σε όλο τον κόσμο όπως για παράδειγμα η Metro Group στην Ευρώπη έχουν αποσύρει τα RFID προγράμματα μετά ενστάσεις των καταναλωτών και κάποιες τοποθεσίες στο διαδίκτυο έχουν καταγγείλει εφαρμογές RFID με προειδοποιήσεις για την ιδιωτική ζωή λόγω κλοπών ταυτότητας και σωματικών βλαβών από αδέσποτα ραδιοσήματα.

2.3.2 **Βιομετρικές τεχνολογίες**

Ιδιαίτερη σημασία έχουν απόκτηση πλέον οι βιομετρικές τεχνολογίες για τη συλλογή και ταυτοποίηση προσωπικών δεδομένων. Η χρήση βιομετρικών τεχνολογιών αποτελεί μια μέθοδος μέτρησης βιολογικών χαρακτηριστικών όπως για παράδειγμα τα δακτυλικά αποτυπώματα, η ίριδα ματιού, η γεωμετρία παλάμης και των δαχτύλων, η αναγνώριση προσώπου και φωνής, το σχήμα αυτιών, η

αμφιβληστροειδής χιτώνας, η μυρωδιά, η θερμότητα προσώπου, η φλέβα χεριού, το DNA, τα αποτύπωμα παλάμης, όπως και χαρακτηριστικά συμπεριφοράς όπως ο τρόπος βαδίσματος, η υπογραφή, η φωνή, ο τρόπος πληκτρολόγησης που πηγάζουν από το ανθρώπινο σώμα και είναι συνήθως αναλλοίωτα.

Σε αρκετές χώρες οι δημόσιες αρχές κάνουν χρήση των βιομετρικών στοιχείων για έγγραφα ταυτότητας, όπως passports. Ακόμα, ιδιωτικές τράπεζες εκδίδουν έξυπνες κάρτες με βιομετρικά στοιχεία για τους πελάτες τους για τις οικονομικές συναλλαγές τους καθώς επίσης και σχολεία έχουν ξεκινήσει να προσδιορίσουν τους μαθητές τους, ώστε να μην επιτρέπεται σε μη εξουσιοδοτημένους νέους η πρόσβαση στα εστιατόρια τους.

Γενικά, οι βιομετρικοί έλεγχοι ταυτότητας προσφέρουν απαντήσεις στο «ποιος είναι» κάποιος και προσδιορίζουν την ταυτότητά του. Βασικές μετρήσεις απόδοσης για τα βιομετρικά χαρακτηριστικά (Sahoo, Prasanna, Choubisa, 2012) αποτελεί σε ένα πρώτο επίπεδο, το ψευδές ποσοστό αποδοχής (FAR), δηλ. η πιθανότητα το σύστημα να συσχετίζει εσφαλμένα το πρότυπο εισόδου σε μη-ταίριασμα προτύπου στη βάση δεδομένων. Μετρά το ποσοστό των άκυρων εισροών που λανθασμένα είναι αποδεκτά. Ακόμα, το ψευδές ποσοστό απόρριψης σε εξουσιοδοτημένα πρόσωπα (FAR ή FRR), η πιθανότητα δηλ. να αποτύχει το σύστημα να προσδιορίζει το ποσοστό μεταξύ του τρόπου εισόδου και ένα αντίστοιχο πρότυπο στη βάση δεδομένων και μετρά το ποσοστό των έγκυρων εισροών που εσφαλμένα έχουν απορριφθεί. Ακόμα, η αποτυχία να εγγραφούν τα δεδομένα που εισέρχονται από τον αισθητήρα (FER), όταν δηλ. ο χρήστης δεν έχει την δυνατότητα να περάσει το βιομετρικό έλεγχο. Η αποτυχία του συστήματος να συλλάβει τον χρήστη (FTC), δηλ. η πιθανότητα το σύστημα να αποτυγχάνει να συλλάβει ένα βιομετρικό προσδιοριστικό στοιχείο εισόδου.

Τα βιομετρικά στοιχεία υπάρχει η δυνατότητα να γίνει χρήση τους για τη προστασία της ιδιωτικής ζωής και την ενίσχυση της τεχνολογίας, όπως αναφέρει το Council of Europe (2005), αφού υπάρχει η δυνατότητα να αποφευχθεί η χρήση μιας τραπεζικής κάρτας από μη εξουσιοδοτημένο δικαιούχο, καθώς επίσης να μη είναι δυνατή η πρόσβαση σε βάσεις δεδομένων από πρόσωπα που δεν διαθέτουν νόμιμη πρόσβαση και δεν αναγνωρίζονται στην βάση των βιομετρικών χαρακτηριστικών τους. Παρόλα αυτά, πολλά είναι τα ερωτήματα που προκύπτουν ως προς το ζήτημα

της παραβίασης της ιδιωτικότητας και της ανθρώπινης αξιοπρέπειας που περνά μέσα από την χρήση της τεχνολογίας των βιομετρικών δεδομένων, γι αυτό και επιβάλλεται να εξισορροπείται ο σκοπός χρήσης τους με τα συμφέροντα και τις αξίες που διακυβεύονται και να λαμβάνονται υπόψη οι κοινωνικοπολιτισμικές πτυχές και ενδεχόμενη απροθυμία προς την οργανική χρήση του ανθρώπινου σώματος και το άτομο να είναι ενημερωμένο για τους σκοπούς του συστήματος και την ταυτότητα του ελεγκτή (Council of Europe, 2005).

2.3.3 E-TOKEN

Το E-token προσδιορίζει μια καινούργια συσκευή τεχνολογίας, όπου σύμφωνα με το Computing of Dartmouth (2013) παρέχει έλεγχο ταυτότητας και προστασία, καθώς για να έχει την δυνατότητα κάποιος να μιμηθεί επιβάλλεται να έχει τόσο τη συσκευή όσο και τον κωδικό κατά την πρόσβαση σε συστήματα που απαιτούν αυτού του είδους τον έλεγχο ταυτότητας. Αφορά ένα μηχανισμό υλικού στον οποίον γίνεται έλεγχος ταυτότητας μέσω κωδικού πρόσβασης μέσω τεχνικής διαχείρισης ταυτότητας. Είναι δυνατόν να εφαρμοστεί σε μια υποδοχή USB ή μια έξυπνη κάρτα και τα δεδομένα προστατεύονται μέσα από την ιδία την συσκευή. Ο χρήστης έχει ένδειξη πρόσβασης μέσω ενός κωδικού, όπου προσφέρεται και παράλληλα γίνεται και ο έλεγχος ταυτότητας και ψηφιακής υπογραφής. Το e-token έχει την δυνατότητα να αποθηκεύσει τα διαπιστευτήρια, όπως κωδικούς πρόσβασης ψηφιακές υπογραφές, τα πιστοποιητικά και τα ιδιωτικά κλειδιά. Η συσκευή e-token διακρίνεται για την χρησιμότητα της σε εταιρικές επιχειρήσεις και οργανισμούς, βιβλιοθήκες, τράπεζες, χρηματοοικονομικές εταιρίες, εκπαιδευτικά ιδρύματα, εταιρείες παροχής ασφάλειας και άμυνας. Έχει δυνατότητες που την καθιστούν ικανή να χρησιμοποιηθεί ευρύτατα στις συναλλαγές μέσω διαδικτύου όπως το e-banking και το e-commerce, καθώς και στις χρηματιστηριακές συναλλαγές προσφέροντας ασφαλή λύση απομακρυσμένης πρόσβασης (https://safenet.gemalto.com/data-protection/password-protection-applications/?aldn-true).

2.3.4 Smart cards

Οι έξυπνες κάρτες έχουν την δυνατότητα να παρέχουν αναγνώριση, πιστοποίηση, αποθήκευση και επεξεργασία των δεδομένων μιας εφαρμογής, να προσφέρουν ισχυρή ασφάλεια ελέγχου ταυτότητας τόσο σε ιδιώτες όσο και σε μεγάλους οργανισμούς. Οι έξυπνες κάρτες μπορούν να χρησιμευόσουν και ως πιστωτικές κάρτες ή κάρτες σε ATM, ως κάρτες καυσίμων, για κινητά τηλέφωνα ως κάρτες SIM , ως κάρτες άδειας για συνδρομητική τηλεόραση, ως υψηλής ασφάλειας και ταυτότητας ελέγχου πρόσβασης κάρτες και για τα μέσα μαζικής μεταφοράς. Ακόμα, έχουν την δυνατότητα χρήσης ως ηλεκτρονικά πορτοφόλια. Η έξυπνη κάρτα με τσιπ μπορεί να «φορτωθεί» με χρήματα για να πληρώσει παρκόμετρα, μηχανήματα αυτόματης πώλησης ή εμπόρους. Τα κρυπτογραφικά πρωτόκολλα παρέχουν προστασία κατά την ανταλλαγή των χρημάτων ανάμεσα στην έξυπνης κάρτας και του μηχανήματος χωρίς απαιτείται σύνδεση με την τράπεζα και ο κάτοχός της μπορεί να χρήσης της ακόμη και αν δεν είναι ο ιδιοκτήτης.

Τα οφέλη των έξυπνων καρτών σχετίζονται άμεσα με τον όγκο των πληροφοριών και των εφαρμογών που έχουν προγραμματιστεί για χρήση σε μια κάρτα. Μια έξυπνη κάρτα έχει την δυνατότητα προγραμματιστεί με πολλαπλά διαπιστευτήρια τραπεζών, ιατρικά δικαιώματα, άδεια οδήγησης, δικαίωμα δημόσιας μεταφοράς, προγράμματα πιστότητας και συνδρομές σε γυμναστήρια. Ακόμα, υπάρχει η δυνατότητα να ενσωματωθεί σε έξυπνες κάρτες έλεγχος ταυτότητας για την μεγαλύτερη ασφάλεια όλων των υπηρεσιών στην κάρτα. Παρ’ αλλά αυτά, οι κίνδυνοι που υπάρχουν από τη χρήση έξυπνων καρτών εντοπίζονται καταρχήν, στη φυσική καταστροφή τους, λόγο του μεγέθους και της συχνή τους χρήση. Ακόμα είναι δυνατόν, να σπάσουν αν ο κάτοχος του λογαριασμού φιλοξενεί κακόβουλο λογισμικό ή να δεχτούν επιθέσεις που βάζουν σε κίνδυνο τα χαρακτηριστικά της ασφάλειάς τους και να μιμηθεί κάποιος το λογαριασμό τους.

Σύμφωνα με το Council of Europe (2004) η συλλογή και επεξεργασία των προσωπικών δεδομένων μέσα από την χρήση έξυπνων καρτών επιβάλλεται να είναι δίκαιη και νόμιμη, τα δεδομένα να συλλέγονται και να αποθηκεύονται για νόμιμους και σαφείς σκοπούς και τα άτομα των δεδομένων επιβάλλεται να διαθέτουν το δικαίωμα της πρόσβασης σε δεδομένα προσωπικού τους χαρακτήρα που υπάρχουν στην κάρτα και θα πρέπει να έχουν τη δικαίωμα να απατήσουν τη διόρθωση όπου θεωρούν απαραίτητο. Είναι προφανές ότι οι νέες τεχνολογίες μέσω των δυνατοτήτων

συλλογής και επεξεργασίας μεγάλου όγκου προσωπικών πληροφοριών για το άτομο, έχουν την δυνατότητα παραβίασης της ιδιωτικότητάς του. Ωστόσο, σε κάποιες περιπτώσεις φορές προκαλούνται υπερβολικές ανησυχίες στους καταναλωτές, οι οποίες θα μπορέσουν να αποτρέψουν οι ίδιες οι δυνάμεις της αγοράς, οι επιχειρήσεις, οι οργανισμοί, και πάνω από όλα το ισχυρό και στοιχείο θεσμοθετημένο νομοθετικό πλαίσιο με ισχυρούς μηχανισμούς για την εφαρμογή κανόνων προστασίας (Haibo, 2007).

