ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

Διατήρηση Δεδομένων Επικοινωνίας και Διασφάλιση του Απορρήτου και της Ιδιωτικότητας: Τεχνικά Και Νομικά Θέματα

Σπύρος Γιολδάσης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Νοέμβριος 2013

ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

Διατήρηση Δεδομένων Επικοινωνίας και Διασφάλιση του Απορρήτου και της Ιδιωτικότητας: Τεχνικά Και Νομικά Θέματα

Σπύρος Γιολδάσης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Νοέμβριος 2013

Περίληψη

Η Διατήρηση δεδομένων αποτελεί βασική και αναγκαία ενέργεια για την εύρυθμη λειτουργία των ηλεκτρονικών υπηρεσιών, όπως των υπηρεσιών τηλεπικοινωνίας, κοινωνικής δικτύωσης, ηλεκτρονικού εμπορίου και πολλών άλλων που παρέχονται τα τελευταία χρόνια στους καταναλωτές. Ωστόσο, αν και ο προφανής λόγος εφαρμογής της αφορά την ευκολότερη, ασφαλέστερη και γρηγορότερη εξυπηρέτηση τους, εγείρονται σημαντικά ζητήματα εξαιτίας περιπτώσεων όπου εφαρμόζεται καταχρηστικά, ξεπερνώντας τα όρια της ιδιωτικότητας των ατόμων και απειλώντας την ασφάλεια των πληροφοριών τους.

Η παρούσα Μεταπτυχιακή Διατριβή έχει ως στόχο να συνθέσει μια ολοκληρωμένη εικόνα για θέματα που αφορούν την Ιδιωτικότητα κατά την Διατήρηση των δεδομένων, αναλύοντας σχετικές έννοιες και δίνοντας έμφαση σε μηχανισμούς και θεσμούς ενίσχυσης της προστασίας της Ιδιωτικότητας.

Πρωταρχικά, επιχειρείται η ανάλυση της έννοιας της Ιδιωτικότητας, στην συνέχεια η κατηγοριοποίηση των δεδομένων που σχετίζονται με την Ιδιωτικότητα καθώς και μια πλήρης καταγραφή των εννοιών και των ενεργειών που περιλαμβάνει η διαδικασία της Διατήρησης των δεδομένων. Ακολούθως γίνεται μια κατηγοριοποίηση των τεχνολογιών προστασίας της Ιδιωτικότητας και για την κάθε κατηγορία παρουσιάζονται τα σημαντικότερα εργαλεία που χρησιμοποιούνται στις σύγχρονες υπηρεσίες ηλεκτρονικών επικοινωνιών. Τέλος καταγράφονται θεσμικά πλαίσια και νόμοι που προστατεύουν τα δεδομένα των χρηστών ανά τον κόσμο. Έμφαση δίνεται στην Ευρωπαϊκή νομοθεσία και το πως αυτή ενσωματώνεται στα Ελληνικά δεδομένα.

Summary

Data retention is an essential and necessary step for the proper functioning of electronic services, such as telecommunication services, social networking, e-commerce and many others which provided recent years to the consumers. Although the obvious reason of application is the easier, safer and faster service of consumers, some important questions raised because of situations where retention is improperly applied, surpassing the privacy limits of individuals and threatening the security of their information.

This work aims to compose a complete picture of issues regarding privacy during data retention, analyzing concepts and focusing on the mechanisms and institutions that strengthen the protection of privacy.

Primarily, an analysis of the privacy concept attempted, then a categorization of data related to privacy and a complete record of concepts and actions required during the data retention. Subsequently privacy technologies were categorized and for each category presented the most important tools used in modern electronic communications. Finally, the institutional frameworks and laws that protect user data around the world are recorded, emphasizing to the European legislation and how it is incorporated in Greece.

Ευχαριστίες

Θερμές ευχαριστίες εκφράζω στον υπεύθυνο και επιβλέποντα της εργασίας μου, κ. Στέφανο Γκρίτζαλη, για την πολύτιμη βοήθεια και καθοδήγηση που μου παρείχε καθ' όλη τη διάρκεια του μεταπτυχιακού προγράμματος, πρώτα στα μαθήματα της Ασφάλειας Πληροφοριακών Συστημάτων και μετέπειτα στην εκπόνηση της παρούσας Μεταπτυχιακής Διατριβής.

Επιπλέον, τις ευχαριστίες μου θα ήθελα να εκφράσω τόσο στο Ανοικτό Πανεπιστήμιο Κύπρου για την ποιότητα της εκπαίδευσης που μου παρείχε, όσο και στους καθηγητές τον οποίων παρακολούθησα τις διδασκαλίες τους.

Τέλος, θέλω να ευχαριστήσω την οικογένεια μου και τα προσφιλή μου πρόσωπα για τη στήριξη που μου προσέφεραν αλλά και για την κατανόηση που επέδειξαν καθ' όλη τη διάρκεια των σπουδών μου.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

« Όλα τα ανθρώπινα όντα έχουν τρεις ζωές: τη δημόσια, την ιδιωτική και τη μυστική»

Gabriel García Márquez

Η ιδιωτικότητα δεν αποτελεί ένα ζήτημα που ξαφνικά απασχόλησε την ανθρωπότητα με την «γέννηση» της ηλεκτρονικής πληροφορίας αλλά ανάγεται στις απαρχές της ανθρώπινης ιστορίας ως η προστασία έναντι σε οποιαδήποτε εξωτερική παρέμβαση, παρατήρηση, ή επιτήρηση της ανθρώπινης ύπαρξης και ζωής. Η έννοια της ωστόσο δεν ήταν ποτέ σταθερή αλλά είναι μια έννοια ασαφής που κανείς δεν μπορεί να περιγράψει με ακρίβεια την σημασία της.

Η προστασία της ιδιωτικής ζωής πάσχει από «μια αμηχανία των νοημάτων», κάτι που είναι ιδιαίτερα εμφανές σε περιπτώσεις αντικρουόμενων συμφερόντων, για παράδειγμα τα συμφέροντα μια κρατικής εξουσίας σχετικά με την αξία της ιδιωτικότητας μπορεί να είναι εκ διαμέτρου αντίθετα με τα συμφέροντα των πολιτών της, και για αυτό το λόγο ο προσδιορισμός της διαμορφώνεται κάθε φορά ανάλογα κοινωνικούς ή πολιτικούς παράγοντες οι οποίοι και τελικά καθορίζουν το τι είναι ιδιωτικό και τι δημόσιο.

1.1 Ορισμός της Ιδιωτικότητας [01]

Εξαιτίας της μεταβλητής έννοιας της ιδιωτικότητας (privacy), ο προσδιορισμός της φαίνεται αδύνατος, καταλήγοντας έτσι να είναι εύκολο κανείς να την επικαλεστεί και να την υπερασπιστεί, αλλά δύσκολο να την περιγράψει και ειδικότερα να την ορίσει. Άλλη μια δυσκολία στον προσδιορισμό της προκύπτει εκ του γεγονότος ότι η ιδιωτικότητα πρωτίστως είναι ελευθερία, πράγμα που σημαίνει ότι συναντά τα όριά της στην ιδιωτικότητα του άλλου. Ωστόσο με μια γενική περιγραφή ως ιδιωτικότητα θα ορίζαμε το δικαίωμα στην ιδιωτική ζωή, τον έλεγχο της προσβασιμότητας και της πρόσβασης σε ιδιωτικό χώρο, την περιορισμό των εξωτερικών "παρεμβάσεων", την προσδοκία της εχεμύθειας και το δικαίωμα στο απόρρητο και στην ανωνυμία. Πιο συγκεκριμένα η επικρατέστερη σήμερα έννοια της ιδιωτικότητας προσδιορίζεται ακριβώς ως «η αξίωση των ατόμων, των ομάδων και των θεσμών, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους». [Westin 1967]

ΕΙΚΟΝΑ 1.1: ΙΔΙΩΤΙΚΟΤΗΤΑ

1.2 Ιδιωτικότητα της πληροφορίας [01] [02]

Με την εξέλιξη των νέων τεχνολογιών και της δόμησης μιας Κοινωνίας της Πληροφορίας, γίνεται πλέον αντιληπτό ότι η ιδιωτικότητα σαν αξία επηρεάζεται άμεσα, καθώς οι μεταλλάξεις της

τεχνολογίας οδηγούν και σε μετάλλαξη της έννοιας της ιδιωτικότητας. Τα Πληροφοριακά Συστήματα δημιούργησαν μια νέα μορφή πληροφοριών και δεδομένων όπως και νέους τρόπους επεξεργασίας και συλλογής αυτών, με συνέπεια να απαιτείται πλέον η διεύρυνση και του προς προστασία αγαθού αλλά και του πλαισίου αντιμετώπισης των προσβολών της ιδιωτικότητας.

Οι νέες τεχνολογίες που αναπτύχθηκαν έδωσαν δυνατότητα καταχώρησης, διαμοιρασμού και επεξεργασίας, δεδομένων που αφορούν την επικοινωνία, την προσωπικότητα, και την καθημερινότητα των χρηστών και κατά συνέπεια την δυνατότητα διείσδυσης στην προσωπική τους ζωή. Όσο περισσότερο φαίνεται να αυξάνεται η ανάπτυξη και η χρήση των τεχνολογιών, αναλόγως αυξάνεται και ο βαθμός προσβολής της ιδιωτικότητας, με κίνδυνο την απώλεια του έλεγχου της προσωπικής πληροφορίας από το άτομο το οποίο το αφορά.

Εν κατακλείδι, η ουσία της ιδιωτικότητας δεν έχει αλλάξει, έχουν αλλάξει όμως οι τεχνικές δυνατότητες της διαχείρισής της όπως επίσης και της παραβίασής της, με αποτέλεσμα την εύκολη συλλογή της πληροφορίας, αλλά και την εξίσου εύκολη μεταβίβαση της στον χώρο σε ελάχιστο χρόνο, γεγονός που επιτρέπει τον συνδυασμό των πληροφοριών και τη εξαγωγή και δημιουργία νέων πληροφοριών για το άτομο.

1.3 Μορφές της Ιδιωτικότητας [03] [04]

Για την καλύτερη κατανόηση της έννοιας της Ιδιωτικότητας και κατ' επέκταση και καλύτερη αντιμετώπιση των παραβιάσεων αυτής, προέκυψε η ανάγκη ενός πλαισίου κατηγοριοποίησης της. Έτσι στα μέσα του 90' παρουσιάστηκε για πρώτη φορά από τον καθηγητή Roger Clarke ένα πλαίσιο στο οποίο αναγνωριζόταν διαφορετικές κατηγορίες Ιδιωτικότητας και ταυτόχρονα προτεινόμενοι τρόποι διαφύλαξης και προστασίας τους. Στην έρευνα του υποστηρίζει ότι η ιδιωτικότητα δεν μπορεί να θεωρείται απλό θέμα αλλά αντίθετα αποδεικνύεται ότι έχει πολλαπλές διαστάσεις και ως εκ τούτου προτείνει τον ακόλουθο διαχωρισμό σε τέσσερις διαφορετικούς τύπους ιδιωτικότητας:

1. **Ιδιωτικότητα του ατόμου**

   Η ιδιωτικότητα του ατόμου μερικές φορές αναφέρεται και ως «σωματική ιδιωτικότητα», αναφέρεται σε θέματα που αφορούν την ακεραιότητα του σώματος του ατόμου . Περιλαμβάνει θέματα όπως η υποχρεωτική ανοσοποίηση , η μετάγγιση αίματος χωρίς

συγκατάθεση, την υποχρεωτική παροχή των δειγμάτων των υγρών και των ιστών του σώματος, και την υποχρεωτική στείρωση.

2. **Ιδιωτικότητα της προσωπικής συμπεριφοράς**

   Αφορά όλες τις πτυχές της συμπεριφοράς του ατόμου, αλλά κυρίως ευαίσθητα θέματα, όπως τις σεξουαλικές προτιμήσεις και συνήθειες, τις πολιτικές δραστηριότητες και θρησκευτικές πρακτικές, τόσο σε ιδιωτικό όσο και σε δημόσιο χώρο.

3. **Ιδιωτικότητα των προσωπικών επικοινωνιών**

   Αφορά το δικαίωμα των ατόμων να είναι σε θέση να επικοινωνούν μεταξύ τους, χρησιμοποιώντας διάφορα μέσα επικοινωνίας, χωρίς τον κίνδυνο της παρακολούθησης των επικοινωνιών τους από άλλα πρόσωπα ή οργανισμούς.

4. **Ιδιωτικότητα των προσωπικών δεδομένων**

   Αφορά το δικαίωμα των ατόμων να ελέγχουν ότι τα προσωπικά τους στοιχεία, δεν θα είναι αυτόματα διαθέσιμα σε άλλους, είτε ιδιώτες, είτε οργανισμούς, και ότι, ακόμη και όταν τα δεδομένα διαχειρίζονται από ένα άλλο οργανισμό, τα άτομα πρέπει να είναι σε θέση να ασκούν ένα σημαντικό βαθμό ελέγχου για τον τρόπο που αυτά τα στοιχεία χρησιμοποιούνται.

Ωστόσο οι πρόσφατες τεχνολογικές εξελίξεις έχουν αναδείξει ότι ο παραπάνω διαχωρισμός δεν είναι πλέον επαρκής για να καλύψει το εύρος των πιθανών ζητημάτων που αφορούν την προστασία της ιδιωτικής ζωής.

Για παράδειγμα, τεχνολογίες όπως οι σαρωτές απεικόνισης σώματος, η τεχνολογία RFID (Radio Frequency Identification), τα μη επανδρωμένα εναέρια οχήματα, οι τεχνολογίες της αλληλουχίας του DNA δεύτερης γενιάς, οι τεχνολογίες ανθρώπινης βελτίωσης και χρήσης βιομετρικών δεύτερης γενιάς κ.α., εγείρουν την ανάγκη για πρόσθετα ζητήματα προστασίας της ιδιωτικής ζωής, και συνεπώς καθιστούν απαραίτητη την επέκταση των τεσσάρων κατηγοριών διαχωρισμού της ιδιωτικότητας.

Μια πιο πρόσφατη έρευνα, που παρουσιάστηκε τον Ιανουάριο του 2013 από τους Rachel Finn David Wright και Michael Friedewald[04], επιχειρεί τον διαχωρισμό της ιδιωτικότητας βασισμένη στις πιο πρόσφατες τεχνολογικές εξελίξεις και προτείνει πλέον εφτά κατηγορίες:

1. **Ιδιωτικότητα του ατόμου**

Περιλαμβάνει το δικαίωμα του ατόμου να προστατεύει τις λειτουργίες και τα χαρακτηριστικά του σώματος του. Η βασική ιδέα δεν διαφέρει από την αντίστοιχη κατηγορία της κατηγοριοποίησης του Clark, πάρα μόνο ότι στα υπό προστασία αγαθά εμπίπτουν και στοιχεία που προέκυψαν από πρόσφατες τεχνολογικές ή επιστημονικές εξελίξεις (όπως στοιχεία DNA, βιομετρικά στοιχεία κ.α.). Η προστασία τέτοιου είδους στοιχείων είναι βέβαιο ότι αυξάνει την αίσθηση της ελευθερίας του ατόμου και βοηθά στην υποστήριξη μιας υγιούς και καλά δομημένης κοινωνίας.

2. **Ιδιωτικότητα της προσωπικής συμπεριφοράς και δράσης**

Αυτή η κατηγορία περιλαμβάνει ευαίσθητα θέματα, όπως τις σεξουαλικές προτιμήσεις και συνήθειες του ατόμου, τις πολιτικές του δραστηριότητες και θρησκευτικές του πεποιθήσεις. Αφορά την δυνατότητα του ατόμου να συμπεριφέρεται στον δημόσιο, ημι-δημόσιο ή ιδιωτικό χώρο του, χωρίς οι ενέργειες του να παρακολουθούνται ή να ελέγχονται από άλλους. Η προστασία αυτού του τύπου της ιδιωτικότητας συμβάλλει στην εξέλιξη και την άσκηση της αυτονομίας και την ελευθερία της σκέψης και της δράσης.

3. **Ιδιωτικότητα της επικοινωνίας**

Έχει ως στόχο να αποφευχθεί η υποκλοπή δεδομένων επικοινωνίας με τη χρήση μέσων όπως την υποκλοπή ταχυδρομείου, τη χρήση κοριών ή μικρόφωνων, την υποκλοπή τηλεφωνικών ή ασύρματων επικοινωνιών και την πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου. Αυτή η πτυχή της ιδιωτικής ζωής ωφελεί τα άτομα και την κοινωνία, διότι επιτρέπει και ενθαρρύνει την ελεύθερη συζήτηση ενός ευρέου φάσματος απόψεων και επιλογών, και επιτρέπει την ανάπτυξη στον τομέα των επικοινωνιών.

4. **Ιδιωτικότητα των προσωπικών δεδομένων**

Για την εφαρμογή της στις σύγχρονες τεχνολογίες περιλαμβάνει και την προστασία εικόνων που αφορούν το άτομο και ως εκ τούτου αποτελούν και αυτές προσωπικά δεδομένα. Η προστασία δεδομένων και εικόνας αφορά τη διασφάλιση ότι τα δεδομένα των ατόμων δεν θα είναι αυτόματα διαθέσιμα σε άλλα άτομα ή οργανισμούς και ότι τα

άτομα θα μπορούν να έχουν σημαντικό βαθμό ελέγχου επί αυτών των στοιχείων και της χρήσης τους. Αυτός ο έλεγχος επί των προσωπικών δεδομένων ενισχύει την αυτοπεποίθηση των ατόμων και τους επιτρέπει να νιώθουν ότι έχουν την εξουσία των προσωπικών τους στοιχείων. Έτσι επέρχεται η ισορροπία μεταξύ της εξουσίας του κράτους και του ατόμου.

5. Ιδιωτικότητα των σκέψεων και των συναισθημάτων

Αυτή η πτυχή της ιδιωτικής ζωής μπορεί να είναι υπό απειλή, ως άμεσο αποτέλεσμα των νέων και αναδυόμενων τεχνολογιών. Διακρίνεται από την ιδιωτικότητα του ατόμου, με τον ίδιο τρόπο που το μυαλό μπορεί να διακριθεί από το σώμα. Αφορά το δικαίωμα των ατόμων να μοιράζονται ή όχι, τις σκέψεις και τα συναισθήματά τους, όποτε και όπου αυτοί θέλουν. Αυτή η δημιουργική ελευθερία ωφελεί την κοινωνία , επειδή σχετίζεται με την ισορροπία εξουσίας μεταξύ του κράτους και του ατόμου.

6. Ιδιωτικότητα της τοποθεσίας και του χώρου

Τα άτομα έχουν το δικαίωμα να μετακινούνται σε δημόσιο ή ημι-δημόσιο χώρο, χωρίς να μπορούν να ταυτοποιηθούν, να παρακολουθηθούν, να εντοπιστούν ή να ελέγχονται. Αυτή η μορφή της ιδιωτικότητας περιλαμβάνει επίσης το δικαίωμα στην απομόνωση και το δικαίωμα της ιδιωτικότητας σε χώρους όπως η οικία, το αυτοκίνητο ή το γραφείο εργασίας. Μια τέτοια αντίληψη της ιδιωτικής ζωής έχει κοινωνική αξία . Όταν οι πολίτες είναι ελεύθεροι να κινούνται σε δημόσιο χώρο, χωρίς το φόβο της αναγνώρισης, της παρακολούθησης ή της ανίχνευσης, βιώνουν μια αίσθηση δημοκρατίας και ελευθερίας. Και τα δύο αυτά υποκειμενικά αισθήματα συμβάλουν σε μια υγιή, καλά δομημένη δημοκρατική κοινωνία. Αυτή η κατηγορία της ιδιωτικής ζωής δεν ήταν τόσο προφανής όταν έγινε η πρώτη κατηγοριοποίηση από τον Clarke, ωστόσο έγινε εμφανής με τις απειλές της κατά ιδιωτικότητας που έφερε η τεχνολογική πρόοδος.

7. Ιδιωτικότητα του συνεταιρίζεσθαι

Αφορά το δικαίωμα του ατόμου να συσχετίζεται με οποιονδήποτε επιθυμεί χωρίς να ελέγχεται. Αποτελεί αναγκαίο δικαίωμα των ανθρώπων μιας δημοκρατικής κοινωνίας καθώς ενισχύει και προωθεί την ελευθερία του λόγου, συμπεριλαμβανομένου του πολιτικού λόγου, την ελευθερία της λατρείας και άλλες μορφές σχέσεων. Η κοινωνία

ωφελείται από αυτή την πτυχή της ιδιωτικότητας καθώς ενισχύει μια ευρεία ποικιλία ομάδων ανθρώπων, πράγμα που μπορεί να βοηθήσει να διασφαλιστεί ότι οι περιθωριοποιημένες φωνές θα ακούγονται, και θα μπορούν να πιέσουν για πολιτικές και οικονομικές αλλαγές.

1.4 Προκλήσεις για την Ιδιωτικότητα [05]

Ολοκληρώνοντας την ανάλυση εννοιών περί ιδιωτικότητας δεν δύναται να παραληφθούν οι προκλήσεις που υπάρχουν, ή και συνεχίζουν να δημιουργούνται λόγω των τεχνολογικών εξελίξεων, οι οποίες φαίνονται να απειλούν την ιδιωτικότητα των ατόμων. Κατανοώντας τις προηγούμενες έννοιες εύλογα δημιουργούνται ερωτήματα όπως «Ποιες είναι οι απειλές κατά τις Ιδιωτικότητας;» και «με ποια μορφή αυτές μπορούν να διαταράξουν την Ιδιωτικότητα ενός ατόμου;». Για τα παραπάνω ερωτήματα επιχειρείται μία κατηγοριοποίηση των προκλήσεων κατά της Ιδιωτικότητας.

1.4.1 Συλλογή Δεδομένων

Κατά την συλλογή πληροφορίας (Information Collection) μπορεί να δημιουργηθούν προβλήματα που θα εμπίπτουν στην παραβίαση της ιδιωτικότητας, και θα οφείλονται στον τρόπο ή την διαδικασία της συλλογής δεδομένων. Ακόμη και αν καμιά πληροφορία δεν αποκαλύπτεται δημόσια, η συλλογή των δεδομένων μπορεί να έχει επιβλαβείς συνέπειες. Οι κίνδυνοι κατά την συλλογή πληροφοριών διακρίνονται σε δύο μορφές:

1. **Παρακολούθηση (Surveillance)**

   Η παρακολούθηση της κίνησης ή της συμπεριφοράς ενός ατόμου δεν είναι απαραίτητα κάτι το επιζήμιο και μερικές φορές ίσως να είναι και αναπόφευκτο. Για παράδειγμα, οποιοσδήποτε μπορεί να έρθει σε μια τέτοια θέση από την στιγμή που θα κυκλοφορήσει και θα συναναστραφεί με άλλα άτομα, σε δημόσιο χώρο. Ωστόσο όταν η παρακολούθηση αυτή γίνεται συστηματική ή επίμονη αυτόματα προκαλεί αλλαγή συναισθημάτων και συμπεριφοράς στο άτομο το οποίο παρακολουθείται. Ακριβώς για αυτό τον λόγο, η παρακολούθηση μπορεί να χρησιμοποιηθεί ως εργαλείο ελέγχου της συμπεριφοράς των ατόμων, κάτι που ασφαλώς έχει και θετικές προεκτάσεις καθώς ενισχύει του κανόνες

δικαίου που διέπουν μια δημοκρατική κοινωνία ή και προλαμβάνει πιθανές εγκληματικές ενέργειες.

Ωστόσο τι γίνεται όταν το συγκεκριμένο εργαλείο χρησιμοποιείται ανεξέλεγκτα και για διαφορετικούς σκοπούς; Μπορούμε σε τέτοιες περιπτώσεις να μιλάμε για ελευθερία των ατόμων; Για παράδειγμα, ακόμα και αν ένα άτομο δεν έχει απαραίτητα διαπράξει κάποιο ποινικό αδίκημα, η συσχέτιση των πληροφοριών κίνησης και συμπεριφοράς του μπορεί να οδηγήσει σε συμπεράσματα που θα επηρεάσουν την κοινωνική του θέση. Ως εκ τούτου η συλλογή πληροφοριών μέσω της παρακολούθησης αποτελεί μια πρόκληση για την Ιδιωτικότητα καθώς η διάκριση μεταξύ θετικών και αρνητικών συνεπειών είναι συχνά ασαφής.

2. **Ανάκριση (Interrogation)**

Η συλλογή δεδομένων με την μορφή της ανάκρισης οδηγεί σε συμπεράσματα που δημιουργούν το πλήρες προφίλ ενός ατόμου. Μπορεί να οδηγήσει ακόμα σε συμπεράσματα που να ερμηνεύονται διαφορετικά ή και κατά την κρίση του «ανακριτή». Φυσικά μια τέτοια διαδικασία συλλογής πληροφοριών, και ειδικότερα σε ότι αφορά τον χώρο του Διαδικτύου, δεν γίνεται πάντα μέσω εξαναγκασμού του ατόμου. Συχνά το άτομο υποπίπτει στο λάθος να δίνει πληροφορίες, στις οποίες φυσιολογικά δεν θα απαντούσε, λόγω της ανησυχίας του μήπως παρεξηγηθεί ή μήπως θεωρηθεί λανθασμένη η άρνηση του.

1.4.2 Επεξεργασία της Πληροφορίας

Η επεξεργασία της Πληροφορίας (Information Processing) αναφέρεται στη χρήση, την αποθήκευση και το χειρισμό των δεδομένων που έχουν συλλεχθεί. Διαφέρει από τη συλλογή της Πληροφορίας επειδή τα πιθανά προβλήματα εμφανίζονται μετά την ενοποίηση των δεδομένων και κατά την διαχείριση αυτών, και όχι λόγω των μέσων με τα οποία συγκεντρώνονται. Η επεξεργασία πληροφοριών δεν περιλαμβάνει τη συλλογή των δεδομένων αλλά την διαδικασία με την οποία τα ήδη συλλεχθέντα δεδομένα αντιμετωπίζονται, δηλαδή τους διάφορους τρόπους σύνδεσης δεδομένων μεταξύ τους αλλά και σύνδεσή τους με τους ανθρώπους, στους οποίους αφορούν. Διακρίνονται πέντε προκλήσεις κατά την επεξεργασία της Πληροφορίας:

1. **Συνάθροιση Δεδομένων (Aggregation)**

Η ιδιωτικότητα διαταράσσεται από την συλλογή μεγάλου όγκου Δεδομένων, η οποία επιτρέπει την παρακολούθηση σε μαζική κλίμακα μέσω της συνάθροισης των δεδομένων που αφορούν ένα πρόσωπο. Μπορεί η ύπαρξη δεδομένων διαφορετικού τύπου και σε διαφορετικά σημεία να μην αποκαλύπτει κάτι για ένα άτομο, εντούτοις η δυνατότητα συλλογής και συνυπολογισμού αυτών των πληροφοριών μπορεί να αποκαλύψει στοιχεία για το εν λόγω άτομο, με άμεσο αποτέλεσμα την παραβίαση της ιδιωτικότητας του. Αυτό συμβαίνει καθώς ο συνδυασμός των μεμονωμένων πληροφοριών μπορεί να οδηγήσει στην εξαγωγή ενός πλήρους προφίλ για ένα άτομο. Η παραβίαση έγκειται στο γεγονός ότι ενώ ο χρήστης γνωρίζει και έχει συγκαταθέσει για την συλλογή δεδομένων, συνήθως αγνοεί ότι αυτά μπορεί να χρησιμοποιηθούν συνδυαστικά για την εξαγωγή περισσότερων πληροφοριών για αυτόν.

Η συνάθροιση των πληροφοριών σίγουρα δεν αποτελεί μια καινούρια δραστηριότητα, καθώς πάντα ήταν δυνατό να συνδυαστούν διαφορετικά κομμάτια προσωπικών πληροφοριών, ώστε να εξαχθεί μια καινούρια πληροφορία σχετικά με ένα πρόσωπο. Αλλά η εξουσία και το πεδίο εφαρμογής της συνάθροισης είναι διαφορετικά στην εποχή της πληροφορίας. Τα στοιχεία που συγκεντρώνονται για τους ανθρώπους είναι σημαντικά πιο εκτεταμένα, η διαδικασία συνδυασμού είναι πολύ πιο εύκολη και οι τεχνολογίες ανάλυσης τους είναι πιο εξελιγμένες και ισχυρές.

Ο συνδυασμός των δεδομένων και η ανάλυση τους σαφώς έχει και επωφελείς χρήσεις. Σε πολλά ηλεκτρονικά καταστήματα για παράδειγμα, χρησιμοποιούνται συγκεντρωτικά δεδομένα για τις αγορές ενός ατόμου, ώστε να είναι σε θέση το κατάστημα να συστήσει άλλα προϊόντα που θα εμπίπτουν στα ενδιαφέροντα του πελάτη. Παρόμοια επίσης, εφαρμόζεται και η αξιολόγηση καταστημάτων-πωλητών σε ιστοχώρους όπως το Amazon ή το Ebay, όπου η συγκέντρωση δεδομένων αξιολόγησης από πελάτες οδηγεί σε ένα προφίλ αξιολόγησης του εκάστοτε πωλητή.

Παράλληλα με τα οφέλη όμως, η συνάθροιση δεδομένων μπορεί να επιφέρει επιβλαβείς συνέπειες καθώς μπορεί να ξεπερνά τα όρια που θέτουν τα άτομα σχετικά με το τι μπορεί να είναι γνωστό για αυτούς. Ο συνδυασμός δεδομένων περιλαμβάνει απρόβλεπτους τρόπους για να αποκαλύψει στοιχεία σχετικά με ένα πρόσωπο που δεν είναι άμεσα γνωστά. Οι άνθρωποι δίνουν τα κομμάτια των πληροφοριών σε διαφορετικά περιβάλλοντα, αποκαλύπτοντας μόνο ένα μικρό μέρος από τον εαυτό τους σε κάθε περίπτωση, έχοντας την

προσδοκία ότι αποκαλύπτουν σχετικά λίγα για τον εαυτό τους. Όταν αυτά τα κομμάτια όμως ενοποιούνται, ο εκάστοτε συλλέκτης τους αποκτά πολύ μεγαλύτερη γνώση για τη ζωή του ατόμου.

2. Προσδιορισμός (Identification)

Ο προσδιορισμός ή ταυτοποίηση αφορά την σύνδεση πληροφοριών με ένα συγκεκριμένο άτομο. Επιτρέπει την εξακρίβωση της ταυτότητάς ενός άτομου που είναι κάτοχος ενός λογαριασμού και επιβεβαιώνει την πρόσβαση σε αυτόν. Η ταυτοποίηση είναι παρόμοια με τη συσσώρευση καθώς και οι δύο αφορούν τον συνδυασμό των διαφόρων πληροφοριών ενός ατόμου, ωστόσο, διαφέρει στο γεγονός ότι η ταυτοποίηση συνεπάγεται μια σύνδεση με το φυσικό πρόσωπο.

Η ταυτοποίηση έχει πολλά οφέλη, όπως η μείωση την εξαπάτησης και η ενίσχυση της ανάληψης ευθύνης, καθώς οποιαδήποτε πρόσβαση σε έναν λογαριασμό συνεπάγεται και την επαλήθευση της ταυτότητας των ατόμων. Για παράδειγμα μπορεί να αποτρέψει παραπλανητικές πολιτικές διαφήμισης ή και να βοηθήσει στην ανακάλυψη παράνομων ενεργειών.

Παρόλα αυτά η ταυτοποίηση της ταυτότητας του ατόμου αποτελεί απειλή κατά της ιδιωτικότητας καθώς στέκεται εμπόδιο στην ανωνυμία των ατόμων. Ως συνέπεια έχουμε τον περιορισμό κάποιων ελευθεριών αλλά και την δυνατότητα των κυβερνήσεων να ασκούν μεγαλύτερο έλεγχο στους πολίτες τους.

3. Ανασφάλεια (Insecurity)

Η έλλειψη ασφάλειας που πιθανότατα να εμφανίζεται στα συστήματα αποτελεί μία από τις μεγαλύτερες απειλές για την ιδιωτικότητα, καθώς οι συνέπειες της μπορεί να είναι καταστροφικές για ένα άτομο. Δυσλειτουργίες, κενά ασφαλείας, καταχρήσεις, και η παράνομη χρήση των προσωπικών πληροφοριών εμπίπτουν στην κατηγορία αυτή. Η ανασφάλεια, με λίγα λόγια, είναι ένα πρόβλημα που προκαλείται από λανθασμένη χρήση, αντιμετώπιση και προστασία των πληροφοριών μας.

Ένα παράδειγμα αποτελεί η κλοπή ταυτότητας που είναι από τα ταχύτερα αναπτυσσόμενα οικονομικά εγκλήματα (white collar crime). Ένας κλέφτης ταυτότητας ανοίγει λογαριασμούς και διενεργεί την απάτη στο όνομα του θύματος. Το θύμα ακόμα και όταν θα δικαιωθεί θα έχει υποστεί τεράστια οικονομικά και κοινωνικά προβλήματα. Άλλη μια περίπτωση αντίστοιχων επιβλαβών συνεπειών που μπορεί να επιφέρει η έλλειψη ασφάλειας των συστημάτων αποτελεί η παραμόρφωση των προσωπικών δεδομένων.