ΚΕΦΑΛΑΙΟ_3: Προοπτικές για την ιδιωτικότητα και τα προσωπικά δεδομένα.

3.1 Προοπτικές για την ιδιωτικότητα και τα προσωπικά δεδομένα.

Η προστασία των προσωπικών δεδομένων αποτελεί πια αναπόσπαστο κομμάτι της νέας πληροφοριακής έννομης τάξης, μέσα από την σταδιακή οροθέτηση και προσπάθεια προσδιορίσου της εξελισσόμενη Εποχή της Πληροφορίας (*Information Age*). Τα όρια της ιδιωτικότητας και της προστασίας των δεδομένων των ατόμων και κατ' επέκταση της ιδιωτικότητας συσχετίζονται έντονα πια, με τεχνολογικούς παράγοντες, την παγκοσμιοποίηση της επεξεργασίας που τα δεδομένα αυτά υφίστανται και την επικοινωνίας, τις μεταβολές του προσδιορισμού από τα άτομα όσο και των κρατικών και κοινωνικών δομών ως προς το περιεχόμενο της ιδιωτικότητας όσο και ως προς τη σχέση της με άλλα δημόσια και ιδιωτικά αγαθά και προσδοκίες. Η πληροφοριακή ιδιωτικότητα βρίσκεται σε ένα κρίσιμο σταυροδρόμι και αυτό λόγω η παρούσα κατάσταση όσο και τα βασικά δομικά χαρακτηριστικά των Τεχνολογιών Πληροφορικής και Επικοινωνίας (ΤΠΕ), όπως αυτές εξελίσσονται και λειτουργούν. Οι σύγχρονες τεχνολογίες αποτελούν αποτέλεσμα της κοινωνίας, η πηγή και η εξέλιξή τους προκύπτουν από αυτή, όμως από την άλλη πλευρά επηρεάζουν, και σε κάποιες περίπτωσης προσδιορίζουν την ποριά της κοινωνίας και των θεσμών της. Η ανάπτυξη των τεχνολογιών της πληροφορίας και επικοινωνίας με

την τεραστία πρόοδό τους επιδρούν πάνω στο τοπίο, στη νέα κοινωνία της πληροφορίας οι υπηρεσίες που προσφέρονται από τις νέες τεχνολογίες, συνιστούν σημαντικο παράγοντα καθορισμού των κοινωνικών και οικονομικών δομών και σχέσεων (Μήτρου, 2010).

Μία από τις ποιο συχνές προσεγγίσεις της ιδιωτικότητας είναι ότι περιγράφει τον απόρρητο χαρακτήρα ορισμένων θεμάτων και υπό αυτήν την έννοια η ιδιωτικότητα παραβιάζεται μέσα από την δημοσία εμφάνιση αυτής της απόρρητης πληροφορίας. Ειδικότερα η «κλασική» προσέγγιση της ιδιωτικότητας ως καταφυγίου προσδιορίζει στοιχεία ταύτισης ή και σύγχυσης σχετικά με την έννοια του απορρήτου αλλά και της εμπιστευτικότητας. Οι όροι αυτή μπορεί να είναι γενικότερα αντιληπτή από την πλειοψηφία και να γίνεται χρήση τους ως ισοδύναμοι, παρόλα αυτά, τελευταία προσεγγίσεις τους παρουσιάζουν αξιώσεις προστασίας, που διακρίνονται από μια γενικότερη ταύτιση τους. Αναλυτικότερα η έννοια του απορρήτου προσδιορίζεται είτε από τη μη προσπελασιμότητα ορισμένων πληροφοριών που αφορούν το πεδίο επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να παρέχουν ασφάλεια στις εν’ λόγω πληροφορίες, που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης, είτε διαθέτουν λόγω του θεσμικού τους ρόλου στην κοινωνική οργάνωση. Σε περίπτωσης που σχετίζονται με δεδομένα που αφορούν τη δημόσια σφαίρα δεν είναι αντιληπτή η προστασία από το απόρρητο. Για να είναι απόρρητα και εμπιστευτικά τα δεδομένα πληροφορία επιβάλλεται να βρίσκεται σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ.. Προς αυτή την κατεύθυνση πραγματοποιείται ακολουθεί μία ολοκληρωμένη επισκόπηση και καταγραφή των σημαντικότερων παραμέτρων για την αποτίμηση της επικινδυνότητας, μέσα από τον προσδιορισμό και ανάλυσης τόσο των δυνητικών απειλών που στις οποίες υπόκεινται οι συναλλαγές που μπορούν να προσβάλλουν τόσο τον στον παροχή της υπηρεσίας αλλά και το άτομο (Μήτρου, 2010).

Σαν απειλεί θα ήταν δυνατόν να προσδιοριστεί η «πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων-χαρακτηριστικών ασφάλειας ενός πλη-ροφοριακού συστήματος» (Λαμπρινουδάκης, et al., 2010).

Οι απειλές που παρουσιάζονται στα πληροφοριακά συστήματα, δεν αποτελούν αποκλειστικά στοιχεία κακόβουλων ενεργειών που προκύπτουν τόσο από εξωτερικές ή εσωτερικές οντότητες, αλλά είναι δυνατόν να προκύψουν και μέσα από λάθη που αφορούν το σχεδιασμό ή και μη ηθελημένες ενέργειες που πολύ πιθανόν να συντελέσουν στην μη πραγματοποιήσει των λειτουργιών και των στόχων που έχουν εναποτεθεί πληροφοριακό σύστημα.

Η ανάλυση επικινδυνότητας αποτελεί μια διαδικασία που αφορά την αναγνώρισης κινδύνων αλλά και τον υπολογισμό της επικινδυνότητας. Η εκτίμηση επικινδυνότητας σχετίζεται με την διαδικασία της αξιολόγησης της υπολογισμένης επικινδυνότητας σε σύγκριση με κριτήρια αξιολόγησης της σημαντικότητάς της (Tsohou, et al., 2010).

Η γενικότερη διαδικασία ανάλυσης και υπολογισμού της επικινδυνότητας προσδιορίζει μια συνολικότερη διαδικασία αποτίμησης της επικινδυνότητας που αφορά τα προσωπικά δεδομένα. Η αποτίμηση και διαχείριση επικινδυνότητας στηρίζεται στην αρχή ότι συνολική ασφάλεια δεν είναι εφικτή, άρα το ορθότερο που είναι δυνατόν να πραγματοποιηθεί είναι να εξισορροπηθεί η έκταση των πιθανών κινδύνων με το κόστος εφαρμογής των κατάλληλων αντιμέτρων. Στα πλαίσια αυτά είναι αναγκαίες οι μεθοδολογίες που θα παράσχουν υπολογισμό των κινδύνων και την έκφρασή τους σε κοινές μονάδες υπολογισμού με την αποτελεσματικότητα των αντιμέτρων με στόχο να προκύψουν συγκρίσιμα στοιχεία. Αυτός είναι και ο λόγος που επιβάλλεται ο υπολογισμός του για ένα σύστημα ως συσχέτιση των ακόλουθων παραγόντων:

- Των περιουσιακών του στοιχείων, ως συνολική αξία *(A).*
- Της φύσης και του βαθμού διαβλητότητας που το διακρίνει *(V).*
- Της φύσης και της δυνατότητα υπάρξει και παρουσίασης απειλών εναντίον του *(T).*
- Της φύσης και έντασης των ζημιών που θα παράγουν οι απειλές στην περίπτωση που πραγματοποιηθούν *(I).*

Επικινδυνότητα (risk)=f(A,V,T,I)

3.2 **Τεχνολογικές ανακαλύψεις και ιδιωτικότητα.**

Συμφώνα με τα όσα έχουν αναφερθεί σε προγουμενά κεφαλαία της εργασίας η επιβαλλόμενη χρήση των νέων τεχνολογιών αλλά και του διαδικτύου επιβάλλεται να πραγματοποιείται από τα άτομα μέσα με προσοχή στην παροχή και στην αποκάλυψη πληροφοριών που σχετίζονται με την δηκτικότητα τους, παρόλα αυτά είναι απαραίτητη προϋπόθεση για την πρόσβαση σε υπηρεσίες, για την πραγματοποίηση ηλεκτρονικών αγορών αλλά και την προσωποποίηση τους σε αυτές της υπηρεσίες (Metzger, 2006).

Η μεγαλύτερη χρήση υπολογιστών είναι δυνατόν συμβάλει στην καλύτερη και ασφαλέστερη διαχείριση των προσωπικών δεδομένων περιορίζοντας την αβεβαιότητας μέσα από την άτομα αλληλεπίδραση (Tidwell & Walther, 2002) ή για τον προσδιορισμό της νομιμότητας όταν λαμβάνουν μέρος σε μια ομάδα που έχει δημιουργηθεί με την βοήθεια του διαδικτύου (Galegher, Sproull και Kiesler, 1998).

Οι εξελίξεις τα τελευταία χρόνια στις νέες τεχνολογίες πληροφορικής και επικοινωνιών, στο πλαίσια της δημιουργίας κοινωνιών της πληροφορίας (*ΤΠΕ, ICT: Information and Communication Technology)* προσφέρουν την δυνατότητα συλλογής και διαχώρισης προσωπικών δεδομένων. Τεχνολόγιες αυτου του είδους είναι η ηλεκτρονική μάθηση (e-learning), το ηλεκτρονικό επιχειρείν (e-business), η ηλεκτρονική διακυβέρνηση (e-government),η ηλεκτρονική εφοδιαστική (e-logistics), η ιχνηλασιμότητα (traceability), το ηλεκτρονικό εμπορίο (e-commerce), τα συστήματα υποστήριξης αποφάσεων (Decision Support Systems), η ηλεκτρονική ανταλλαγή δεδομένων (Electronic Data Interchange) καθώς και τα έμπειρα συστήματα (Expert Systems).

Από την βασικότερες ανακαλύψεις το τελευταίο χρονικό διάστημα αναφέρατε αυτή του διάχυτου υπολογισμού (pervasive ή ubiquitous computing), που ενσωματώνει τον υπολογισμό στο περιβάλλον, αφού διασυνδεδεμένοι υπολογιστές, σκορπισμένοι στον χώρο δεν μπορούν να γίνουν αντιληπτοί από τους ανθρώπους ή αντικείμενα και παρέχουν εξατομικευμένες υπηρεσίες για κάθε χρήστη προϋπολογίζοντας τα χαρακτηριστικά του, την προσωπικότητάς του, το πεδίο ενδιαφερόντων του, τον τρόπο Ζώης του κ.α. Χαρακτηρίστηκα οι York και Pendharkar (2004), αναφέρουν ότι η πανταχού παρούσα υπολογιστική προσδιορίζεται

ως οι «μηχανές που ταιριάζουν με το ανθρώπινο περιβάλλον αντί το περιβάλλον να αναγκάζει τους ανθρώπους να εισάγουν τις δικές τους». (York, 2004).

3.2.1 RFID ετικέτες

Ως «Αναγνώριση/Ταυτοποίηση μέσω Ραδιοσυχνοτήτων» (Radio Frequency IDentification – RFID) προσδιορίζεται ένας γενικευμένος όρος και μάλλον εμπορευματοποιημένος, που προσδιορίζει μία τεχνολογία, η οποία διακρίνεται από πρακτικές υλοποιήσεις και εφαρμογές.

Η RFID τεχνολογία, δείχνει να διακρίνεται και από χρήσεις περνάν των ραδιοσυχνοτήτων που αφορούν την επικοινωνία, η χρήσης του μπορούν να επεκταθούν. Η τεχνολογία RFID έκανα την εμφάνιση της Πρωτώ φορά τη δεκαετία του ‘40 και σχετιζόταν με την στρατιωτική βιομηχανία σχετικά με την αναγνώριση φιλικών και εχθρικών πολεμικών αεροσκαφών. Το 1960 πραγματοποιούνται οι πρώτες προσπαθείς για την εμπορικής χρήσης της τεχνολογίας αυτής σε ζητήματα που αφορούν την αποτροπή κλοπής για ηλεκτρονικά αγαθά σημαντικής αξίας. Η επαναδημιουργία της όμως το τελευταίο χρονικό διάστημα προσέφερε την δυνατότητα για την κατασκευή πιο πολύπλοκων, μικρών, αξιόπιστων και φθηνών κυκλωμάτων, στοιχεία που συντέλεσαν στην εμπορική επιτυχία της εφαρμογής των RFID, με σημαντικότερη αυτήν σε συστήματα logistics.