Παρόλη την επικινδυνότητα της συγκεκριμένης μορφής πρόκλησης της ιδιωτικότητας και την τεχνολογική εξέλιξη των συστημάτων ασφαλείας, ακόμα και σήμερα η κλοπή ταυτότητας θεωρείται ένα πολύ «εύκολο έγκλημα» με ιδιαίτερες δυσκολίες στην καταπολέμηση του και ως εκ τούτου ένα από τα πιο διαδεδομένα. Η αντιμετώπιση του ωστόσο φαίνεται να είναι περισσότερο θέμα πολιτικής για την ορθή χρήση των δεδομένων που συλλέγονται παρά διασφάλισης της ακεραιότητας των δεδομένων.

4. Δευτερεύουσα χρήση (Secondary Use)

Δευτερεύουσα χρήση, είναι η χρήση των δεδομένων για σκοπούς άσχετους με τους σκοπούς για τους οποίους τα δεδομένα αρχικά συλλέχθηκαν και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων. Σίγουρα υπάρχουν πολλές επιθυμητές περιπτώσεις δευτερεύουσας χρήσης των συλλεχθέντων δεδομένων, όπως η αποτροπή ενός εγκλήματος ή η διάσωση μιας ζωής. Η ποικιλία των πιθανών δευτερευουσών χρήσεων των δεδομένων είναι σχεδόν ανεξάντλητη και κυμαίνονται από καλοήθεις σε κακοήθεις.

Προβλήματα που επέρχονται από κακοήθεις χρήσεις των δεδομένων περιλαμβάνουν την αποστολή ενοχλητικών αυτόκλητων μηνυμάτων και την διακίνηση στοχευμένης διαφήμισης με τελικό αποτέλεσμα την απώλεια της αξιοπιστίας και εμπιστοσύνης των χρηστών απέναντι στα συστήματα, απόρροια της ευπάθειας και της αδυναμίας που πιθανότατα αισθάνονται.

5. Αποκλεισμός (Exclusion)

Πρόκειται για την περίπτωση όπου τα συστήματα αποτυγχάνουν ή αποφεύγουν να παρέχουν στους χρήστες τους πληροφορίες και ειδοποιήσεις για την χρήση των αρχείων τους. Αιτίες που δικαιολογούν αυτό τον αποκλεισμό φαίνεται να είναι το υψηλό κόστος που κάποιες φορές απαιτείται για την υλοποίηση τέτοιων λειτουργιών ή και η πιθανή ανάγκη

χρήσης αυτών των πληροφοριών στη πρωτότυπη μορφή τους σε περιπτώσεις ατόμων τα οποία μπορεί να τελούν υπό διερεύνηση για μη σύννομες πράξεις.

Για να περιοριστεί ο αποκλεισμός των ατόμων από τα στοιχεία τους οφείλεται να τηρούνται τρείς βασικές αρχές: (1) Η ύπαρξη των συστημάτων καταγραφής δεν μπορεί να κρατηθεί μυστική, (2) ένα άτομο πρέπει να είναι σε θέση να γνωρίζει τι πληροφορίες γι' αυτόν διατηρούνται σε ένα αρχείο αλλά και πώς αυτές χρησιμοποιούνται και (3) ένα άτομο πρέπει να είναι σε θέση να διορθώσει ή να τροποποιήσει μια καταγραφή των αναγνωρίσιμων πληροφοριών γι 'αυτό. Μαζί αυτές οι αρχές αποσκοπούν στο να επιτρέπουν στα άτομα να έχουν κάποια γνώση και συνεισφορά στα αρχεία που διατηρούνται γι' αυτούς από κρατικούς φορείς και από επιχειρήσεις.

Ποια τα προβλήματα ή οι βλάβες που προκαλούνται, όταν οι άνθρωποι δεν είναι ενημερωμένοι σχετικά με τις πληροφορίες που διατηρούνται γι 'αυτούς; Ο αποκλεισμός μειώνει την υποχρέωση λογοδοσίας εκ μέρους των κρατικών υπηρεσιών και των επιχειρήσεων που διατηρούν αρχεία σχετικά με τα άτομα . Ο αποκλεισμός σχετίζεται επίσης με την έλλειψη ασφάλειας στα συστήματα καταγραφής των προσωπικών δεδομένων. Επίσης η αδυναμία των ατόμων να συμμετάσχουν στην συντήρηση και χρήση των πληροφοριών που τα αφορούν μπορεί να οδηγήσει σε αισθήματα ανικανότητας και απογοήτευσης καθώς, σε μια κοινωνία όπου οι προσωπικές πληροφορίες χρησιμοποιούνται όλο και περισσότερο για να ληφθούν σημαντικές αποφάσεις για τη ζωή μας, η αδυναμία ελέγχου μπορεί να είναι σημαντικά ενοχλητική και επιβλαβής.

1.4.3 Διάδοση της Πληροφορίας

Η διάδοση των πληροφοριών (Information Dissemination) συμπεριλαμβανομένων των τρόπων με τους οποίους αυτή συντελείται, αποτελεί μια από τις ευρύτερες κατηγορίες απειλών για την παραβίαση της ιδιωτικής ζωής και του απόρρητου των προσωπικών δεδομένων. Οι κίνδυνοι κατά την διάδοση της πληροφορίας συνεπάγονται την αποκάλυψη προσωπικών δεδομένων ή την ανεξέλεγκτη διασπορά πληροφοριών. Περιλαμβάνονται πέντε κατηγορίες κινδύνων κατά την Διάδοση της Πληροφορίας:

1. Παραβίαση της Εμπιστευτικότητας (Breach of Confidentiality)

Η περίπτωση κατά την οποία παραβιάζονται ή αποκαλύπτονται τα δεδομένα «εμπιστοσύνης» δηλαδή δεδομένα που διαβιβαστήκαν σε τρίτους οι οποίοι έχουν σχέση εμπιστοσύνης με τους κατόχους των δεδομένων. Σε αυτές τις περιπτώσεις ανήκουν ως επί το πλείστον ιατρικές, νομικές, οικονομικές πληροφορίες που συναλλάσσονται μεταξύ του κατόχου των δεδομένων και του εκάστοτε επαγγελματία.

Η παραβίαση της εμπιστευτικότητας εκτός ότι αποτελεί από μόνο του ένα γεγονός επιβλαβές καθώς συνεπάγεται την αποκάλυψη πληροφοριών χωρίς την συναίνεση του κατόχου τους, επιπλέον αποτελεί κίνδυνο για την σχέση των επαγγελματιών και των πελατών τους. Για παράδειγμα, μπορούμε να φανταστούμε ότι η σχέση εμπιστοσύνης μεταξύ γιατρού και ασθενούς θα ήταν ανύπαρκτη αν δεν υπήρχε νομικό πλαίσιο που να ενισχύει το απόρρητο των μεταξύ τους συναλλασσόμενων πληροφοριών.

Στην εποχή της πληροφορίας η διαβίβαση δεδομένων σε τρίτους είναι πλέον μια συνηθισμένη ενέργεια. Κάθε χρήστης του Διαδικτύου δύναται να εμπιστεύεται πληροφορίες του σε τρίτους, οι οποίοι οφείλουν να αναπτύσσουν ένα πλαίσιο προστασίας των πληροφοριών που διαχειρίζονται αλλά και ενημέρωσης των χρηστών για τον τρόπο διαχείρισης.

2. Αποκάλυψη (Disclosure)

Το δικαίωμα στην ιδιωτικότητα ουσιαστικά βασίζεται στην ατομική επιθυμία της μη αποκάλυψης προσωπικών πληροφοριών. Η "Αποκάλυψη" πληροφοριών εντοπίζεται σε περιπτώσεις όπου ορισμένες αληθείς πληροφορίες για ένα άτομο αποκαλύπτονται σε άλλους. Διαφέρει από την παραβίαση της Εμπιστευτικότητας, επειδή η βλάβη που συνεπάγεται η αποκάλυψη, αφορά την φήμη του ατόμου το οποίο αντιπροσωπεύουν οι πληροφορίες που αποκαλύφθηκαν και διαδόθηκαν, ενώ η ζημιά με την παραβίαση της Εμπιστευτικότητας αφορά την παραβίαση και ρήξη μιας σχέσης εμπιστοσύνης.

Οι συνέπειες της αποκάλυψης πληροφοριών ενέχουν κινδύνους όπως ο περιορισμός της ελεύθερης έκφρασης, η καταπάτηση του δικαιώματος στην ανωνυμία, απειλές κατά της ασφάλειας, παρεμπόδιση της ατομικής εξέλιξης και ανάπτυξης και παραμόρφωση του ατομικού προφίλ. Ο περιορισμός λοιπόν της αλόγιστης αποκάλυψης πληροφοριών για ένα

άτομο όχι μόνο δεν περιορίζει την ελευθερία λόγου και έκφρασης, αντίθετα μπορεί να την ενισχύσει.

3. Έκθεση (Exposure)

Η συγκεκριμένη κατηγορία περιλαμβάνει την έκθεση σε άλλους, ορισμένων σωματικών και συναισθηματικών χαρακτηριστικών για ένα πρόσωπο. Αυτά είναι τα χαρακτηριστικά που οι άνθρωποι αντιλαμβάνονται ως βαθιά αρχέγονα, και η έκθεσή τους συχνά δημιουργεί αμηχανία, ντροπή και ταπείνωση. Χαρακτηριστικά όπως θλίψη, πόνος, τραύμα, γύμνια, σεξ, ούρηση, αφόδευση και όλα όσα περιλαμβάνουν αρχέγονες πτυχές της ζωής μας τις οποίες στην εξέλιξη της κοινωνικοποίησης μας κρατήσαμε κρυφές, ωστόσο αποτελούν ενστικτώδεις, φυσικές και αναγκαίες λειτουργίες.

Η Έκθεση είναι παρόμοια με την Αποκάλυψη των πληροφοριών, τόσο στον τρόπο αποκάλυψης και διάδοσης αυτών, όσο και στο γεγονός ότι πρόκειται για πραγματικές πληροφορίες. Ωστόσο έχουν μια μεγάλη διαφορά καθώς η έκθεση πληροφοριών για ένα άτομο δεν μπορεί να διαμορφώσει ένα κοινωνικό προφίλ για αυτό, όπως δηλαδή θα συνέβαινε στην περίπτωση της αποκάλυψης. Αυτό συμβαίνει λόγω της φύσης των πληροφοριών που αποκαλύπτονται οι οποίες αφορούν χαρακτηριστικά ή λειτουργίες, κοινές για όλους τους ανθρώπους.

Ως εκ τούτου, η φύση των πληροφοριών που αποκαλύπτονται και σχετίζονται με την Έκθεση δεν συνεπάγεται κινδύνους ή ζημιές στρέβλωσης του κοινωνικού προφίλ του άτομου το οποίο αφορούν. Παρόλα αυτά οι συνέπειες είναι εξίσου ζημιογόνες καθώς το άτομο το οποίο εκτίθεται βιώνει συναισθήματα ντροπής και ταπείνωσης που επηρεάζουν την μετέπειτα πορεία της ζωής του. Για παράδειγμα, από την διάρρευση οπτικού υλικού ενός ατόμου σε πολύ ιδιαίτερες προσωπικές στιγμές, σίγουρα δεν μπορεί να εξαχθεί κανένα συμπέρασμα σχετικά με τον χαρακτήρα του, όμως οι συνέπειες θα είναι καταστροφικές για αυτό.

4. Αυξημένη προσβασιμότητα (Increased Accessibility)

Η κατηγορία αυτή αφορά την αμεσότητα και την ευκολία με την οποία μπορεί κάποιος να έχει πρόσβαση σε πληροφορίες ενός προσώπου ή οργανισμού. Πληροφορίες οι οποίες όμως

ούτως ή άλλως θα κατέληγαν σε δημοσιοποίηση. Παράδειγμα αποτελεί η ανάρτηση πληροφοριών σε κυβερνητικές σελίδες για την ανάληψη ενός δημοσίου έργου ή για τις κυρώσεις που μπορεί να επιβλήθηκαν σε ένα κατάστημα υγειονομικού ενδιαφέροντος.

Αν και ο τελικός σκοπός της αυξημένης προσβασιμότητας, είναι, εκμεταλλευόμενη την σημερινή τεχνολογία, να ενισχύσει την διαφάνεια, να μειώσει την γραφειοκρατία και να διευκολύνει διάφορες ενέργειες των πολιτών, δεν μπορούμε να παραβλέψουμε το γεγονός πως εμπεριέχονται κίνδυνοι από την ταχύτητα και την αμεσότητα της πρόσβασης στις πληροφορίες. Για παράδειγμα, εταιρείες μπορούν να έχουν άμεση πρόσβαση σε δημόσιες πληροφορίες προσώπων ώστε να τις χρησιμοποιήσουν για την σκιαγράφηση τους ή και για την ανάπτυξη διαφημιστικών ή εμπορικών σχεδίων.

5. Εκβιασμός (Blackmail)

Ο «Εκβιασμός» περιλαμβάνει τον εξαναγκασμό ενός ατόμου, με την απειλή της αποκάλυψης προσωπικών μυστικών, αν δεν προσχωρήσει στις απαιτήσεις του εκβιαστή, που συχνά περιλαμβάνουν την καταβολή δωροδοκίας. Σχετίζεται και με προηγούμενες κατηγορίες καθώς οι πληροφορίες μπορεί να εμπίπτουν στην κατηγορία της Έκθεσης, της Αποκάλυψης ή της παραβίασης της εμπιστοσύνης.

Εκτός από του κινδύνους και τις συνέπειες που επέρχονται με την αποκάλυψη των πληροφοριών ο μεγαλύτερος κίνδυνος είναι η αλλαγή στην σχέση μεταξύ εκβιαστή και θύματος. Η σχέση μετατρέπεται σε σχέση αφέντη-σκλάβου, με τον εκβιαστή να είναι σε μια θέση ισχύος και ελέγχου έναντι του θύματος, για όσο καιρό είναι κάτοχος και διαχειριστής της πληροφορίας.

6. Οικειοποίηση (Appropriation)

Η «Οικειοποίηση» είναι η χρήση της ταυτότητας ή της προσωπικότητας ενός ατόμου, για τους σκοπούς και τους στόχους ενός άλλου. Η «Οικειοποίηση», όπως και οι διαταραχές της ιδιωτικής ζωής σαν την αποκάλυψη και την στρέβλωση, αφορά τον τρόπο με τον οποίο ένα άτομο επιθυμεί να παρουσιάσει τον εαυτό του στην κοινωνία.

Ως κυριότερη ζημιογόνα επίπτωση της «Οικειοποίησης» θεωρείται η καταπάτηση του δικαιώματος της ιδιοκτησίας. Παρόλα αυτά, εμβαθύνοντας στις συνέπειες της μπορούμε να καταλάβουμε ότι η οικειοποίηση δεδομένων αποτελεί μία προσβολή της αξιοπρέπειας του ατόμου και μια πράξη που περιορίζει την ελευθερία και την προσωπική εξέλιξη.

7. Στρέβλωση (Distortion)

Ως «Στρέβλωση» ή «Παραμόρφωση» ορίζεται η χειραγώγηση του τρόπου με τον οποίο ένα άτομο γίνεται αντιληπτό και κρίνεται από τους άλλους, και περιλαμβάνει την ανακριβή δημόσια έκθεση του θύματος. Η «Παραμόρφωση», όπως και η «Αποκάλυψη», περιλαμβάνει τη διάδοση των πληροφοριών που επηρεάζουν τον τρόπο με τον οποίο η κοινωνία βλέπει ένα πρόσωπο. Τόσο η παραμόρφωση και η αποκάλυψη μπορούν να οδηγήσουν σε αρνητικές συνέπειες και συναισθήματα όπως αμηχανία, ταπείνωση, στιγματισμό και βλάβη της υπόληψης. Και οι δύο αφορούν τον έλεγχο των πληροφοριών για ένα άτομο, εντούτοις η Παραμόρφωση διαφέρει από την αποκάλυψη, καθώς οι πληροφορίες διαδίδονται είναι ψευδείς και παραπλανητικές.

Οι παραπάνω αρνητικές συνέπειες της «Παραμόρφωσης» μπορούν να γίνουν αντιληπτές αν σκεφτούμε την σημαντικότητα εννοιών-χαρακτηριστικών όπως η φήμη και η υπόληψη, στην σημερινή κοινωνία. Για οποιοδήποτε τομέα της ζωής μας εξαρτόμαστε άμεσα από την «εικόνα» που έχουμε δημιουργήσει για τον εαυτό μας μέσα σε μια κοινωνία, συνεπώς οποιαδήποτε στρέβλωση αυτής, μπορεί να επιφέρει οδυνηρές συνέπειες.

1.4.4 Εισβολή

Στην κατηγορία της εισβολής (Intrusion) περιλαμβάνονται κίνδυνοι για τους οποίους δεν εμπλέκεται πάντα η πληροφορία. Διακρίνονται σε δύο μορφές:

1. Παρείσφρηση (Intrusion)

Η έννοια της «Παρείσφρησης», περιλαμβάνει όλες εκείνες τις δράσεις οι οποίες έχουν την μορφή της «εισβολής». Περιλαμβάνονται δηλαδή επιδρομές στη ζωή ενός ατόμου οι οποίες διαταράσσουν τις καθημερινές δραστηριότητες του, αλλάζουν την ρουτίνα του, καταστρέφουν την απομόνωση του, και συχνά το κάνουν να νιώθει άβολα και αμήχανα. Η

προστασία κατά της διείσδυσης, προϋποθέτει την προστασία του ατόμου από τις ανεπιθύμητες κοινωνικές επιδρομές, παρέχοντας του το δικαίωμα στην απομόνωση.

Οι αρνητικές επιπτώσεις της παρείσφρηση είναι κοινές με αυτές της ανάκρισης, της παρακολούθησης και της αποκάλυψης. Επιπλέον αρνητικές επιπτώσεις που μπορούν να προκύψουν είναι η διακοπή ή και η μεταβολή των δραστηριοτήτων ή της καθημερινότητας του ατόμου.

2. Παρεμβολές λήψης αποφάσεων (Decisional Interference)

Αφορά περιπτώσεις κυβερνητικής παρεμβολής στις ζωές των ανθρώπων, για θέματα που αφορούν μόνο τους ίδιους και συγκεκριμένους τομείς της ζωής τους. Σε αυτήν την κατηγορία ανήκουν περιπτώσεις που αφορούν το φύλο, την σεξουαλικότητα και την ανατροφή των παιδιών.

Είναι εύκολα αντιληπτό ότι οποιαδήποτε παρέμβαση στην λήψη αποφάσεων ενός προσώπου, επιδρά αρνητικά σε αγαθά όπως η αυτονομία, η ανεξαρτησία και η ελευθερία του. Επιπλέον όμως οποιαδήποτε κυβερνητική παρέμβαση στις ζωές των ανθρώπων μπορεί να έχει ως συνέπειες την παραβίαση του απορρήτου, την αποκάλυψη πληροφοριών την εισβολή, ή και τον εκβιασμό.

1.5 Προστασία της ιδιωτικότητας

Οι αυξημένες προκλήσεις και απειλές κατά της Ιδιωτικότητας αλλά και οι οδυνηρές συνέπειες που αυτές είναι δυνατόν να επιφέρουν , δεν θα μπορούσαν παρά να δημιουργήσουν την ανάγκη ύπαρξης απαιτήσεων ασφαλείας με σκοπό την προστασία της ιδιωτικότητας και τον περιορισμό ή την ελαχιστοποίηση των παραβιάσεων. Φυσικά αυτές οι απαιτήσεις δεν εμπίπτουν μόνο στον τομέα της «Τεχνολογίας» αλλά επιπλέον περιλαμβάνουν απαιτήσεις νομοθετικού και θεσμικού πλαισίου. Αναλυτικότερα οι απαιτήσεις που ενισχύουν την προστασία της ιδιωτικότητας αφορούν:

- Το νομοθετικό πλαίσιο για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, το οποίο προωθείται από την κάθε κυβέρνηση.

- Την αυτορρύθμιση από τους κώδικες δεοντολογίας σχετικά με τις δίκαιες πρακτικές πάνω σε πληροφορίες, που προωθούνται από οργανισμούς και επιχειρήσεις.

- Τις τεχνολογίες ενίσχυσης της ιδιωτικότητας που δημιουργούνται και κατά συνέπεια που υιοθετούνται από τα άτομα.

- Την εκπαίδευση των καταναλωτών και των επαγγελματιών Πληροφορικής, σχετικά με την ιδιωτικότητα.

Κεφάλαιο 2
Δεδομένα

«Τα δεδομένα είναι ένα πολύτιμο πράγμα και θα διαρκέσουν περισσότερο απ' ότι τα ίδια τα συστήματα»

Sir Timothy John Berners-Lee

Γνωρίζοντας ότι ως δεδομένα (data) ορίζονται οποιαδήποτε σύμβολα, χαρακτήρες, ή αριθμοί τα οποία είναι ερμηνεύσιμα είτε μεμονωμένα, είτε ως σύνολα, συμπεραίνουμε ότι ο όρος «Ψηφιακά δεδομένα» (digital data) αναφέρεται στα δεδομένα εκείνα που μπορούν να αποθηκευτούν, να διαχειριστούν και να μεταβιβαστούν μέσω υπολογιστικών συσκευών και φυσικά αφορούν τον χώρο της Πληροφορικής και των Τηλεπικοινωνιών.

Γιατί όμως τα δεδομένα αποτελούν τόσο σημαντικό κεφάλαιο για τα συστήματα αλλά και για τους χρήστες τους; Ποιες είναι οι διαφορές τους και γιατί υπάρχει ο διαχωρισμός τους; Τα δεδομένα διακρίνονται ανάλογα την χρήση τους από τα συστήματα. Ως εκ τούτου, τα δεδομένα κατηγοριοποιούνται ανάλογα την σημασία και το είδος τους όπως επίσης και ανάλογα με την πληροφορία την οποία συνδέονται ή το υποκείμενο το οποίο αντιπροσωπεύουν.

Συνεπώς τα δεδομένα που αφορούν τις τηλεπικοινωνίες μπορούν να ορισθούν ως δεδομένα επικοινωνίας και η σημαντικότητα τους είναι ανάλογη της πληροφορίας της οποίας συνθέτουν, για το υποκείμενο το οποίο αντιπροσωπεύουν. Έτσι έχουμε ένα διαχωρισμό σε προσωπικά δεδομένα, δηλαδή δεδομένα άμεσα συνδεδεμένα με το υποκείμενο, αλλά και ευαίσθητα προσωπικά δεδομένα, δηλαδή προσωπικά δεδομένα που καθορίζουν ή φανερώνουν στάση ή ποιότητα ζωής του υποκειμένου.

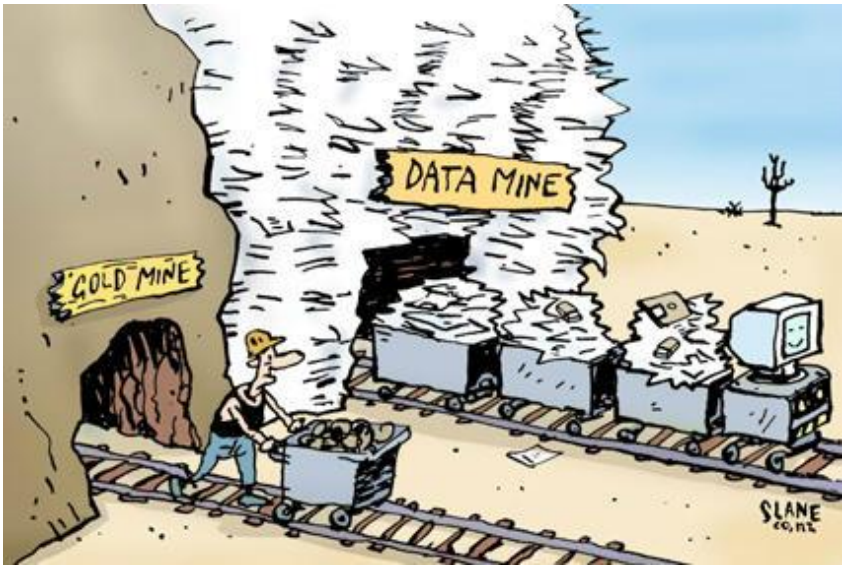
2.1 Δεδομένα Επικοινωνίας

Κατά την χρήση υπηρεσιών ηλεκτρονικής επικοινωνίας δια μέσω των δικτύων και των ηλεκτρονικών συσκευών διαβιβάζονται, επεξεργάζονται και διατηρούνται δεδομένα τα οποία σχετίζονται με τον κάθε χρήστη. Αυτά τα δεδομένα ορίζονται ως δεδομένα επικοινωνίας (Communications Data) και ως τέτοια θεωρούνται τα δεδομένα κίνησης (traffic data), τα δεδομένα τοποθεσίας (Location Data) και γενικότερα το σύνολο των δεδομένων από τα οποία μπορούν να εξαχθούν συμπεράσματα σχετικά με την ταυτότητα συνδρομητών ή χρηστών, οποιασδήποτε υπηρεσίας ηλεκτρονικής επικοινωνίας.

Αν και οι λόγοι και ο σκοπός της μεταβίβασης αυτών των δεδομένων μέσω των συστημάτων είναι κατανοητοί από τους περισσότερους χρήστες - καθώς μόνο έτσι θα μπορούσαν να εξυπηρετηθούν οι ανάγκες τους - οι λόγοι της επεξεργασίας και της διατήρησης δεδομένων από εταιρείες ή οργανισμούς αντιμετωπίζονται καχύποπτα. Οι χρήστες δυσκολεύονται να εμπιστευτούν τα συστήματα και τις νέες τεχνολογίες καθώς αγνοούν ή φοβούνται τους λόγους για τους οποίους τρίτοι μπορούν να έχουν πρόσβαση και δυνατότητα διαχείρισης των δεδομένων τους. Φυσικά τέτοιου είδους ανησυχίες από την πλευρά των χρηστών δεν μπορούν μονομιάς να χαρακτηριστούν αβάσιμες, αφού οι λόγοι είτε δεν είναι πάντα ξεκάθαροι ή επιπλέον δεν είναι και καλοπροαίρετοι. Ακόμα και αν οι οργανισμοί που διατηρούν και διαχειρίζονται τα δεδομένα των χρηστών φαντάζουν εκ πρώτης όψεως απόλυτα έμπιστοι, όπως για παράδειγμα ένας κυβερνητικός οργανισμός ή υπηρεσία, δεν συνεπάγεται πάντα ότι αυτές οι ενέργειες γίνονται με καλό σκοπό και έχοντας ως πρώτο γνώμονα την προστασία των χρηστών.

Η ανάπτυξη όμως των τεχνολογιών που αφορούν την επικοινωνία απαιτεί από τον χρήστη να είναι εξοικειωμένος με αυτή την συναλλαγή δεδομένων, καθώς είναι απαραίτητη για οποιαδήποτε κοινωνική, πολιτική ή πολιτισμική του δραστηριότητα, όπως επίσης να κατανοεί ενέργειες όπως η επεξεργασία και η διατήρηση δεδομένων και τους λόγους για τους οποίους

υφίστανται. Επιπλέον πρέπει να κατανοεί έννοιες όπως προσωπικά ή ευαίσθητα δεδομένα και να γνωρίζει τρόπους με τους οποίους να διασφαλίζει την σωστή συνδιαλλαγή και χρήση τους.



ΕΙΚΟΝΑ 2.1: ΔΕΔΟΜΕΝΑ

2.2 Προσωπικά δεδομένα [06] [07]

Με τον όρο «Προσωπικά δεδομένα» (Personal Data) ορίζεται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, δηλαδή στο άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα. Αναλυτικότερα ως «Προσωπικά δεδομένα» ορίζεται κάθε πληροφορία που αναφέρεται ή και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Ως δεδομένα προσωπικού χαρακτήρα δεν λογίζονται τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία και δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.

Επιπλέον ως «Ευαίσθητα» (Sensitive Personal Data) χαρακτηρίζονται τα προσωπικά δεδομένα τα οποία η ταύτιση τους με το υποκείμενο είναι απόλυτη και άμεση. Τα δεδομένα αυτά διαθέτουν μοναδικά χαρακτηριστικά, είναι αδύνατον δηλαδή να ταυτιστούν με οποιαδήποτε άλλα και είναι ιδιαίτερα περιεκτικά διότι εμπεριέχουν πληροφορίες του προσώπου που συνδέονται με την ιδιωτικότητά του, όπως δεδομένα που αναφέρονται στη φυλετική ή εθνική

του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα προσωπικά δεδομένα που εμπίπτουν στην κατηγορία των ευαίσθητων δεδομένων, τυγχάνουν αυστηρότερης νομοθετικής προστασίας από ότι τα απλά προσωπικά δεδομένα καθώς η προστασία των δεδομένων αυτών έχει την ιδιότητα να επιτρέπει στο πρόσωπο να διατηρεί τη διαφορετικότητά. Η παραβίαση των ευαίσθητων δεδομένων, μέσω της πρόσβασης, της επεξεργασία τους, ή της διάδοσης τους συνιστά συνήθως και μια ολική παραβίαση της ιδιωτικότητας και της αξιοπρέπειας του ατόμου.

2.3 Κατηγορίες Δεδομένων Επικοινωνίας [01] [08]

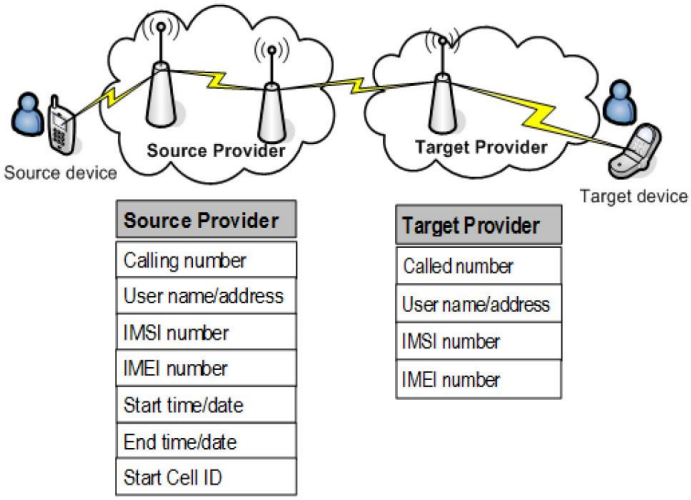
Εκτός της διάκρισης των δεδομένων ανάλογα την σημαντικότητα την οποία έχουν για το υποκείμενο τους, δηλαδή σε προσωπικά ή ευαίσθητα προσωπικά, τα δεδομένα μπορούν επίσης να κατηγοριοποιηθούν ανάλογα την φύση τους, την υπηρεσία με την οποία διακινούνται ή και ανάλογα το χαρακτηριστικό ή την πληροφορία του χρηστή τον οποίο αντιπροσωπεύουν. Σε πρώτη φάση τα δεδομένα μπορούν να διαχωριστούν ανάλογα την φύση τους σε εσωτερικά δεδομένα (content data) και εξωτερικά δεδομένα (context data) :

- Τα εσωτερικά δεδομένα (content data) αφορούν το πραγματικό περιεχόμενο μιας επικοινωνίας, δηλαδή είναι εκείνα τα δεδομένα που διαβιβάζονται από την μία πηγή επικοινωνίας στην άλλη. Αυτονόητο είναι ότι πιθανή έκθεση των εσωτερικών δεδομένων αυτομάτως αποτελεί παραβίαση απορρήτου της επικοινωνίας και της ιδιωτικότητας, συνεπώς η προστασία αυτού του τύπου δεδομένων θεωρείται αναγκαία και η συλλογή και διατήρηση τους είναι παράνομη.

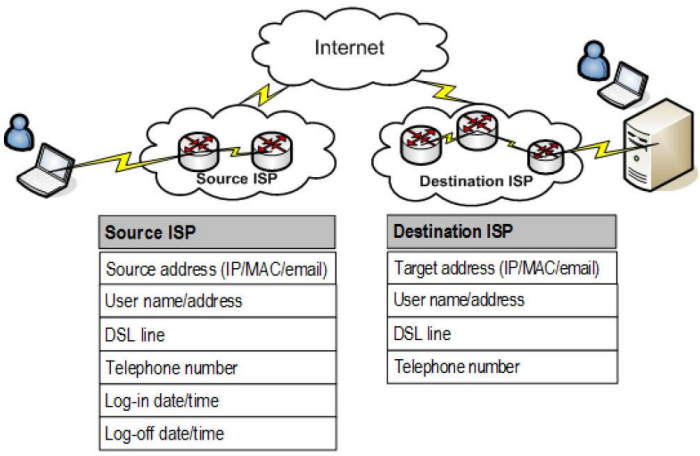
- Τα εξωτερικά δεδομένα (context data) αποτελούν τα δεδομένα τα οποία χρησιμοποιούνται για τον έλεγχο, την διευθυνσιοδότηση και την παροχή της επικοινωνίας, όπως ο τηλεφωνικός αριθμός, η διεύθυνση IP, η διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail), η διεύθυνση MAC (Media Access Control), και η ημερομηνία και ώρα σύνδεσης ή αποσύνδεσης. Η έκθεση των εξωτερικών δεδομένων, μπορεί επίσης να επηρεάσει την ιδιωτικότητα του ατόμου έμμεσα

αποκαλύπτοντας στοιχεία για τον τύπο, την ταυτότητα και την θέση και τον χρόνο της επικοινωνίας.

Τα εξωτερικά δεδομένα συνεπώς είναι τα δεδομένα επικοινωνίας τα οποία πρέπει να προστατευθούν και να οριστούν θεσμικοί κανόνες για αυτά. Ως εκ τούτου προκύπτει μια κατηγοριοποίηση των εξωτερικών δεδομένων με σκοπό την ενίσχυση των θεσμών που τα προστατεύουν, ανάλογα με την τεχνολογία την οποία διαβιβάζονται. Έτσι έχουμε τον διαχωρισμό σε δεδομένα κινητής ή σταθερής τηλεφωνίας και δεδομένα υπηρεσιών Διαδικτύου.