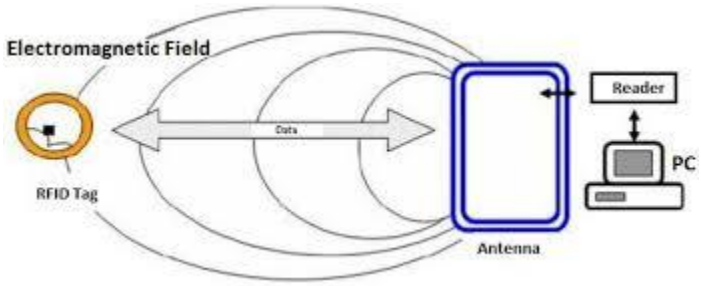
Στο πλαίσιο της εφαρμογής της τεχνολογίας του RFID μπορούν να προσδιοριστούν αρκετές και διαφορετικές τεχνολογίες, από τις τυπικές ετικέτες RFID που δημιουργούν το πρότυπο του Ηλεκτρονικού Κώδικα Προϊόντος της EPC global, έως τις ετικέτες που έχουν πιστοποιηθεί για εμφύτευση σε ζωντανούς οργανισμούς (πρότυπα ISO 11784, 11785. 14223) και τις ανεπαφικές κάρτες (contactless cards) που ορίζονται στο πρότυπο ISO 14443 και γίνεται χρίση τους σε στα ηλεκτρονικά διαβατήρια.

Στην βάση αυτών των πρακτικών, ένας γενικότερος ορισμός που προσδιορίζει την RFID ως μία τεχνολογία που προσφέρει την δυνατότητα στην συλλογή δεδομένων με ανεπαφικές ηλεκτρονικές ετικέτες και ασύρματους αναμεταδότες - αναγνώστες για ταυτοποίηση και άλλους σκοπούς. Σε μια απλοποιημένοι περιγραφή θα μπορούσε να περιγράφει ότι τα χαρακτηριστικά σε ένα τυπικό σύστημα RFID προσδιορίζεται από τέσσερα συστατικά: ετικέτες (tags), αναγνώστες (readers), back-

end υπολογιστικό σύστημα ξενιστή (host computer system) και το λογισμικό που περιλαμβάνει τις εφαρμογές του back-end, τα πρωτόκολλα επικοινωνίας.

Μία RFID ετικέτα προσδιορίζεται ως μια μικρή ραδιο-συσκευή, που επικολλάται πάνω ή ενσωματωνεται στο αντικείμενο που επιδιώκεται να ταχτοποιηθεί. Η ετικέτα διαθέτει από ένα απλό κύκλωμα σιλικόνης, προσκολλημένο σε μία σχετικά μικρή επίπεδη κεραία και τοποθετημένο σε ένα υπόστρωμα. Η όλη συσκευή είναι δυνατόν να περιβληθεί από ένα προστατευτικό κάλυμμα, που μπορεί να είναι πλαστικό ή γυαλί που σχετίζεται με την εφαρμογή. Η ετικέτα, πέρα από τις συνήθως περιορισμένες επεξεργαστικές δυνατότητες που πιθανόν να έχει, διαθέτει και μνήμη, στην οποία είναι δυνατόν να αποθηκευτούν δεδομένα μικρού σχετικά μεγέθους, όπως ένας μοναδικός αναγνωριστικός κωδικός EPC που αποτελεί μοναδική ταυτότητα για κάθε ετικέτα-αντικείμενο. Ο RFID αναγνώστης χαρακτηρίζεται ως μία συσκευή, στις περισσότερες περιπτώσεις φορητή, που αποστέλλει και δέχεται δεδομένα προς και από τις ετικέτες, με ασύρματο τρόπο μέσω των κεραιών που διαθέτει. Τα δεδομένα που λαμβάνει ο αναγνώστης, συνήθως ο μοναδικός αναγνωριστικός κωδικός EPC που αποστέλλει η ετικέτα, προωθούνται ακολούθως στο back-end υπολογιστικό σύστημα, με σκοπό αυτό να τα επεξεργαστεί και να δημιουργήσει δεδομένα που θα χαρακτηρίζονται ως χρήσιμα, όπως το να αναζητήσει σε μία βάση δεδομένων τις πληροφορίες αυτές που είναι συσχετισμένες με την ταυτότητα.

Σχήμα 1. Τυπικό σύστημα RFID



Πηγή : OECD, *“Radio-Frequency Identification (RFID),2008.*

Η μικρή χωρητικότητα της μνήμης της ετικέτας στις περισσότερες περιπτώσεις περιορίζει σημαντικά τις δυνατότητες επεξεργασίας, αποθήκευσης και διασύνδεσης των αναγνωστών, δημιουργούν εμπόδια ως ένα βαθμό στο σύνολο των πιθανών εφαρμογών (OECD, 2008).

Τα RFID συστήματα έχουν προταθεί σε εύρη πεδίο εφαρμογών, έχει συντελέσει σε δημιουργία ετικετών με διαφορετικά στοιχεία και δυνατότητες. Αυτό προσφέρει την δυνατότητα να ακολουθούντα διάφορες ομαδοποιήσεις στην βάση των χαρακτηριστικών που αφόρα την εργασία. Ένας συχνός διαχωρισμός είναι αυτός μεταξύ ενεργών και παθητικών ετικετών. Οι ενεργές ετικέτες λαμβάνουν ενεργεία από μπαταρία ή έστω από κάποια αυτόνομη πηγή ενέργειας. Έχουν την δυνατότητα να εκπέμψουν ένα σήμα προς τον αναγνώστη σε μακρινές αποστάσεις, όπως για παράδειγμα μερικές εκατοντάδες μέτρα και στις περισσότερες περιπτώσεις γίνεται χρίση τους για την ιχνηλάτηση αγαθών σημαντικής αξίας, όπως για παράδειγμα αυτοκίνητα και εμπορευματοκιβώτια. Οι ενεργές ετικέτες κάνουν χρίση των στις συχνότητες UHF και μικροκυμάτων, αξιοποιώντας τα ραδιοκύματα που εκπέμπει ο αναγνώστης. Ο αναγνώστης εκπέμπει σε μία ραδιοσυχνότητα χαμηλής ενέργειας, και ακολούθως η ετικέτα λαμβάνει τα ραδιοκύματα αυτά με την κεραία της και τα μετατρέπει στην ενέργεια που έχει ανάγκη για τη λειτουργία της. Ο τρόπος πρόσληψης της ενέργειας, για τις παθητικές ετικέτες υφίστανται περιορισμούς στην απόσταση εκπομπής, τυπικά μέχρι 3 μέτρα και μέγεθος της μνήμης που μπορούν να διαθέτουν. Το χαμηλό τους κόστος, μικρότερο του ενός ευρώ και η μεγάλη διάρκεια ζωής τους, τις καθιστά ελκυστικές για σημαντικό εύρος εφαρμογών, όπως αυτές στις οποίες γίνεται χρήση μεραβδόμορφοικώδικες.

Οι παθητικές ετικέτες έχουν την δυνατότητα λειτουργία, πέραν των UHF και μικροκυματικών συχνοτήτων και στις LF και HF συχνότητες. Οι ενεργές ετικέτες παρέχουν και κάποια από τα πλεονεκτήματα έναντι των παθητικών. Όπως προαναφερθηκε το σήμα που έχουν την δυνατότητα να εκπέμψουν είναι πιο ισχυρό και άρα μπορούν να επικοινωνήσουν με τον αναγνώστη από μεγαλύτερες αποστάσεις. Ακόμα, λόγω του ότι ο αναγνώστης δεν είναι υποχρεωμένος να τροφοδοτήσει την ετικέτα με το σήμα του, έχει την δυνατότητα χρήσης ενός σήματος με πολύ μικρότερη ισχύ. Το στοιχειό που διαθέτουν της ενεργητικής αυτονομίας, προσφέρει την δυνατότητα ενεργές ετικέτες, να εκκινούν μία επικοινωνία, στοιχείο που είναι σημαντικό σε αρκετές εφαρμογές, όπως για παράδειγμα οι εφαρμογές που απαιτούν από μία ετικέτα-αισθητήρα να ενημερώνει των αναγνώστη όταν μία περιβαλλοντική ένδειξη φτάσει κάποια τιμή κατωφλίου.

Η εξέλιξη της τεχνολογίας και των διαδικασιών κατασκευής ηλεκτρονικών κυκλωμάτων έχει προσφέρει την δυνατότητα αρκετοί κατασκευαστές να δημιουργούν συνεχώς νέα μοντέλα ετικετών με διαφορετικά χαρακτηριστικά. Μες στόχο τις

φθηνότερες, μικρότερες και ανθεκτικότερες ετικέτες, που θα δέχονται κυκλώματα μεγαλύτερης πολυπλοκότητας και θα έχουν την δυνατότητα να αναγνωστούν από μεγαλύτερη απόσταση. Κάποια από αυτά της εταιρία Hitachi η οποί δημιούργησε ετικέτες RFID με μέγεθος μόλις 0.05 x 0.05 χιλιοστά. Το και πάλι της Hitachi, η μ-Chip, με μέγεθος 0,4 x 0,4 χιλιοστά, ενώ η εταιρία Mojix το 2008 παρουσίασε το Mojix STAR System, ένα RFID σύστημα με εμβέλεια ανάγνωσης, σε εσωτερικό περιβάλλον, έως και περίπου 180 μέτρα. Ακόμα, η εταιρία Fujitsu έχει δημιουργήσει RFID ετικέτες οι έχουν την δυνατότητα επιτρεπτό να πλένονται και να σιδερώνονται. Στοιχεία που προσδιορίζουν την χρηστικότητα και την πολλαπλότητα των εφαρμογών των RFID ετικετών (RFID Journal, 2003, & http://www.rfidjournal.com/article/articleview/609/-1/1).

3.3 **Αρχές Σχεδιασμού Συστημάτων Πιστοποίησης**.

Στον περιβάλλον των τεχνολογιών και της πληροφορίας, με τον όρο πιστοποίηση περιγράφεται η διαδικασία επιβεβαίωσης ότι η ταυτότητα ενός ανθρώπου είναι αυθεντική. Το σύνολο των διαδικτύων πιστοποίησης της ταυτότητας ενός ατόμου προσδιορίζεται πιστοποίηση χρήστη.

Για την πιστοποίηση ενός πρόσωπου διακρίνονται τρεις πρακτική:

1. Ο χρήστης αναφέρει κάτι που γνωρίζει, όπως ένας κωδικός. Αυτή η προσέγγιση είναι εύρος γνωστή ως παράγων γνώσης (knowledge factor).
2. Ο χρήστης αναφέρει κάτι που διαθέτει, όπως για παράδειγμα μια κάρτα. Αυτή η πρακτική είναι γνωστή ως παράγων κατοχής (possession factor).
3. Ο χρήστης διακρίνεται προσωπικό φυσικό χαρακτηριστικό, όπως το δακτυλικό του αποτύπωμα. Αυτή η πρακτική είναι γνωστή ως παράγων ύπαρξης (being factor).

Η καλύτερη και ασφαλέστερη για την πραγματοποίηση της πιστοποίησης χρήστη είναι η τελευταία προσέγγιση που περιλαμβάνει την ανάλυση μοναδικών φυσικών χαρακτηριστικών του ατόμου, όπως για παράδειγμα το δακτυλικό αποτύπωμα ή την ίριδα του ματιού. Ως βιομετρική (Biometrics) περιγράφεται η επιστήμη που ασχολείται με αυτές τις διαδικασίες.

Βασικοί τύποι βιομετρικής:

- Σάρωση δακτυλικού αποτυπώματος η διαδικασία μπορεί να γίνει οπτικά, με πυρίτιο, με υπέρηχο, χωρίς επαφή κ.α.
- Σάρωση προσώπου αυτή η διαδικασία πραγματοποιείται είτε οπτικά είτε θερμικά.
- Σάρωση ίριδας ματιού
- Σάρωση φωνής
- Σάρωση αμφιβληστροειδούς χιτώνα ματιού
- Σάρωση υπογραφής
- Σάρωση χεριού
- Σάρωση πατήματος πλήκτρου
- Σάρωση παλάμης

Τύποι βιομετρικής με μειωμένη εμπορική βιωσιμότητα ή τύποι βιομετρικής σε ερευνητικό στάδιο :

- DNA
- Οσμή
- Σάρωση φλέβας (Vein-scan)
- Σχήμα αυτιού

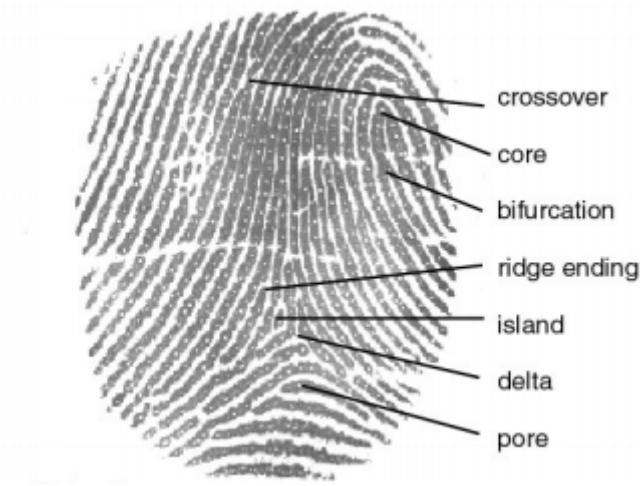
- Γεωμετρία δακτύλου, δηλαδή το σχόλα και η δομή του δάκτυλου ή δάκτυλων.
- Σάρωση νυχιού
- Αναγνώριση βηματισμού, ο τρόπος με τον οποίο κάποιος περπατά (Μπόζιος, 2004).

3.3.1 **Δακτυλικά αποτυπώματα**

Η μοναδικότητα και η σταθερότητα των δακτυλικών αποτυπωμάτων είναι κάτι που έχει ανακαλυφθεί αρκετά χρόνια πριν και αποτελεί αδιαμφισβήτητο στοιχειό για κάθε άτομο. Έρευνες έχουν δείξει ότι η πιθανότητα δύο ανθρώπων, ανάμεσα και σε δίδυμα, το να έχουν το ίδιο δακτυλικό αποτύπωμα είναι μικρότερη απο ένα

δισεκατομμύριο. Αρκετές είναι συσκευές στην αγορά πια που πραγματοποιούν ανάλυση της θέση πολύ μικρών σημείων, που καλούνται λεπτομέρειες. Οι συσκευές προσδιορίζουν τη θέση των λεπτομερειών κάνοντας χρήση x, y και κατευθυντικές μεταβλητές. Άλλες συσκευές προσεγγίζουν το δάκτυλο ως ένα ζήτημα μέσα από την επεξεργασίας εικόνας. Τα δακτυλικά αποτυπώματα απαιτούν ένα από τα μεγαλύτερα περιγράμματα δεδομένων στο πεδίο τη βιομετρικής, που είναι δυνατόν να πάρει από μερικά bytes έως και πάνω από 1.000 bytes, ανάλογα με την προσέγγιση και το επίπεδο ασφάλειας που είναι αναγκαίο για την πραγματοποίηση μια διεργασίας. Την δεδομένη χρονική στιγμή η μεγαλύτερη εφαρμογή με τεχνολογία δακτυλικών αποτυπωμάτων είναι στο αυτοματοποιημένο σύστημα αναγνώρισής δακτυλικών αποτυπωμάτων (AFIS) στο οποίο γίνεται χρήση από τις αστυνομικές αρχές σε πάνω από 30 χώρες (Μπόζιος, 2004).

Εικόνα 1 : Τοπογραφία δακτυλικού αποτυπώματος.



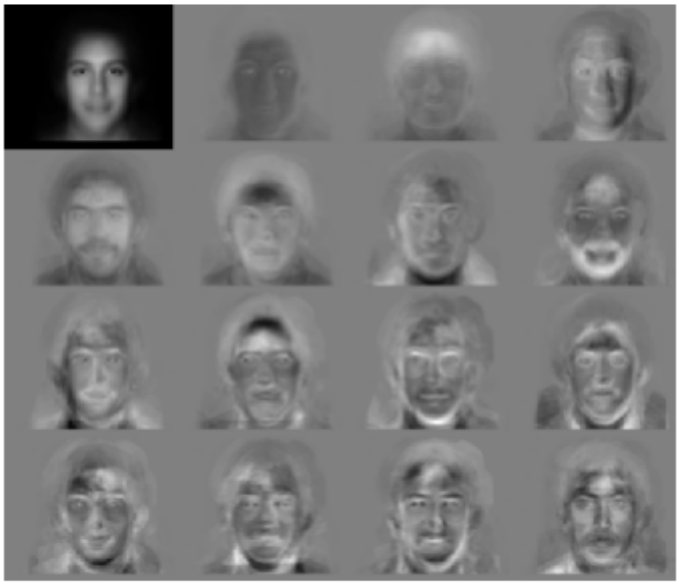
Πηγή: Μπόζιος, 2004,σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων, Α.Τ.Ε.Ι. Θεσσαλονίκης.

3.3.2 Χαρακτηριστικά προσώπου.

Από τα ποιο αναπτυσσόμενα πεδία της βιομετρικής, είναι η αναγνώριση και επαλήθευση προσώπου. Πολλοί οργανισμοί εργάζονται πάνω σε τεχνικές και τεχνολογίες συστήματα που κάνουν χρήση προηγμένων τεχνικών αναγνώρισης αντικειμένου, συμπεριλαμβανομένων των MIT Media Lab, το πανεπιστήμιο του Harvard, ένας αρκετά σημαντικός αριθμός αμυντικών βιομηχανιών και αρκετών

ακόμα σημαντικών επιχειρήσεων. Τα πλεονεκτήματα της αναγνώρισης προσώπου είναι κάτι παραπάνω από εμφανή. Ένα από αυτά είναι ότι αποτελούν μια διαδικασία που βρίσκεται πιο κοντά στον τρόπο που τα άτομα θα αναγνωρίζαμε ένα άτομο και επιπλέον μια εικόνα προσώπου είναι δυνατό να ληφθεί αρκετά μακρινή απόσταση με την δεδομένη τεχνολογία. Στη σάρωση προσώπου ιδιαίτερη προσοχή δίνεται σε τμήματα του προσώπου που είναι δύσκολο να μεταβληθούν, όπως τα περιγράμματα πάνω από τα μάτια, οι περιοχές γύρω από τα ζυγωματικά και την όψη των χειλιών. Τα περισσότερα συστήματα δεν έχουν παρουσιάσει προβλήματα προβλήτα σε μεταβολές των μαλλιών, όπως επίσης δεν κάνουν χρήση των περιοχών του προσώπου γύρω από τα μαλλιά. Όλα τα βασικά συστήματα είναι διαμορφωμένα ώστε να είναι αρκετά δυνατά για να διενεργούν αναζητήσεις 1-προς-πολλά, δηλαδή να έχουν την δυνατότητα να βρίσκουν ένα πρόσωπο, μέσα από μια βάση δεδομένων χιλιάδων ή ακόμα και εκατοντάδων χιλιάδων προσώπων. Οι σημαντικότερος δυσκολίες που έχουν εντοπιστεί σε αυτά τα είναι στο να πετύχουν σημαντικά επίπεδα απόδοσης όταν το μέγεθος της βάσης δεδομένων αυξάνεται σε δεκάδες χιλιάδες και περισσότερο. Για την σάρωση προσώπου είναι αναγκαία η ανάλυση 320x240 και τουλάχιστον 3 – 4 frames το δευτερόλεπτο. Περισσότερα frames το δευτερόλεπτο μαζί με καλύτερη ανάλυση συμβάλουν σε καλύτερη λειτουργία της διαδικασίας της αναγνώρισης. Η δαπάνη για κάμερα είναι μικρή και εκδόσεις demo των κυριοτέρων εφαρμογών προσφέρεται δωρεάν στο διαδίκτυο. Έτσι η αναγνώριση προσώπου είναι ένα από τα λίγα βιομετρικά με το οποίο κάποιος έχει την δυνατότητα να διεξάγει με ένα πολύ μικρό κόστος (Μπόζιος, 2004).

Εικόνα 2.: Αποτέλεσμα σάρωσης προσώπου Source: MIT Face Recognition Demo Page



Πηγή: MIT Face Recognition Demo Page

3.3.3 **Σάρωση φωνής** (Voice scan)

Στην περίπτωση σάρωσης φωνής γίνεται χρήση των φωνητικών προσδιοριστικών στοιχείων για να αναγνωριστεί ένα άτομο. Αποτελεί μια τεχνολογία αρκετά ελκυστική λόγω της αποδοχής που δέχεται από τους χρήστες. Τα συστήματα σάρωσης φωνής αναλύουν και προσδιορίζουν το μοναδικό ηχητικό σήμα που παράγει ο κάθε χρήστης καλώντας μια προσδιορισμένη φράση κλειδί (pass-phrase). Το βασικό πλεονέκτημα την εν' λόγο τεχνολογίας είναι η ικανότητα να πιστοποιεί κάποιον από μακρινή απόσταση. Δεν είναι υποχρεωτικό ο χρήστης να στέκεται σε κάποιο αμηχανία ή συσκευή του συστήματος, όπως και στην περίπτωση αναγνώρισης δακτυλικού αποτυπώματος ή προσώπου, αλλά σε αυτή την περίπτωση αυτός μπορεί να βρίσκεται χιλιόμετρα μακριά κάνοντας χρήση του smart phone του ή να βρίσκεται στο σπίτι του και να κάνει χρήση ενός κοινού μικρόφωνο.

Στην περίπτωση αναγνώρισης της φωνής. Η φράση- κλειδί στις περισσότερες περιπτώσεις επιβάλλεται να είναι μια φράση μερικών δευτερόλεπτων δευτερολέπτων. Δεν είναι υποχρεωτικό να περιέχει μυστικές πληροφορίες και χαρακτηρίστηκες λέξεις. Μπορεί να περιλαμβάνει λέξεις όπως για παράδειγμα το ονοματεπώνυμο, η διεύθυνση και πόλη του χρήστη.

Ένα από τα μειονεκτήματα που προκύπτει σε αυτή την περίπτωση ταυτοποίησης είναι ότι συχνά μαζί με τη φράση-κλειδί εισέρχονται και θόρυβοι που προκαλούνται τυχαία, όπως θόρυβος με τα χείλη, θόρυβος αναπνοής, βήχας, άσχετες συλλαβές κλπ. Ένα από τα ζήτημα που απασχολούν τους χρηστές συστημάτων αναγνώρισης φωνής είναι οι απομιμήσεις. Αυτό δεν είναι σημαντικό, γιατί οι συσκευές σκόπιμα εστιάζουν σε διαφορετικά στοιχεία της ομιλίας, σε σχέση με τους ανθρώπους. Οι απομιμητές εστιάζονται στα χαρακτηριστικά που ως άνθρωποι ακούν και κάνουν φτωχή δουλειά με τα υπόλοιπα. Επίσης μια απειλή για τα συστήματα φωνής είναι η κλωνοποίηση της φωνής. Αλλά ακόμα και αυτός ο φόβος είναι ελάχιστος αν υπολογίσει κανείς ότι για να δημιουργηθεί ένας κλώνος φωνής χρειάζονται 10-40 ώρες ομιλίας του πραγματικού χρήση και το κόστος πλησιάζει τα 200 χιλ. δολάρια.