ΕΙΚΟΝΑ 3.2: ΕΞΩΤΕΡΙΚΑ ΔΕΔΟΜΕΝΑ ΚΙΝΗΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ



ΕΙΚΟΝΑ 4.3: ΕΞΩΤΕΡΙΚΑ ΔΕΔΟΜΕΝΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΔΙΑΔΙΚΤΥΟΥ

2.3.1 Δεδομένα τηλεφωνίας σταθερού δικτύου ή κινητής τηλεφωνίας [08]

1. **Δεδομένα ανίχνευσης και προσδιορισμού της πηγής επικοινωνίας**

   Αφορά τα δεδομένα από τα οποία μπορεί να προσδιοριστεί η πηγή της επικοινωνίας δηλαδή της τηλεφωνικής συσκευής, σταθερής ή κινητής και του ατόμου από τα οποία ξεκινάει η επικοινωνία. Ως τέτοια θεωρούνται:

   - ο τηλεφωνικός αριθμός του καλούντος,
   - το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή του εγγεγραμμένου χρήστη

2. **Δεδομένα προσδιορισμού του προορισμού της επικοινωνίας**

   Αφορά τα δεδομένα από τα οποία μπορεί να προσδιοριστεί ο προορισμός της επικοινωνίας δηλαδή της τηλεφωνικής συσκευής, σταθερής ή κινητής και του ατόμου τα οποία καλούνται από τον εκκινητή της επικοινωνίας. Ως τέτοια θεωρούνται:

   - ο καλούμενος αριθμός ή αριθμοί και σε περιπτώσεις όπου υπεισέρχονται συμπληρωματικές υπηρεσίες όπως προώθηση/εκτροπή κλήσης, ο αριθμός ή οι αριθμοί προς τους οποίους προωθήθηκε ή εκτράπηκε η κλήση.
   - Τα ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή των εγγεγραμμένων χρηστών

3. **Δεδομένα χρονικού προσδιορισμού της επικοινωνίας**

   Περιλαμβάνονται τα δεδομένα που φανερώνουν την ημερομηνία που πραγματοποιήθηκε η κλήση όπως επίσης και την ώρα έναρξης και λήξης της επικοινωνίας, στοιχεία από τα οποία μπορεί να εξαχθεί και η διάρκεια της επικοινωνίας.

4. **Δεδομένα προσδιορισμού του είδους της επικοινωνίας**

   Αφορά δεδομένα από τα οποία εξάγονται πληροφορίες για το είδος της τηλεφωνικής υπηρεσίας που χρησιμοποιήθηκε για να επιτευχθεί η επικοινωνία.

5. Δεδομένα προσδιορισμού του εξοπλισμού επικοινωνίας των χρηστών

Αναφέρεται στα δεδομένα από τα οποία συνθέτονται πληροφορίες σχετικά με τον χρησιμοποιούμενο εξοπλισμό κατά την επικοινωνία των χρηστών. Τέτοια είναι:

- Οι τηλεφωνικοί αριθμοί καλούντος
- Οι τηλεφωνικοί αριθμοί καλούμενων

Όπως επιπλέον για την κινητή τηλεφωνία:

- η διεθνής ταυτότητα συνδρομητή κινητής τηλεφωνίας (IMSI - International mobile Subscriber Identity) του καλούντος,
- η διεθνής ταυτότητα εξοπλισμού κινητής τηλεφωνίας (IMEI -) του καλούντος,
- η IMSI του καλουμένου,
- η IMEI του καλουμένου,
- στην περίπτωση προπληρωμένων ανώνυμων υπηρεσιών, η ημερομηνία και ώρα της αρχικής ενεργοποίησης της υπηρεσίας και ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) από την οποία πραγματοποιήθηκε η ενεργοποίησης

6. Δεδομένα προσδιορισμού της θέσης του εξοπλισμού κινητής επικοινωνίας:

Ως δεδομένα θέσης του εξοπλισμού θεωρούνται τα δεδομένα από τα οποία μπορούν να προκύψουν πληροφορίες σχετικά με την γεωγραφική περιοχή στην οποία βρίσκεται ο εξοπλισμός που χρησιμοποιείται για την πραγμάτωση της επικοινωνίας. Τα δεδομένα που εμπεριέχονται εδώ μπορούν να είναι είτε τηλεφωνικής είτε διαδικτυακής επικοινωνίας, αλλά πάντα θα αφορούν δεδομένα που διαβιβάζονται μέσω κινητών συσκευών. Στην κατηγορία ανήκουν:

- ο κωδικός θέσης (κωδικός ταυτότητας κυψέλης) κατά την έναρξη και λήξη της επικοινωνίας
- δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών βάσει των κωδικών θέσης (κωδικών ταυτότητας κυψέλης), κατά το χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών.

2.3.2 Δεδομένα Υπηρεσιών Διαδικτύου [08]

1. **Δεδομένα ανίχνευσης και προσδιορισμού της πηγής επικοινωνίας**

   Αναφέρεται στα δεδομένα από τα οποία εξάγονται πληροφορίες σχετικά με τον εκκινητή της διαδικτυακής επικοινωνίας. Περιλαμβάνονται:

   - ο αποδοθείς κωδικός ταυτότητας χρήστη,
   - ο κωδικός ταυτότητας χρήστη και ο τηλεφωνικός αριθμός που δίνονται σε κάθε επικοινωνία που εισέρχεται στο δημόσιο τηλεφωνικό δίκτυο,
   - το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου

2. **Δεδομένα προσδιορισμού του προορισμού της επικοινωνίας**

   Αναφέρεται στα δεδομένα από τα οποία εξάγονται πληροφορίες σχετικά με τον παραλήπτη των δεδομένων μιας διαδικτυακής επικοινωνίας. Ως τέτοια θεωρούνται:

   - το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας,
   - ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης

3. **Δεδομένα χρονικού προσδιορισμού της επικοινωνίας**

   Αφορά τα δεδομένα που φανερώνουν την ημερομηνία και ώρα σύνδεσης ή αποσύνδεσης στο Διαδίκτυο ή σε διαδικτυακές υπηρεσίες

   - Η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης στο Διαδίκτυο, καθώς και η διεύθυνση πρωτοκόλλου του διαδικτύου (IP), είτε δυναμική είτε στατική, που απέδωσε στην επικοινωνία ο πάροχος υπηρεσιών πρόσβασης στο διαδίκτυο, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη,
   - Η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου,

4. **Δεδομένα προσδιορισμού του είδους της επικοινωνίας**

   Αφορά δεδομένα από τα οποία εξάγονται πληροφορίες για το είδος της διαδικτυακής υπηρεσίας που χρησιμοποιήθηκε.

5. **Δεδομένα προσδιορισμού του εξοπλισμού επικοινωνίας των χρηστών**

   Περιλαμβάνονται τα δεδομένα από τα οποία μπορούν να εξαχθούν πληροφορίες σχετικά με τον χρησιμοποιούμενο εξοπλισμό. Ως τέτοια θεωρούνται:

   - ο τηλεφωνικός αριθμός καλούντος αν πρόσβαση γίνεται μέσω τηλεφώνου,
   - η ψηφιακή συνδρομητική γραμμή (DSL) ή άλλη απόληξη της πηγής της επικοινωνίας

Στον παρακάτω πίνακα παρουσιάζονται συγκεντρωτικά οι κατηγορίες προσωπικών δεδομένων :

Κατηγορίες Δεδομένων Επικοινωνίας		
Εξωτερικά Δεδομένα (Context Data)		
	Δεδομένα σταθερής ή κινητής τηλεφωνίας	**Δεδομένα Υπηρεσιών Διαδικτύου**
Δεδομένα πηγής επικοινωνίας	• ο τηλεφωνικός αριθμός του καλούντος, • το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή του εγγεγραμμένου χρήστη	• κωδικός ταυτότητας χρήστη • ο κωδικός ταυτότητας και ο τηλεφωνικός αριθμός του δημόσιου τηλεφωνικού δικτύου • ονοματεπώνυμο και διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί IP, κωδικός ταυτότητας χρήστη ή αριθμός τηλεφώνου
Δεδομένα προορισμού επικοινωνίας	• ο καλούμενος αριθμός ή αριθμοί (συμπεριλαμβανομένων και αυτών που κλήθηκαν από εκτροπή/προώθηση). • Ονοματεπώνυμα και οι διευθύνσεις των συνδρομητών ή των εγγεγραμμένων χρηστών	• το ονοματεπώνυμο και η διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη και ο κωδικός ταυτότητας χρήστη του παραλήπτη της επικοινωνίας, • ο κωδικός ταυτότητας χρήστη ή ο αριθμός τηλεφώνου του παραλήπτη διαδικτυακής τηλεφωνικής κλήσης

Δεδομένα χρονικού προσδιορισμού της επικοινωνίας	• Ημερομηνία κλήσης • ώρα έναρξης και λήξης της επικοινωνίας	• Η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης στο Διαδίκτυο, η IP, καθώς και ο κωδικός ταυτότητας χρήστη του συνδρομητή ή εγγεγραμμένου χρήστη, • Η ημερομηνία και η ώρα σύνδεσης και αποσύνδεσης με την υπηρεσία ηλεκτρονικού ταχυδρομείου ή τηλεφωνίας μέσω διαδικτύου
Δεδομένα του είδους της επικοινωνίας	• χρησιμοποιούμενη τηλεφωνική υπηρεσία • Οι τηλεφωνικοί αριθμοί καλούντος • Οι τηλεφωνικοί αριθμοί καλούμενων	• χρησιμοποιούμενη διαδικτυακή υπηρεσία
Δεδομένα προσδιορισμού του εξοπλισμού επικοινωνίας των χρηστών	κινητή τηλεφωνία: • IMSI του καλούντος, • IMEI του καλούντος, • η IMSI του καλουμένου, • η IMEI του καλουμένου, • Για προπληρωμένες ανώνυμες υπηρεσίες: ημερομηνία και ώρα της αρχικής ενεργοποίησης και ο κωδικός θέσης	• ο τηλεφωνικός αριθμός καλούντος αν πρόσβαση γίνεται μέσω τηλεφώνου, • η ψηφιακή συνδρομητική γραμμή (DSL) ή άλλη απόληξη της πηγής της επικοινωνίας
Δεδομένα προσδιορισμού της θέσης του εξοπλισμού κινητής επικοινωνίας	• ο κωδικός θέσης κατά την έναρξη και λήξη της επικοινωνίας • δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών βάσει των κωδικών θέσης, κατά το χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών	• ο κωδικός θέσης κατά την έναρξη και λήξη της επικοινωνίας • δεδομένα με τα οποία προσδιορίζεται η γεωγραφική θέση των κυψελών βάσει των κωδικών θέσης, κατά το χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα των επικοινωνιών

ΠΙΝΑΚΑΣ 2. 1: ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ

2.4 Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Τα δεδομένα ίσως να μην είχαν καμία ιδιαίτερη αξία αν μέσω συγκεκριμένων ενεργειών, που ανήκουν στο πλαίσιο της επεξεργασίας δεδομένων (data processing), δεν μπορούσαν να αποτελέσουν μεταβιβαζόμενες πληροφορίες. Συνειδητοποιεί λοιπόν κανείς ότι πρόκειται για ενέργειες αναγκαίες για την υλοποίηση και την ανάπτυξη των ηλεκτρονικών επικοινωνιών. Με μια απλή προσέγγιση θα ορίζαμε την επεξεργασία δεδομένων ως το σύνολο των ενεργειών διαχείρισης που εφαρμόζονται στα δεδομένα. Πιο αναλυτικά, κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπου ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, ορίζεται ως επεξεργασία δεδομένων προσωπικού χαρακτήρα [06].

Αυτές οι εργασίες μπορούν να συσχετίζονται, να συνδυάζονται, να ακολουθούν ή να προηγούνται σε σχέση με άλλες, ωστόσο διαφέρουν στον σκοπό τους και στο αποτέλεσμα το οποίο επιτελούν. Το συγκεκριμένο γεγονός μας δίνει την δυνατότητα να τις διαχωρίσουμε σε κατηγορίες ανάλογα με τον τρόπο και τον σκοπό εφαρμογής τους. Έτσι επιχειρείται ο ακόλουθος διαχωρισμός τους σε πέντε βασικές κατηγορίες:

1. **Συγκέντρωση (Collection)**

   Στην κατηγορία αυτή εντάσσονται οι πρώτες ενέργειες που γίνονται σε σχέση με τα δεδομένα. Περιλαμβάνονται εργασίες όπως η συλλογή, η οργάνωση, η καταχώρηση και η τροποποίηση ή προσαρμογή των δεδομένων.

2. **Διατήρηση (Retention)**

   Η διαδικασία της διατήρησης είναι μια επακόλουθη διαδικασία των ενεργειών που περιλαμβάνει η Συγκέντρωση και αφορά ενέργειες αναγκαίες ώστε να επιτυγχάνεται διαρκής πρόσβαση στα δεδομένα. Τέτοιου είδους ενέργειες αποτελούν η απόκτηση, η καταγραφή, η συντήρηση και η φύλαξη των δεδομένων.

3. **Διαχείριση (Control)**

Η Διαχείριση έχει να κάνει με ενέργειες που αφορούν την γενικότερη χρήση των δεδομένων αλλά και την επιμέλεια ή την ανάκτηση αυτών.

4. **Διάθεση (Disposal)**

Η Διάθεση εμπεριέχει ενέργειες σχετικές με την διάδοση των δεδομένων ή των πληροφοριών που αυτά συνθέτουν. Ενέργειες όπως η δημοσιοποίηση των πληροφοριών ή δεδομένων και η διαβίβαση τους εμπίπτουν σε αυτήν την κατηγορία.

5. **Μεταχείριση (Conduct)**

Οποιαδήποτε ενέργεια ακολουθεί την οποιασδήποτε μορφής διάθεση των δεδομένων, εμπίπτει στη κατηγορία της Μεταχείρισης. Σε αυτές περιλαμβάνονται ο συνδυασμός ή η συσχέτιση των δεδομένων ή πληροφοριών, η δέσμευση τους, και η διαγραφή ή η καταστροφή τους.

2.5 Παραβίαση δεδομένων προσωπικού χαρακτήρα

Οι δυνατότητες που η σύγχρονη τεχνολογία παρέχει για τη δημιουργία και τη διάδοση των προσωπικών δεδομένων, ενισχύουν την πιθανότητα εμφάνισης απειλών κατά της ιδιωτικότητας, εξ αιτίας της ιδιαίτερης φύσης των πληροφοριών. Αν οι απλές, συμβατικές πληροφορίες με την χρήση παλαιότερων τεχνολογιών μπορούσαν να διαχέονται γρήγορα, με την σύγχρονη τεχνολογία των επικοινωνιών και ιδιαίτερα του διαδικτύου η κυκλοφορία τους γίνεται σε σχεδόν μηδενικό χρόνο, πέρα από εθνικά σύνορα και προς απεριόριστο αριθμό παραληπτών. Η σύγχρονη πληροφορία μπορεί να αποθηκεύεται και να καθίσταται αντικείμενο επεξεργασίας επιτρέποντας την δημιουργία της «επώνυμης» πληροφορίας, υπερβαίνοντας με τον τρόπο αυτό την φυσική διάσταση του ανθρώπου, μετατρέποντας τον σε ένα ψηφιδωτό πληροφοριών.

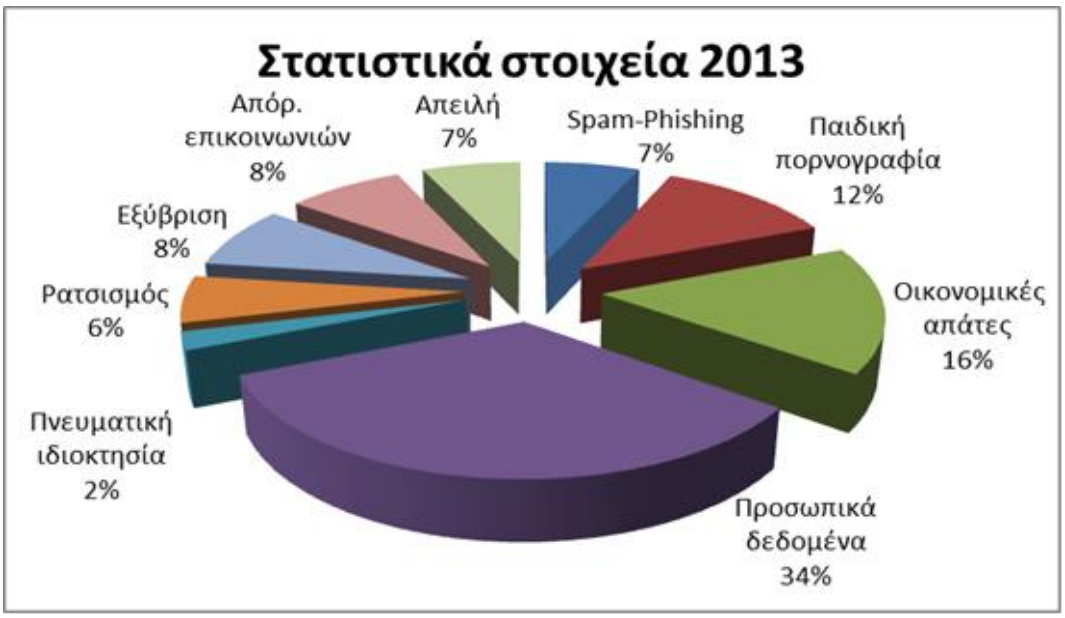
Καθώς λοιπόν η τεχνολογία αλλάζει ο κόσμος μας γεμίζει με δεδομένα από παντός και διαφορετικού είδους συσκευές (smartphones, tablets, sensors, laptops, PCs, κ.α.) αυξάνονται και

οι προκλήσεις της σωστής και ασφαλούς διαχείρισης. Οι περιπτώσεις επιθέσεων και παραβιάσεων στα πληροφοριακά συστήματα οργανισμών ή επιχειρήσεων, που φέρουν σαν επακόλουθο τη διαρροή δεδομένων των χρηστών, συνεχώς αυξάνονται παγκοσμίως και συνεπώς δημιουργούνται συνέχεια ανάγκες προσαρμογής της νομοθεσίας αλλά και των τρόπων ενίσχυσης της ασφάλειας που εφαρμόζουν οι εταιρείες και οι οργανισμοί.

Τι αποτελεί όμως παραβίαση της ασφάλειας των δεδομένων μας και που αποσκοπεί; Σύμφωνα με το Ευρωπαϊκό νομικό πλαίσιο[06], ως παραβίαση της ασφάλειας ορίζεται οποιαδήποτε ενέργεια οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλο τρόπο σε επεξεργασία, σε συνάρτηση με την παροχή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών. Πιο απλά μπορούμε να ορίσουμε ως παραβίαση οποιαδήποτε συνειδητή ή μη συνειδητή ενέργεια που έχει επιζήμια επίπτωση στα προσωπικά δεδομένα που διαβιβάζονται μέσω υπηρεσιών ηλεκτρονικής επικοινωνίας.

Η παραβίαση προσωπικών δεδομένων φέρεται ως η μεγαλύτερη απειλή των Διαδικτυακών Υπηρεσιών. Σύμφωνα με τα στατιστικά στοιχεία για το έτος 2013 που δημοσίευσε η Ελληνική εταιρεία Safe Line**[09]**, μια ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο, η κατηγορία που διακρίνεται από τον μεγάλο αριθμό καταγγελιών που την αφορά είναι αυτή της παραβίασης Προσωπικών Δεδομένων (34%). Ακολουθεί η κατηγορία που σχετίζεται με οικονομικές απάτες (16%) και 3η η κατηγορία της Παιδικής Πορνογραφίας (12%).

Ακολουθεί το διάγραμμα με τα στατιστικά στοιχεία της εταιρείας Safe Line:



ΣΧΗΜΑ 2. 1: ΣΤΑΤΙΣΤΙΚΑ ΚΑΤΑΓΓΕΛΙΩΝ ΤΗΣ SAFE LINE (2013)

Επιπλέον σύμφωνα με την ετήσια έκθεσης της Symantec[10] για τις απειλές στο διαδίκτυο («Internet Security Threat Report»), όσον αφορά στη συνολική εικόνα της Ελλάδας στον τομέα των διαδικτυακών απειλών (Internet Security Threat), η Ελλάδα καταλαμβάνει την 43η θέση στην παγκόσμια κατάταξη.

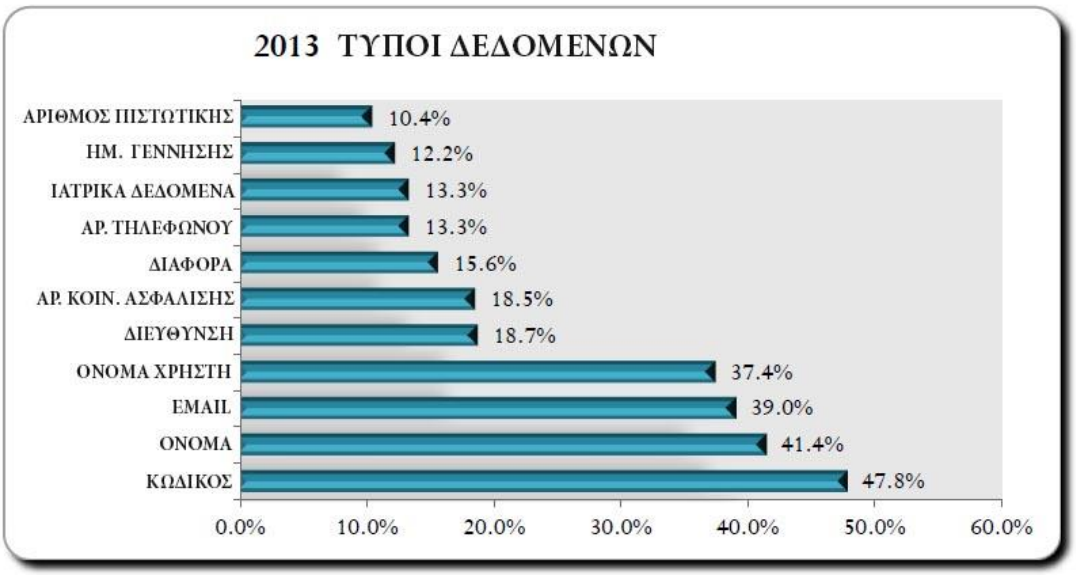
Αναλυτικότερα, στους επιμέρους τομείς, η Ελλάδα βρέθηκε στην 30ή θέση παγκοσμίως στο επίπεδο της ανεπιθύμητης και κακόβουλης ηλεκτρονικής αλληλογραφίας (spam) με ποσοστό 0,7% των συνολικών μηνυμάτων «spam» διεθνώς. Στη δραστηριότητα κακόβουλου κώδικα, το 2013 η Ελλάδα κατατάχθηκε στη 58η θέση της παγκόσμιας κατάταξης (με ποσοστό 0,2% του συνόλου). Στη φιλοξενία κακόβουλων ιστοσελίδων (phishing hosts), η Ελλάδα βρέθηκε στη 63η θέση παγκοσμίως, ενώ το κακόβουλο λογισμικό μέσω e-mail ήταν κατά μέσο όρο περίπου ένα στα 719 (έναντι ενός στα 392 που είναι ο μέσος όρος παγκοσμίως).

Σύμφωνα με την ίδια πηγή τα στατιστικά εμφανίζουν μια παγκόσμια αύξηση των απειλών στο διαδίκτυο σε ποσοστό 62%. Τα κύρια ευρήματα της έρευνας εμφανίζουν:

- Αύξηση 91% σε εκστρατείες στοχευμένων επιθέσεων
- Αύξηση κατά 62% στον αριθμό των παραβιάσεων
- Έκθεση από παραβιάσεις πάνω από 552 εκατομμύριων ταυτοτήτων

- Ανακαλύψη 23 zero-day (άγνωστες μέχρι την ημέρα που παραβιάστηκαν) ευπαθειών
- 38% των χρηστών κινητής τηλεφωνίας βίωσαν περιστατικά εγκλημάτων που σχετίζονται με το Διαδίκτυο
- Μείωση 66% του όγκου των Spam μηνυμάτων επί του συνόλου της κίνησης email
- 1 σε 392 μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν επιθέσεις phishing
- Οι επιθέσεις μέσω του ιστοχώρου (web-based attacks) εμφάνισαν αύξηση 23%
- Ο 1 στους 8 νόμιμους ιστοχώρους εμφανίζει μια κρίσιμη ευπάθεια

Αναλογικά με την έρευνα, σε όλες αυτές τις μαζικές διαρροές εκτέθηκαν προσωπικά στοιχεία που περιλαμβάνουν από αριθμούς πιστωτικών καρτών και ιατρικών αρχείων, μέχρι κωδικούς και λεπτομέρειες τραπεζικών λογαριασμών. Η βασικότερη αιτία των επιθέσεων ήταν η υποκλοπή δεδομένων και ιδιαίτερα σε περιόδους όπου αυξάνεται η ανταλλαγή ευαίσθητων οικονομικών δεδομένων. Τα στοιχείο που φαίνεται να αποτελεί τον πρώτο σε προτίμηση στόχο των επιτιθέμενων είναι ο κωδικός χρήστη αφού εμφανίζεται να καταλαμβάνει την πρώτη θέση στα περιστατικά παραβίασης καθώς στο 47.8% των περιπτώσεων είναι το πρώτο στοιχείο που αποκαλύπτεται, κάτι που φαίνεται λογικό, αν σκεφτεί κανείς πως από τον κωδικό εισόδου ενός λογαριασμού, ο επιτιθέμενος πιθανά θα οδηγηθεί και στην αποκάλυψη περισσότερων δεδομένων που αφορούν τον χρήστη.



ΣΧΗΜΑ 2. 2: ΤΥΠΟΙ ΠΑΡΑΒΙΑΣΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ (2013)

Το 2013 επίσης χαρακτηρίστηκε ως η χρονιά των μεγάλων παραβιάσεων (mega-breaches), δηλαδή παραβιάσεων που ταυτόχρονα αποσπούν δεδομένα ενός τεράστιου συνόλου λογαριασμών χρηστών (>10 εκατομμυρίων) καθώς υπήρξαν τουλάχιστον 8 τέτοια περιστατικά, 7 περισσότερα του 2012. Χαρακτηριστικά παραδείγματα η παραβίαση των λογαριασμών των χρηστών της αμερικανικής εταιρείας Target όπου εκτέθηκαν 110 εκατομμύρια λογαριασμοί χρηστών, το κοινωνικό δίκτυο Pinterest με παραβίαση 70 εκατομμύριων λογαριασμών χρηστών και ενός εκ των κολοσσών της Πληροφορικής της εταιρείας Adobe, όπου παραβιάστηκαν 152 εκατομμύρια λογαριασμοί χρηστών!

Καθώς αυξάνεται η συχνότητα και ο ρυθμός των επιθέσεων οι συνέπειες για των χώρο των επικοινωνιών και της πληροφορικής είναι ιδιαίτερα επιζήμιες. Υπολογίζονται σε τεράστιο αριθμό κόστους για δαπάνες των εταιρειών ώστε να ενισχύσουν τα μέτρα ασφαλείας των συστημάτων τους, αλλά και σε αυστηρότερα μέτρα των αρμόδιων αρχών κάθε χώρας. Οι συνέπειες είναι επίσης αρνητικές και για τους χρήστες, καθώς οι συχνότητα των παραβιάσεων τους προκαλεί ανησυχία και ανασφάλεια που ίσως επιφέρουν την αποστροφή τους για κάποιες από τις προσφερόμενες υπηρεσίες των παρόχων.

Δεν είναι λοιπόν δύσκολο αν θέλουμε να ερμηνεύσουμε τα παραπάνω γεγονότα και τα αποτελέσματα των στατιστικών ερευνών να διαπιστώσουμε την διαφαινόμενη αύξηση του ενδιαφέροντος τρίτων για τα προσωπικά μας δεδομένα καθώς και να συμπεράνουμε την σημαντικότητα των προσωπικών δεδομένων όπως και την τεράστια ανάγκη που προκύπτει για την προστασία και την διαφύλαξη της ακεραιότητα τους.

2.6 Προστασία Δεδομένων

Η προστασία των δεδομένων συνήθως αναφέρεται στην εμπιστευτικότητα, την διαθεσιμότητα και την ακεραιότητα των δεδομένων. Δηλαδή, είναι το σύνολο των πρακτικών και διαδικασιών που είναι σε θέση να διασφαλίσουν ότι τα δεδομένα δεν χρησιμοποιούνται ή εκτίθενται από μη εξουσιοδοτημένα άτομα ή οργανισμούς. Η προστασία των δεδομένων λοιπόν αφορά διαδικασίες που εξασφαλίζουν ότι τα δεδομένα θα είναι ακριβή, αξιόπιστα και διαθέσιμα όταν τα άτομα που κατέχουν εξουσιοδοτημένη πρόσβαση τα χρειαστούν.

Παρόλο που η προστασία των δεδομένων συχνά χρησιμοποιείται ως συνώνυμη με την προστασία της Ιδιωτικότητας, ουσιαστικά αποτελούν δύο διαφορετικές έννοιες και η σχέση τους μπορεί να χαρακτηριστεί ως συμβιωτική. Αν επιχειρούσαμε ένα παραλληλισμό, θα λέγαμε ότι όπως τα μέτρα προστασίας μιας κατοικίας προστατεύουν την Ιδιωτικότητα των ενοίκων της, έτσι ακριβώς και τα μέτρα προστασίας των δεδομένων προστατεύουν την Ιδιωτικότητα του ατόμου που αυτά αφορούν. Δηλαδή η προστασία των προσωπικών μας δεδομένων είναι κατ' επέκταση και προστασία της ίδιας της Ιδιωτικότητας μας και συνεπώς διατηρώντας τον έλεγχο των προσωπικών δεδομένων, διατηρούμε και τον έλεγχο αυτής.

Πέρα λοιπόν από τις οποιαδήποτε πιθανές τεχνολογικές ή θεσμικές λύσεις που υπάρχουν και οφείλουν να ανανεώνονται και να εξελίσσονται, είναι σημαντικό να κατανοήσουμε ότι η ασφάλεια των προσωπικών μας δεδομένων δεν είναι δεδομένη και είναι ζήτημα πρωτίστως ατομικό. Με άλλα λόγια, οποιοδήποτε νομικό πλαίσιο, πολιτική ασφαλείας ή τεχνολογικό αντίμετρο δεν μπορεί να εξασφαλίσει την ασφάλεια των δεδομένων των χρηστών των ψηφιακών επικοινωνιών, αν πρωτίστως οι ίδιοι δεν γνωρίζουν σωστές πρακτικές διαχείρισης και προστασίας τους.

ΕΙΚΟΝΑ 2. 4: ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

2.6.1 Δικαιώματα – υποχρεώσεις των χρηστών

Γίνεται λοιπόν αντιληπτό, ότι για να διασφαλιστούν υψηλές προδιαγραφές προστασίας για τα προσωπικά δεδομένα, η εκπαίδευση και η ενημέρωση των χρηστών σε θέματα προάσπισης των δικαιωμάτων τους σχετικά με αυτά αποτελεί πρώτη προτεραιότητα. Δεν ζητείται βέβαια από όλους τους χρήστες να κατέχουν το ίδιο επίπεδο γνώσεων όσον αφορά την Ασφάλεια των Πληροφοριών, κάτι που ούτως ή άλλως είναι ανέφικτο, ωστόσο μπορούν να γνωρίζουν βασικούς κανόνες χρήσης των υπηρεσιών ηλεκτρονικής επικοινωνίας που ακολουθώντας τους ενισχύουν και τους θεσμικούς κανόνες προστασίας των δεδομένων.

Κάθε χρήστης λοιπόν οφείλει να γνωρίζει:

- Ότι για οποιαδήποτε χρήση των δεδομένων του πρώτα πρέπει να υπάρξει η συγκατάθεση του
- την ταυτότητά του ατόμου ή οργανισμού που αιτείται τα δεδομένα του, τον σκοπό για τον οποίο χρειάζεται τα δεδομένα σου, αν και σε ποιους άλλους αυτά θα διαβιβαστούν, καθώς και ποιοι θα έχουν πρόσβαση σε αυτά.
- ποια δεδομένα τηρούν οι άλλοι (οργανισμοί ή άτομα) για αυτόν και να ενημερώνεται για αυτά όταν το επιθυμεί.
- η διαγραφή ή τη διόρθωση των προσωπικών του δεδομένων, είναι εφικτή και μπορεί να την αιτηθεί αν θεωρεί ότι η πληροφορίες που εκτίθενται είναι παραπλανητικές, προσβλητικές ή λανθασμένες, ή όταν διαφωνεί με την επεξεργασία αυτών των δεδομένων

Κεφάλαιο 3
Διατήρηση Δεδομένων και Ιδιωτικότητα

«Δεδομένα! Δεδομένα! Δεδομένα!» φώναξε ανυπόμονα. «Δεν μπορώ να φτιάξω τούβλα, χωρίς πηλό.»

Σέρλοκ Χολμς

Οι πάροχοι δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών σε όλο τον κόσμο, είναι υποχρεωμένοι από τους νόμους των χωρών στις οποίες εδρεύουν να διατηρούν τα δεδομένα επικοινωνίας των συνδρομητών τους για συγκεκριμένο χρονικό διάστημα. Συνεπώς οι πολιτικές ασφαλείας για τις κατηγορίες των δεδομένων επικοινωνίας που διατηρούνται αλλά και των τρόπων επεξεργασίας τους, οφείλουν έρχονται σε συμφωνία με τις πολιτικές του εκάστοτε νομοθετικού πλαισίου.