Μπόζιος Ε.,(2004),σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων, για τις διδακτικές ανάγκες του μαθήματος ασφάλεια πληροφοριακών συστημάτων, Α.Τ.Ε.Ι. Θεσσαλονίκης

Εικόνα 3: Λογισμικό αναγνώρισης φωνής

Πηγή: https://opensource.ellak.gr/2017/07/20/common-voice-ena-sistima-anagnorisis-omilias-anichtou-kodika-apo-to-mozilla/

3.3.4 **Σάρωση ίριδας** (Iris-scan)

Η αναγνώριση ίριδας ματιού στηρίζεται στα ορατά, στοιχεία της ίριδας. Η ίριδα αποτελεί ένα προστατευμένο εσωτερικό όργανο του ματιού, που βρίσκεται ακριβώς πίσω από τον κερατοειδή χιτώνα, αλλά και μπρέστο από τον κρυσταλλοειδή χιτώνα του ματιού. Είναι το μόνο εσωτερικό όργανο του ανθρωπινού σιούτος πού είναι ορατό από το εξωτερικό περιβάλλον. Σύμφωνα με έρευνες που έχουν γίνει η ανθρώπινη ίριδα έχει σχεδόν 250 χαρακτηριστικά και καθένα από διακρίνεται από μοναδικότητα στον κάθε άνθρωπο. Αυτό σε συνδυασμό με την μοναδικότητα των στοιχειών που περιέχονται στην ίριδα μεγαλώνουν την καταλληλότητα της ίριδας για χρήση σε υψηλής ασφάλειας συστήματα αναγνώρισης και αυτά είναι :

(1) Η έμφυτη απομόνωση και προστασία από το εξωτερικό περιβάλλον.
(2) Το ότι δεν μπορεί να μεταβληθεί με χειρουργικής μεταβολή, χωρίς ανεπιθύμητους κινδύνους στην όραση.
(3) Η φυσιολογική αντίδραση στο φως, η οποία διασφαλίζει έναν από τους αρκετούς φυσικούς ελέγχους.

Η ίριδα διαθέτει ακόμα περισσότερα πρακτικά πλεονεκτήματα σε σύγκριση με τα δακτυλικά αποτυπώνατε και από τα υπόλοιπα βιομετρικά στοιχεία ενός ατόμου. Αυτά είναι :

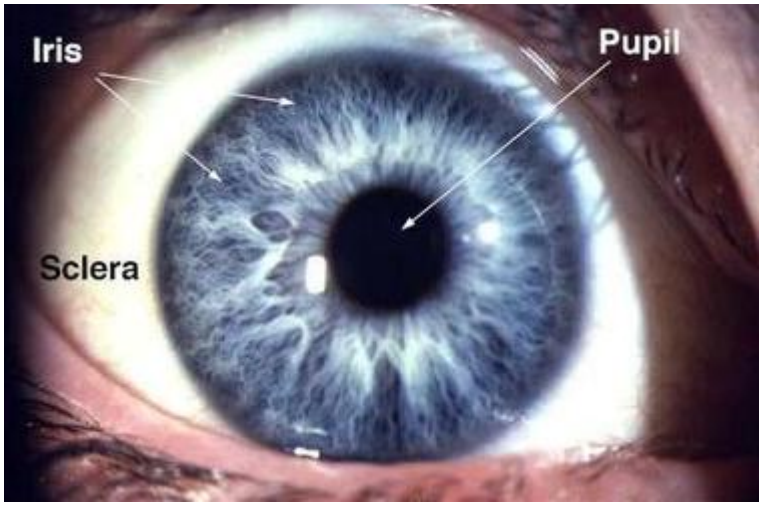
(1) Ότι έχει την δυνατότητα να δημιουργηθεί μια εικόνα από απόσταση, χωρίς φυσική επαφή.
(2) Τα χαρακτηριστικά της παραμένουν ίδια καθ΄ όλη τη διάρκεια ζωή του ατόμου.

Η σάρωση ίριδας πραγματοποιείται από μια συσκευή, η οποία διαθέτει μια κάμερα και φακούς κοντινής λήψης, που λαμβάνει μια στατική εικόνα του ματιού. Το σύστημα αναλύει την εικόνα και παράγει έναν κώδικα 512 bytes που χαρακτηρίζεται ως κώδικας ίριδας. Αποθηκεύεται ένα πρότυπο για μελλοντική προσπάθεια εξακρίβωσης του ατόμου. 512 bytes είναι αρκετά συμπαγές μέγεθος για ένα βιομετρικό πρότυπο, όμως η ποσότητα της πληροφορίας που προέρχεται από μια ίριδα διακρίνεται από επιπλέον μέγεθος. Για μια ίριδα διαμέτρου 11 χιλιοστών, απαιτούνται 3,4 bits ανά χιλιοστό.

Αρχικά για την αναγνώριση μέσο ίριδας θα πρέπει να τοποθετηθεί το άτομο μπροστά στην κάμερα σε απόσταση 2-18 ίντσες, με βάση της οδηγίες που απαιτεί η συσκευή. Ακολούθως εστιάζει το μάτι στη συσκευή, ώστε θα πρέπει να μπάρει να δει την αντανάκλαση του ματιού. Η διαδικασία της αναγνώρισης δεν απαιτεί πολύ χρόνο. Η εικόνα του ματιού παράγεται σε 0,25 του δευτερολέπτου, ο κώδικας ίριδος εντός δευτερόλεπτου, η αναζήτηση στη βάση δεδομένων είναι άμεση, με εκατοντάδες χιλιάδες εγγραφών να αναλύονται το δευτερόλεπτο. Παρόλα αυτά υπάρχουν κάποιες ενστάσεις, κατά πόσον η αναζήτηση σ’ ένα πραγματικά μεγάλο αριθμό εγγραφών θα ήταν δυνατόν να διεξάγεται τόσο γρήγορα όσο απαιτείται. Η σάρωση ίριδας είναι μία τρομακτικά ακριβής βιομετρική τεχνολογία. Μόνο η σάρωση του αμφιβληστροειδούς χιτώνα είναι δυνατόν να παράσχει σχεδόν τόσο καλή ασφάλεια από αυτή που προσφέρει η ίριδα. Τα περισσότερα κοινά βιομετρικά προσφέρουν λογικά αποτελέσματα, αλλά δεν έχουν την δυνατότητα να γίνει χρήση τους σε μεγάλης κλίμακας υλοποιήσεις αναγνώρισης όπως η αναγνώριση ίριδας.

Μπόζιος Ε.,(2004),σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων, για τις διδακτικές ανάγκες του μαθήματος ασφάλεια πληροφοριακών συστημάτων, Α.Τ.Ε.Ι. Θεσσαλονίκης

Εικόνα 4: Σάρωση ίριδας



Πηγή: http://ahci.wikispaces.com/Eye-tracking

3.3.5 Σάρωση αμφιβληστροειδούς χιτώνα ματιού

Η σάρωση αμφιβληστροειδούς, μαζί με τη σάρωση ίριδας αποτελούν ίσως την πιο ακριβής και αξιόπιστη βιομετρική τεχνολογία, όμως είναι και μεταξύ των πιο δύσκολων στην διαχείριση και στην χρήση του. Η σάρωση αμφιβληστροειδούς χαρακτηρίζεται από τα παλαιότερα βιομετρικά. Από το 1930 έρευνες προσδιόρισαν ότι η μορφή των αγγείων αίματος στο πίσω μέρος του ανθρώπινου ματιού είναι διαφορετική σε κάθε άτομο, ακόμα και στην περίπτωση δίδυμων. Επίσης ο αμφιβληστροειδής παραμένει καθ' όλη την ζωή του ατόμου, με ελάχιστες εξερεσεις. Ο αμφιβληστροειδής χιτώνας του ματιού είναι ένα μικρό νεύρο (1/50ο της ίντσας) στο πίσω μέρος του ματιού, είναι το τμήμα του ματού το οποίο αισθάνεται το φως και μεταδίδει παλμούς δια μέσου του οπτικού νεύρου προς τον εγκέφαλο.. Οι συσκευές σάρωσης αμφιβληστροειδούς διαβάζουν δια μέσου της κόρης του ματιού, γι' αυτό είναι σημαντικό ο χρήστης να τοποθετήσει το μάτι του εντός μισής ίντσας από τη συσκευή και να παραμένει ακίνητος μέχρι η συσκευή ανάγνωσης εξακριβώσει την ταυτότητα του.

Ο χρήστης εστιάζει σ' ένα περιστρεφόμενο πράσινο φως. Παίρνονται 350 έως 400 σημεία αναφοράς και αποθηκεύονται σ' ένα πεδίο 96 bytes, εξασφαλίζοντας ότι ο υπολογισμός είναι ορθώς, με ένα αμελητέο βαθμό σφάλματος. Συγκριτικά με το δακτυλικό αποτύπωμα που απαιτούνται 30-70 διακριτά σημεία, γίνεται διακριτό το

πολύ υψηλό επίπεδο ακρίβειας της τεχνολογίας αυτής. Στα πλεονεκτήματα αυτής της μεθόδου προσδιορίζονται τα ακόλουθα :

- Ανύπαρκτη πιθανότητα κάποιος χρήστης να διεκδικήσει λάθος ταυτότητα και να γίνει αποδεκτός
- Σταθερότητα στο βιομετρικό δείγμα
- Ανθεκτικότητα στην απάτη. Θα ήταν αρκετά δύσκολο και χρονοβόρο να κατασκευαστεί ένα ψεύτικο δείγμα αμφιβληστροειδούς
- Πολύ μικρή ποσότητα δεδομένων

Στα μειονεκτήματα συνυπολογίζουμε τα ακόλουθα:

- Μη εύχρηστο
- Διστακτικότητα από τους χρήστες. Το μάτι και ειδικά το εσωτερικό του ματιού, διακρίνεται από μεγάλη ευαισθησία και γι' αυτό αρκετοί χρήστες είναι διστακτικοί στην χρήση τέτοιων συσκευών.
- Στατικός σχεδιασμός. Σε αντίθεση με τις προαναφερθείσες τεχνολογίες, οι οποίες έχουν την δυνατότητα εκμετάλλευσης τα πλεονεκτήματα των νέων τεχνολογιών, όπως καλύτερης ποιότητας κάμερα ή αξιοποίηση πυριτίου, ή σάρωση αμφιβληστροειδούς είναι περιορισμένη σε συγκεκριμένους μηχανισμούς σύλληψης του δείγματος και συγκεκριμένα πρωτοκόλλα
- Το σημαντικά υψηλό κόστος. Οι συσκευές σάρωσης αμφιβληστροειδούς κοστίζουν περίπου $2000-$2500 (Μπόζιος, 2004).

3.3.6 **Σάρωση Χεριού**

Η σάρωση χεριού έχει λάβει και την ονομασία και ως γεωμετρία χεριού. Είναι μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δακτύλων. Στην τεχνολογία αυτή γίνεται χρήση τεχνολογία το ύψος των δακτύλων, η απόσταση ανάμεσα στις κλειδώσεις και το σχήμα των αρθρώσεων για να πιστοποιήσει την ταυτότητα του ατόμου-χρηστή. Ο χρήστης τοποθετεί το χέρι του στην συσκευή

ακουμπώντας την παλάμη του σε μία επιφάνεια διαστάσεων 8x10. Στη συνέχεια ο χρήστης ευθυγραμμίζει το χέρι του σύμφωνα με τα πέντε ειδικά σημεία, που είναι σχεδιασμένα ώστε να υποδείξουν την ορθή θέση του αντίχειρα, του δείκτη και του μεσαίου. Το σύστημα κάνει χρήση μιας 32.000 pixel CCD (charged coupled device) ψηφιακή κάμερα, εξάγοντας συμπεράσματα για το μήκος, το πλάτος, το πάχος και την επιφάνεια του χεριού από τις εικόνες των περιγραμμάτων που σχεδιάζονται μέσα στον σαρωτή. Γίνονται πάνω από 90 υπολογισμοί και τα χαρακτηριστικά του χεριού αναπαριστούνται σ' ένα πρότυπο 9 bytes.

Εικόνα 5: Τοποθέτηση παλάμης

Πηγή: https://securityreport.gr/magazine-archive/year-2015/item/1344-ayksisi-14-etisios-gia-tin-agora-viometrikon-systimaton-asfaleias-os-to-2020

Στα πλεονεκτήματα της σάρωσης χεριού, εντάσσονται :

- Ευκολία στη χρήση. Χαρακτηρίζεται ως μια διαδικασία και με κατάλληλη εκπαίδευση είναι δυνατόν να περιοριστούν και τα λάθη στην τοποθέτηση του χεριού. Με μια μικρή εξαίρεση στα άτομα μεγάλης ηλικίας ή σε άτομα με αρθριτικά προβλήματα στα χέρια, που ίσως να μην έχουν την δυναότητα να ανοίξουν τα δάκτυλα και να τοποθετήσουν το χέρι τους πάνω στην συσκευή.
- Ανθεκτική στην απάτη.
- Μικρό σχετικά μέγεθος προτύπου. Μόλις 9 Bytes.

- Αντίληψη του χρήστη. Σε αντίθεση με τη σάρωση προσώπου ή τις τεχνολογίες βασισμένες στο μάτι, οι οποίες είναι δυνατόν να συναντούν κάποιες αντιδράσεις, η σάρωση χεριού είναι αποδεκτή από τη μεγάλο πλήθος χρηστών.

Μειονεκτήματα της σάρωσης χεριού :

- Στατικός σχεδιασμός. Η τεχνολογία της σάρωσης χεριού είναι σε σημαντικό βαθμό αμετάβλητη για πολλά χρόνια.
- Μικρό κόστος. Το όποιο για τους σαρωτές χεριού φτάνει περίπου $1400 - $2000
- Κακώσεις στο χέρι. Όπως σε όλα τα βιομετρικά φυσικές αλλαγές είναι δυνατόν να προκαλέσουν εσφαλμένη απόρριψη των χρηστών.
- Ακρίβεια. Παρόλο που είναι πιο αξιόπιστη από τα βιολογικά βιομετρικά, όπως η φωνή και η υπογραφή, η σάρωση χεριού δεν είναι δυνατόν να πραγματοποιήσει αναζητήσεις ένα -προς- πολλά.

(Μπόζιος, 2004).

3.3.7 **Σάρωση υπογραφής**

Η σάρωση υπογραφής που αναφέρετε και ως δυνητική εξακρίβωση υπογραφής (Dynamic Signature Verification). Αποτελεί και αυτή μια βιομετρική τεχνολογία η οποία δεν έχει συχνή χρήση, που προσδοκάτε στο μέλλον να συμβάλει στην αντιμετώπιση της πιστοποίησης επίσημων εγγράφων. Υπολογίζοντας τον τρόπο με τον οποίο ένας χρήστης σημειώνει το όνομα του, ένα συνθηματικό, μια έκφραση κλειδί, η σάρωση υπογραφής ερευνά τον τρόπο, την ταχύτητα, την πίεση και άλλα στοιχεία τα οποία σχετίζονται με τη διαδικασία της υπογραφής.

Εικόνα 6: Σάρωση υπογραφής

Πηγή: https://citrixready.citrix.com/signotec-gmbh.html

Ένα τυπικό σύστημα επαλήθευσης υπογραφής θα πρέπει να περιλαμβάνει διαδικασίες εξασφάλισης και αξιόπιστη αναγνώριση χρηστών, με βάση την υπογραφή τους. Στην διαδικασία γίνονται υπολογισμοί του μοναδικού τρόπου με τον οποίο προκύπτει μια χειρόγραφη υπογραφή, ώστε να επαληθευτεί η ταυτότητα του χρήστη. Σε μεγάλες εταιρίες ή μέσο διαδικτύου μια ψηφιακή υπογραφή καθιστά ικανές τις λειτουργίες να προσφέρουν υψηλή μυστικότητα και αξιόπιστη ηλεκτρονική εξουσιοδότηση, σε αντίθεση με ένα συνθηματικό, ένα PIN ή μια keycard, που είναι αρκετά συχνό το φαινόμενο να ξεχύνουνε, να χάνονται ακόμα και να υποκλέπτονται κλαπούν.

Τα συστήματα αυτά αναλύουν και τα δυναμικά και τα ”του χώρου” στοιχεία και γνωρίσματα της χειρόγραφης υπογραφής για να επαληθευόσουν την ταυτότητα του χρηστή που υπογράφει. Επειδή κάθε χρηστής διακρίνεται από τον προσωπικό του γραφικό χαρακτήρα, το σύστημα λαμβάνει τα χαρακτηριστικά του τρόπου γραφής και αναλύει τη δυναμική του χτυπήματος, την ταχύτητα και την πίεση. Ενώ με εξάσκηση κάποιος πιθανόν να καταφέρει να αντιγράψει την οπτική εικόνα της υπογραφής κάποιου χρηστή, είναι πολύ πολύπλοκο, έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Επίσης και αν η υπογραφή είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η πίεση δεν είναι δυνατόν να αντιγράφουν.

Αρκετά συστήματα σάρωσης υπογραφής εμπεριέχουν μια συνάρτηση μάθησης, η οποία μπορεί αυτομάτως να απορροφά και να απεικονίζει κάθε φυσική αλλαγή στην υπογραφή σε βάθος χρόνου. Τα εν λόγω συστήματα κάνουν χρήση αλλαγών στην πίεση, στη μορφή, στην κατεύθυνση και στην ταχύτητα σε συνάρτηση με το χρόνο. Έτσι τα στοιχεία αναλύονται σε τέσσερις διαστάσεις – x (οριζόντια ταχύτητα), y (κάθετη ταχύτητα), z (πίεση) και t (χρόνος) (Μπόζιος, 2004).

3.3.8 **Δυναμική πατήματος πλήκτρου**

Η δυναμική πατήματος πλήκτρου αναφέρετε και ως ρυθμός δακτυλογράφησης. Όπως υποδηλώνει και το αυτή η μέθοδος υπολογίζει τον τρόπο με τον οποίο ένα άτομο δακτυλογραφεί ή ασκεί πιέσει τα πλήκτρα του υπολογιστή ή μιας ηλεκτρονικής συσκευής. Η αυθεντική τεχνολογία προέρχεται από την ιδέα αναγνώρισης ενός αποστολέα σημάτων Morse, μέσα από την χρήση ενός κλειδιού τηλεγραφίας γνωστό ως " γροθιά του αποστολέα", δια του οποίου οι χειριστές έχουν την δυνατότητα να αναγνωρίσουν τους αποστολείς που διαβίβαζαν ένα μήνυμα από το ρυθμό, το μέτρο και τη βραχύτητα του μηνύματος. Η τεχνολογία αυτή αναλύει στοιχεία όπως η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα κάποιου άλλου συγκεκριμένου πλήκτρου.

Τα πλεονεκτήματα της δυναμικής πατήματος πλήκτρου :

- Η επιβεβαίωση στηρίζεται στην παραδοχή ότι ο τρόπος με τον οποίο δακτυλογραφεί ο χρήστης είναι μοναδικός και ειδικότερα ο ρυθμός του. Επίσης και αν κάποιος μπορεί να βρει το σωστό συνθηματικό, δεν έχει την δυνατότητα να το δακτυλογραφήσει με τον σωστό ρυθμό.
- Η συσκευή εισόδου είναι δυνατόν να είναι το υπάρχον πληκτρολόγιο. Έτσι περιορίζεται σημαντικά το κόστος.

Τα μειονεκτήματα αυτής της δυναμικής πατήματος πλήκτρου :

- Διακρίνονται αρκετές τεχνικές δυσκολίες που καθιστούν την τεχνολογία αυτή να μην αποδίδει τα επιδιωκόμενα αποτελέσματα.

- Οι μισές προσπάθειες να εισέρθει στην αγορά η τεχνολογία πατήματος πλήκτρου δεν επέτυχαν.
- Οι διαφορές στα πληκτρολόγια, ακόμα και παρόμοιας εταιρίας, και στα πρωτόκολλα επικοινωνίας προβάλουν ζητήματα στις εταιρίες ανάπτυξης την τεχνολογίας αυτής (Μπόζιος, 2004).

3.3.9 DNA

Ένα καίριο ζήτημα είναι το κατά πόσο το DNA μπορεί να αποτελεί μέρος των βιομετρικών τεχνολογιών. Το DNA διαφέρει από τα τυπικά βιομετρικά σε αρκετά σημεία:

- Για το DNA είναι απαραίτητο απαιτεί ένα χειροπιαστό φυσικό δείγμα, ενώ στην προαναφερθείσες περιπτώσεις είναι αποδεκτή μια εικόνα, ένα αποτύπωμα και μια εγγραφή.
- Η ταυτοποίηση του DNA και μπορεί να πραγματοποιηθεί πραγματικό χρόνο και συγχρόνως δεν είναι όλα τα στάδια της σύγκρισης αυτοματοποιημένα.
- Η ταυτοποίηση του DNA δεν κατασκευάζει πρότυπα ή εξαγωγή χαρακτηριστικών, αλλά αντιθέτως αναπαριστά τη σύγκριση με υπαρκτά δείγματα.

Παρά τις σημαντικές διαφορές, το DNA αποτελεί έναν τύπος βιομετρικής αφού κάνει χρήση του φυσικού χαρακτηριστικού στην επαλήθευση και τον προσδιορισμό ενός χρήστη. Το αν το DNA θα βρει χρήση εκτός από την παρούσα χρήση του και σε άλλες ανάλογες εφαρμογές κάνει δεν μπορεί να το προβλέψει. Οι συνθήκες κάτω από τις οποίες η χρήση, η συλλογή, η αποθήκευση και η διάθεση πρέπει να είναι οροθετημένες και ενισχυόμενες αποτελούν αντικείμενο έρευνας και προσδιορισμού των αρχών για τα προσωπικά δεδομένα. Αυτοί οι προσδιορισμοί θα είναι διαφορετική από εφαρμογή σε εφαρμογή (Μπόζιος, 2004)..

3.4 **Απαιτήσεις Ασφάλειας και Ιδιωτικότητας Δεδομένων**

Η έννοια του απόρρητου-ιδιωτικότητας περιγράφει είτε στη μη προσπελασιμότητα ορισμένων στοιχείων που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να πρέπει να φυλάσσουν τις εν΄ λόγω πληροφορίες που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους στις οργανωτικές διαδικασίες μιας πολιτική οργάνωσης μιας κοινωνιας. Εάν μάλιστα πρόκειται για πληροφορία που σχετίζεται με την δημόσια σφαίρα δεν είναι αυτονόητη η προστασία από το απόρρητο. Για να είναι απόρρητη/εμπιστευτική η πληροφορία επιβάλλεται να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.α (Solove, 2002).

Το "απόρρητο" τοποθετεί εμπόδια σε τρίτους από τη γνώση, τη χρήση και αξιοποίηση των στοιχειών, εφόσον δεν υπάρχει και δεν προσδιορίζεται ο λόγος που αν πηγάζει από το νόμο και οι ανάλογες διαδικασία που παρέχουν την δυνατότητα παύσης του απορρήτου. Παρόλα αυτά σε ορισμένες έννομες τάξεις, όπως αυτή των ΗΠΑ, ήδη το γεγονός ότι ένα πρόσωπο παρέχει μία πληροφορία που το αφορά με αυτό σε ένα άλλο πρόσωπο ή οργανισμό ανοίγει το δικαίωμα στη στέρηση της προστασίας που επιφυλάσσεται στην ιδιωτικότητα. Η άποψη αυτή ακολουθείται από κρίσιμες για τα πρόσωπα επιπτώσεις, όπως για παράδειγμα το εύρος και οι προϋποθέσεις για περαιτέρω δημοσιοποίηση των πληροφοριών αυτών. Το Supreme Court (Ανώτατο Δικαστήριο στις ΗΠΑ) έκρινε ότι ένα πρόσωπο δεν έχει εύλογη προσδοκία ιδιωτικότητας, όσον αφορά πληροφορίες που προσέφερε εθελοντικά σε ένα τρίτο πρόσωπο ή οργανισμό και ακολούθως διαβιβάστηκαν από αυτό σε μία δημόσια αρχή, ακόμη και εάν η πληροφορία στο πρώτο στάδιο προσφέρθηκε με την προϋπόθεση ότι θα χρησιμοποιηθεί για κάποιο συγκεκριμένο σκοπό. Αυτό όμως προσδιορίζει μια σημαντική παρεκτροπή της επίκλησης της ιδιωτικότητας ως πληροφοριακής απομόνωσης: η χρησιμότητά της και εν τέλει παύει να υφίσταται κατά τη στιγμή που η πληροφορία "παραδίδεται" σε κάποιον άλλον, "διαφεύγει" από το πρόσωπο που αφορά και παύει να προσδιορίζεται ως "μυστική" (Simitis).