Οι κατηγορίες των δεδομένων επικοινωνίας, όπως είδαμε και στο προηγούμενο κεφάλαιο, περιλαμβάνουν δεδομένα, που φανερώνουν κυρίως θέση, κίνηση και υπηρεσία του συνδρομητή, ωστόσο από τον συνδυασμό αυτών των δεδομένων μπορεί να εξαχθεί πληροφορία η οποία ίσως να είναι ευαίσθητη για τον κάτοχο της, και η πιθανή αποκάλυψη της, ή η λανθασμένη διαχείριση

της να του προκαλεί ανησυχία ή αμηχανία. Οποιαδήποτε απόκλιση, στην επεξεργασία των δεδομένων, σε σχέση με τα όρια και τους κανόνες που καθορίζονται από τις Πολιτικές Ιδιωτικότητας, αποτελεί δίχως αμφιβολία παραβίαση του απορρήτου και απώλεια της ιδιωτικότητας των συνδρομητών.

Πως επιτυγχάνεται όμως η διατήρηση των Δεδομένων Επικοινωνίας; Οι οργανισμοί που διατηρούν δεδομένα μπορούν να αρκεστούν μόνο στους θεσμούς και στην κρίση των συνδρομητών τους ώστε να προστατευτούν τα προσωπικά τους δεδομένα και κατ' επέκταση η Ιδιωτικότητα τους, ή χρειάζεται και αυτοί να έχουν αναπτύξει ένα πλαίσιο που θα συμπίπτει με τους θεσμικούς κανόνες και την υπάρχουσα τεχνολογία; Κάθε οργανισμός λοιπόν, πέρα από την σύμπτωση με τους νόμους, χρειάζεται να έχει αναπτύξει την δική του πολιτική διαχείρισης δεδομένων, για την οποία και οφείλει να ενημερώνει τους συνδρομητές του.

3.1 Διατήρηση Δεδομένων επικοινωνίας [01] [11]

Η ευρύτερη έννοια της Διατήρηση Δεδομένων, αφορά όλες εκείνες τις ενέργειες που χρειάζονται να γίνουν από τους παρόχους των δικτύων και υπηρεσιών ηλεκτρονικής επικοινωνίας, ώστε να εξασφαλίζεται ότι τα δεδομένα θα παραμένουν προσβάσιμα και ακέραια για όσο καιρό ορίζεται ή είναι αναγκαίο. Ειδικότερα η Διατήρηση Δεδομένων Επικοινωνίας αφορά ανάλογες ενέργειες που εξασφαλίζουν την ακεραιότητα και την προσβασιμότητα των δεδομένων που συναλλάσσονται ή μεταβιβάζονται μέσω υπηρεσιών τηλεφωνικής ή διαδικτυακής επικοινωνίας. Όπως προαναφέρθηκε σε προηγούμενο κεφάλαιο τα δεδομένα αυτά είναι συγκεκριμένα και συνθέτουν πληροφορίες σχετικά με το είδος, την θέση, την διάρκεια και τον εξοπλισμό της επικοινωνίας. Είναι απαραίτητο για κάθε πάροχο να διατηρεί και να επεξεργάζεται τέτοιου είδους δεδομένα των συνδρομητών του, για λόγους τεχνικής υποστήριξης αλλά και για την υποστήριξη διαδικασιών χρέωσης, για όσο χρονικό διάστημα χρειάζεται. Για παράδειγμα για την έκδοση λογαριασμών το τμήμα χρέωσης ενός παρόχου τηλεφωνίας χρειάζεται να έχει πρόσβαση στα αρχεία δεδομένων κλήσεων και ένας πάροχος υπηρεσιών Διαδικτύου χρειάζεται να διατηρεί δεδομένα κίνησης του ηλεκτρονικού ταχυδρομείου, για λόγους διασφάλισης και ελέγχου της ορθής λειτουργίας της υπηρεσίας.

Παρόλα αυτά ο βασικός σκοπός της διατήρησης των δεδομένων είναι η διευκόλυνση που μπορεί να προσφέρει στις αρχές μιας χώρας στην διερεύνηση και την εξιχνίαση πιθανών ερευνών, σε μελλοντικό χρόνο με το να διασφαλίζει ότι τα δεδομένα θα είναι ανά πάσα στιγμή διαθέσιμα για τέτοιου είδους διερεύνηση. Είναι αξιοσημείωτο το γεγονός ότι η διατήρηση των δεδομένων αποτελεί μια πολύπλοκη και υψηλού κόστους διαδικασία για τους οργανισμούς και τις εταιρείες επικοινωνιών που, ωστόσο η ανάγκη για ενίσχυση της ασφάλειας των πολιτών έκανε τους νομοθέτες να εστιάσουν την προσοχή τους σε αυτόν τον τομέα και να υποχρεώσουν τους παρόχους να συμμορφωθούν με τους θεσπιζόμενους κανόνες.

ΕΙΚΟΝΑ 3. 1: ΔΙΑΤΗΡΗΣΗ ΔΕΔΟΜΕΝΩΝ

3.2 Σκοπός της διατήρησης δεδομένων [01] [11] [12]

Η πρόσβαση στα δεδομένα των επικοινωνιών και το περιεχόμενό της ήταν πάντα ένας από τους πιο συχνά χρησιμοποιούμενους τρόπους για τη συλλογή πληροφοριών για τις ποινικές έρευνες και τις δραστηριότητες των υπηρεσιών πληροφοριών. Στην αναδυόμενη κοινωνία των πληροφοριών, με την αυξανόμενη κοινωνική αλληλεπίδραση, καθώς τις επιχειρηματικές δραστηριότητες να διεξάγονται μέσω δικτύων ηλεκτρονικών επικοινωνιών το αποτέλεσμα είναι τα παραδοσιακά διαδικαστικά μέτρα συλλογής πληροφοριών μέσω των αρχών επιβολής του νόμου, να πρέπει να προσαρμόζονται στη δυναμική φύση των δεδομένων και των ροών πληροφοριών και γενικότερα στο νέο τεχνολογικό και κοινωνικό περιβάλλον.

Στο πλαίσιο της πρόληψης, διερεύνησης, εξιχνίασης και δίωξης αξιόποινων πράξεων ή τρομοκρατικών επιθέσεων, που διαπράττονται ή υποστηρίζονται μέσω των δικτύων ηλεκτρονικών επικοινωνιών, τα δεδομένα που αφορούν την χρήση των υπηρεσιών της επικοινωνίας είναι πολύτιμα για τον εντοπισμό της πηγής και της διαδρομή των πληροφοριών, καθώς και για την συλλογή και την εξασφάλιση αποδεικτικών στοιχείων. Η διατήρηση των δεδομένων είναι ζωτικής σημασίας για την διερεύνηση σοβαρών εγκλημάτων και την ανάπτυξη της προληπτικής ασφάλειας των πληροφοριών για θέματα που αφορούν όχι μόνο την οργανωμένη εγκληματική δραστηριότητα, αλλά και την εθνική ασφάλεια.

3.3 Απειλές κατά την Διατήρηση Δεδομένων [01][13]

Στο 1ο κεφάλαιο αναλύθηκαν οι προκλήσεις κατά της Ιδιωτικότητας, που υπάρχουν ή έχουν δημιουργηθεί τα τελευταία χρόνια με την εξέλιξη της τεχνολογίας. Η διατήρηση δεδομένων είναι μια διαδικασία που αν και αναγκαία και εκ πρώτης όψης καλοπροαίρετη, μπορεί να οδηγήσει σε επιζήμιες συνέπειες που σχετίζονται άμεσα με τις προκλήσεις κατά της Ιδιωτικότητας που προαναφέρθηκαν. Είναι ευνόητο ότι από την στιγμή που τα δεδομένα επικοινωνίας σχετίζονται άμεσα με τον κάτοχό τους, την πηγή, τον χρόνο, τον χώρο αλλά και το περιεχόμενο της επικοινωνίας, θα αποτελούν και στόχο κακόβουλων ενεργειών – απειλών, με αποτελέσματα επιζήμια ως προς το απόρρητο της επικοινωνίας και την ιδιωτικότητα των ατόμων. Οι απειλές αυτές περιλαμβάνουν:

1. **Αποκάλυψη δεδομένων**

   Το απόρρητο του ατόμου κινδυνεύει να παραβιαστεί από ενέργειες που πιθανότατα να οδηγήσουν στην αποκάλυψη των δεδομένων που διατηρούνται από τους παρόχους, σε μη εξουσιοδοτημένους χρήστες. Οι χρήστες αυτοί μπορεί να είναι εξωτερικοί ή εσωτερικοί χρήστες του παρόχου οι οποίοι όμως δεν θα κατέχουν τα απαιτούμενα δικαιώματα πρόσβασης στα διατηρούμενα δεδομένα.

2. **Τροποποίηση δεδομένων**

   Η τροποποίηση δεδομένων αφορά περιπτώσεις όπου τα δεδομένα τροποποιούνται με τέτοιο τρόπο που να επηρεάζεται η ακεραιότητα τους, η αξία τους ή η αξιοπιστία τους. Αν χρησιμοποιηθεί καταχρηστικά και κακόβουλα με σκοπό την στρέβλωση της

πληροφορίας που συνθέτουν τα δεδομένα μπορεί να οδηγήσει σε ακόμα πιο ακραίες και επιβλαβείς συνέπειες. Για παράδειγμα κάποιος μπορεί να χρησιμοποιήσει τέτοιου είδους ενέργειες με σκοπό την διαστρέβλωση πληροφοριών που αφορούν το κοινωνικό προφίλ ενός ατόμου και κατ' επέκταση την δυσφήμιση του.

3. Μη εξουσιοδοτημένη πρόσβαση

Μια πιθανή πρόσβαση σε έναν λογαριασμό, χωρίς τα απαιτούμενα δικαιώματα είναι μια ενέργεια που μπορεί να προηγηθεί των δύο προηγούμενων που αναφέρθηκαν με σκοπό τα αποτελέσματα αυτών. Για παράδειγμα μία μη εξουσιοδοτημένη πρόσβαση σε ένα λογαριασμό μπορεί να επιφέρει και την αποκάλυψη στοιχείων του λογαριασμού ή και την στρέβλωση ή τροποποίηση των πληροφοριών του.

4. Παράνομη καταγραφή δεδομένων

Στις πολιτικές ιδιωτικότητας κάθε παρόχου ηλεκτρονικής επικοινωνίας ορίζονται κανόνες για τα είδη των δεδομένων που συλλέγονται, οι οποίοι οφείλουν να συμπίπτουν με το θεσμικό πλαίσιο κάθε χώρας. Η συλλογή ή καταγραφή δεδομένων που δεν περιέχονται σε αυτές τις πολιτικές ιδιωτικότητας αποτελεί παραβίαση της ιδιωτικότητας των συνδρομητών.

5. Παράνομη χρήση δεδομένων

Οποιαδήποτε χρήση των διατηρούμενων δεδομένων δεν συμπίπτει με τους συμφωνηθέντες, μεταξύ παρόχου-συνδρομητή, σκοπούς χρήσης που καθορίζονται στους κανόνες των πολιτικών ιδιωτικότητας, αποτελεί παράνομη χρήση. Για παράδειγμα μπορούν να χρησιμοποιηθούν τέτοιες πρακτικές για σκοπούς στοχευμένης διαφήμισης, σε περίπτωση σύνδεσης του συνδρομητή με τα δεδομένα που θα αφορούν τις αγοραστικές του συνήθειες.

6. Παρατεταμένη διατήρηση δεδομένων

Παρατεταμένη θεωρείται η διατήρηση δεδομένων που υπερβαίνει το χρονικό διάστημα το οποίο αναφέρεται στην πολιτική ιδιωτικότητας του παρόχου. Δεν μπορεί βέβαια να θεωρηθεί ως μια άμεση παραβίαση της ιδιωτικότητας, αλλά η υπέρβαση του χρονικού

ορίου διατήρησης αυξάνει το κίνδυνο τα διατηρούμενα δεδομένα να εκτεθούν σε οποιαδήποτε άλλη απειλή.

7. **Αδυναμία καταλογισμού ευθύνης**

Αφορά την αδυναμία σύνδεσης οποιωνδήποτε ενεργειών σε σχέση με τα δεδομένα με το άτομο που δικαιούται να έχει την πρόσβαση σε αυτά. Σε μια τέτοια περίπτωση που οποιαδήποτε ενέργεια δεν μπορεί να καταλογιστεί στον κάτοχο των δεδομένων, πιθανές συνέπειες είναι η κατάχρηση και παράνομη χρήση από τρίτους κακόβουλους χρήστες.

3.4 Αρχές για την Διατήρηση δεδομένων και την Προστασία της Ιδιωτικότητας [13]

Η διατήρηση δεδομένων όπως είδαμε ενέχει κινδύνους που αφορούν το απόρρητο της επικοινωνίας και της ιδιωτικότητας των ατόμων, για την αποτροπή των οποίων οι πάροχοι υπηρεσιών επικοινωνίας που είναι υπεύθυνοι για την διατήρηση και την επεξεργασία τους θα έπρεπε ακολουθούν κάποιες αρχές. Οι βασικές κοινωνικές αρχές που αφορούν τη διατήρηση δεδομένων επικοινωνίας είναι οι ακόλουθες:

- **Αρχή της αναλογικότητας**

Η ιδιωτικότητα των πολιτών θα επηρεάζεται από την διατήρηση δεδομένων σε ανάλογο βαθμό με την προστασία που παρέχεται στα δεδομένα του. Μέτρο της αναλογικότητας είναι ο σκοπός, που καθορίζει όχι μόνο την νομιμότητα του ποια δεδομένα και αν πρέπει να διατηρηθούν αλλά και το σε ποια έκταση αυτά θα διατηρηθούν. Η αρχή της αναλογικότητας αποτελεί σημαντικό δίχτυ ασφαλείας για την προστασία του δικαιώματος της ελευθερίας στην επικοινωνία.

- **Αρχή της αναγκαιότητας**

Τα διατηρούμενα δεδομένα θα είναι τα ελάχιστα δυνατά και θα διατηρούνται για τον ελάχιστο δυνατό χρόνο που απαιτείται για το σκοπό της προστασίας του κοινωνικού συνόλου.

- **Αρχή της αποτελεσματικότητας**

  Η διατήρηση των δεδομένων επικοινωνίας θα πρέπει να εφαρμόζεται ώστε να προστατεύει αποτελεσματικά το κοινωνικό σύνολο από εγκληματικές ενέργειες που διενεργούνται μέσω των ηλεκτρονικών επικοινωνιών.

3.4.1 Αρχές Διατήρησης δεδομένων του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης [13][14]

Η προστασία της Ιδιωτικότητας και η συμμόρφωση των παρόχων δεν θα μπορούσε να βασίζεται μόνο στις κοινωνικές αρχές. Αναπόφευκτα λοιπόν δημιουργήθηκε η ανάγκη να θεσπιστούν κοινοί κανόνες που να υιοθετηθούν από το σύνολο των οργανισμών και να λειτουργήσουν μετέπειτα ως σημείο έναρξης για την δημιουργία οποιουδήποτε νομικού πλαισίου. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) θέσπισε ένα πλαίσιο τέτοιων κανόνων που χρησιμοποιείται ως βάση για την δημιουργία πρακτικών προστασίας της Ιδιωτικότητας από τις ρυθμιστικές αρχές και κατευθυντήριο εργαλείο για την ανάπτυξη πολιτικών ασφαλείας από τους υπεύθυνους για την συλλογή και επεξεργασία των προσωπικών δεδομένων.

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) είναι ένας διεθνής οργανισμός που δημιουργήθηκε και αποτελείται από ένα σύνολο αναπτυγμένων χώρων που υποστηρίζουν τις αρχές της αντιπροσωπευτικής δημοκρατίας και της οικονομίας της ελεύθερης αγοράς. Σκοπός της δημιουργίας του πλαισίου των αρχών προστασίας της Ιδιωτικότητας που θεσπίστηκε το 1980 από τον Ο.Ο.Σ.Α ήταν η αποφυγή πολλών και διαφορετικών οδηγιών που πιθανότατα να δημιουργούνταν για την προστασία της Ιδιωτικότητας και θα είχαν αρνητικό αντίκτυπο για την οικονομική ανάπτυξη, αφού έτσι θα δημιουργούσαν εμπόδια στις εμπορικές και οικονομικές συναλλαγές μεταξύ των χωρών. Οι κατευθυντήριες αρχές όπως ορίζονται από τον οργανισμό είναι:

1. **Αρχή της περιορισμένης συλλογής δεδομένων**

   Η αρχή της περιορισμένης συλλογής των δεδομένων αφορά τα όρια που πρέπει να υπάρχουν στην συγκέντρωση και συλλογή δεδομένων, ενέργειες οι οποίες θα πρέπει να

γίνονται λαμβάνοντας υπόψη νόμιμες και δίκαιες διαδικασίες εφόσον φυσικά έχει προηγηθεί και η συγκατάθεση του ατόμου το οποίο αφορούν τα δεδομένα.

2. Αρχή της ποιότητας των δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή με τους σκοπούς για τους οποίους πρόκειται να χρησιμοποιηθούν και, στο βαθμό που απαιτείται για τους σκοπούς αυτούς, θα πρέπει να είναι ακριβή, πλήρη και να διατηρούνται ενημερωμένα.

3. Αρχή του προσδιορισμένου σκοπού

Οι σκοποί για τους οποίους συλλέγονται τα δεδομένα προσωπικού χαρακτήρα πρέπει να προσδιορίζονται το αργότερο κατά τη στιγμή της συλλογής των δεδομένων και η επακόλουθη χρήση τους να περιορίζεται στην εκπλήρωση των εν λόγω σκοπών ή άλλων οι όποιοι όμως θα είναι συμβατοί με τους σκοπούς αυτούς και θα διευκρινίζονται σε κάθε περίπτωση αλλαγής τους.

4. Αρχή της περιορισμένης χρήσης των δεδομένων

Η συγκεκριμένη αρχή αφορά τα όρια που πρέπει να προκαθορίζονται σχετικά με την έκταση της χρήσης τους. Σύμφωνα με αυτή τα προσωπικά δεδομένα δεν θα πρέπει να αποκαλύπτονται, να διατίθενται ή να χρησιμοποιούνται για σκοπούς άλλους από αυτούς που καθορίζονται εκτός των περιπτώσεων:

- που υπάρχει συγκατάθεση του υποκειμένου των δεδομένων
- που απαιτείται η χρήση τους από την δικαστική αρχή

5. Αρχή μέτρων προστασίας των δεδομένων

Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται από λογικές εγγυήσεις ασφάλειας έναντι των κινδύνων στους οποίους εκτίθενται. Δηλαδή θα πρέπει να υπάρχουν και να εφαρμόζονται μέτρα προστασίας που να μπορούν να διασφαλίσουν την ακεραιότητα των προσωπικών δεδομένων. Οι κίνδυνοι στους οποίους εκτίθενται μπορούν να είναι η απώλεια ή μη εξουσιοδοτημένη πρόσβαση, η καταστροφή, η παράνομη χρήση και η τροποποίηση ή αποκάλυψη των δεδομένων.

6. Αρχή της διαφάνειας

Θα πρέπει να υπάρχει μια γενική πολιτική διαφάνειας σχετικά με τις εξελίξεις, τις πρακτικές και τις πολιτικές που αφορούν τα προσωπικά δεδομένα. Θα πρέπει να υπάρχουν μέσα που να είναι άμεσα διαθέσιμα να αποδείξουν την ύπαρξη και τη φύση των δεδομένων προσωπικού χαρακτήρα, καθώς και τους κύριους στόχους της χρήσης τους, καθώς και την ταυτότητα και τη έδρα του υπεύθυνου επεξεργασίας των δεδομένων.

7. Αρχή της συμμετοχής του ατόμου

Αφορά τα δικαιώματα συμμετοχής που έχει το άτομο το οποίο αφορούν τα δεδομένα σε συγκεκριμένες ενέργειες που πρόκειται να συμβούν και που σχετίζονται με τα προσωπικά του δεδομένα. Ένα άτομο θα πρέπει να έχει το δικαίωμα:

- να αιτείται και να λαμβάνει τα δεδομένα του από τον υπεύθυνο επεξεργασίας δεδομένων, ή αλλιώς, να λαμβάνει επιβεβαίωση του κατά πόσον ο υπεύθυνος επεξεργασίας δεδομένων έχει δεδομένα που τον αφορούν ή όχι

- να του κοινοποιούνται τα δεδομένα που το αφορούν σε εύλογο χρονικό διάστημα, με μη υπερβολική επιπλέον χρέωση, αν υπάρχει, με λογικό τρόπο και σε μορφή που να είναι εύκολα κατανοητή από αυτό

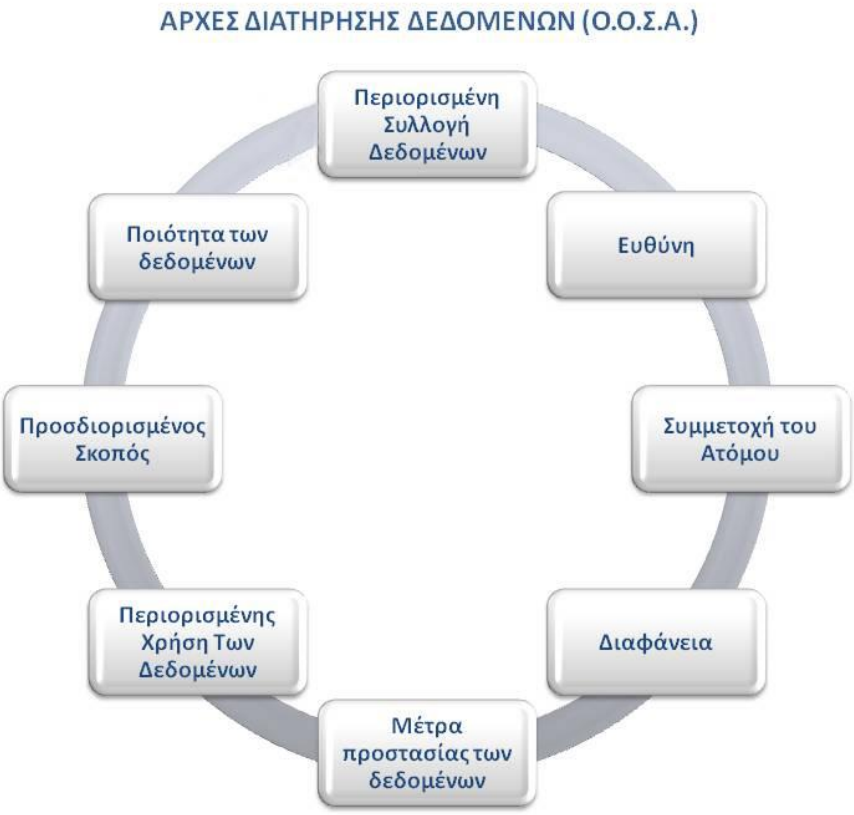
- αν έχει υποβληθεί αίτημα κοινοποίησης ή λήψης των στοιχείων, το οποίο όμως απορρίφθηκε, πρέπει να αναφέρονται οι λόγοι για τους οποίους απορρίφθηκε και να είναι σε θέση το άτομο να αμφισβητήσει την απόρριψη.

- να αμφισβητήσει τα δεδομένα που τον αφορούν και, αν η αμφισβήτηση είναι επιτυχής να μπορούν τα δεδομένα να διαγράφονται, να διορθώνονται, να συμπληρώνονται ή να τροποποιούνται.

8. Αρχή της ευθύνης

Η οντότητα που ενεργεί ως υπεύθυνος επεξεργασίας δεδομένων πρέπει να θεωρείται και υπεύθυνος για τη συμμόρφωση με τα μέτρα που δίνουν ισχύ στις προαναφερθείσες αρχές, άρα και υπόλογος για οποιαδήποτε αρνητική επίπτωση θα υποστούν τα δεδομένα λόγω της μη συμμόρφωσης σε αυτές.

Παρατηρούμε ότι όλες οι αρχές που θεσπίστηκαν λειτουργούν ως συμπληρωματικές μεταξύ τους δημιουργώντας ένα κύκλο αλληλοεξαρτούμενων κομματιών που έχει ως σκοπό την θωράκιση της Ιδιωτικότητας. Οποιαδήποτε λοιπόν παράλειψη ή παραβίαση σε μία από της αρχές, αυτόματα αποδυναμώνει το σύνολο των κανόνων και μοιραία θέτει σε κίνδυνο την Ιδιωτικότητα και την προστασία του απορρήτου.



ΣΧΗΜΑ 3. 1: ΑΡΧΕΣ ΔΙΑΤΗΡΗΣΗΣ ΔΕΔΟΜΕΝΩΝ ΤΟΥ Ο.Ο.Σ.Α.

3.5 Απαιτήσεις ασφαλείας κατά την Διατήρηση [15]

Προκειμένου να περιοριστούν οι απειλές ασφαλείας που απορρέουν από την διατήρηση των δεδομένων επικοινωνίας και να αφομοιωθούν οι αρχές διατήρησης, σημαντική προϋπόθεση είναι η ύπαρξη ορισμένων θεμελιωδών απαιτήσεων ασφαλείας που αφορούν τα προσωπικά δεδομένα. Κριτήρια δηλαδή τα οποία πρέπει να πληρούν τα δεδομένα, σύμφωνα με τα οποία θα μπορεί να χαρακτηριστεί ασφαλής η διαδικασία της διατήρησης τους. Οι απαιτήσεις αυτές περιλαμβάνουν τα ακόλουθα:

1. **Εμπιστευτικότητα των δεδομένων**

Τα δεδομένα που διατηρούνται, οφείλουν να προστατεύονται από τον υπεύθυνο επεξεργασίας τους, από πιθανή μη εξουσιοδοτημένη αποκάλυψη σε εσωτερικούς ή και εξωτερικούς χρήστες κατά την διάρκεια των διαδικασιών που περιλαμβάνει η επεξεργασία δεδομένων.

2. **Ακεραιότητα των δεδομένων**

Τα διατηρούμενα δεδομένα επικοινωνίας πρέπει να προστατεύονται από οποιαδήποτε τυχαία ή εσκεμμένη τροποποίηση τους από εσωτερικούς ή και εξωτερικούς χρήστες, ώστε να διασφαλίζεται η ακεραιότητα τους. Σε περίπτωση που η αποφυγή οποιασδήποτε πιθανής τροποποίησης είναι αδύνατη, οφείλεται τουλάχιστον να διασφαλίζεται η ανίχνευσή της.

3. **Ελεγχόμενη πρόσβαση**

Η πρόσβαση στα διατηρούμενα δεδομένα πρέπει να είναι εφικτή μόνο για χρήστες που διαθέτουν εξουσιοδοτημένη πρόσβαση. Η διαδικασία μπορεί να ελεγχθεί εφαρμόζοντας αυστηρές πολιτικές προστασίας.

4. **Καταγραφή, ανίχνευση και έλεγχος**

Για να επιτευχθεί η ανίχνευση οποιασδήποτε παράνομης πρόσβασης, τροποποίησης ή κατάχρησης των δεδομένων, θα πρέπει να καταγράφονται και να ελέγχονται με μη τροποποιήσιμο τρόπο οποιεσδήποτε κινήσεις πρόσβασης ή επεξεργασίας των δεδομένων.

5. **Ασφαλής καταστροφή των δεδομένων**

   Με το πέρας του νόμιμου προκαθορισμένου διαστήματος διατήρησης των δεδομένων, αυτά οφείλουν να καταστρέφονται με ασφαλή και μη αναστρέψιμο τρόπο ώστε να αποφεύγεται η οποιαδήποτε πιθανότητα κατάχρησης των δεδομένων και παραβίασης του απορρήτου και της Ιδιωτικότητας των συνδρομητών.

Γνωρίζοντας ότι όλοι οι πάροχοι ηλεκτρονικών επικοινωνιών δεν είναι δυνατό να κατέχουν κοινή αρχιτεκτονική δικτύων και ίδιο τεχνολογικό επίπεδο, η υλοποίηση των απαιτήσεων αυτών φαντάζει σύνθετη και μη εφικτή. Για αυτό τον λόγο απαιτείται η σχεδίαση ενός γενικού μοντέλου ασφάλειας των διατηρούμενων δεδομένων επικοινωνίας.

3.6 Γενικό μοντέλο Διατήρησης Δεδομένων [01] [15]

Η Διατήρηση Δεδομένων, όπως τελικά προκύπτει, για να λειτουργεί σωστά τόσο ως προς τον σκοπό της αλλά και ως προς την προστασία της Ιδιωτικότητας, περιλαμβάνει διαδικασίες που δεν αφορούν μοναδικά την μία διαφαινόμενη οντότητα, δηλαδή των πάροχο των υπηρεσιών επικοινωνίας, αλλά και οντότητες που θα ορίζουν τους κανόνες των διαδικασιών όπως επίσης και θα ελέγχουν την ορθότητα ή την τήρηση αυτών των κανόνων.

Προκύπτει συνεπώς ένα γενικό μοντέλο για την ασφαλή διατήρηση των προσωπικών δεδομένων επικοινωνίας που θα περιλαμβάνει τις οντότητες οι οποίες θα έχουν την ευθύνη τόσο για την υποστήριξη των τεχνολογιών προστασίας του απορρήτου και της Ιδιωτικότητας όσο και για την υποστήριξη και την συμμόρφωση με τις αρχές διατήρησης των δεδομένων. Είναι σημαντικό για την σωστή λειτουργία του μοντέλου να τηρούνται βασικοί κανόνες όπως η ύπαρξη διαχωρισμού των καθηκόντων (separation of duties) μεταξύ των οντοτήτων, όπως επίσης και ο διπλός έλεγχος (dual control) οποιωνδήποτε ενεργειών. Ακολουθεί ένα γενικό μοντέλο το οποίο περιλαμβάνει αυτές τις λογικές οντότητες:

- **Πάροχος Ηλεκτρονικών Επικοινωνιών (Communication Service Provider - CSP)**

  Η συγκεκριμένη οντότητα αναφέρεται στον πάροχο των υπηρεσιών της επικοινωνίας, ο οποίος μπορεί να είναι είτε πάροχος διαδικτυακών υπηρεσιών (Internet service Provider - ISP) είτε πάροχος τηλεπικοινωνιών (Telecommunication Service Provider - TCP). Ο

πάροχος ηλεκτρονικών επικοινωνιών είναι υπεύθυνος για την ανάπτυξη και την τήρηση πολιτικών προστασίας της ιδιωτικότητας που θα καθορίζουν τους κανόνες βάσει των οποίων θα πραγματοποιείται μια επικοινωνία μέσω των υπηρεσιών που αυτός προσφέρει.

Στο πλαίσιο των ευθυνών τους εντάσσονται η συλλογή και ασφαλής αποθήκευση των δεδομένων, η διατήρηση και η χρήση τους σύμφωνα με προκαθορισμένους κανόνες και για το επιτρεπόμενο χρονικό διάστημα καθώς και η ασφαλής καταστροφή τους.

- **Αρχή Επιβολής του Νόμου**

Αναφέρεται σε κάθε διωκτική αρχή που σκοπός της είναι ο εντοπισμός, η πρόληψη και η διερεύνηση αξιόποινων πράξεων ή εγκληματικών δραστηριοτήτων, και η οποία κατέχει το δικαίωμα αίτησης για παροχή πρόσβασης σε δεδομένα επικοινωνίας που διατηρούνται από τον πάροχο ηλεκτρονικής επικοινωνίας, με σκοπό τη δίωξη πιθανών τέτοιων δραστηριοτήτων.

- **Δικαστική Αρχή**

Η Δικαστική Αρχή είναι αρμόδια για την ανάθεση του δικαιώματος πρόσβασης σε διατηρούμενα προσωπικά δεδομένα. Η αρχή επιβολής του νόμου μπορεί να αποκτήσει πρόσβαση στα δεδομένα κάποιου, μέσω του παρόχου ηλεκτρονικών επικοινωνιών, μόνο μετά από την έκδοση δικαστικής εντολής της Δικαστικής αρχής και μόνο για το συγκεκριμένο συνδρομητή στον οποίο αναφέρεται η δικαστική εντολή.

- **Ρυθμιστική Αρχή**

Για την εξασφάλιση της διαφάνειας και της ορθότητας των διαδικασιών, συνυπάρχει άλλη μία οντότητα, αυτή της ρυθμιστικής αρχής. Η ρυθμιστική αρχή είναι μία ανεξάρτητη αρχή η οποία λειτουργεί ως έμπιστη τρίτη οντότητα και η αρμοδιότητά της είναι να ελέγχει κατά πόσο και εάν τηρούνται οι απαιτούμενες διαδικασίες που αφορούν την επεξεργασία των δεδομένων από του υπόλοιπους εμπλεκόμενους φορείς.

3.6.1 Διαδικασία λειτουργίας του μοντέλου [01] [15]

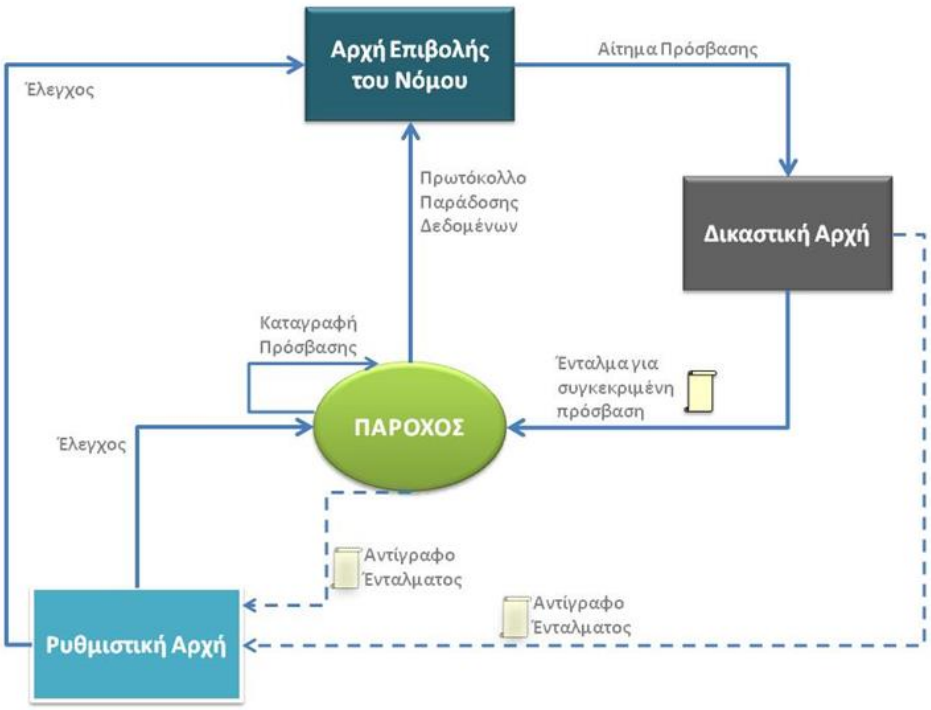
Στο σχήμα 3.2 παρουσιάζεται συνοπτικά ο τρόπος λειτουργίας των αρχών που συνθέτουν το γενικό μοντέλου που περιγράφηκε, και οι διαδικασίες που πρέπει να ενεργοποιηθούν για μια περίπτωση άρσης του απορρήτου των επικοινωνιών.

1. Αρχικά προβλέπεται η αίτηση προς την Δικαστική Αρχή για την απόκτηση του δικαιώματος της πρόσβασης στα προσωπικά δεδομένα συγκεκριμένου προσώπου. Το αίτημα υποβάλλεται από την αρχή της Επιβολής του Νόμου, συνοψίζοντας όλα τα απαραίτητα στοιχεία που να αποδεικνύουν μη σύννομες ενέργειες του κατόχου των δεδομένων.

2. Η Δικαστική αρχή σε περίπτωση που η αίτηση για άρση ευσταθεί, αποστέλλει ένταλμα στον πάροχο τον Ηλεκτρονικών επικοινωνιών όπου του γνωστοποιεί την απόφαση για άρση του απορρήτου ενός συγκεκριμένου λογαριασμού.

3. Η Ρυθμιστική αρχή λειτουργεί ως επιτηρητής της διαδικασίας καθώς λαμβάνει την ίδια στιγμή, ένα αντίγραφο του εντάλματος και από την Δικαστική αρχή όπως επίσης και από τον πάροχο.

4. Εφόσον όλες οι διαδικασίες ακολουθήθηκαν μέσα στα πλαίσια των κανονισμών και των αρχών προστασίας της Ιδιωτικότητας και του απορρήτου, ο πάροχος οφείλει να άρει το απόρρητο της επικοινωνίας και να παραδώσει τα ζητούμενα δεδομένα στην Αρχή της Επιβολής του Νόμου



ΣΧΗΜΑ 3. 2: ΓΕΝΙΚΟ ΜΟΝΤΕΛΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΗ ΔΙΑΤΗΡΗΣΗ ΔΕΔΟΜΕΝΩΝ

3.7 Στρατηγικές Διατήρησης [16]

Η διατήρηση δεδομένων προϋποθέτει την ανάπτυξη στρατηγικών από την πλευρά των παρόχων των ηλεκτρονικών υπηρεσιών ώστε να διασφαλίζεται η ακεραιότητα και η χρηστικότητα των δεδομένων για όσο καιρό αυτά διατηρούνται στα συστήματά τους. Στρατηγικές διατήρησης δεδομένων αποτελούν:

- **Αντιγραφή της ροής δεδομένων (Bitstream copying)**

Είναι ευρύτερα γνωστή ως "δημιουργία αντιγράφων ασφαλείας" και αναφέρεται στη διαδικασία της λήψης αντίγραφου ενός ψηφιακού αντικειμένου. Η λήψη αντιγράφων ασφαλείας είναι απαραίτητη σε κάθε σύστημα διατήρησης δεδομένων, ώστε να προστατεύει τα δεδομένα από οποιαδήποτε δυσλειτουργία ή φυσική καταστροφή και συνηθίζεται τα αντίγραφα να διατηρούνται σε διαφορετικό και απομακρυσμένο σύστημα ώστε να αποφεύγεται η συνύπαρξη τους στο ίδιο καταστροφικό γεγονός.

- **Ανανέωση (Refreshing)**

Η διαδικασία της ανανέωση αφορά την επανάληψη της αντιγραφής των δεδομένων από ένα αποθηκευτικό μέσο σε ένα άλλο ίδιου τύπου ώστε να διασφαλίζεται η ύπαρξη του ψηφιακού αντικειμένου ανεξάρτητα από την φθορά των μέσων.

- **Ανθεκτικότητα των μέσων (Durable/Persistent Media)**

Η χρήση τεχνολογίας και αποθηκευτικών μέσων με μεγαλύτερη ανθεκτικότητα και αντοχή στον χρόνο και στην αναπόφευκτη φθορά, ενδέχεται να μειώσει την ανάγκη για συχνή ανανέωση. Ωστόσο δεν μπορεί να προστατεύσει από ενδεχόμενες καταστροφές και δυσλειτουργίες του συστήματος.

- **Διατήρηση της Τεχνολογίας (Technology Preservation)**

Βασίζεται στη διατήρηση του τεχνικού περιβάλλοντος και εξοπλισμού, συμπεριλαμβανομένων των λειτουργικών συστημάτων και του λογισμικού εφαρμογών. Είναι περισσότερο μια στρατηγική πρόληψης και αποκατάστασης των καταστροφών και ζημιών που πιθανότατα κάποια στιγμή θα επηρεάσουν ένα σύστημα. Αν και η διατήρηση του τεχνολογικού εξοπλισμού

είναι αναγκαία, δεν μπορεί να είναι μόνιμη καθώς ένας οργανισμός δεν μπορεί να λειτουργεί και να διατηρεί απαρχαιωμένη τεχνολογία.

- **Ψηφιακή Αρχαιολογία (Digital Archaeology)**

Περιλαμβάνει τις μεθόδους και τις διαδικασίες για τη διάσωση περιεχομένου από κατεστραμμένα ή απαρχαιωμένα μέσα όπως και από βλάβες υλικού και λογισμικού. Ψηφιακή αρχαιολογία είναι μια στρατηγική ανάκαμψης έκτακτης ανάγκης και συνήθως περιλαμβάνει εξειδικευμένες τεχνικές για την ανάκτηση των δεδομένων από μέσα που έχουν καταστεί δυσανάγνωστα, λόγω βλάβης ή αστοχίας υλικού.

- **Αναλογικά αντίγραφα ασφαλείας (Analog Backups)**

Συνδυάζει την μετατροπή ψηφιακών αντικειμένων σε αναλογική μορφή με την χρήση ανθεκτικών αναλογικών μέσων. Ένα αναλογικό αντίγραφο μπορεί να διατηρήσει το περιεχόμενο του και όντας πιο ανθεκτικό να το προστατεύσει από την απαρχαίωση, θυσιάζοντας εντούτοις τα ψηφιακά πλεονεκτήματα και για τον λόγο αυτό χρησιμοποιείται για συγκεκριμένες περιπτώσεις δεδομένων.

- **Μετανάστευση (Migration)**

Πρόκειται για την αντιγραφή ή την μετατροπή των δεδομένων από μια τεχνολογία, υλικού ή λογισμικού, σε μία άλλη, διατηρώντας όμως τα κύρια χαρακτηριστικά των δεδομένων. Η μετανάστευση είναι ευρύτερη και πιο πλούσια έννοια από την ανανέωση καθώς αποτελεί ένα σύνολο οργανωμένων καθηκόντων που έχουν σχεδιαστεί για να επιτευχθεί η περιοδική μεταφορά των ψηφιακών υλικών από ένα υλικό ή λογισμικο σε ένα άλλο, ή από μια γενιά υπολογιστικής τεχνολογίας στην επόμενη της.

- **Αναπαραγωγή (Replication)**

Στρατηγική που σχετίζεται άμεσα με την λήψη αντιγράφων ασφαλείας αλλά και την διαδικασία της μετανάστευσης των ψηφιακών πληροφοριών με την διαφορά ότι προϋποθέτει την αναπαραγωγή των ψηφιακών αντικειμένων σε πολλαπλά αντίγραφα και τοποθεσίες αποθήκευσες ώστε να διασφαλίζεται η χρηστικότητα και η λειτουργικότητα τους για μεγάλα χρονικά διαστήματα.

- **Εμπιστοσύνη στους κανόνες προτυποποίησης (Reliance on Standards)**

Αφορά την εξάρτηση του λογισμικού από τους κανόνες προτυποποίησης. Η συμπόρευση του λογισμικού των οργανισμών με τα πρότυπα της τεχνολογίας εξασφαλίζει την συμβατότητα των συστημάτων και την ελαχιστοποίηση των σφαλμάτων.

- **Ομαλοποίηση (Normalization)**

Στρατηγική κατά την οποία τα ψηφιακά αρχεία που αποθηκεύονται στα συστήματα ενός οργανισμού και είναι παρόμοιας μορφής, μπορούν να μετατραπούν σε συγκεκριμένο τύπο αρχείων που να διατηρεί τα κύρια χαρακτηριστικά από όλες τις μορφές των αρχείων.

- **Κανονικοποίηση (Canonicalization)**

Τεχνική που έχει σχεδιαστεί για να επιτρέπει τον προσδιορισμό του αν τα ουσιώδη χαρακτηριστικά ενός εγγράφου παρέμειναν ανέπαφα κατά την μετατροπή από μια μορφή σε μια άλλη. Βασίζεται στη δημιουργία μιας αναπαράστασης ενός ψηφιακού αντικειμένου που εμπεριέχει όλες τις βασικές πτυχές του πρωτοτύπου. Η αναπαράσταση θα μπορούσε να χρησιμοποιηθεί για να επαληθεύσει αλγοριθμικά ότι ένα αρχείο που έχει μετατραπεί, δεν έχει χάσει την ουσία του.

- **Εξομοίωση (Emulation)**

Η εξομοίωση συνδυάζει λογισμικό και υλικό ενός οργανισμού για να αναπαράγει τα βασικά σχεδιαστικά και αποδοτικά χαρακτηριστικά ενός διαφορετικού τεχνολογικά συστήματος ώστε εφαρμογές και μέσα που έχουν σχεδιαστεί για αυτό το σύστημα, να μπορούν να προσπελαστούν και να χρησιμοποιηθούν και από το σύστημα του οργανισμού. Η διαδικασία απαιτεί την δημιουργία εξομοιωτών, δηλαδή εφαρμογών που να μπορούν να μεταφράσουν κώδικα διαφορετικού συστήματος και να τον αποδώσουν στο σύστημα στο οποίο χρησιμοποιούνται.

- **Ενθυλάκωση (Encapsulation)**

Διαδικασία κατά την οποία ομαδοποιούνται ψηφιακά αρχεία μαζί με τα μετα-δεδομένα (metadata) τους τα οποία είναι απαραίτητα για την παροχή πρόσβασης στο αρχείο. Μορφές των μεταδεδομένων που μπορούν να ενσωματωθούν σε ένα ψηφιακό αντικείμενο μπορεί να

αφορούν την αναφορά, την προέλευση, την κατάσταση του αρχείου ή και πληροφορίες για το περιεχόμενο του αρχείου.

Κεφάλαιο 4
Τεχνολογίες Προστασίας της Ιδιωτικότητας των Επικοινωνιών

« Θα πρέπει να αγωνιστείς για τη προστασία της ιδιωτικότητας σου, ειδάλλως την χάνεις »

Eric Schmidt

Δεδομένου ότι τα δίκτυα επικοινωνιών και ιδιαίτερα το Διαδίκτυο, αποτελούν έναν κοινόχρηστο πόρο, χρησιμοποιούμενο από πολλές και διαφορετικές εφαρμογές αλλά και πολλές και διαφορετικές οντότητες, είναι λογικό η λειτουργία τους να επηρεάζεται από αλληλοσυγκρουόμενα συμφέροντα. Συμφέροντα τα οποία έχουν άμεσα αρνητικές επιπτώσεις στην ασφάλεια των δεδομένων των οποίων διαβιβάζονται μέσω των τεχνολογιών και των μέσων δικτύωσης. Παρότι το Διαδίκτυο αρχικά σχεδιάστηκε ως μια τεχνολογία που θα μπορούσε να αντέξει το βάρος πιθανών φυσικών καταστροφών, δεν είχε προβλεφτεί καμία από τις σημερινές απειλές κατά της ασφάλειας των δεδομένων που διαβιβάζονται δια μέσω αυτού. Αν τα δεδομένα που διακινούνται μέσω των δικτύων διατρέχουν κίνδυνο και απειλείται η

ακεραιότητα τους, τότε κανείς αντιλαμβάνεται ότι ο κίνδυνος αυτός πολλαπλασιάζεται όσο αυτά διατηρούνται στα πληροφοριακά συστήματα που χρησιμοποιούνται για την εξυπηρέτηση της Δικτύωσης.

Εντωμεταξύ δεν είναι λίγα τα περιστατικά που έχουν αποκαλυφθεί τα τελευταία χρόνια με παραβιάσεις στα συστήματα μεγάλων οργανισμών ή ακόμα και μαζικές παρακολουθήσεις πολιτών από κυβερνήσεις στο όνομα τις εθνικής ασφάλειας. Σοβαρές απειλές όπως υποκλοπή επικοινωνιών, η παραποίηση δεδομένων, η κατασκόπευση, η άρνηση υπηρεσίας ή ακόμα και η αποκάλυψη απλών πληροφοριών κινδυνεύουν να καταστρέψουν την ιδέα της δικτύωσης καθώς έχουν άμεσες συνέπειες τόσο στην συμπεριφορά των χρηστών ως προς την αντιμετώπιση των ηλεκτρονικών υπηρεσιών όσο και στην διεθνή οικονομία. Οι χρήστες αισθάνονται εκτεθειμένοι και ανασφαλείς, αφού νιώθουν ότι οποιαδήποτε κίνηση τους μπορεί να καταγραφεί και να παρακολουθηθεί. Ως άμεση συνέπεια αυτών, παρουσιάζεται η έλλειψη ενδιαφέροντος των χρηστών για τις νέες τεχνολογίες ηλεκτρονικής επικοινωνίας.

Πως όμως μπορεί κάποιος να «κινηθεί» με ασφάλεια σε αυτόν τον άγνωστο κόσμο της Πληροφορίας; Όπως και για κάθε πρόβλημα υπάρχει μια λύση ή έστω προληπτική αντιμετώπιση έτσι και για τους κινδύνους που παρουσιάζονται κατά την χρήση των ηλεκτρονικών επικοινωνιών έχουν αναπτυχθεί διάφοροι μηχανισμοί ασφαλείας ή μέτρα αντιμετώπισης που είναι σε θέση να προσφέρουν ένα επίπεδο προστασίας της ιδιωτικότητας του ατόμου και του απορρήτου του. Μηχανισμοί όπως η κρυπτογραφία, οι αντιπυρικές ζώνες, η ελεγχόμενη πρόσβαση, η καταγραφή ενεργειών, η ανάπτυξη γλωσσών πολιτικών ιδιωτικότητας και αρκετοί άλλοι που ανήκουν στις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δημιουργήθηκαν με αυτό το σκοπό.

4.1 Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας [01][17] [18]

Οι Τεχνολογίες Ενίσχυσης Της Ιδιωτικότητας (PETs - Privacy Enhancing Technologies) είναι ένας γενικός όρος για ένα σύνολο εργαλείων πληροφορικής, εφαρμογών και μηχανισμών που όταν ενσωματώνονται σε δικτυακές υπηρεσίες ή εφαρμογές, ή όταν χρησιμοποιούνται σε συνδυασμό με αυτές, επιτρέπουν στους συνδεδεμένους χρήστες ή συνδρομητές να προστατεύουν τις προσωπικές πληροφορίες και τα δεδομένα που παρέχονται και διαχειρίζονται από τις εν λόγω υπηρεσίες ή εφαρμογές κατά την διάρκεια της χρήσης τους. Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (privacy enhancing technologies) αναπτύχθηκαν προκειμένου να ενισχύσουν την

προστασία της ιδιωτικής ζωής στα σύγχρονα πληροφοριακά και επικοινωνιακά συστήματα, τα οποία υποστηρίζουν υπηρεσίες ή υποδομές, περιορίζοντας τη συλλογή προσωπικών δεδομένων ή εμποδίζοντας τη μη αναγκαία ή ανεπιθύμητη επεξεργασία τους, διατηρώντας ταυτόχρονα τη λειτουργικότητα των συστημάτων.

Σε ένα περιβάλλον ηλεκτρονικής επικοινωνίας όπου μηνύματα συναλλάσσονται μεταξύ δύο πηγών επικοινωνίας οι Τεχνολογίες Ενίσχυσης Της Ιδιωτικότητας πρέπει να εξασφαλίζουν τέτοιο επίπεδο προστασίας ώστε να πληρούνται τα ακόλουθα κριτήρια:

- Η ανωνυμία ή οποία θα εξασφαλίζει ότι ένας χρήστης μπορεί να χρησιμοποιήσει έναν πόρο ή μια υπηρεσία, χωρίς να αποκαλύπτεται η ταυτότητα του.

- Ψευδωνυμία εξασφαλίζει ότι ο χρήστης μπορεί να χρησιμοποιήσει έναν πόρο ή μια υπηρεσία, χωρίς να αποκαλύπτει η ταυτότητα του, αλλά να εξακολουθεί να να είναι υπόλογος για την εν λόγω χρήση.

- Μη-συνδεσιμότητα εξασφαλίζει ότι ο χρήστης μπορεί να κάνει πολλαπλές χρήσεις των πόρων ή των υπηρεσιών, χωρίς άλλοι να είναι σε θέση να συνδέσουν αυτές τις χρήσεις μεταξύ τους.

- Μη-ανιχνευσιμότητα

- Μη-Παρατηρισιμότητα εξασφαλίζει ότι ο χρήστης μπορεί να χρησιμοποιήσει έναν πόρο ή μια υπηρεσία, χωρίς τρίτοι να είναι σε θέση να παρατηρήσουν ότι ο πόρος ή υπηρεσία αυτή χρησιμοποιείται.

Η ανάπτυξη τεχνολογιών ενίσχυσης της ιδιωτικότητας έχει τους εξής στόχους [17] [19]:

- Αύξηση του έλεγχου των προσωπικών δεδομένων που διακινούνται, αποθηκεύονται και διαχειρίζονται δια μέσου του Διαδικτύου

- ελαχιστοποίηση των δεδομένων, δηλαδή ελαχιστοποίηση των προσωπικών δεδομένων που συλλέγονται και χρησιμοποιούνται από τους παρόχους υπηρεσιών

- επιλογή του βαθμού της ανωνυμίας

- επιλογή του βαθμού της μη συνδεσιμότητας

- επίτευξη συναίνεσης για την παροχή προσωπικών δεδομένων

- παροχή της δυνατότητας διαπραγμάτευσης των όρων και των προϋποθέσεων βάσει των οποίων θα παρέχονται προσωπικά δεδομένα

- παροχή της δυνατότητας απομακρυσμένου ελέγχου αυτών των όρων και προϋποθέσεων

- παροχή της δυνατότητας παρακολούθησης του ιστορικού των προσωπικών δεδομένων διευκόλυνση της χρήσης των νομικών δικαιωμάτων για τα προσωπικά δεδομένα

4.2 Γλώσσες πολιτικών Ιδιωτικότητας [01]

Οι Γλώσσες Πολιτικών Ιδιωτικότητας (Privacy Policy Languages) είναι μια γνωστή προσέγγιση για την προστασία της ασφάλειας και της ιδιωτικής ζωής των χρηστών, καθώς και για την ευέλικτη διαχείριση εμπιστοσύνης σε κατανεμημένα περιβάλλοντα. Αποτελούν ένα σημαντικό εργαλείο για τους οργανισμούς ώστε να αυξήσουν την επιχειρηματικότητα τους, χτίζοντας θεμέλια εμπιστοσύνης με τους καταναλωτές τους. Ουσιαστικά πρόκειται για πρακτικές προστασίας της ιδιωτικότητας που παρουσιάζονται ως πολιτικές, σε μορφή αναγνώσιμη και κατανοητή με σκοπό να βοηθήσουν τους χρήστες να κάνουν συνειδητές αποφάσεις κατά την χρήση των ηλεκτρονικών υπηρεσιών. Η δημιουργία τους, η επιβολή τους και η εποπτεία τους είναι ενέργειες που εμπίπτουν στις αρμοδιότητες των παρόχων των ηλεκτρονικών υπηρεσιών.

Οι γλώσσες πολιτικών ιδιωτικότητας μπορεί να ταξινομηθούν σε τρεις βασικές κατηγορίες ανάλογα με το σκοπό της υλοποίησης αλλά και της χρήσης κάθε γλώσσας. Μια κατηγορία αφορά τις Γλώσσες Προτιμήσεων οι οποίες δίνουν τη δυνατότητα έκφρασης συγκεκριμένων προτιμήσεων από μέρους των συμβαλλόμενων μερών. Ακολουθούν οι Γλώσσες Πολιτικών Ιδιωτικότητας Επιχειρήσεων όπου ανήκουν γλώσσες που χρησιμοποιούνται για τον καθορισμό των πολιτικών ιδιωτικότητας ενός παρόχου, περιγράφοντας το επίπεδο πρόσβασης στα δεδομένα που έχουν συλλεγεί, ενώ τα τελευταία χρόνια έχουν προταθεί και κάποιες γλώσσες σχετικές με Υπηρεσίες Ιστού.

4.2.1 Γλώσσες Προτιμήσεων [01]

Η αποτελεσματικότητα των Γλωσσών προτιμήσεων βασίζεται στην παροχή δυνατότητας ορισμού συγκεκριμένων ρυθμίσεων για την προστασία των πληροφοριών μεταξύ δύο συμβαλλόμενων μερών, από τα ίδια τα μέλη. Αντιπροσωπευτικό παράδειγμα αποτελεί η γλώσσα Platform for Privacy Preferences 1.0 (P3P). Η P3P έχει καθιερωθεί ως το πρότυπο για την έκφραση του είδους των δεδομένων αλλά και του σκοπού συλλογής των δεδομένων από μέρους των ιστοχώρων. Η μέθοδος κωδικοποίησης των πρακτικών συλλογής και χρήσης των δεδομένων που παρέχεται είναι σε μορφή XML, στοιχείο που την καθιστά αυτόματα ανεξάρτητη πλατφόρμας και υπολογιστικού συστήματος. Στο πλαίσιο της προδιαγραφής P3P μέσω του καθορισμού της γλώσσας προτιμήσεων P3P Preference Exchange Language (APPEL) παρέχεται η δυνατότητα και στο χρήστη να εκφράσει τις προτιμήσεις ιδιωτικότητάς του.

- **Στόχοι [01][20]**

Η χρήση της πλατφόρμας P3P στοχεύει πρωτίστως στην παροχή δυνατότητας στους ιστοχώρους να παρουσιάσουν τις πρακτικές συλλογής των δεδομένων τους σε μια τυποποιημένη, υπολογιστικά αναγνώσιμη και εύκολα εντοπίσιμη μορφή. Επιπλέον, επιτρέπει στους χρήστες του διαδικτύου να καταλάβουν τι είδους δεδομένα θα συλλέγονται από τους ιστοχώρους τους οποίους επισκέπτονται, πώς αυτά θα χρησιμοποιηθούν, καθώς και ποια από αυτές τις ενέργειες συλλογής ή χρήσης μπορούν να απορρίψουν (opt-out) ή να αποδεχτούν (opt-in).

- **Λειτουργία [01][20]**

Η P3P έχει σχεδιαστεί για να ενημερώνονται οι χρήστες σχετικά με τις πολιτικές απορρήτου των υπηρεσιών (ιστοσελίδες και εφαρμογές). Όταν ένας «πελάτης» (client) συμβατός με P3P ζητά έναν πόρο, μια υπηρεσία στέλνει ένα σύνδεσμο σε μια αναγνώσιμη από μηχανή πολιτική προστασίας της ιδιωτικότητας στην οποία ο υπεύθυνος πάροχος της υπηρεσίας δηλώνει τις πρακτικές προστασίας. Στην πολιτική προστασίας καθορίζονται τα στοιχεία δεδομένων που ο πάροχος προτίθεται να συλλέξει, ο τρόπος με τον οποίο θα χρησιμοποιηθούν, αν και σε ποιους τρίτους θα διαμοιραστούν όπως επίσης και για πόσο καιρό θα διατηρηθούν.

Οι πολιτικές παρόχου εκφράζονται σε γλώσσα XML (eXtensible Markup Language) και αναλύονται αυτόματα από τους «διαχειριστές του χρήστη» (user agents), δηλαδή από

εφαρμογές όπως φυλλομετρητές, βοηθητικά προγράμματα φυλλομετρητή (browser plug-ins) και διακομιστές μεσολάβησης (proxys), και συγκρίνονται με τις προτιμήσεις που καθορίζονται από τον χρήστη οι οποίες εκφράζονται στην γλώσσα APPEL που ενσωματώνεται στο πλαίσιο P3P για την κωδικοποίηση των προτιμήσεων απορρήτου του χρήστη, (P3P Preference Exchange Language (APPEL)). Ανάλογα με αυτές τις προτιμήσεις, ένας «διαχειριστής χρήστη» μπορεί στη συνέχεια να εμφανίσει πληροφορίες για το χρήστη, να δημιουργήσει προτροπές, ή να λάβει οποιαδήποτε άλλα μέτρα καθορίζονται.

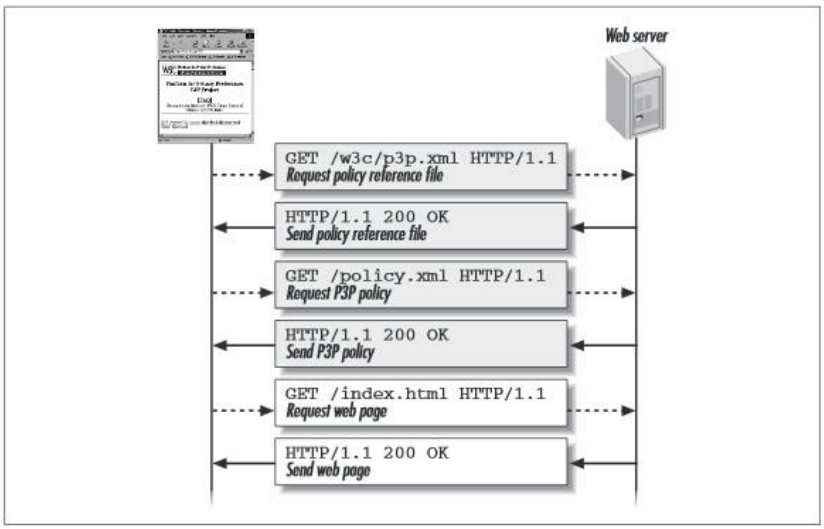
Μια βασική αλληλεπίδραση σε πλαίσιο P3P θα μπορούσε να είναι η ακόλουθη:

- Ο «διαχειριστής χρήστη» ζητά μια ιστοσελίδα από μια υπηρεσία.

- Η υπηρεσία απαντά στέλνοντας μια αναφορά σε μια ένα αρχείο πολιτικής P3P στην κεφαλίδα απόκρισης HTTP. Στο αρχείο πολιτικής παραθέτονται τμήματα μιας ιστοσελίδας και τα URIs (Uniform Resource Locator) των αντίστοιχων πολιτικών ιδιωτικότητας. Μια πολιτική αποτελείται από μία ή περισσότερες δηλώσεις σχετικά με τις πρακτικές προστασίας της ιδιωτικότητας μιας υπηρεσίας.

- «Ο διαχειριστής χρήστη» ανακτά το αρχείο πολιτικής και καθορίζει το URI της πολιτικής που ισχύει για τη σελίδα που ζητήθηκε από τον «πελάτη».

- Ο «διαχειριστής χρήστη», αξιολογεί την πολιτική σύμφωνα με το σύνολο κανόνων του χρήστη και καθορίζει ποια μέτρα πρέπει να ληφθούν.



ΣΧΗΜΑ 4. 1: ΛΕΙΤΟΥΡΓΙΑ P3P

4.2.2 Γλώσσες Πολιτικών Ιδιωτικότητας Επιχειρήσεων [01]

Οι γλώσσες που περιλαμβάνονται στην κατηγορία, χρησιμοποιούνται κυρίως για τον καθορισμό των πολιτικών ιδιωτικότητας ενός παρόχου ηλεκτρονικών υπηρεσιών. Έχουν διαδοθεί περισσότερο η Enterprise Privacy Authorization Language (EPAL) γλώσσα της εταιρείας IBM και η eXtensible Access Control Markup Language (XACML) γλώσσα του οργανισμού προτυποποίησης OASIS. Όπως και η P3P, και οι δύο αυτές γλώσσες είναι ανεξάρτητες πλατφόρμας, στοιχείο που οφείλεται στην αναπαράστασή τους μέσω της XML. Η XACML αποτελεί ένα πρότυπο του οργανισμού OASIS και η χρήση της συνοψίζεται σε δύο βασικές κατευθύνσεις: ως μία γλώσσα πολιτικών και ως μια γλώσσα ελέγχου πρόσβασης αίτησης/απόκρισης. Η EPAL αποτελεί μια γλώσσα που αναπτύχθηκε από την IBM και έχει προταθεί για προτυποποίηση στον W3C από το Νοέμβριο του 2003.

- **Στόχοι**

Η EPAL[22] στοχεύει στην παροχή της δυνατότητας στις εταιρείες και οργανισμούς να κωδικοποιήσουν τις πολιτικές και τις πρακτικές με τις οποίες χειρίζονται τα προσωπικά δεδομένα και στην αφομοίωση της από συστήματα που προστατεύουν την Ιδιωτικότητα.

Η XACML[23] στην ουσία αναπτύχθηκε για να προσφέρει έλεγχο επιχειρηματικής πρόσβασης διευθετώντας ζητήματα τα οποία προέκυπταν στα διανεμημένα συστήματα. Το μοντέλο XACML υποστηρίζει και ενθαρρύνει το διαχωρισμό της απόφασης πρόσβασης από τον λόγο χρήσης.

- **Λειτουργία [01][24]**

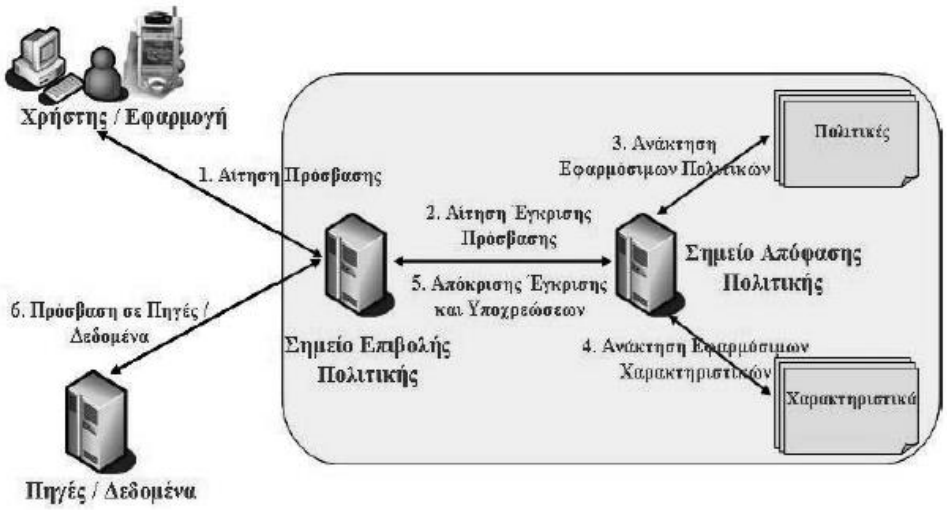
Οι γλώσσες XACML και EPAL χρησιμοποιούν το ίδιο μοντέλο επιβολής πολιτικών που ακολουθεί:

- ένας χρήστης/εφαρμογή επιδιώκει να αποκτήσει πρόσβαση σε ένα σύνολο πηγών/δεδομένων, υποβάλλοντας ένα αίτημα στο Σημείο Επιβολής Πολιτικής (Policy Enforcement Point (PEP)).

- Το συστατικό αυτό διαμορφώνει μια αίτηση που περιέχει τα χαρακτηριστικά της αίτησης του χρήστη/εφαρμογής. Τα χαρακτηριστικά που περιέχονται στη νέα αίτηση είναι η ταυτότητα του αιτούντος, η πηγή για την οποία ζητείται η πρόσβαση, η ενέργεια που θα εκτελεστεί στην πηγή και ο σκοπός πρόσβασης. Η αίτηση έγκρισης της πρόσβασης υποβάλλεται στο Σημείο Απόφασης Πολιτικής (Policy Decision Point (PDP)).

- Το συστατικό αυτό, μόλις λάβει την αίτηση, ανακτά τις εφαρμόσιμες πολιτικές, μαζί με τα πρόσθετα στοιχεία που απαιτούνται για την αξιολόγηση των πολιτικών και αξιολογεί τις πολιτικές, ώστε να καθορίσει την απόφαση έγκρισης.