Ως προς την ευρωπαϊκή προσέγγιση, ο απόρρητος χαρακτήρας των προσωπικών πληροφοριών δεν πηγάζει μόνο από τη φύση τους αλλά προσδιορίζεται και στο σχετικό κανονιστικό πλαίσιο. Το άρθρο 16 της Οδηγίας 95/46/ΕΚ για την

προστασία προσωπικών δεδομένων προσφέρει μία ιδιότυπη αρνητική διατύπωση που σχετίζεται με το απόρρητο, καθώς προσδιορίζει ότι όποιος επεξεργάζεται και διαχειρίζεται δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας ή του εκτελούντος επεξεργασία το πραγματοποιεί μόνο με εντολή του υπεύθυνου επεξεργασίας. Ο ελληνικός νόμος για την προστασία προσωπικών δεδομένων (ν. 2472/97) στο άρθρο 10 § 1 εμπεριέχει ανάλογη διατύπωση αλλά παράλληλα προσδιορίζει συνολικά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως απόρρητη (Ν. 2472/97 άρθρου 10).

Το απόρρητο υπό την έννοια της εμπιστευτικότητας αφορά ακόμα την ασφάλεια των πληροφοριών αλλά δεν ταυτίζεται απόλυτα με αυτή. Η ασφάλεια της πληροφορίας δεν προάγεται μόνο από την εγγύηση της εμπιστευτικότητας. Η εμπιστευτικότητα αποτελεί ένα μόνο από τα στοιχεία που αποπλέουν την ασφάλεια των πληροφοριών, θα πρέπει να συμπεριληφθούν η εγκυρότητα, η αυθεντικότητα, η ακεραιότητα και η διαθεσιμότητα. Η ασφάλεια αποτελεί προϋπόθεση σε ένα οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που είναι αναγκαίο για να προστατευτούν τα στοιχεία ενός πληροφοριακού συστήματος και προφανώς δεν διασφαλίζεται μόνο, ίσως ούτε καν κυρίως, από νομικές επιταγές (Γκρίτζαλη, 2004).

Σε κάθε περίπτωση, τόσο η κοινοτική όσο και η ελληνική νομοθεσία για την προστασία προσωπικών δεδομένων είναι αναγκαίο να δημιουργήσουν τις «κατάλληλες» προοπτικές και να λάβουν τα κατάλληλα μέτρα ασφάλειας, ώστε να προστατεύονται τα δεδομένα από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, απαγορευμένη διάδοση ή πρόσβαση και οποιαδήποτε μορφή αθέμιτης επεξεργασίας. Ο νομοθέτης επάγει μάλιστα στον υπεύθυνο επεξεργασίας την υποχρέωση να διαμορφώνει ένα ορθό επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που εκπέμπει η επεξεργασία και η φύση των δεδομένων. Αξίζει να επισημανθεί ότι ο Έλληνας νομοθέτης συνδέει την υποχρέωση της εμπιστευτικότητας με τις υπόλοιπες διαστάσεις της ασφάλειας, προσδιορίζοντας μάλιστα να περιλάβει τις υποχρεώσεις απορρήτου και ασφαλείας σε ένα άρθρο .(Ν. 2472/97 Άρθρο 10 § 3 και άρθρο 17 της Οδηγίας 95/46/ΕΚ).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το δικαίωμα του πληροφοριακού αυτοπροσδιορισμού των ατόμων αποτελεί θεμελιακό στοιχειό των σύγχρονων δημοκρατικών κοινωνιών. Ο πολίτης θα πρέπει να έχει το δικαίωμα της επιλογής να αποφασίζει ποιος θα έχει γνώση για τα προσωπικά του δεδομένα, πώς θα το μεταχειρίζεται και με ποια πρόθεση.

Οι δυο τελευταίες δεκαετία με την απίστευτη ανάπτυξη των τεχνολογιών του διαδικτύου, σε συνδυασμό με το σύνολο των διάφορων πολιτικοοικονομικών και κυρίως τεχνολογικές μεταβολών γενικότερα προσδιορίζουν ένα περιβάλλον με νέα δεδομένα και καινούριες προκλήσεις για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων.

Οι ιδιωτικές επιχειρήσεις στην πλαίσια της ανταγωνιστικής επιχειρηματικότητας έναντι των άλλων επιχειρήσεων συμπεριφέρονται στα προσωπικά δεδομένα ως οικονομικούς πόρους και προσδιορίζουν τις στρατηγικές μάρκετινγκ που πρόκειται να αναπτύξουν οι οποίες στοχεύουν σε συγκεκριμένες ανάγκες που πηγάζουν μέσα από τα προσωπικά δεδομένα που είναι δεδομένο ότι έχουν στην κατοχή τους, μέσα από αυτήν την τακτική είναι ορατό το ενδεχόμενο των κινδύνων που τίθεται η ιδιωτική ζωή.

Στις αρχές του 21^{ου} αιώνα ο «πόλεμο κατά της τρομοκρατίας» συντέλεσε στην συχνή υπονόμευση, παραβίαση και χαλάρωση διαφόρων μέτρων προστασίας της ιδιωτικότητας και την είσοδο σε προσωπικά δίδυμα ατόμων. Στο πλαίσιο της σύγχρονης κοινωνίας της πληροφορίας, υιοθετείται η χρήση συστημάτων ηλεκτρονικής διακυβέρνησης, ηλεκτρονικής υγείας και ηλεκτρονικού εμπορίου, τα οποία προφανώς και διαθέτουν την ικανότητα συλλογής και επεξεργασίας μεγάλου όγκου προσωπικών δεδομένων, καθιστώντας πιο απλή την διαδικασία και περεχώντας μεγαλύτερες δυνατότητες στην παραβίαση της ιδιωτικής ζωής και των προσωπικών δεδομένων. Οι εξελίξεις στον τομέα των Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (ΤΠΕ) κάνουν αδύνατη τη συμμετοχή των πολιτών στη σύγχρονη κοινωνία χωρίς οι δραστηριότητές τους να αφήνουν «ηλεκτρονικά αποτυπώματα», στοιχειό που συντελεί στην συρρίκνωση της ιδιωτικότητας και της ασφάλειας των προσωπικών τους δεδομένων.

Οι επιπτώσεις των εξελίξεων στον χώρο των ΤΠΕ στην ιδιωτική ζωή είναι ευδιάκριτε. Μέσα από την εύρεση νέων των τεχνολογιών διαδικτύου που η χρήση του από το ευρύ κοινό για πρόσβαση σε διάφορες υπηρεσίες ή πληροφορίες προσφέρει τη δυνατότητα συλλογή και επεξεργασία προσωπικών δεδομένων. Ο χρήστης κατά την είσοδο και περιπλάνηση του στο διαδίκτυο αφήνει «ηλεκτρονικά αποτυπώματα», όπως οι ιστοσελίδες που κίνησαν το ενδιαφέρον του, οι λέξεις που έκανε χρήση στις μηχανές αναζήτησης, ο χρόνος παραμονής σε κάθε ιστοσελίδες κ.α. Τα δεδομένα μπορούν να αποτελέσουν στοιχεία για την εξαγωγή συμπερασμάτων σχετικά με προσωπικά ενδιαφέροντα και προτιμήσεις του ατόμου, σε ζητήματα υγείας που έχει, καταναλωτικές του συνήθειες και αλλά στοιχεία που χαρακτηρίζονται από χρησιμότητα με στόχο την άμεσης διαφήμισης και προώθησης προϊόντων.

Τα σύγχρονα ψηφιακά τηλεπικοινωνιακά δίκτυα προσφέρουν την ικανότητα καταγραφής των στοιχείων επικοινωνίας στη σταθερή τηλεφωνία όπως για παράδειγμα των αριθμών τηλεφώνου των χρηστών, του χρόνου που έγινε η κλίση και του χρόνου που διήρκησε. Τα στοιχεία αυτά καταγράφεις βρίσκουν εφαρμογή και στην κινητή τηλεφωνία στην οποία υπάρχει ακόμα η δυνατότητα να εντοπισθεί και να καταγραφεί η ακριβής γεωγραφική τοποθεσία των ατόμων που επικοινωνούν και είναι δυνατόν να αξιοποιηθούν με τρόπου που είναι αντίθετες προς την ιδιωτικότητα.

Η ανάπτυξη των τεχνολογιών του διάχυτου υπολογισμού συντελεί στην μεγαλύτερη και εκτενέστερη απειλή της ιδιωτικής ζωής. Ο διάχυτος υπολογισμός ενσωματώνει τον υπολογισμό στο περιβάλλον, αφού διασυνδεδεμένοι υπολογιστές, σκορπισμένοι στον χώρο, παρέχουν υπηρεσίες χωρίς να είναι αντιληπτοί και χωρίς την επέμβαση του ανθρώπου. Οι υπηρεσίες είναι εξατομικευμένες για κάθε χρήστη και συνυπολογίζουν στοιχεία που τον επηρεάζουν, όπως το προφίλ της προσωπικότητάς του, τη θέση του, συνθήκες του περιβάλλοντός του κ.α. Μία από τις βασικές τεχνολογίες του διάχυτου υπολογισμού είναι η RFID (Radio Frequency Identification) η οποία δίνει την δυνατότητα την ανάθεση μιας μοναδικής ετικέτας αναγνώρισης σε οποιοδήποτε αντικείμενο ή πρόσωπο. Στις RFID ετικέτες είναι δυνατόν να αποθηκευτούν μεγάλες ποσότητες πληροφοριών και, αυτές να είναι εύκολο να αξιοποιηθούν για την ταυτοποίηση ενός συγκεκριμένου αντικειμένου ή προσώπου.

Η τεχνολογικές εξελίξεις της βιομετρικής τεχνολογίας είναι δυνατόν να προσφέρουν την δυνατότητα αξιοποίησης της ομιλίας, τα βιομετρικών του χαρακτηριστικών αλλά και της συμπεριφοράς-συναισθηματικής κατάστασης ενός ατόμου για την ταυτοποίησή του.. Η χρήση των τεχνολογιών του διάχυτου υπολογισμού σαφώς και αντίκεινται στις θεμελιώδες αρχές της ισχύουσας νομοθεσίας για την προστασία της ιδιωτικής ζωής, όπως, για παράδειγμα ότι ως κανόνας ορίζεται πως η επεξεργασία των προσωπικών δεδομένων επιτρέπεται αποκλειστικά και μόνο όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του ενώ οι λοιπές προϋποθέσεις νομιμότητας τίθενται ως εξαιρέσεις

Είναι δεδομένο ότι η ανάπτυξη των ΤΠΕ παρέχει την δυνατότητα συλλογής και επεξεργασίας μεγάλου όγκου πληροφοριών που σχετίζονται με το άτομο και αναφέρονται στην ταυτότητά του, στις συνήθειές του, στις πεποιθήσεις του κτλ., καθιστώντας σε πολύ σημαντικό βαθμό δυνατή την παραβίαση της ιδιωτικής του ζωής. Ωστόσο η πρόοδος των ΤΠΕ είναι δυνατόν μπορεί να αξιοποιηθεί και για την προστασία της ιδιωτικότητα. Αυτό μπορεί να γίνει μέσα από την συγκατάθεση για τη συλλογή και την επεξεργασία των δεδομένων με ευκολότερο και πιο προσιτό τρόπο. Ακόμα μέσα από την χρήση των πληροφοριακών και επικοινωνιακών συστημάτων να δημιουργηθούν με τέτοιο τρόπο έτσι ώστε να παρέχεται η δυνατότητα στα άτομα πρόσβασης στα προσωπικά τους δεδομένα, καθώς στην ικανότητα στο χειρισμό των πληροφοριών αυτών όπως το ποιος τα συγκέντρωσε, τα τροποποίησε έχει γνώση για αυτά. Τεχνικές όπως η ανωνυμία ή η ψευδωνυμία μπορούν να υιοθετηθούν κατά τρόπο αποδεκτό αυτόν που προσφέρει τις υπηρεσίες, ώστε να διασφαλίζεται η πρόσβαση των χρηστών στις υπηρεσίες χωρίς να κινδυνεύει η ιδιωτικότητά τους.

Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας δημιουργήθηκαν με σκοπό να συμβάλουν και να ενισχύσουν την προστασία της ιδιωτικότητας στα σύγχρονα πληροφοριακά και επικοινωνιακά συστήματα, τα οποία υποστηρίζουν υπηρεσίες και υποδομές, θέτοντας άμυνες στη συλλογή προσωπικών δεδομένων ή εμποδίζοντας τη μη αναγκαία ή ανεπιθύμητη επεξεργασία τους, διατηρώντας ταυτόχρονα τη λειτουργικότητα των συστημάτων. Όμως σε πολλές περιπτώσεις η χρήση των τεχνολογιών ενίσχυσης της ιδιωτικότητας δεν είναι εφικτή είτε διότι περιορίζει την πρόσβαση στις υπηρεσίες και μειώνει την απόδοσή τους είτε διότι επαφίεται στον τελικό χρήστη των υπηρεσιών, ο οποίος δεν διαθέτει ιδικές γνώσεις που απαιτούνται για τον σκοπό αυτόν.

Προκειμένου να υποστηρίζουν το δικαίωμα της ιδιωτικότητας, οι τεχνολογίες ενίσχυσής της επιβάλλεται να συνυπολογιστεί στον σχεδιασμό και στην υλοποίηση των πληροφοριακών και επικοινωνιακών συστημάτων. Αν η εφαρμογή των τεχνολογιών απολέσει αποκλειστική ευθύνη των πολίτες, τότε είναι πιθανόν να βιώσουμε ένα «χάσμα προστασίας της ιδιωτικής ζωής» ανάμεσα σε αυτούς που έχουν την ικανότητα και τις γνώσεις να προστατέψουν την ιδιωτική τους ζωή και εκείνων που δεν την έχουν.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική

- Αλεξανδροπούλου – Αιγυπτιάδου Ε., (2007). "Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους", Εκδόσεις Αντ. Ν. Σάκκουλα.
- Αλεξανδρίδου(2004), Το δίκαιο του ηλεκτρονικού εμπορίου, Σακουλά, Αθηνα,2004,σελ.,185-186 και 193.
- Γκρίτζαλη Δ.,(2004), Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση, σε Σ. Κάτσικα/Δ. Γκρίτζαλη./Σ. Γκρίτζαλη (επιμ.), Ασφάλεια Πληροφοριακών Συστημάτων, Αθήνα 2004, σελ. 24 επ.
- Δόνος Π., Μήτρου Λ., Μίττλεττον Φ., Παπακωνσταντίνου Ευ.,(2002). Η Αρχή Προστασίας Προσωπικών Δεδομένων & η επαύξηση της προστασίας των δικαιωμάτων, Αθήνα-Θεσσαλονίκη 2002, σελ. 25.
- ΕΔΔΑ,(2008) I. κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008 και ΕΔΔΑ, K.U. κατά Φινλανδίας, προσφυγή αριθ. 2872/02, .2 Δεκεμβρίου 2008.
- ΕΔΔΑ, ***Von Hannover*** *κατά Γερμανίας* (προσφυγή αριθ. 2) [Τμήμα Ευρείας Σύνθεσης], προσφυγή αριθ. 40660/08 και 60641/08, 7 Φεβρουαρίου 2012. ΔΕΕ, DP (2013) Νομολογία.
- Ενδεικτικά ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, ***Volker und Markus Schecke GbR*** *και* ***Hartmut Eifert*** *κατά* ***Land Hessen***, 9 Νοεμβρίου 2010, σκέψη 48.
- Ευρωπαϊκή Επιτροπή (2012), COM(2012) 10 τελικό, Βρυξέλλες, 25 Ιανουαρίου 2012.
- Γκρίτζαλης Σ., Κάτσικας, Σ. & Γκρίτζαλης Δ., (2003). Ασφάλεις Δικτύων Υπολογιστών. 2003 ed. Αθήνα: Παπασωτηρίου.
- Ιγγλεζάκης, Ι., (2007). Εισαγωγή στο δίκαιο της πληροφορικής. 1 ed. Αθήνα: Σάκκουλα.
- Καίσης Κ.,(2002). Προστασία προσωπικών δεδομένων, Εκδόσεις Σακούλα, Αθήνα 2002.

- Καμπουράκης, Γ., ΓΚρίτζαλης, Σ. & Κάτσικας, Σ., 2006. *Ασφάλεια Ασυρμάτων και Κινητών Δικτών Επικοινωνιών*. 1 ed. Αθήνα : Παπασωτηρίου.
- Κάτσικας Σ., & Μήτρου Λ., (2002). Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων στο χώρο του Ηλεκτρονικού Επιχειρειν, 2ος Κύκλος Λειτουργίας ομάδα εργασίας Β1,
- Λαμπρινουδάκης, Κ., Γκρίτζαλης, Σ., Μήτρου, Λ. & Κάτσικας, Σ., 2010. Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών. 1 ed. Αθήνα: Παπασωτηρίου.
- Μήτρου, Λ., 2010. Η Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. Η νομική διάσταση. In: Κ. Λαμπρινουδάκης, ed. *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών*. Αθήνα: Παπασωτηρίου, pp. 505 - 552.
- Μπόζιος Ε.,(2004). Σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων, για τις διδακτικές ανάγκες του μαθήματος ασφάλεια πληροφοριακών συστημάτων, Α.Τ.Ε.Ι. Θεσσαλονίκης.
- Νόμος 2472/97, άρθρο 10, για την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, Οδηγίας 95/46/ΕΚ.
- Οργανισμός Ηνωμένων Εθνών (ΟΗΕ), Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα, 10 Δεκεμβρίου 1948.
- Παπαδημητρίου Γ.,(2004).Νέες τεχνολογίες και συνταγματικά δικαιώματα, Αθήνα-Θεσσαλονίκη 2004, σελ. 87.
- ΣτΕ, (1950).Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου, CETS αριθ. 005.
- ΣτΕ, Τροποποιήσεις της Σύμβασης (ETS αριθ. 108), και εγκρίθηκαν από την Επιτροπή Υπουργών στο Στρασβούργο στις 15 Ιουνίου 1999. Άρθρο 23 παράγραφος 2 της Σύμβασης 108 όπως τροποποιήθηκε
- ΣτΕ, Πρόσθετο πρωτόκολλο στη Σύμβαση για την προστασία του ατόμου, CETS αριθ. 181, 2001.
- Συνθήκης για την Ευρωπαϊκή Ένωση, Ευρωπαϊκές Κοινότητες (2012), ΕΕ 2012 C 326 και της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης, Ευρωπαϊκές Κοινότητες (2012), ΕΕ 2012 C 326.

Ξένη

- Auerbach N., (2004). Anonymous Digital Identity in e-Government, Zurich: University of Zurich.
- Bentham J.,(1995). The Panopticon Writings, Ed. Miran Bozovic (London: Verso, 1995), σελ. 29-95.
- Burr W. et al., (2011). Electronic Authentication Guidelines - Special Publication 800-63-1, Gaithersburg: NIST.
- Council of Europe, Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, T-PD Strasbourg 2005
- Evangelidis A., (2004). Frames- A Risk Assessment Framework for e-Services. Electronic Journal of e-Government, 2(1), pp. 21 - 30.
- Ferguson N. & Schneier B., (2003). Practical Cryptography. 1 ed. New York: John Wiley & Sons.
- Galegher, J., Sproull, L., & Kiesler, S. (1998). Legitimacy, authority and community in electronic support groups. Written Communication, 15, 493–530
- Gaskin V. (1989). Για την τελευταία απόφαση βλ. και σχόλια Ι. Σαρμά, Κράτος και Δικαιοσύνη Ι – Ελευθερία με υπεροχή του δικαίου, Αθήνα 2003, σελ. 102.
- Haibo H.,(2007). Smart Shopping Cart, I pledge my honor that I have abided by the Stevens Honor System.
- Hustinx P.,(2005) Public access to documents and data protection, Background Paper Series 1Ιούλιου July 2017, σελ. 15 επ.
- Jun S., Zhenfu C. & Rongxing L., (2006). An improved deniable authentication protocol. Networks, 48(4), p. 179 – 181.
- Laurie G.,(2002). Genetic Privacy – A challenge to Medico-Legal Norms, Cambridge 2002, σελ 83.
- Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. Communication Research, 33, 155–179
- NZ eGov, (2009). Online Authentication Threats and Attacks | ICT.govt.nz. [Online] Available.

- OECD, “Radio-Frequency Identification (RFID): A Focus on Information Security and Privacy”, Organisation for Economic Co-operation and Development (OECD), 2008,.
- Pfitzman, B. & Waidner M., (2003). Federated identity-management protocols. Cambridge, Springer – Verlag.
- Rosenberg R., (1992). The Social Impact of Computers, San Diego: Academic Press.
- RFID Journal, “Military's RFID Alternative: IPv6”, *RFID Journal*, 2003.
- Samuelson P.,(2000). Privacy as Intellectual Property? 52 Stanford Law Review (2000), σελ. 1142.
- Simitis H., Bundesdaten S.– Kommentar, Baden-Baden (2006), σελ. 136 επ.
- Solove D.,(2008). Understanding Privacy,Harvard University Press, σελ. 21.
- Solove D.J.,(2002). Digital dossiers and the dissipation of Fourth Amendment Privacy, Southern California Law Review, 75 (2002), σελ. 1084 επ.
- Tidwell, L. C., &Walther, J. B. (2002).Computer-mediated communication effects ondisclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. Human Communication Research, 28, 317–348.
- Tsohou, A., Kokolakis, S., Lambrinoudakis, C. & Gritzalis, S., (2010). Unifying ISO Security Standards Practices into a Single Security Framework. Port Elisabeth, Springer LNCS.
- York J. , Pendharkar P.C.(2004), "Human–computer interaction issues for mobile computing in a variable work context", Int. J. Human-Computer Studies 60 (2004) 771–797.
- Westin A. F., Privacy and Freedom, New York 1967, σελ. 7 επ.

Διαδικτυακές πήγες

- http://www.nytimes.com/2014/11/26/world/un-urges-protection-of-privacy-in-digital-era.html?ref=technology&_r=5 (Προσπελάστηκε στις 01.8.2017)
- http://www.pewinternet.org/2014/12/18/future-of-privacy/ (Προσπελάστηκε στις 25.08.2017)
- www.coe.int/t/ dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

- http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/authentication-key-strengths-standard/5-online-authenticati/ [Accessed 27 3 2017].
- http://www.lifo.gr/now/digital-life/58035 (Προσπελάστηκε στις 7.08.2017)
- http://www.olis.oecd.org/olis/2007doc.nsf/linkto/dsti-iccp-reg(2007)9-final
- http://www.rfidjournal.com/article/articleview/609/-1/1
- http//e-trial.blogspot.com
- https://safenet.gemalto.com/data-protection/password-protection-applications/?aldn-true