- Η ληφθείσα απόφαση επιστρέφεται στο Σημείο Επιβολής Πολιτικής, το οποίο επιτρέπει ή απαγορεύει την πρόσβαση στο χρήστη/εφαρμογή.



ΣΧΗΜΑ 4. 2: ΜΟΝΤΕΛΟ ΛΕΙΤΟΥΡΓΙΑΣ EPAL ΚΑΙ XACML

4.2.3 Γλώσσες Ιδιωτικότητας Υπηρεσιών Ιστού[01]

Οι Υπηρεσίες Ιστού προκειμένου να επικοινωνήσουν μεταξύ τους απαιτούν επιπλέον πληροφορίες σχετικά με θέματα όπως ο καθορισμός των απαιτούμενων μηχανισμών

εμπιστευτικότητας και των απαραίτητων στοιχείων αυθεντικοποίησης, ποιότητας υπηρεσιών και ιδιωτικότητας. Οι γλώσσες ιδιωτικότητας των Υπηρεσιών Ιστού στοχεύουν στην περιγραφή του συνόλου των στοιχείων των Υπηρεσιών Ιστού που απαρτίζουν τα μη λειτουργικά χαρακτηριστικά μιας υπηρεσίας, διευκολύνοντας με αυτό τον τρόπο τη διαλειτουργικότητα, την προσβασιμότητα και την αξιοπιστία των Υπηρεσιών.

Οι πιο ευρέως γνωστές και χρησιμοποιούμενες γλώσσες έχουν κοινή δόμηση όπου η πολιτική τους αποτελεί ένα συνδυασμό κατηγορημάτων ή ισχυρισμών, μέσω των οποίων καθορίζονται οι κατάλληλες τιμές για ένα ή περισσότερα χαρακτηριστικά. Αντιπροσωπευτικά παραδείγματα τέτοιων γλωσσών αποτελούν η Web Service Policy Language (WSPL), η γλώσσα "Features and Properties" της Oracle, για προσθήκη "συνθετικών" (λογικών συνδέσμων) στην WSDL 2.0 και το μοντέλο Web Services Policy Framework(WS-Policy).

Η WSPL[01][25] αποτελεί ένα υποσύνολο του προτύπου XACML καθώς αναπτύχθηκε από την Τεχνική Επιτροπή OASIS XACML.. Είναι κατάλληλη για τον καθορισμό ενός ευρέου φάσματος πολιτικών, που καλύπτουν την εξουσιοδότηση, την ποιότητα της υπηρεσίας, την προστασία, την αξιοπιστία της επικοινωνίας, την ιδιωτικότητα και την επιλογή υπηρεσιών για συγκεκριμένες εφαρμογές. Υποστηρίζει τη συγχώνευση δύο πολιτικών, με αποτέλεσμα να προκύπτει μια απλή ενιαία πολιτική που να ικανοποιεί τις απαιτήσεις και των δύο, αν υποτεθεί υπάρχει μια τέτοια πολιτική. Με τη χρήση τυποποιημένων τύπων δεδομένων και λειτουργιών για την έκφραση των παραμέτρων της πολιτικής δεδομένων, μια τυπική μηχανή πολιτικών μπορεί να υποστηρίξει οποιαδήποτε πολιτική.

Η WSDL 2.0[26] παρέχει ένα μοντέλο και μια μορφή XML για την περιγραφή των υπηρεσιών ιστού. Η συγκεκριμένη γλώσσα επιτρέπει σε κάποιον να διαχωρίσει την περιγραφή της γενικής λειτουργίας που προσφέρεται από μια υπηρεσία από συγκεκριμένες λεπτομέρειες της περιγραφής υπηρεσιών, όπως το «πώς» και το «πού» αυτή η λειτουργία προσφέρεται. Περιγράφει μια υπηρεσία Web σε δύο βασικά στάδια: ένα αφηρημένο και ένα συγκεκριμένο. Μέσα σε κάθε στάδιο, η περιγραφή χρησιμοποιεί μια σειρά κατασκευασμάτων για την προώθηση της επαναχρησιμοποίησης της περιγραφής και για το διαχωρισμό ανεξάρτητων ζητημάτων σχεδιασμού. Η πρόταση Features and Properties[27]έχει στόχο να ενισχύσει το τμήμα των χαρακτηριστικών γνωρισμάτων που είναι διαθέσιμα στην WSDL 2.0, ώστε να διευθετηθούν πλήρως οι ανάγκες των Υπηρεσιών Ιστού για γνωστοποίηση των απαιτήσεών τους. Με την ενίσχυση αυτή επιτρέπεται στις Υπηρεσίες Ιστού να κοινοποιήσουν τα χαρακτηριστικά τους

χωρίς όμως να παρέχεται σημαντική εκφραστικότητα εξαιτίας της έλλειψης τελεστών για το συνδυασμό των ισχυρισμών.

Το Web Services Policy Framework (WS-Policy)[27] παρέχει ένα ευέλικτο και επεκτάσιμο συντακτικό για την έκφραση των δυνατοτήτων, των απαιτήσεων και των γενικών χαρακτηριστικών των οντοτήτων σε ένα σύστημα υπηρεσιών ιστού βασισμένο σε XML. Η WS-Policy καθορίζει το πλαίσιο για την έκφραση αυτών των ιδιοτήτων ως πολιτικών. Κάθε πολιτική αποτελεί μια συλλογή εναλλακτικών πολιτικών, ενώ κάθε εναλλακτική πολιτική αποτελεί μια συλλογή πολιτικών ισχυρισμών. Η WS-Policy προκειμένου να δηλώσει τους ισχυρισμούς αυτούς χρησιμοποιεί λεξιλόγιο το οποίο δανείζεται από γλώσσες διαφορετικών τεχνολογιών.

4.3 Τεχνολογίες Ανωνυμίας [28]

Οι τεχνολογίες που προσφέρουν ανώνυμη χρήση των ηλεκτρονικών και δικτυακών υπηρεσιών εμπίπτουν σε αυτή την κατηγορία. Παρέχουν ελαχιστοποίηση των δεδομένων που αποκαλύπτονται και προστασία της ταυτότητας των χρηστών, με στόχο τη διατήρηση της ιδιωτικότητας και της ανωνυμίας. Συγκεκριμένα προστατεύονται ορισμένα προσωπικά δεδομένα επικοινωνίας του χρήστη όπως για παράδειγμα οι διευθύνσεις των πηγών επικοινωνίας δύο επικοινωνούντων μερών.

Χρησιμοποιούνται διάφορες τεχνικές όπως η χρήση αξιόπιστων ενδιάμεσων εικονικών χρηστών (proxy) που αποκρύπτουν τα προσωπικά δεδομένα, ανάμιξη δικτύων για να καλυφθεί η πηγή της επικοινωνίας, προσθήκη κίνησης δεδομένων ώστε τα πραγματικά δεδομένα να είναι πιο δύσκολο ανιχνευθούν με τεχνικές εξόρυξης. Ο πυρήνας αυτών των τεχνολογιών λειτουργεί κρύβοντας την συσχέτιση μεταξύ εισόδου και εξόδου, προκειμένου να προστατευθεί η ταυτότητα του τελικού χρήστη (υποκείμενο των δεδομένων). Διάφορες τεχνολογίες, όπως Onion Routing, Hordes, Crowds, Anonymizer και ιδιωτικά πρωτόκολλα ελέγχου ταυτότητας για κινητές υπηρεσίες, έχουν προταθεί με στόχο να προστατεύσουν την ιδιωτικότητα και να κρατήσουν την ανωνυμία των χρηστών.

4.3.1 Tor [29][30][31]

Το Tor (The onion router) είναι ένα σύστημα που χρησιμοποιώντας την τεχνολογία Onion Routing, δίνει στους χρήστες του τη δυνατότητα διατήρησης της ανωνυμίας στο διαδίκτυο. Το

λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης.

Ονομάστηκε έτσι εξαιτίας της στρωματοποιημένης φύσης της υπηρεσίας κρυπτογράφησης: τα αρχικά δεδομένα κρυπτογραφούνται και επανα-κρυπτογραφούνται πολλές φορές, έπειτα στέλνονται μέσω διαδοχικών κόμβων του Tor, ο καθένας από τους οποίους αποκρυπτογραφεί ένα «στρώμα» κρυπτογράφησης προτού μεταφέρει τα δεδομένα στον επόμενο κόμβο και τελικά στον προορισμό τους. Αυτό μειώνει την πιθανότητα να αποκρυπτογραφηθούν ή να γίνουν κατανοητά κατά τη μεταφορά τους τα αρχικά δεδομένα.

- **Στόχοι**

Η χρήση Tor κάνει δύσκολη την ανίχνευση της διαδικτυακής δραστηριότητας του χρήστη, συμπεριλαμβανομένου και των επισκέψεων σε κάποια ιστοσελίδα, των διαδικτυακών αναρτήσεων, των εφαρμογών άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας, κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του.

- **Λειτουργία**

Μια εφαρμογή, αντί να δημιουργήσει μια (socket) σύνδεση απευθείας σε μια μηχανή προορισμού, κάνει μια σύνδεση σε μια θέση Onion Routing Proxy η οποία χτίζει μια ανώνυμη σύνδεση με διάφορους άλλους Onion Routers μέχρι τον προορισμό. Κάθε Onion Router μπορεί να προσδιορίσει μόνο γειτονικά Onion Router κατά μήκος της διαδρομής. Πριν από την αποστολή δεδομένων μέσω μιας ανώνυμης σύνδεσης, ο πρώτος Onion Router προσθέτει ένα στρώμα της κρυπτογράφησης για κάθε Onion Router στη διαδρομή. Όσον τα δεδομένα κινούνται μέσα από την ανώνυμη σύνδεση, κάθε Onion Router αφαιρεί ένα στρώμα της κρυπτογράφησης, έτσι ώστε τελικά να φτάσουν ως απλό κείμενο. Αυτή η στρωματοποίηση διενεργείται κατά την αντίστροφη σειρά για τα δεδομένα που κινούνται πίσω προς τον εκκινητή Onion Router. Τα δεδομένα που περνούν κατά μήκος της ανώνυμης σύνδεσης εμφανίζονται διαφορετικά σε κάθε Onion Router, έτσι ώστε να μην μπορούν να παρακολουθούνται και οι Onion Routers που βρίσκονται σε κίνδυνο να μην μπορούν να συνεργαστούν.

4.3.2 Anonymizer [32][33][34]

Ο anonymizer ή anonymous proxy είναι ένα εργαλείο που προσπαθεί να κάνει την δραστηριότητα στο Διαδίκτυο μη ανιχνεύσιμη. Πρόκειται για έναν proxy server υπολογιστή που ενεργεί ως μεσάζων και ως ασπίδα προστασία της ιδιωτικότητας μεταξύ ενός υπολογιστή-πελάτη και του υπόλοιπου Διαδικτύου. Κάνει την πρόσβαση στο Διαδίκτυο για λογαριασμό του χρήστη, και προστατεύει τα προσωπικά του δεδομένα, αποκρύπτοντας πληροφορίες αναγνώρισης του υπολογιστή-πελάτη.

- **Στόχοι**

Ο anonymizer βοηθά στην ελαχιστοποίηση των κινδύνων κατά την πρόσβαση στο Διαδίκτυο. Μπορεί να χρησιμοποιηθεί για να αποτρέψει την κλοπή ταυτότητας, ή για την προστασία των ιστορικών αναζήτησης από δημοσιοποίηση. Επίσης χρησιμοποιείται την ελεύθερη πρόσβαση σε όλο το περιεχόμενο του Διαδικτύου για την επίτευξη ελευθερίας κινήσεων και μη στοχευόμενης ενημέρωσης και διαφήμισης.

- **Λειτουργία**

Ο anonymizer λειτουργεί εξομοιώνοντας έναν proxy server μεταξύ του χρήστη και της ιστοσελίδας που προορίζεται για πρόσβαση. Υπό κανονικές συνθήκες όταν μια ιστοσελίδα είναι προσβάσιμη από τον υπολογιστή του χρήστη, ο υπολογιστής αναγνωρίζεται από την ιστοσελίδα. Η διαδικασία είναι ένα είδος διαλόγου μεταξύ των δύο: με ένα αίτημα για πρόσβαση στην τοποθεσία από το φυλλομετρητή του υπολογιστή πελάτη και μια χορήγηση άδειας για τη χρήση από τον server του ιστοτόπου. Μέρος αυτού του διαλόγου είναι και η αναγνώριση του υπολογιστή πελάτη από τον server του ιστοτόπου.

Με την χρήση anonymizer αυτή η διαδικασία αλλάζει ένας ανώνυμος proxy server χρησιμοποιείται για την πρόσβαση στον δικτυακό τόπο. Είναι ο proxy server ο οποίος αιτείται την πρόσβαση στο δικτυακό τόπο και όχι ο υπολογιστή του χρήστη. Ο φυλλομετρητής του υπολογιστή του χρήστη θα επικοινωνήσει με το proxy server πρώτα, αλλά στη συνέχεια ο proxy server επικοινωνεί για την προβολή της ιστοσελίδας. Ως αποτέλεσμα, η ιστοσελίδα δεν αναγνωρίζει τον υπολογιστή του χρήστη αλλά τον ανώνυμο proxy server.

4.4 Κρυπτογραφία [18][35]

Η κρυπτογραφία αναφέρεται σε ένα σύνολο διαδικασιών κρυπτογράφησης-αποκρυπτογράφησης, το οποίο έχει ως στόχο να δώσει την δυνατότητα σε δύο οντότητες να επικοινωνήσουν μέσα από ένα μη ασφαλές κανάλι με τέτοιο τρόπο ώστε ένα τρίτο πρόσωπο, μη εξουσιοδοτημένο (ένας επιτιθέμενος), να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να κατανοήσει το περιεχόμενο των μηνυμάτων. Υπάρχουν δύο κατηγορίες κρυπτοσυστημάτων οι οποίες διακρίνονται ανάλογα τα κλειδιά που χρησιμοποιούνται και τον τρόπο κρυπτογράφησης των μηνυμάτων. Έτσι διακρίνονται σε συμμετρικά κρυπτοσυστήματα (Symmetric-key cryptography) ή κρυπτοσυστήματα ιδιωτικού κλειδιού (secret-key encryption) και σε ασύμμετρα κρυπτοσυστήματα ή κρυπτοσυστήματα δημόσιου κλειδιού (asymmetric ή public key encryption).

4.4.1 Συμμετρικό Κρυπτοσύστημα

Ως συμμετρικό ορίζεται το σύστημα εκείνο το οποίο κατά την διαδικασία της κρυπτογράφησης-αποκρυπτογράφησης χρησιμοποιεί ένα κοινό κλειδί Κ. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού. Τα συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων. Σε ένα Συμμετρικο Κρυπτοσυστυμά το ίδιο κλειδί , για το οποίο τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων, χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση δεδομένων. Χαρακτηριστικά παραδείγματα τέτοιων κρυπτοσυστημάτων αποτελούν οι Συμμετρικοί αλγόριθμοι DES, Triple-DES, Blowfish, SAFER, CAST, RC2, RC4 (ARCFOUR), RC5, RC6.

4.4.2 Ασύμμετρο Κρυπτοσύστημα

Το ασύμμετρο κρυπτοσύστημα δημιουργήθηκε για να καλύψει το κενά στην αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Η βασική ιδέα είναι ότι αποστολέας και παραλήπτης δεν μοιράζονται πλέον ένα κοινό κλειδί, αλλά έχουν διαφορετικά κλειδιά για κάθε λειτουργία. Χρησιμοποιούνται δηλαδή άλλα κλειδιά για κρυπτογράφηση και άλλα για αποκρυπτογράφηση. Χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα ιδιωτικό και ένα δημόσιο, τα οποία σχετίζονται μεταξύ τους με μονόδρομες συναρτήσεις (one-way functions) και

τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται αποκλειστικά με το άλλο. Μόνο μία φυσική οντότητα γνωρίζει το ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί είναι εύκολα διαθέσιμο στο κοινό. Χαρακτηριστικά παραδείγματα τέτοιων κρυπτοσυστημάτων αποτελούν οι ασύμμετροι αλγόριθμοι RSA, Diffie-Hellman Key Exchange, ElGamal, Digital Signature Standard (DSS).

4.4.3 Πρωτόκολλο Secure Sockets Layer (SSL) [18] [36]

Το πρωτόκολλο Secure Sockets Layer (SSL) αποτελεί ίσως την πιο διαδεδομένη εφαρμογή της κρυπτογραφίας, η οποία αποτελεί μια μορφή υβριδικής κρυπτογραφίας (hybrid encryption), υπό την έννοια ότι πρόκειται για ένα συνδυασμό συμμετρικής και ασύμμετρης κρυπτογραφίας. Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών, όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών και πλέον χρησιμοποιείται από οποιαδήποτε εφαρμογή/υπηρεσία περιλαμβάνει συλλογή και επεξεργασία προσωπικών δεδομένων. Η τελική του έκδοση SSL 3.0 όπως χρησιμοποιείται σήμερα, παρουσιάστηκε το 1996 και έκτοτε χρησιμοποιείται ευρέως ως de-facto μηχανισμός διασφάλισης ενός διαύλου επικοινωνίας και κρυπτογράφησης των δεδομένων τα οποία διέρχονται από αυτόν. Το πρωτόκολλο SSL αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανή και απλό.

- **Στόχοι** [36][37]

Το πρωτόκολλο SSL στοχεύει στην διασφάλιση της επικοινωνίας και της προστασίας των δεδομένων μεταξύ δύο επικοινωνούντων πηγών. Απαραίτητες προϋποθέσεις για την επίτευξη αυτού του σκοπού θεωρούνται η κρυπτογραφική ασφάλεια, η διαλειτουργικότητα και η επεκτασιμότητα, ιδιότητες που θα το καθιστούν ανεξάρτητο εφαρμογής ή προγραμματιστή και εξελίξιμο ως προς την αποδοτικότητα του και τέλος η σχετικά γρήγορη απόδοση καθώς οι κρυπτογραφικές διαδικασίες τείνουν να είναι ιδιαίτερα επιβαρυντικές για τους υπολογιστές.

- **Λειτουργία** [37] [38]

Μόλις ένας πελάτης (client) και ένας εξυπηρετητής (server) ξεκινούν την επικοινωνία, το πρωτόκολλο SSL διασφαλίζει ότι η σύνδεση είναι ιδιωτική και ασφαλής παρέχοντας βασικές ενέργειες ασφαλείας όπως η αυθεντικοποίηση, η κρυπτογράφηση, και ο έλεγχος της ακεραιότητας.

Η αυθεντικοποίηση επιβεβαιώνει ότι ο εξυπηρετητής, και προαιρετικά ο πελάτης, είναι αυτοί που ισχυρίζονται. Η Κρυπτογράφηση μέσω ανταλλαγής κλειδιών, στη συνέχεια, δημιουργεί έναν ασφαλές δίαυλο μεταξύ των οντοτήτων ο οποίος αποτρέπει οποιαδήποτε τρίτη μη εξουσιοδοτημένη από τα σύστημα οντότητα να αναγνώσει τα δεδομένα. Ο έλεγχος ακεραιότητας παράλληλα εγγυάται ότι οποιαδήποτε επίσης μη εξουσιοδοτημένη οντότητα δεν θα τροποποιήσει το κρυπτογραφημένο μήνυμα, τουλάχιστον χωρίς να μπορεί να εντοπιστεί.

Πελάτες συμβατοί με το πρωτόκολλο SSL (φυλλομετρητές) και εξυπηρετητές επίσης συμβατοί, αλληλο-επιβεβαιώνουν την ταυτότητα τους χρησιμοποιώντας ψηφιακά πιστοποιητικά. Τα ψηφιακά πιστοποιητικά εκδίδονται από αξιόπιστες τρίτες οντότητες, τις αρχές έκδοσης πιστοποιητικών (Certificate Authorities - CA) και παρέχουν πληροφορίες σχετικά με την δηλωθείσα ταυτότητα ενός ατόμου, καθώς και το δημόσιο κλειδί του, που χρησιμοποιείται από τον εκάστοτε αποστολέα ενός μηνύματος για την κρυπτογράφηση των δεδομένων. Ο παραλήπτης του μηνύματος μπορεί να αποκρυπτογραφήσει τα δεδομένα μόνο με το αντίστοιχο ιδιωτικό κλειδί.

Τα δημόσια κλειδιά είναι γνωστά σε όλους, αντίθετα τα ιδιωτικά κλειδιά είναι μυστικά και γνωστά μόνο στον ιδιοκτήτη του πιστοποιητικού. Επικυρώνοντας την ψηφιακή

υπογραφή των πιστοποιητικών από την αρχή έκδοσης πιστοποιητικών, τα δύο μέρη μπορούν να βεβαιωθούν ότι ένας υποκλοπέας δεν έχει παρέμβει στη μετάδοση.

4.5 Τεχνολογίες Φιλτραρίσματος

Η κατηγορία των τεχνολογιών φιλτραρίσματος αφορά όλους εκείνους τους μηχανισμούς που έχουν σχεδιαστεί ώστε να ελέγχουν και να διακρίνουν ποιο περιεχόμενο είναι επιτρεπτό να προσπελαστεί από έναν χρήστη του Διαδικτύου, να αποκλείουν ή να περιορίζουν επικίνδυνες ή μη επιθυμητές ενέργειες και ανταλλαγή δεδομένων, να περιορίζουν την λήψη ανεπιθύμητων μηνυμάτων ή ενοχλητικών κλήσεων. Περιλαμβάνονται μηχανισμοί όπως τα αναχώματα ασφαλείας (firewall), εργαλεία αποκλεισμού αρχείων cookies (cookie-cutters), εργαλεία ελέγχου πρόσβασης βάσει περιεχομένου (Web Content Filtering Tools) και αντι-κατασκοπευτικά (antispyware) ή αντι – ικά προγράμματα (antivirus).

Η εφαρμογή των τεχνολογιών αυτών μπορεί να εφαρμοστεί είτε σε επίπεδο αρχιτεκτονικής του Διαδικτύου, είτε στους παρόχους υπηρεσιών Διαδικτύου και Τηλεπικοινωνιών, είτε ακόμα σε επίπεδο οργανισμών ή ατομικών υπολογιστών. Υπάρχουν αρκετές λύσεις που εφαρμόζονται σήμερα οι οποίες προστατεύουν αποτελεσματικά την ιδιωτικότητα των χρηστών είτε λειτουργώντας ατομικά είτε συνδυαστικά με άλλα εργαλεία.

4.5.1 Αναχώματα Ασφαλείας [39] [40]

Τα αναχώματα ασφαλείας ή τείχη προστασίας (firewalls) αφορούν τρόπους προστασίας που αναπτύχθηκαν για την εκ των προτέρων αντιμετώπιση κάποιων εκ των κινδύνων που ελλοχεύουν κατά την χρήση των δικτυακών τεχνολογιών και για την διατήρηση του ελέγχου της πρόσβασης και της κυκλοφορίας μεταξύ των δικτύων. Αν και ο συγκεκριμένος μηχανισμός σχετίζεται περισσότερο με Διαδικτυακές υπηρεσίες, εντούτοις βρίσκει εφαρμογή και σε άλλα δικτυακά περιβάλλοντα.

Ένα ανάχωμα ασφάλειας λειτουργεί ως ρυθμιστής της κυκλοφορίας δεδομένων παρεμβαίνοντας ανάμεσα σε δύο δίκτυα υπολογιστών τα οποία έχουν διαφορετικό επίπεδο εμπιστοσύνης, εκ των οποίων συνήθως το ένα και το πιο χαμηλού επιπέδου είναι το Διαδίκτυο. Ως ανάχωμα ασφάλειας δεν νοείται απαραίτητα μόνο ένα λογισμικό σύστημα ή μόνο ένα υλικό σύστημα αλλά πιο συγκεκριμένα ορίζεται ως σύστημα ή ομάδες συστημάτων, υλικού ή

λογισμικού τα οποία ελέγχουν και προστατεύουν την πρόσβαση μεταξύ δικτύων και υλοποιούν τους κανόνες μιας πολιτικής ασφάλειας.

- **Στόχοι** [40] [41]

Ένα ανάχωμα ασφαλείας αναλαμβάνει πρωτίστως να αποτρέψει οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση σε μια ασφαλή περιοχή αλλά και επιπλέον να αποτρέψει την μη εξουσιοδοτημένη έξοδο πληροφορίας για την ίδια περιοχή. Σημαντικό ρόλο στην επίτευξη αυτών των στόχων αναλαμβάνει, πέραν των τεχνικών δυνατοτήτων του αναχώματος, και η ενσωμάτωση μιας πολιτικής ασφαλείας όταν χρησιμοποιείται από οργανισμούς ή η σωστή διαχείριση από τους χρήστες όταν η χρήση γίνεται σε προσωπικό επίπεδο. Το ανάχωμα ασφαλείας για να λειτουργήσει σωστά πρέπει να υλοποιεί και να ενισχύει την πολιτική ασφαλείας που ισχύει κάθε φορά.

- **Λειτουργία** [39][42]

Η λειτουργία ενός αναχώματος ασφαλείας εξαρτάται από τον τρόπο που δρα ώστε να διασφαλίσει την θωράκιση μιας περιοχής. Κατά συνέπεια υπάρχουν τρείς βασικές κατηγορίες αναχωμάτων ασφαλείας και διακρίνονται σε αυτά που εφαρμόζουν φιλτράρισμα των πακέτων δεδομένων και αναφέρονται ως δρομολογητές φιλτραρίσματος (packet filtering), σε αυτά που χρησιμοποιούν πληρεξούσιους εξυπηρετητές (proxy servers) και τέλος στα αναχώματα ελέγχου κατάστασης (stateful packet inspection - SPI)

Τα αναχώματα ασφαλείας που εφαρμόζουν φιλτράρισμα των πακέτων δεδομένων που κινούνται σε ένα δίκτυο αφορούν την πρώτη γενιά συσκευών αναχωμάτων όπου ήταν ενσωματωμένες σε δρομολογητές του δικτύου και λειτουργούσαν στα τρία πρώτα επίπεδα του μοντέλου αναφοράς OSI (Open Systems Interconnection model). Ο μηχανισμός τους αναζητά πακέτα που να ταιριάζουν σε οποιονδήποτε κανόνα φιλτραρίσματος έχει προ-ρυθμιστεί από τους διαχειριστές του δικτύου, και αναλόγως προχωρά σε αποδοχή ή απόρριψη του πακέτου. Οι κανόνες φιλτραρίσματος μπορούν να βασίζονται μόνο σε στοιχεία όπως η διεύθυνση IP προέλευσης και προορισμού, και οι θύρες TCP (Transmission Control Protocol) ή UDP (User Datagram Protocol) προέλευσης και προορισμού. Συνεπώς η εφαρμογή αυτού του είδους των αναχωμάτων γίνεται μόνο σε επίπεδο, δικτύου γεγονός που αποτελεί και την αδυναμία των δρομολογητών φιλτραρίσματος καθώς αδυνατούν να ελέγξουν πληροφορίες που σχετίζονται με το περιεχόμενο ενός πακέτου, παρά μόνο πληροφορίες σύνδεσης.

Ένα ανάχωμα τύπου πληρεξούσιου εξυπηρετητή (Proxy Server Firewall) λειτουργεί στα ανώτερα επίπεδα της στοίβας πρωτοκόλλων του μοντέλου αναφοράς OSI παρέχοντας εσωτερικά του δικτύου, τερματικά με πληρεξούσιες υπηρεσίες (πληρεξούσιος εξυπηρετητής ή εξυπηρετητής μεσολάβησης - proxy server) προς τα εξωτερικά δίκτυα. Όλη η επικοινωνία μεταξύ ενός πελάτη με τον πραγματικό εξυπηρετητή γίνεται μέσω του πληρεξούσιου εξυπηρετητή. Έτσι, ένας πληρεξούσιος εξυπηρετητής λειτουργεί ουσιαστικά ως μεσίτης στην επικοινωνία μεταξύ των πελατών και των πραγματικών εξυπηρετητών εφαρμογής. Οι πληρεξούσιοι εξυπηρετητές μπορούν να λειτουργήσουν είτε στο επίπεδο εφαρμογής είτε στο επίπεδο μεταφοράς για αυτό προκύπτουν δύο κατηγορίες αναχωμάτων, τα αναχώματα επιπέδου μεταφοράς (Circuit-Level Firewall) και τα αναχώματα επιπέδου εφαρμογής (Application-Level Firewall).

Το ανάχωμα επιπέδου μεταφοράς λειτουργεί στο στρώμα συνόδου του μοντέλου OSI όπου παρακολουθεί τις «χειραψίες» (handshakes) TCP και UDP μεταξύ των πακέτων για να καθορίσει εάν η σύνοδός που ζητήθηκε είναι επιτρεπτή. Μετέπειτα ένα εικονικό "κύκλωμα" μεταφοράς δημιουργείται μεταξύ των εσωτερικών τερματικών και του εξυπηρετητή μεσολάβησης. Όλες οι αιτήσεις από τα εξωτερικά δίκτυα περνούν από αυτό το "κύκλωμα" στο εξυπηρετητή μεσολάβησης, ο οποίος με την σειρά του αναμεταδίδει τα αιτήματα αυτά προς τα εξωτερικά δίκτυα αλλάζοντας τις διευθύνσεις IP των πακέτων ώστε οι ιδιωτικές διευθύνσεις IP να μην είναι εκτεθειμένες σε πιθανούς εισβολείς.

Ένα ανάχωμα ασφαλείας επίπεδου εφαρμογής παρέχει όλα τα χαρακτηριστικά του αναχώματος επιπέδου μεταφοράς με επιπλέον μια εκτεταμένη ανάλυση των πακέτων που διακινούνται. Επιπλέον της αξιολόγησης των IP διευθύνσεων, ένα ανάχωμα ασφαλείας επιπέδου εφαρμογής αποφασίζει που θα παραδοθεί το πακέτο δεδομένων ή αν θα απορριφθεί, σύμφωνα με τις πληροφορίες εφαρμογής που περιλαμβάνει το πακέτο. Αυτό επιτυγχάνεται καθορίζοντας πολλαπλούς πληρεξούσιους εξυπηρετητές, διαφορετικούς για κάθε τύπο εφαρμογής.

Πιο εξελιγμένη θεωρείται η τεχνολογία των αναχωμάτων ελέγχου κατάστασης τα οποία λειτουργούν σε πολλαπλά επίπεδα του μοντέλου αναφοράς OSI, όπως των επιπέδων Δικτύου (Network Layer), Μεταφοράς (Transport Layer) και Εφαρμογών (Application Layer). Αναλαμβάνουν την παρακολούθηση της κατάστασης των ενεργών συνδέσεων, αναλύουν τα μοτίβα κίνησης προς το Επίπεδο Εφαρμογής και εντοπίζουν ανωμαλίες με βάση τα αποτελέσματα της ανάλυσης. Το ανάχωμα διατηρεί πληροφορίες κατάστασης για κάθε σύνδεση, η οποία κατάσταση περιλαμβάνει έναν συνδυασμό της φάσης επικοινωνίας και της

κατάσταση του τελικού σημείου εφαρμογής. Όταν παραλαμβάνεται ένα πακέτο δεδομένων, συγκρίνεται με μια γνωστή κατάσταση σύνδεσης και αν το πακέτο αποκλίνει από την αναμενόμενη κατάσταση διακόπτεται το υπόλοιπο της δεδομένης χρονικής στιγμής.

4.5.2 Εργαλεία Ελέγχου Πρόσβασης Βάσει Περιεχομένου [43]

Οι λύσεις που περιλαμβάνονται σε αυτή την κατηγορία δίνουν την δυνατότητα σε ένα χρήστη του Διαδικτύου να ελέγξει το περιεχόμενο των ιστοσελίδων του κατά την περιήγησή του στον ιστό. Η προστασία των χρηστών από ανεπιθύμητο Διαδικτυακό περιεχόμενο δεν είναι γενικά ένα πρόβλημα ιδιωτικότητας, δεδομένου ότι οι πληροφορίες συνήθως δεν είναι στοχευμένες στον χρήστη που επισκέπτεται τον εκάστοτε ιστότοπο. Ωστόσο, τελευταία ορισμένες διαδικτυακές εφαρμογές συλλέγουν, συσχετίζουν και χρησιμοποιούν τα δεδομένα του χρήστη (π.χ. όνομα τομέα, διεύθυνση IP) ώστε να προσαρμόσουν ανάλογα το περιεχόμενο του ιστοτόπου ή να προσθέσουν διαφημίσεις ανάλογες των ενδιαφερόντων του. Ακόμα πιο επικίνδυνες θεωρούνται σελίδες ιστοχώρων που παρουσιάζουν παράνομο υλικό ή υλικό ακατάλληλο που έρχεται σε αναντιστοιχία με τα χαρακτηριστικά του χρήστη, για παράδειγμα πορνογραφικό υλικό, «πειρατικό» λογισμικό κ.α. Επιπλέον στις σελίδες κοινωνικής δικτύωσης που απολαύουν τεράστια αποδοχή και εν πρώτοις φαντάζουν αθώες, δεν μπορούμε να παραβλέψουμε ότι η χρήση τους δεν είναι αποκλειστικά μονομερής, οπότε οι κίνδυνοι μπορούν να ποικίλλουν ανάλογα με τον αριθμό αλλά και την ποιότητα των υπολοίπων χρηστών, ιδιαίτερα όταν στην θέση του θύματος μπορούν να βρίσκονται ανήλικοι χρήστες.

4.5.3 Εργαλεία Αποκλεισμού Αρχείων Cookies

Η πιο κοινή μέθοδος που χρησιμοποιείται για την παρακολούθηση των ατόμων στο Διαδίκτυο είναι τα «Cookies», δηλαδή μικρά αρχεία που είναι αποθηκευμένα στον υπολογιστή του χρήστη με τις πληροφορίες που παρέχονται από τον ιστότοπο. Αν και η πλειοψηφία των ιστοτόπων χρησιμοποιεί αυτό το εργαλείο εντός των προβλεπόμενων και νόμιμων πλαισίων, υπάρχουν και αυτοί οι οποίοι εκμεταλλεύονται τις πληροφορίες αυτών των αρχείων με αθέμιτο τρόπο. Προγράμματα αποκλεισμού των αρχείων cookies (cookie-cutters) επιτρέπουν στους χρήστες να αποφασίσουν ποια cookies μπορούν να μείνουν στο σύστημά τους, και ποια cookies θα πρέπει να αποκλειστούν ή να διαγραφούν. Πλέον λογισμικά που να επιτελούν μόνο τις συγκεκριμένες

διαδικασίες δεν αναπτύσσονται και δεν έχουν ευρεία αποδοχή καθώς η λειτουργία τους έχει ενσωματωθεί είτε σε ολοκληρωμένα πακέτα αντι-ιικής προστασίας είτε στους φυλλομετρητές.

4.5.4 Εργαλεία αποκλεισμού ανεπιθύμητων μηνυμάτων και κλήσεων

Η αποστολή αυτόκλητων ή ανεπιθύμητων μηνυμάτων (spam) αποφέρει σχετικά εύκολο και μεγάλο κέρδος στον αποστολέα (spammer), λειτουργώντας ως μέσο άμεσης διαφήμισης, το οποίο σε αντίθεση με τις κλασσικές μεθόδους όπως ραδιόφωνο, τηλεόραση, διαφημιστικά φυλλάδια και άλλα γνωστά μέσα, έχει για αυτόν ελάχιστο ή μηδενικό κόστος. Η προβολή ενός τέτοιου μηνύματος δεν αποτελεί μια ευθεία παραβίαση της ιδιωτικότητας των χρηστών, εντούτοις τις περισσότερες φορές τα αυτόκλητα μηνύματα δρουν ως μηνύματα απάτες (hoaxes) παρουσιάζοντας ψευδείς πληροφορίες με μόνο σκοπό την απορρόφηση πληροφοριών από τον παραλήπτη. Τα αυτόκλητα μηνύματα μπορούν να συγκεντρώνουν προσωπικά στοιχεία από τους παραλήπτες τα οποία μπορούν να χρησιμοποιηθούν για απάτες ή για μεταπώληση σε άλλους spammers.

Με ανάπτυξη νέων μορφών διαδικτυακών υπηρεσιών τεχνολογιών ηλεκτρονικής επικοινωνίας εξελίχθηκαν παράλληλα και νέες μορφές ανεπιθύμητων μηνυμάτων. Μορφές spam που αφορούν τις εφαρμογές άμεσων μηνυμάτων (Instant messaging spam), τις μηχανές αναζήτησης (spamdexing) και γενικότερα ιστοτόπων και υπηρεσιών που επιτρέπουν την αλληλεπίδραση και την επικοινωνία μεταξύ των χρηστών τους. Ακόμα και σε τεχνολογίες τηλεφωνίας όπως η κινητή τηλεφωνία ή η τηλεφωνία μέσω διαδικτύου (voice over IP- VoIP), οι ανεπιθύμητες μορφές επικοινωνίας απειλούν την ιδιωτικότητα των χρηστών.

Διάφορες τεχνικές έχουν αναπτυχθεί στην προσπάθεια αντιμετώπισης των ανεπιθύμητων μηνυμάτων, που η διακίνηση τους στα δίκτυα επικοινωνιών οδηγεί σε μεγάλη απώλεια πόρων, και σε απώλεια χρόνου και παραγωγικότητας. Και μπορεί το φαινόμενο αν υπολογιστεί ατομικά να μην είναι τόσο τραγικό αν όμως υπολογιστεί αθροιστικά, για παράδειγμα όσον αφορά την παραγωγικότητα των εταιρειών μιας χώρας, οι απώλειες μπορούν να φτάσουν μέχρι και δεκάδες δισεκατομμύρια. Οι τεχνικές αφορούν τρόπους για να προλαμβάνουν την λήψη τέτοιου περιεχομένου, άλλους για να τα διακρίνουν από το σύνολο των μηνυμάτων και άλλους για την διαχείριση τους μετά την λήψη.

- **Στόχοι** [43] [44] [45]

Οι στόχοι των τεχνικών αντιμετώπισης spam είναι η προστασία των χρηστών από πιθανές απάτες και ενέργειες παραβίασης του απορρήτου τους, αλλά και η αντιμετώπιση επιβλαβών συνεπειών των ανεπιθύμητων μηνυμάτων που σχετίζονται με κατανάλωση υπολογιστικών αλλά και ανθρώπινων πόρων. Είναι γεγονός πως τα spam ευθύνονται για την υπερφόρτωση δικτύων και χώρων αποθήκευσης όσο και για την κατατριβή χρόνου εργασίας.

- **Λειτουργία** [43] [44] [45]

Οι λειτουργία αντιμετώπισης των μηχανισμών ανεπιθύμητων μηνυματων εξαρτάταται τόσο από την τεχνολογία για την οποία εφαρμόζεται όσο και από τον τρόπο δράσης. Υπάρχουν τρεις κατηγορίες οι τεχνικές πρόληψης, οι τεχνικές εντοπισμού και οι τεχνικές διαχείρισης.

Οι τεχνικές πρόληψης των αυτόκλητων μηνυμάτων αφορούν μηχανισμούς που προσπαθούν να αποτρέψουν την αποστολή τους. Γνωστό παράδειγμα αποτελούν οι Λίστες, μια τεχνική που βασίζεται σε λίστες στις οποίες καταγράφονται οι αποστολείς που θεωρούνται αξιόπιστοι (Λευκές Λίστες – Whitelists) και οι αποστολείς οι οποίοι έχουν κριθεί ως spammers (Μαύρες Λίστες- Blacklists). Υπάρχουν και οι Γκρίζες Λίστες (Greylisting) κρίνεται η αξιοπιστία του αποστολέα σύμφωνα με τον αριθμό αποστολών των μηνυμάτων. Αξιόπιστοι αποστολείς συνηθίζουν να στέλνουν περισσότερες από μία φορές. Με την τεχνική Challenge/Response στέλνεται μια αποστολή αίτησης (response) προς τον αποστολέα εισερχόμενου email και αναμονή απάντησης (response) έτσι ώστε να εξασφαλιστεί η ανθρώπινη πηγή του μηνύματος και να αποφευχθεί η δυνατότητα αυτόματης παραγωγής μαζικών emails. Η τεχνική Consent token στηρίζεται στην ύπαρξη κάποιου «κόστους», υπολογιστικού ή οικονομικού, από την μεριά του αποστολέα για κάθε μήνυμα που αυτός αποστέλλει, με στόχο να αποδείξει ότι δεν πρόκειται για spammer. Τέλος η τεχνική Αυθεντικοποίησης (Authentication) αφορά την επιβεβαίωση του αποστολέα, δηλαδή στην πιστοποίηση της ταυτότητας του.

Οι τεχνικές εντοπισμού είναι αυτές οι οποίες προσπαθούν να εντοπίσουν τα spam μηνύματα και να τα διακρίνουν από τα κανονικά μηνύματα ηλεκτρονικού ταχυδρομείου. Τεχνικές όπως τα Συστήματα Φήμης (Reputation systems) όπου καθορίζονται εκτιμήσεις (ratings) για κάθε αποστολέα ηλεκτρονικής αλληλογραφίας οι οποίες στηρίζονται στην απόδοση ενός βαθμού αξιοπιστίας του αποστολέα. Οι Λίστες Στατικού Περιεχομένου (Static content filtering lists) κατά την οποία ερευνάται ολόκληρο το περιεχόμενο των μηνυμάτων για συγκεκριμένες λέξεις που

φανερώνουν περιεχόμενο spam μηνυμάτων. Πιο εξελιγμένη τεχνική θεωρούνται τα συστήματα μάθησης περιεχομένου (Learning content filtering systems) όπου βασισμένη σε Bayesian φίλτρα και σε μηχανισμούς λήψης αποφάσεων και με την συνεργασία του χρήστη το σύστημα «εκπαιδεύεται» στον εντοπισμό περιεχομένου που υποδηλώνει ανεπιθύμητο μήνυμα. Άλλες τεχνικές όπως η Quantity και η Checksum-based filter εξετάζουν την πιθανότητα ανεπιθύμητου μηνυμάτος βασισμένες σε τεχνικές σχετικές με την ποσότητα των μηνυμάτων που έχουν αποσταλεί.

Οι τεχνικές διαχείρισης λειτουργούν μετά τον εντοπισμό ανεπιθύμητων μηνυμάτων δίνοντας την δυνατότητα στους χρήστες να επιλέξουν πως θα τα διαχειριστούν. Υπάρχει η δυνατότητα τοποθέτηση ενός spam σε προσωρινή απομόνωση (Quarantine), η τεχνική περιορισμού των μηνυμάτων που αποστέλλονται από συγκεκριμένο χρήστη, η οποία εφαρμόζεται σε επίπεδο παρόχων, η επιλογή απόρριψης του μηνύματος και η μέθοδος χρέωσης του αποστολέα για κάθε spam που αποστέλλει.

4.5.6 Αντι – ιικά Προγράμματα

Τα αντι-ιικά ή και αντιβιοτικά προγράμματα εσκεμμένα περιγράφονται τελευταία δεδομένου ότι πλέον οι λειτουργίες τους δύναται να συνδυάζουν τις περισσότερες από τις λειτουργίες που περιγράφηκαν στις προηγούμενες μεθόδους. Ένα σύγχρονο αντι-ιικό λογισμικό για παράδειγμα μπορεί να συνδυάζει τις λειτουργίες πρόσβασης βάσει περιεχομένου, να ενσωματώνει ένα ανάχωμα ασφαλείας, να αποκλείει αρχεία cookies και φυσικά να προστατεύει τον χρήστη από ιούς (viruses) και λοιπές μορφές κακόβουλου λογισμικού (malicious software). Ένα κακόβουλο λογισμικό έχει σκοπό να επιφέρει την αστάθεια ενός πληροφοριακού συστήματος ή να παραβιάσει την πρόσβαση σε αυτό. Οι τρόποι αντιμετώπισης τέτοιου είδους προγραμμάτων κατηγοριοποιούνται ανάλογα την τον τρόπο και τον χρόνο δράσης, Για παράδειγμα υπάρχουν τεχνικές αντιμετώπισης με προληπτική δράση, άλλες που προσπαθούν να ανιχνεύσουν πιθανά προβλήματα και τέλος αυτές που δρουν διαδοχικά του προβλήματος.

- **Στόχοι**

Η συνδυαστική χρήση των μέτρων πρόληψης, ανίχνευσης και επανόρθωσης αποσκοπεί στο να επιτύχει την απαλοιφή των πιθανών κακόβουλων λογισμικών που θα προσβάλουν ένα σύστημα, την αποφυγή της προσβολής του συστήματος από ένα τέτοιο λογισμικό, ή τουλάχιστον την ελαχιστοποίηση των ζημιών που μπορεί αυτό να επιφέρει σε περίπτωση που

καταφέρει να «προσβάλλει» ένα υπολογιστικό σύστημα. Ένα αντι-ιικό λογισμικό για να ικανοποιήσει τα προαναφερθέντα αποτελέσματα θα πρέπει πρωτίστως να πληροί και κάποια τεχνικά κριτήρια όπως η ενημέρωση της βάσης δεδομένων του, καθώς η εμφάνιση νέων ιών είναι καθημερινή και η διαλειτουργικότητα του αφού θα πρέπει να λειτουργεί και να συνεργάζεται σε διαφορετικά αρχιτεκτονικά πλαίσια και με διάφορα Λειτουργικά συστήματα.

- **Λειτουργία [46]**

Η πιο σημαντική λειτουργία ενός αντι-ιικού προγράμματος είναι αυτή της μηχανής σάρωσης (scan engine). Σαρώνει τις πληροφορίες ενός πληροφοριακού συστήματος και σε περίπτωση που διαπιστωθεί ύπαρξη ιών, τους «απολυμαίνει». Η λειτουργία της σάρωση μπορεί να γίνει με διαφορετικούς τρόπους:

Σύμφωνα με το μέγεθος: η μηχανή μπορεί εύκολα να ανιχνεύσει αν το αρχείο έχει μολυνθεί ή αλλοιωθεί. Δεδομένου ότι ορισμένοι ιοί προσαρτούν τον κακόβουλο κώδικα στο τέλος του αρχείου. Η μηχανή σαρώνει και συγκρίνει το μεγέθη των αρχείων πριν και μετά την σάρωση. Αν υπάρχει μεταβολή στο μέγεθος, η οποία δεν έχει γίνει από το χρήστη, δημιουργούνται υποψίες για ύπαρξη κακόβουλου κώδικα και μόλυνση του αρχείου.

Ταίριασμα Μοτίβου: κάθε ιός έχει μια μοναδική υπογραφή (virus signature) που χρησιμοποιεί για να μολύνει τα αρχεία ή τους υπολογιστές. Αυτή η υπογραφή θα μπορούσε να είναι μερικές γραμμές σε γλώσσα μηχανής που αντικαθιστούν το δείκτη της στοίβας του προγράμματος και μεταπηδούν προς τη νέα γραμμή του κώδικα. Ένα πρόγραμμα προστασίας από ιούς συγκρίνει τις πληροφορίες με μια βάση δεδομένων των υπαρχόντων υπογραφών ιών και στην περίπτωση που οι πληροφορίες ταιριάζουν με οποιαδήποτε από τις υπογραφές ιών της βάσης δεδομένων τότε θεωρείται πως το αρχείο έχει προσβληθεί από τον ιό.

Η ευρετική μέθοδος (heuristic method): Αναλύει τον τρόπο που ενεργεί κάθε στοιχείο ή πληροφορία και τον συγκρίνει με έναν κατάλογο της βάσης δεδομένων όπου αναφέρονται οι επικίνδυνες δραστηριότητες. Όταν ανιχνευθεί η επικίνδυνη δραστηριότητα το πρόγραμμα θεωρεί πιθανή την ύπαρξη κακόβουλου λογισμικού και ακολουθεί στην ενημέρωση του χρήστη ώστε αυτός να αποφασίσει για την επικινδυνότητα ή όχι του ύποπτου στοιχείου όπως και για τον τρόπο που θα διαχειριστεί την κατάσταση.

Κεφάλαιο 5
Θεσμική προστασία της Ιδιωτικότητας των επικοινωνιών

« Η ασφάλεια των ανθρώπων πρέπει να είναι ο υπέρτατος νόμος »

Marcus Tullius Cicero

Αποδομώντας τις έννοιες που αφορούν την Ιδιωτικότητα και τις προκλήσεις που αυτή συναντά κατά την διατήρηση των προσωπικών δεδομένων καταλήγουμε στο συμπέρασμα ότι καμία τεχνολογική θωράκιση δεν είναι αρκετή για να προστατέψει τους συνδρομητές από κινδύνους που ελλοχεύουν κατά την χρήση ηλεκτρονικών υπηρεσιών επικοινωνίας. Παρόλο που, όπως ήδη έχει αναφερθεί, η Ιδιωτικότητα αποτελεί σημαντικό αγαθό και θεμελιώδες δικαίωμα του ατόμου που άμεσα σχετίζεται με άλλα δικαιώματα και αρχές, όπως το δικαίωμα ανάπτυξης της

προσωπικότητας, η αυτονομία και η αξία του ανθρώπου και η αρχή της ισότητας, οι απειλές όχι απλά παραμένουν «ζωντανές», αλλά μέρα με την μέρα γεννιούνται νέες και περισσότερες. Νέες προκλήσεις που απορρέουν και ενισχύονται από την ραγδαία ανάπτυξη των τεχνολογιών, οι οποίες στοχεύουν ή διευκολύνουν την παγκοσμιοποίηση της ροής των δεδομένων, την εμπορευματοποίηση των προσωπικών πληροφοριών και την εξέλιξη της επεξεργασίας των δεδομένων.

5.1 Ανάγκη για Νομική Διασφάλιση της Ιδιωτικότητας

Καθώς λοιπόν η ανθρώπινη σκέψη, γνώση και δραστηριότητα μετουσιώνεται σε πληροφορία, η οποία είναι εν δυνάμει εμπορευματοποιημένη ή επιτηρούμενη, εύλογα γεννιούνται ανάγκες για την θέσπιση κανονιστικών αρχών και οδηγιών που θα ρυθμίζουν τον τρόπο της διαχείρισης και της επεξεργασίας των διατηρούμενων δεδομένων. Πως όμως μπορεί κανείς να οριοθετήσει την χρήση της πληροφορίας όταν εκ φύσεως αυτή η πληροφορία είναι παγκόσμια; Πως μπορεί να επιβάλει κοινωνικές ή πολιτικές διατάξεις όταν η πληροφορία διαχέεται σε τόσες διαφορετικές κοινωνίες και πολιτισμούς; Πόσο μάλλον όταν και οι ίδιες κοινωνίες είναι οντότητες που διαρκώς αλλάζουν και αναπτύσσονται και οι όποιες κοινωνικοπολιτικές εξελίξεις επηρεάζουν σε μεγάλο βαθμό τη σχέση μεταξύ ελευθερίας, προστασίας της ιδιωτικότητας και ασφάλειας.

Η μεγαλύτερη λοιπόν πρόκληση που επιφέρει ο καθορισμός νομικής φύσεως πρακτικών για την διαχείριση των δεδομένων είναι η διαφορετικότητα που παρουσιάζεται σε τομείς όπως η κοινωνία, η πολιτική, η τεχνολογία η οικονομία και ο πολιτισμός, μεταξύ των χώρων στους οποίους διαδίδεται η πληροφορία, καθώς και η επίδραση του χρόνου πάνω σε αυτούς τους τομείς. Αντιλαμβάνεται κανείς ότι η ανάγκη για θεσμική προστασία των διατηρούμενων δεδομένων, πρέπει να βασίζεται σε ένα κοινό παγκόσμιο πλαίσιο το οποίο να είναι ενεργό και να αναδιαμορφώνεται συνεχώς ανάλογα με τις όποιες αλλαγές και εξελίξεις στους προαναφερόμενους τομείς.

Ήδη αναλύθηκε μια τέτοια προσπάθεια που προέκυψε από τον ΟΟΣΑ με τον ορισμό των κατευθυντήριων αρχών, ωστόσο δεν πρόκειται για ένα νομικό πλαίσιο και η συμμόρφωση με αυτό δεν αποτελεί δέσμευση για καμία από τις συμμετέχουσες χώρες. Χώρες όπως η Η.Π.Α. για παράδειγμα, που παρότι υπήρξαν ιδρυτικό μέλος του Οργανισμού και συνέναισαν στην δημιουργία των κατευθυντηρίων αρχών, και παρόλη την ανάπτυξη που εμφανίζουν στις Τεχνολογίες Πληροφορικής και Επικοινωνίας, μέχρι σήμερα δεν έχουν θεσμοθετήσει

υποχρεωτικούς κανονισμούς που να προστατεύουν τα προσωπικά δεδομένα και το απόρρητο των επικοινωνιών. Αντίθετα χώρες της Ευρωπαϊκής Ένωσης, μεταξύ των οποίων και η Ελλάδα, είναι υποχρεωμένες να ακολουθούν και να συγχωνεύουν στο Σύνταγμά τους νομικές διατάξεις που έχουν οριστεί από το Ευρωπαϊκό Κοινοβούλιο.

Η πιο πρόσφατη οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου που αφορά τους νόμους που επιβάλλονται για την διαδικασία της διατήρησης των δεδομένων είναι η Οδηγία 2006/24/ΕΚ «*Για την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών*» και αποτελεί ανανεωμένη και τροποποιημένη έκδοση της παλαιότερης οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Σύμφωνα με το γενικό μοντέλο της διαδικασίας της διασφάλισης των προσωπικών δεδομένων που αναπτύχθηκε στο 3ο κεφάλαιο, σημαντικό ρόλο για την προώθηση των κανονισμών που συμπεριλαμβάνονται σε κάθε Κοινοτική Οδηγία του Ευρωπαϊκού Κοινοβουλίου, έχει η ρυθμιστική αρχή κάθε χώρας. Κάθε χώρα της ευρωπαϊκής ένωσης επιβάλλεται να έχει ορίσει μια τέτοια αρχή η οποία θα αναλαμβάνει τον τόσο σημαντικό ρόλο του «ελεγκτή» των διαδικασιών με απώτερο σκοπό την διασφάλιση του απορρήτου των πληροφοριών.

5.2 Εθνική Ρυθμιστική Αρχή

Υπεύθυνος οργανισμός για την προώθηση, την διατήρηση και την ενίσχυση του νομικού πλαισίου είναι η Εθνική Ρυθμιστική Αρχή κάθε χώρας (NRA – National Regulatory Authority) που συμμετέχει στην Ευρωπαϊκή ένωση. Κάθε Εθνική Ρυθμιστική Αρχή έχει τον ρόλο του επόπτη και ελεγκτή των διαδικασιών της ηλεκτρονικής επικοινωνίας και της επεξεργασίας στις οποίες υπόκεινται τα δεδομένα, όπως επίσης και τον ρόλο του συμβούλου των δικαστικών αρχών κάθε χώρας. Επιπλέον η Εθνική Ρυθμιστική Αρχή οφείλει να είναι ανεξάρτητη, λειτουργώντας δηλαδή με αυτοτέλεια, γεγονός που ενισχύει την λειτουργικότητα και την αποτελεσματικότητά της.

Στην Ελλάδα αυτό τον ρόλο κατέχει η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.). Επιπλέον, με σκοπό την καλύτερη οργάνωση τέτοιου είδους οργανισμών και την ενίσχυση της αποτελεσματικότητάς, έχει συσταθεί το σώμα Ευρωπαίων Ρυθμιστών

Ηλεκτρονικών Επικοινωνιών (BEREC), που αποτελείται από το σύνολο των Εθνικών Ρυθμιστικών Αρχών των χωρών που μετέχουν στην Ευρωπαϊκή Ένωση.

5.2.1 Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC – Body of European Regulators for Electronic Communications) [47]

Το Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC - Body of European Regulators for Electronic Communications) ιδρύθηκε με κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της Ευρώπης, τον Νοέμβριο του 2009, ως μέρος του πακέτου μέτρων που αφορούσε την μεταρρύθμιση στις τηλεπικοινωνίες. Αντικατέστησε την Ευρωπαϊκή Ομάδα Ρυθμιστικών Αρχών για τα δίκτυα και τις υπηρεσίες ηλεκτρονικών επικοινωνιών, το οποίο είχε ιδρυθεί ως συμβουλευτική ομάδα της Επιτροπής το 2002. Την διάρκεια του 2011 το BEREC κατέστη πλήρως λειτουργικό και έτοιμο να εκπληρώσει τις εργασίες και τους σκοπούς για τους οποίους ιδρύθηκε.

ΕΙΚΟΝΑ 5.1: Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών

Κύριος σκοπό του σώματος είναι η ανεξάρτητη και συνεπής, παροχή κανονισμών για τις ηλεκτρονικές επικοινωνίες προς όφελος της Ευρώπης και των πολιτών της. Συμβάλλει στην ανάπτυξη και καλύτερη λειτουργία της εσωτερικής αγοράς για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, με σκοπό να εξασφαλισθεί η συνεπής εφαρμογή του κανονιστικού πλαισίου της ΕΕ και με στόχο την προώθηση μιας αποτελεσματικής εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιών, προκειμένου να φέρει ακόμη μεγαλύτερα οφέλη για τους καταναλωτές όσο και για τις επιχειρήσεις.

Επιπλέον, ο BEREC επικουρεί την Επιτροπή και τις Εθνικές Ρυθμιστικές Αρχές των χωρών της Ευρωπαϊκής Ένωσης στην εφαρμογή του κανονιστικού πλαισίου για τις ηλεκτρονικές επικοινωνίες. Παρέχει συμβουλές, κατόπιν αιτήματος και με δική του πρωτοβουλία για τα ευρωπαϊκά θεσμικά όργανα και συμπληρώνει σε ευρωπαϊκό επίπεδο τα ρυθμιστικά καθήκοντα που εκτελούνται σε εθνικό επίπεδο από την Εθνική Ρυθμιστική Αρχή.

Το Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών έχει τις ακόλουθες Αρμοδιότητες:

- αναπτύσσει και διαδίδει στις Εθνικές Ρυθμιστικές Αρχές βέλτιστες ρυθμιστικές πρακτικές, όπως κοινές προσεγγίσεις, μεθόδους ή κατευθυντήριες γραμμές σχετικά με την εφαρμογή του ρυθμιστικού πλαισίου της Ευρωπαϊκής Ένωσης.

- κατόπιν αιτήματος, παρέχει συνδρομή στις Εθνικές Ρυθμιστικές Αρχές όσον αφορά ρυθμιστικά ζητήματα.

- διατυπώνει γνώμες περί σχεδίων, αποφάσεων, συστάσεων και κατευθυντηρίων γραμμών της Ευρωπαϊκής Επιτροπής, όπως ορίζεται στο ρυθμιστικό πλαίσιο.

- εκδίδει εκθέσεις και παρέχει συμβουλές, κατόπιν αιτιολογημένου αιτήματος της Ευρωπαϊκής Επιτροπής ή με δική της πρωτοβουλία, και γνωμοδοτεί προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, όταν απαιτείται, για κάθε θέμα που εμπίπτει στην αρμοδιότητά του.

- κατόπιν αιτήματος, επικουρεί το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο, την Ευρωπαϊκή Επιτροπή και τις Εθνικές Ρυθμιστικές Αρχές σε σχέσεις, συζητήσεις και ανταλλαγές απόψεων με τρίτους και επικουρεί την Επιτροπή και τις Εθνικές Ρυθμιστικές Αρχές όσον αφορά τη διάδοση βέλτιστων ρυθμιστικών πρακτικών σε τρίτους.

5.2.2 Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)[48]

Η Ε.Ε.Τ.Τ. ιδρύθηκε με τον Ν.2246/1994 «Οργάνωση και Λειτουργία του Τομέα Τηλεπικοινωνιών», όπου ορίζεται ότι συνιστάται Επιτροπή με την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών (Ε.Ε.Τ.), ως αρμόδια για την εποπτεία της τηλεπικοινωνιακής αγοράς. Με τον

Ν.2867/2000 «Οργάνωση και Λειτουργία των Τηλεπικοινωνιών και Άλλες Διατάξεις», τροποποιήθηκε, και η Ε.Ε.Τ. μετονομάστηκε σε Ε.Ε.Τ.Τ. (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων).

Η Ε.Ε.Τ.Τ. χορηγεί άδειες σε Παρόχους Τηλεπικοινωνιακών Υπηρεσιών, στους οποίους ανήκουν και οι Πάροχοι Υπηρεσιών Διαδικτύου, οι γνωστοί και ως Παροχείς Υπηρεσιών Internet ή ISP's (Internet Service Providers). Ο έλεγχος και η ρύθμιση του τομέα των τηλεπικοινωνιών και η εποπτεία της τηλεπικοινωνιακής αγοράς ασκούνται από την Ε.Ε.Τ.Τ., η οποία αποτελεί την Εθνική Ρυθμιστική Αρχή (NRA) σε θέματα τηλεπικοινωνιών και η οποία Ε.Ε.Τ.Τ. είναι ανεξάρτητη διοικητική αρχή, που απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας.

Αρμοδιότητες της Ε.Ε.Τ.Τ. σε σχέση με τις ηλεκτρονικές επικοινωνίες:

- Ρύθμιση θεμάτων που αφορούν προϊόντα ή υπηρεσίες ηλεκτρονικών επικοινωνιών

- Ορισμός των υποχρεώσεων των Παρόχων προϊόντων ή υπηρεσιών ηλεκτρονικών επικοινωνιών, σύμφωνα με την εθνική και κοινοτική νομοθεσία.

- Εποπτεία και έλεγχος των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών όπως και, επιβολή κυρώσεων.

- Έκδοση Κώδικα Δεοντολογίας για την παροχή δικτύων και υπηρεσιών των ηλεκτρονικών επικοινωνιών.

- Μέριμνα για την τήρηση της νομοθεσίας περί ηλεκτρονικών επικοινωνιών και επιβολή κυρώσεων.

- Συνεργασία με τις Ρυθμιστικές Αρχές των λοιπών κρατών μελών της Ευρωπαϊκής Ένωσης ή τρίτων κρατών, καθώς και με κοινοτικούς ή διεθνείς φορείς σε θέματα αρμοδιότητάς της.

- Ρυθμίζει τα θέματα web domain με κατάληξη ".gr" και είναι αρμόδια για θέματα web domain με κατάληξη ".eu".

- Ρυθμίζει τα θέματα πρόσβασης και διασύνδεσης.

- Ρυθμίζει θέματα προστασίας του καταναλωτή στον τομέα των ηλεκτρονικών επικοινωνιών και στον τομέα παροχής ταχυδρομικών υπηρεσιών.

Στην Ελλάδα λειτουργούν δύο ανεξάρτητες Αρχές, που εποπτεύουν σε ζητήματα ασφαλείας και προστασίας στο Διαδίκτυο και στις επικοινωνίες γενικότερα και σ' αυτές μπορούν να αναφερθούν σχετικά προβλήματα. Είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία δημιουργήθηκε σύμφωνα με τον Ν.3115/2003. Αλλά και η Ε.Ε.Τ.Τ. έχει το δικαίωμα να επιβάλλει ιδιαίτερους όρους σχετικά με την τήρηση του απορρήτου των τηλεπικοινωνιών στις εταιρείες που διαθέτουν άδεια χρήσης τηλεπικοινωνιακών δραστηριοτήτων και σ' αυτές φυσικά υπάγονται και οι Πάροχοι Υπηρεσιών Διαδικτύου (ISP's).

5.2.3 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)[49][50]

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών ιδρύθηκε το 2003 με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο. Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας.

ΕΙΚΟΝΑ 5.2: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Η ΑΔΑΕ, για την εκπλήρωση της αποστολής της, έχει τις ακόλουθες αρμοδιότητες:

- Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, τακτικούς και έκτακτους ελέγχους, σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), όπως και άλλων δημοσίων υπηρεσιών, οργανισμών ή επιχειρήσεων του ευρύτερου δημόσιου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

- Λαμβάνει πληροφορίες σχετικές με την αποστολή της, από τις προαναφερθείσες υπηρεσίες, οργανισμούς και επιχειρήσεις, καθώς και από τους εποπτεύοντες Υπουργούς.

- Καλεί σε ακρόαση, από τις υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις που αναφέρονται, τις διοικήσεις, τους νόμιμους εκπροσώπους, τους υπαλλήλους και κάθε άλλο πρόσωπο, το οποίο κρίνει ότι μπορεί να συμβάλλει στην εκπλήρωση της αποστολής της.

- Προβαίνει στην κατάσχεση μέσων παραβίασης του απορρήτου, που υποπίπτουν στην αντίληψή της κατά την ενάσκηση του έργου της και ορίζεται μεσεγγυούχος αυτών μέχρι να αποφανθούν τα αρμόδια δικαστήρια. Προβαίνει στην καταστροφή πληροφοριών ή στοιχείων ή δεδομένων, τα οποία αποκτήθηκαν με παράνομη παραβίαση του απορρήτου των επικοινωνιών.

- Εξετάζει καταγγελίες σχετικά με την προστασία των δικαιωμάτων των αιτούντων, όταν θίγονται από τον τρόπο και τη διαδικασία άρσης του απορρήτου.

- Στις περιπτώσεις άρσης του απορρήτου, η Α.Δ.Α.Ε. υπεισέρχεται μόνο στον έλεγχο της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, χωρίς να εξετάζει την κρίση των αρμόδιων δικαστικών αρχών.

- Τηρεί αρχείο απόρρητης αλληλογραφίας,

- Συνεργάζεται με άλλες αρχές της χώρας ή αντίστοιχες αρχές άλλων κρατών όπως επίσης και με ευρωπαϊκούς και διεθνείς οργανισμούς, για θέματα της αρμοδιότητάς της.

- Συντάσσει κάθε χρόνο την προβλεπόμενη έκθεση πεπραγμένων, στην οποία περιγράφει το έργο της, διατυπώνει παρατηρήσεις, επισημαίνει παραλείψεις και προτείνει τυχόν ενδεικνυόμενες νομοθετικές μεταβολές στον τομέα διασφάλισης του απορρήτου των επικοινωνιών.

- Γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών, καθώς και για τη διαδικασία άρσης αυτού.

- Εκδίδει τον κανονισμό εσωτερικής λειτουργίας της, ο οποίος πρέπει να είναι σύμφωνος με τις διατάξεις του Κώδικα Διοικητικής Διαδικασίας, όπως και κανονιστικές πράξεις, μέσω των οποίων ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις αρμοδιότητές της, καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών. Επιπλέον καταρτίζει τον κανονισμό οικονομικής διαχείρισης.

5.2.4 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[51]

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή η οποία ιδρύθηκε με σκοπό την ενσωμάτωση των ευρωπαϊκών κανονισμών για την προστασία των προσωπικών δεδομένων στην ελληνική νομοθεσία.

ΕΙΚΟΝΑ 5.3: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Αρμοδιότητες της ΑΠΔΠΧ είναι:

- Έκδοση Οδηγιών με σκοπό την ενιαία εφαρμογή των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα

- Συστήνει και υποδεικνύει στους υπεύθυνους επεξεργασίας τις ρυθμίσεις και κώδικες δεοντολογίας σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα.

- Ενημέρωση των υποκειμένων των δεδομένων καθώς και των υπεύθυνων επεξεργασίας ως προς τα δικαιώματα και τις υποχρεώσεις τους, μέσω ετήσιων εκθέσεων απολογισμού, ανακοινώσεων στην Βουλή για παραβάσεις

- Έκδοση αδειών, υπό όρους, για τη συλλογή, την διαβίβαση και επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- Διενέργεια διοικητικών ελέγχων σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα.

- Εξέταση προσφυγών-καταγγελιών-ερωτημάτων σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων, και επιβολή κυρώσεων σε πιθανές παραβάσεις.

5.3 Παρουσίαση της Οδηγίας 2006/24/ΕΚ [52]

Συνοπτικά η νέα Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με τίτλο «Για την διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ» περιγράφει την υποχρέωση μακροπρόθεσμης αποθήκευσης ορισμένων εξωτερικών δεδομένων επικοινωνίας των χρηστών-συνδρομητών υπηρεσιών και δικτύων τηλεπικοινωνιών από τους παρόχους των υπηρεσιών αυτών, για ενδεχόμενη χρήση τους από τις αρχές με σκοπό την διαλεύκανση σοβαρών εγκλημάτων. Αναφέρεται επίσης ότι κατά την διαδικασία ενσωμάτωσης

σε της οδηγίας σε οποιαδήποτε εθνική νομοθεσία, ο νομοθέτης οφείλει να παράγει ρυθμίσεις που να αποδίδουν σεβασμό στα θεμελιώδη ατομικά δικαιώματα.

5.3.1 Αντικείμενο και σχετικοί Ορισμοί [52]

Το αντικείμενο της οδηγίας είναι η εναρμόνιση των διατάξεων που περιγράφονται σε αυτή με το νομικό πλαίσιο κάθε κράτους μέλους. Οι διατάξεις αυτές περιγράφουν τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών όσον αφορά την διατήρηση δεδομένων που παράγονται ή υφίστανται επεξεργασία από αυτούς, ώστε να διασφαλίζεται ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων, σύμφωνα με το εθνικό δίκαιο κάθε χώρας.

Στην οδηγία αποσαφηνίζονται ορισμοί όπως:

- **Υπηρεσίες ηλεκτρονικών επικοινωνιών**

  Οι υπηρεσίες που παρέχονται δωρεάν ή έναντι αμοιβής και των οποίων η παροχή συνίσταται κυρίως στη μεταφορά σημάτων μέσω δικτύων ηλεκτρονικών επικοινωνιών.

- **Δημόσιο δίκτυο επικοινωνιών**

  Το δίκτυο ηλεκτρονικών επικοινωνιών, το οποίο χρησιμοποιείται, εξ ολοκλήρου ή κυρίως, για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών.

- **Πάροχος υπηρεσιών ηλεκτρονικών επικοινωνιών**

  Η επιχείρηση η οποία παρέχει διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών.

- **Πάροχος δημόσιου δικτύου ηλεκτρονικών επικοινωνιών**

Η επιχείρηση η οποία εγκαθιστά, λειτουργεί, ελέγχει και διαθέτει δημόσιο δίκτυο ηλεκτρονικών επικοινωνιών.

- **Δεδομένα**

  τα δεδομένα κίνησης και θέσης και τα συναφή δεδομένα που είναι αναγκαία για την αναγνώριση του συνδρομητή ή χρήστη.

- **Χρήστης**

  κάθε νομική οντότητα ή φυσικό πρόσωπο που χρησιμοποιεί διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών, για ιδιωτικούς ή εμπορικούς σκοπούς χωρίς να είναι απαραίτητα συνδρομητής της εν λόγω υπηρεσίας.

- **Τηλεφωνική υπηρεσία**

  Κλήσεις (συμπεριλαμβανομένων των φωνητικών τηλεφωνημάτων, του φωνητικού τηλεταχυδρομείου, των τηλεδιασκέψεων και της τηλεφωνικής μεταφοράς δεδομένων), συμπληρωματικές υπηρεσίες (συμπεριλαμβανομένης της προώθησης και της εκτροπής κλήσεων), υπηρεσίες μηνυμάτων και πολυμέσων (συμπεριλαμβανομένων των υπηρεσιών γραπτών μηνυμάτων, ενισχυμένων μέσων και πολυμέσων).

- **Κωδικός ταυτότητας χρήστη**

  Ο μοναδικός αναγνωριστικός κωδικός που αποδίδεται σε κάθε πρόσωπο όταν καθίσταται συνδρομητής ή εγγράφεται σε κάποια υπηρεσία πρόσβασης στο Διαδίκτυο ή επικοινωνίας μέσω του Διαδικτύου.

- **Κωδικός ταυτότητας κυψέλης**

  Η ταυτότητα του κυψελωτού κυττάρου από το οποίο ξεκινά ή στο οποίο καταλήγει συγκεκριμένη κλήση κινητής τηλεφωνίας.

- **Ανεπιτυχής κλήση**

Κλήση κατά την οποία επιτυγχάνεται μεν σύνδεση με τον αριθμό προορισμού, η κλήση όμως παραμένει αναπάντητη ή σημειώνεται επέμβαση της διαχείρισης του δικτύου.

5.3.2 Υπόχρεοι Διατήρησης και είδη Διατηρούμενων Δεδομένων [52]

Υποχρεώνονται, σύμφωνα με τις διατάξεις που αναφέρονται στην Οδηγία, να διατηρούν δεδομένα, οι επιχειρήσεις-πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή οι επιχειρήσεις-πάροχοι δημόσιων δικτύων ηλεκτρονικών επικοινωνιών εφόσον κατά την παροχή των υπηρεσιών τα δεδομένα παράγονται ή υποβάλλονται σε επεξεργασία που εμπίπτει στην δικαιοδοσία τους. Υποχρεωτική θεωρείται ακόμα και η διατήρηση των δεδομένων από ανεπιτυχείς κλήσεις όταν τα δεδομένα αυτά παράγονται ή υποβάλλονται σε επεξεργασία και όταν αποθηκεύονται (όσον αφορά τηλεφωνικά δεδομένα) ή καταγράφονται (όσον αφορά διαδικτυακά δεδομένα) από τους παρόχους των διαθέσιμων υπηρεσιών.

Η Οδηγία εξειδικεύει το είδος της ηλεκτρονικής υπηρεσίας για το οποίο επιβάλλεται διατήρηση δεδομένων επικοινωνίας και αναφέρεται συγκεκριμένα σε υποχρέωση διατήρησης δεδομένων επικοινωνίας από παρόχους που προσφέρουν διαθέσιμες στο ευρύ κοινό τις ακόλουθες ηλεκτρονικές υπηρεσίες :

- Υπηρεσίες Σταθερής τηλεφωνίας
- Υπηρεσίες Κινητής τηλεφωνίας
- Υπηρεσίες Πρόσβασης στο Διαδίκτυο
- Υπηρεσίες Τηλεφωνίας μέσω Διαδικτύου
- Υπηρεσίες Ηλεκτρονικού Ταχυδρομείου μέσω Διαδικτύου

Διευκρινίζονται επιπλέον, τα είδη των δεδομένων που οι πάροχοι είναι υποχρεωμένοι να διατηρούν, τα οποία δεδομένα εμπίπτουν στην κατηγορία των εξωτερικών δεδομένων επικοινωνίας όπως κατηγοριοποιήθηκαν στο 1ο κεφάλαιο, δηλαδή ανάλογα με την τεχνολογία

την οποία διαβιβάζονται και τον λόγο χρήσης τους όπως τον έλεγχο, την διευθυνσιοδότηση και την παροχή της επικοινωνίας.

5.3.3 Προστασία Δεδομένων, Πρόσβαση και διάρκεια Διατήρησης [52]

Σχετικά με την διάρκεια διατήρησης η Κοινοτική Οδηγίας κατευθύνει τα κράτη μέλη να ορίζουν χρονικά διαστήματα διατήρησης τα οποία δεν μπορούν να είναι μικρότερα των 6 μηνών, αλλά ούτε όμως μεγαλύτερα των 24 μηνών. Ωστόσο τα χρονικά διαστήματα διατήρησης των δεδομένων επικοινωνίας επαφίενται στην διακριτική ευχέρεια της εθνικής νομοθεσίας του κάθε κράτους μέλους αρκεί να εμπίπτουν στα πλαίσια της δεδομένης κατεύθυνσης που προβλέπει η Κοινοτική Οδηγία.

Γίνεται ειδική αναφορά στην υποχρέωση λήψης κατάλληλων οργανωτικών και τεχνικών μέτρων για την διασφάλιση της ακεραιότητας, της ακρίβειας και της εμπιστευτικότητας των αποθηκευμένων δεδομένων, όπως επίσης προβλέπεται η υποχρέωση πρόσβασης στα δεδομένα μόνον από ειδικά εξουσιοδοτημένο προσωπικό. Τα κράτη μέλη οφείλουν να θεσπίσουν μέτρα σύμφωνα με τα οποία διασφαλίζεται η σύννομη πρόσβαση στα διατηρούμενα δεδομένα μόνον από τις αρμόδιες εθνικές αρχές και για ειδικές περιπτώσεις. Οι διαδικασίες και όροι πρόσβασης ορίζονται από τα κράτη μέλη σύμφωνα με τις αρχές αναλογικότητας και αναγκαιότητας και σεβόμενοι τις διατάξεις που αφορούν τα ανθρώπινα δικαιώματα. Προβλέπεται επίσης η εφαρμογή αποτρεπτικών και αποτελεσματικών μέτρων σχετικά με την απόδοση ποινικών ευθυνών και κυρώσεων ιδίως σε ότι αφορά εκ προθέσεως παράνομες προσπελάσεις και μεταφορές των διατηρούμενων δεδομένων.

Βαρύτητα δίνεται στην ασφαλή καταστροφή των αποθηκευμένων τηλεπικοινωνιακών δεδομένων με το πέρας του χρονικού διαστήματος διατήρησης ως μέρος των μέτρων προστασίας των δεδομένων. Τα δεδομένα επιβάλλεται να καταστρέφονται στο τέλος αυτού του διαστήματος, προβλέπεται όμως εξαίρεση σε περίπτωση όπου ένα κράτος αντιμετωπίζει συνθήκες τέτοιες που να δικαιολογούν περιορισμένη παράταση του διαστήματος διατήρησης. Σε τέτοια περίπτωση προβλέπεται η απόφαση της επιτροπής μετά από την ενημέρωση της για τους λόγους της παράτασης.

5.3.4 Υποχρεώσεις Κρατών Μελών [52]

Κατά την διάρκεια διατήρησης και για την προστασία των πολιτών τους τα κράτη μέλη οφείλουν να διασφαλίζουν ότι τα δεδομένα θα διατηρούνται με τέτοιο τρόπο ώστε αυτά ή οποιαδήποτε άλλη πληροφορία σχετικά με αυτά να μπορούν να διαβιβαστούν έπειτα από αίτημα στις αρμόδιες αρχές χωρίς αδικαιολόγητη καθυστέρηση.

Ιδιαίτερη αναφορά υπάρχει σχετικά με την υποχρέωση, κάθε κράτους μέλους, ορισμού μίας η περισσότερων ανεξάρτητων δημόσιων αρχών οι οποίες και θα είναι αρμόδιες για την εποπτεία των διαδικασιών και της εφαρμογής των διατάξεων που σχετίζονται με την ασφάλεια των διατηρούμενων δεδομένων.

Τα κράτη μέλη υποχρεούνται επίσης να παρέχουν κάθε χρόνο στην επιτροπή τα στατιστικά στοιχεία σχετικά με την διατήρηση δεδομένων, τα οποία παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίου δικτύου επικοινωνιών. Αυτά τα στατιστικά στοιχεία περιλαμβάνουν:

- τις περιπτώσεις στις οποίες παρασχέθηκαν πληροφορίες στις αρμόδιες αρχές σύμφωνα με το εφαρμοστέο εθνικό δίκαιο,
- το χρονικό διάστημα μεταξύ της ημερομηνίας διατήρησης των δεδομένων και της ημερομηνίας υποβολής του αιτήματος από την αρμόδια αρχή για τη διαβίβαση των δεδομένων,
- τις υποθέσεις στις οποίες δεν κατέστη δυνατόν να ικανοποιηθούν τα αιτήματα για δεδομένα.

5.3.5 Προβλήματα στην εφαρμογή της οδηγίας [53]

Η εφαρμογή της οδηγίας δεν θεωρήθηκε από όλους ως μέσο προάσπισης της ιδιωτικότητας. Το αντίθετο μάλιστα, καθώς σύμφωνα με το Ανώτατο Δικαστήριο (High Court) της Ιρλανδίας και το Συνταγματικό Δικαστήριο της Αυστρίας (Verfassungsgerichtshof) με αίτηση για επανεξέταση που υπέβαλλαν στο Ευρωπαϊκό δικαστήριο παραβιάζονται δύο θεμελιώδη δικαιώματα τα οποία εγγυάται ο Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ήτοι το θεμελιώδες δικαίωμα σεβασμού της ιδιωτικής ζωής και το θεμελιώδες δικαίωμα της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Η υπόθεση προέκυψε ύστερα από διαφορά μεταξύ της ιρλανδικής εταιρίας Digital Rights και των ιρλανδικών αρχών σχετικά με τη νομιμότητα των εθνικών μέτρων περί διατηρήσεως δεδομένων που αφορούν ηλεκτρονικές επικοινωνίες και διαφόρων προσφυγών που αφορούν ζητήματα συνταγματικού δικαίου και ασκήθηκαν από την Κυβέρνηση του ομόσπονδου κράτους της Καρινθίας, Αυστρία (Kärntner Landesregierung) καθώς και από τους M. Seitlinger, C. Tschohl και άλλους προσφεύγοντες.

Το Ευρωπαϊκό Δικαστήριο διαπίστωσε ότι παρέχεται η δυνατότητα μέσω των κατευθυντηρίων γραμμών της Οδηγίας, περί της διατήρησης των δεδομένων, να παρέχονται ακριβέστατες ενδείξεις σχετικά με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα διατηρούνται και εκτίμησε ότι η οδηγία επεμβαίνει πολύ σοβαρά στην άσκηση των θεμελιωδών δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Η προδικαστική παραπομπή δεν ακυρώνει εξ ολοκλήρου την Οδηγία αλλά παρέχει στα δικαστήρια των κρατών μελών τη δυνατότητα, στο πλαίσιο της ένδικης διαφοράς της οποίας έχουν επιληφθεί, να υποβάλουν στο Δικαστήριο ερώτημα σχετικό με την ερμηνεία της. Στο εθνικό δικαστήριο εναπόκειται να επιλύσει τη διαφορά σύμφωνα με την απόφαση του Ευρωπαϊκού Δικαστηρίου. Η απόφαση αυτή δεσμεύει, κατά τον ίδιο τρόπο, τα άλλα εθνικά δικαστήρια που επιλαμβάνονται παρόμοιου προβλήματος.

5.4 Ελληνική Νομοθεσία

Η κοινοτική Οδηγία 2006/24/ΕΚ, όπως ήταν αναμενόμενο, έχει υιοθετηθεί πλήρως από την Ελληνική νομοθεσία και οι κανονισμοί που θεσμοθετήθηκαν ενσωματώνονται στον Νόμο 3917/2011. Οι εμπεριεχόμενες διατάξεις και κανονισμοί, όπου ήταν εφικτό, έχουν διαμορφωθεί σύμφωνα με το Σύνταγμα και τις ανάγκες της χώρας, εφόσον βέβαια δεν παρεκκλίνουν από τις συντεταγμένες και τα όρια των κατευθύνσεων που καθορίζει η Οδηγία του Ευρωπαϊκού Συμβουλίου.

5.4.1 Νόμος 3917/2011 για την Διατήρηση των προσωπικών δεδομένων [54]

Στον νόμο 3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις» αφομοιώνονται οι Ευρωπαϊκοί κανονισμοί με τις απαραίτητες τροποποιήσεις όπου αυτό ήταν επιτρεπτό. Οι διατάξεις που εμπεριέχονται περιγράφουν τις υποχρεώσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών σε σχέση με την διατήρηση δεδομένων, ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων και η διαθεσιμότητα τους κατά την διερεύνηση και ανίχνευση σοβαρών ποινικών αδικημάτων.

- **Υπόχρεοι Διατήρησης και είδη Διατηρούμενων Δεδομένων**

Υποχρεώνονται, όπως και στην Οδηγία 2006/24/ΕΚ,, να διατηρούν δεδομένα, οι επιχειρήσεις-πάροχοι διαθέσιμων στο κοινό υπηρεσιών ή δικτύων ηλεκτρονικών επικοινωνιών εφόσον κατά την παροχή των υπηρεσιών τα δεδομένα παράγονται ή υποβάλλονται σε επεξεργασία που εμπίπτει στην δικαιοδοσία τους. Η διατήρηση εφαρμόζεται μόνο σε δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη. Επίσης θεωρείται υποχρεωτική και η διατήρηση των δεδομένων από ανεπιτυχείς κλήσεις εφόσον αυτά υπόκεινται σε διαδικασίες επεξεργασίας. Τα είδη των διατηρούμενων δεδομένων, αποτελούν τα εξωτερικά δεδομένα επικοινωνίας και κατηγοριοποιούνται αντίστοιχα με την Οδηγία.

- **Προστασία Δεδομένων, Πρόσβαση και διάρκεια Διατήρησης**

Τα δεδομένα που διατηρούνται από τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών πρέπει να ακλουθούν κανόνες ασφαλείας για την διασφάλιση της ακεραιότητας τους. Τα διατηρούμενα δεδομένα πρέπει να είναι ίδιας ποιότητας και να έχουν την ίδια προστασία και ασφάλεια με τα δεδομένα που περιέχει το δίκτυο. Για την επίτευξη αυτού πρέπει να λαμβάνονται κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας των δεδομένων όπως επίσης και κατάλληλα τεχνικά και οργανωτικά μέτρα για την διασφάλιση της εξουσιοδοτημένης πρόσβασης σε αυτά.

Ο νόμος υποχρεώνει τους παρόχους να καταρτίζουν και να εφαρμόζουν ειδικό σχέδιο πολιτικής ασφάλειας ως προς τα μέσα, τις μεθόδους και τα μέτρα που θα διασφαλίζουν την τήρηση των διαδικασιών.

Ο πάροχος υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούται να διατηρεί τα δεδομένα κατά τρόπο που να του επιτρέπει να τα επεξεργάζεται ηλεκτρονικά και να τα διαβιβάζει το αργότερο μέσα σε πέντε εργάσιμες ημέρες από τη γνωστοποίηση της διάταξης για πιθανή πρόσβαση η οποία αιτείται από την αρμόδια αρχή.

Για την προστασία των διατηρούμενων δεδομένων τα δεδομένα πρέπει να αποθηκεύονται από τον πάροχο χωρίς υπαίτια καθυστέρηση σε φυσικά μέσα, τα οποία να βρίσκονται αποκλειστικά μέσα στα όρια της Ελληνικής Επικράτειας, και να διατηρούνται για 12 μήνες από την ημερομηνία της επικοινωνίας. Τα δεδομένα καταστρέφονται στο τέλος αυτού του χρονικού διαστήματος με αυτοματοποιημένη διαδικασία από τον πάροχο, εκτός από εκείνα στα οποία έχει αποκτηθεί νομίμως πρόσβαση τα οποία, εφόσον παρήλθε η παραπάνω προθεσμία των 12 μηνών, καταστρέφονται από τον πάροχο μέσα σε δέκα ημέρες μετά από αίτηση των αρμόδιων αρχών.

- **Προϋποθέσεις Πρόσβασης - Άρση του απορρήτου**

Οι προϋποθέσεις για την άρση του απορρήτου των επικοινωνιών ενσωματώνονται στον συγκεκριμένο νόμο από τον νόμο 2225/1994. Γίνεται σαφές ότι η πρόσβαση στα δεδομένα είναι εφικτή μόνο για συγκεκριμένες σοβαρές παραβάσεις των νόμων του κράτους, όπως επίσης και για παραβάσεις που θέτουν σε κίνδυνο την εθνική ασφάλεια, αφορούν δηλαδή την προστασία του συνόλου μιας χώρας, της εδαφικής της ακεραιότητας και της πολιτιστικής της ανεξαρτησίας από ξένη δύναμη ή απειλή ξένης δύναμης. Ωστόσο η άρση σε περιπτώσεις ζητημάτων που αφορούν την εθνική ασφάλεια, δεν είναι ιδιαίτερη ξεκάθαρη καθώς ο ορισμός «εθνική ασφάλεια» είναι γενικός, με κίνδυνο να μπορεί να γίνει καταχρηστική εφαρμογή του.

Την άρση του απορρήτου αποφασίζει το αρμόδιο δικαστικό συμβούλιο μετά από την εισαγγελική ή δημόσια αρχή, ή τον ανακριτή που ζητούν την επιβολή της. Η χρονική διάρκεια της άρσης του απορρήτου δεν μπορεί να υπερβαίνει τους 2 μήνες και παρατάσεις ίδιας διάρκειας διατάσσονται μετά από συγκεκριμένη διαδικασία άρσης του

απορρήτου, υπό την προϋπόθεση ότι ισχύουν οι αρχικοί λόγοι της άρσης. Σε κάθε περίπτωση οι παρατάσεις δεν μπορούν να υπερβαίνουν συνολικά τη διάρκεια των δέκα 10 μηνών, παρά μόνο σε περιπτώσεις εθνικής ασφάλειας.

- **Στατιστικά στοιχεία**

Η Α.Δ.Α.Ε. είναι υποχρεωμένη να διαβιβάζει ανά έτος στην Ευρωπαϊκή Επιτροπή, στατιστικά στοιχεία για το προηγούμενο ημερολογιακό έτος, όπως τις περιπτώσεις στις οποίες παρασχέθηκαν πληροφορίες στις αρμόδιες αρχές, το χρονικό διάστημα μεταξύ της ημερομηνίας έναρξης διατήρησης των δεδομένων και της ημερομηνίας υποβολής του αιτήματος από την αρμόδια αρχή για τη διαβίβαση των δεδομένων και τις περιπτώσεις στις οποίες δεν κατέστη δυνατόν να ικανοποιηθούν τα αιτήματα για τη χορήγηση των δεδομένων.

5.4.2 Νόμοι για την προστασία της Επικοινωνίας και των προσωπικών δεδομένων

Φυσικά οι απειλές κατά των δεδομένων των υποκειμένων αλλά και οι κίνδυνοι παραβίασης της Ιδιωτικότητας τους δεν διατρέχονται μόνο κατά τις διαδικασίες και τις ενέργειες που λαμβάνουν χώρα στο διάστημα κατά το οποία αυτά διατηρούνται από τους παρόχους των ηλεκτρονικών υπηρεσιών. Απαιτούνται λοιπόν κανονιστικές ρυθμίσεις και διατάξεις, επιπλέον του νόμου για την Διατήρηση των προσωπικών δεδομένων, που να προβλέπουν όλες τις πιθανές απειλές που αντιμετωπίζουν τα δεδομένα. Η Ελληνική νομοθεσία περιλαμβάνει επιπλέον νόμους για τους συγκεκριμένους σκοπούς, που είναι πάντα σε εναρμόνιση και συμφωνία με τις κατευθύνσεις της Ευρωπαϊκής Ένωσης.

- **ΝΟΜΟΣ 3674 – «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» [55]**

Ο συγκεκριμένος νόμος αφορά ρυθμίσεις που θωρακίζουν της τηλεφωνικές επικοινωνίες, δηλαδή επικοινωνίες για τη πραγματοποίηση και τη λήψη εθνικών και διεθνών κλήσεων μέσω αριθμού ή αριθμών του εθνικού σχεδίου αριθμοδότησης. Αναφέρονται οι ευθύνες των παρόχων των τηλεφωνικών υπηρεσιών που περιλαμβάνουν την ύπαρξη τεχνικών και οργανωτικών μέτρων για την ασφάλεια των

χώρων, εγκαταστάσεων, συνδέσεων και των συστημάτων υλικού και λογισμικού και για την ανίχνευση παραβιάσεων ή απόπειρας παραβιάσεων του απορρήτου.

Αναφέρεται επίσης πως ο πάροχος υποχρεούται να καταρτίζει και να εφαρμόζει ειδικό σχέδιο πολιτικής ασφάλειας σχετικά με τα μέσα, τις μεθόδους και τα μέτρα που διασφαλίζουν το απόρρητο της επικοινωνίας, όπως και να εφαρμόζει τεχνικές κρυπτογράφησης στα φωνητικά σήματα πληροφοριών που μεταδίδονται από τα εκτός της εποπτείας του φυσικά μέσα μετάδοσης. Συν τις άλλοις όπως και στους υπόλοιπους νόμους, παρουσιάζονται διαχειριστικοί, οι κανονισμοί για την διαδικασία άρσης του απορρήτου και ποινικές ευθύνες και κυρώσεις.

- **ΝΟΜΟΣ 2472 – «Προστασία του ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα»** [06]

Νόμος όπου περιέχονται ρυθμίσεις για την θέσπιση προϋποθέσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την προάσπιση των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής.

Σύμφωνα με τους εμπεριεχόμενους κανονισμούς τα δεδομένα για να μπορούν να υποβληθούν σε οποιαδήποτε διαδικασία νόμιμης επεξεργασίας θα πρέπει να τηρούν κάποιες προϋποθέσεις:

- Η συλλογή τους να έχει γίνει με θεμιτό και νόμιμο τρόπο για καθορισμένους και νόμιμους σκοπούς και να υποβάλλονται σε θεμιτή και νόμιμη επεξεργασία, σύμφωνα με τους εν λόγω σκοπούς.

- Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα απαιτούνται για επεξεργασία

- Να είναι ακριβή και ενημερωμένα.

- Να διατηρούνται σε μορφή από την οποία να προσδιορίζεται η ταυτότητα των υποκειμένων τους και για τη διάρκεια που απαιτείται ή κρίνεται ανάλογα τις αποφάσεις και τους κανονισμούς της αρμόδιας Αρχής.

Ρητά αναφέρεται ότι οποιαδήποτε διαδικασία επεξεργασίας είναι απαγορευμένη σε περίπτωση μη συγκατάθεσης του υποκειμένου των δεδομένων. Εξαιρούνται περιπτώσεις όπου το υποκείμενο των δεδομένων τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, περιπτώσεις όπου ή επεξεργασία επιβάλλεται από τον νόμο ή είναι απαραίτητη για νομικές διαδικασίες των εμπλεκομένων, περιπτώσεις αναγκαίες για την εκτέλεση δημόσιου έργου ή διαδικασιών που εμπίπτουν την αρμοδιότητα δημόσιας αρχής, και τέλος περιπτώσεις όπου απαιτείται για την ολοκλήρωση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος.

- **ΝΟΜΟΣ 3471 – «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»** [56]

Νόμος που εμπεριέχει κυρίως ανάλυση εννοιών και παρουσίαση διαδικασιών που σχετίζονται με τα προσωπικά δεδομένα και την επεξεργασία τους. Εμπεριέχεται η κατηγοριοποίηση των δεδομένων επικοινωνίας καθώς και οι προϋποθέσεις υπό τις οποίες τα δεδομένα μπορούν να είναι αντικείμενο επεξεργασίας.

Συνοπτικά αναφέρεται πως η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της και επιτρέπεται μόνον εφόσον το υποκείμενο των δεδομένων έχει πλήρη ενημέρωση για αυτό και τον σκοπό της επεξεργασίας, ή η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία ο συνδρομητής ή ο χρήστης είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατά το προσυμβατικό στάδιο, μετά από αίτηση του συνδρομητή.

Ενδιαφέρον παρουσιάζει και η πρόβλεψη για τις περιπτώσει μη ζητηθείσας επικοινωνίας, γνωστές ως αυτόκλητα μηνύματα ή κλήσεις (spam) όπου ρητά αναφέρεται η απαγόρευση τους, εφόσον δεν έχει προηγηθεί συγκατάθεση του χρήστη.

- **ΝΟΜΟΣ 3783 – «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις»** [57]

Σκοπός του νόμου είναι η ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας ή άλλης μορφής κινητής τηλεπικοινωνίας, για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Περιλαμβάνονται κανονισμοί που αφορούν τις διαδικασίες ταυτοποίησης του συνδρομητή των υπηρεσιών κινητής τηλεφωνίας. Παρουσιάζονται και εδώ ορισμοί που αφορούν τις τηλεπικοινωνίες αλλά και την Διατήρηση και πρόσβαση στα στοιχεία συνδρομητή μιας υπηρεσίας κινητής τηλεφωνίας.

Η σημαντικότητα του νόμου έγκειται στο γεγονός ότι εδραιώνει νομικά την υποχρεωτική διαδικασία που οφείλουν να ολοκληρώνουν οι πάροχοι των υπηρεσιών κινητής τηλεφωνίας και αφορά την ταυτοποίηση των συνδρομητών τους σε οποιαδήποτε ζητηθείσα υπηρεσία. Δηλαδή πλέον οι πάροχοι υποχρεούνται πριν την έναρξη του συμβολαίου παροχής υπηρεσιών κινητής τηλεφωνίας να γνωρίζουν τα στοιχεία ταυτότητας από τα οποία να μπορεί να ταυτοποιηθεί ο συνδρομητής της.

5.5 Νομοθεσία των Η.Π.Α. [58]

Στις Ηνωμένες Πολιτείες δεν υπάρχει ενιαία νομοθεσία που να παρέχει ένα ολοκληρωμένο πλαίσιο προστασίας σε θέματα που αφορούν τα δεδομένα και την ιδιωτικότητα. Τα δεδομένα προστατεύονται από τις συνταγματικές ερμηνείες που παρέχονται από τα δικαστήρια, από κάποιες διεθνείς συμφωνίες, και μια σειρά από νόμους και εκτελεστικά διατάγματα που ασχολούνται ειδικά με την έννοια της προστασίας δεδομένων. Οι νόμοι αυτοί βέβαια, οι οποίοι σχετίζονται με τα προσωπικά δεδομένα, ελλείψει κοινού πλαισίου προστασίας μπορεί να διαφέρουν ή να αλληλοαναιρούνται μεταξύ των 50 πολιτειών που αποτελούν τις ΗΠΑ.

Οι πιο σημαντικοί και ευρείας βάσης, από αυτούς τους νόμους είναι ο νόμος «Privacy Act of 1974» και ο νόμος «Computer Matching and Privacy Act». Αυτοί οι νόμοι όμως ασχολούνται αποκλειστικά με τις προσωπικές πληροφορίες που κατέχονται από την ομοσπονδιακή κυβέρνηση και δεν έχουν καμία εξουσία σε ότι αφορά την συλλογή και χρήση των προσωπικών πληροφοριών που κατέχονται από άλλους φορείς του ιδιωτικού και του δημόσιου τομέα.

Ο «Privacy Act» εγκρίθηκε τόσο για την προστασία των προσωπικών δεδομένων στις ομοσπονδιακές βάσεις δεδομένων, όσο και για την παροχή ορισμένων δικαιωμάτων στα άτομα στα οποία ανήκουν τα δεδομένα που περιέχονται σε αυτές τις βάσεις δεδομένων. Αναπτύχθηκε ρητά για την αντιμετώπιση των προβλημάτων που προκαλούνται από τις ηλεκτρονικές τεχνολογίες και τα συστήματα καταγραφής προσωπικών πληροφοριών και καλύπτει τη συντριπτική πλειοψηφία αυτών των συστημάτων τα οποία διαχειρίζονται από την

ομοσπονδιακή κυβέρνηση. Παρουσιάζει ορισμένες βασικές αρχές της «δίκαιης πρακτικής πληροφόρησης», και παρέχει στους πολίτες το δικαίωμα πρόσβασης σε πληροφορίες σχετικά με τον εαυτό τους όπως επίσης και το δικαίωμα της αμφισβήτησης αυτού του περιεχομένου. Οι προσωπικές πληροφορίες μπορούν να αποκαλυφθούν μόνο με τη συναίνεση του ατόμου ή για σκοπούς για τους οποίους το άτομο είναι εκ των προτέρων ενημερωμένο. Η πράξη απαιτεί επίσης ομοσπονδιακές υπηρεσίες να δημοσιεύουν κάθε χρόνο κατάλογο των συστημάτων που διαχειρίζονται από αυτές και επεξεργάζονται προσωπικές πληροφορίες.

Στις ΗΠΑ δεν υπάρχει επίσημη εθνική αρχή προστασίας των δεδομένων, ωστόσο αντίστοιχο ρόλο έχει η Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade commission - FTC). Η FTC έχει δικαιοδοσία για τις περισσότερες εμπορικές οντότητες και έχει την εξουσία να εκδίδει και να επιβάλλει κανονισμούς προστασίας προσωπικών δεδομένων σε συγκεκριμένους τομείς. Η FTC χρησιμοποιεί την δικαιοδοσία της ώστε να αποτρέψει αθέμιτες και παραπλανητικές εμπορικές πρακτικές, να επιβάλει κανόνες ενάντια σε ακατάλληλα ή ανεπαρκή μέτρα προστασίας των προσωπικών δεδομένων, καθώς και τις να ορίσει τις πρακτικές συλλογής, επεξεργασίας και χρώσης των δεδομένων. Ανάλογη δικαιοδοσία έχουν κρατικοί εισαγγελείς και ένα ευρύ φάσμα ρυθμιστικών αρχών σε διαφορετικούς τομείς, όπως στους τομείς της υγειονομικής περίθαλψης και των χρηματοπιστωτικών υπηρεσιών.

Κεφάλαιο 6
Επίλογος

«Υποψιάζομαι ότι η ιδιωτικότητα είναι μια πολύ καινούρια έννοια για την ανθρωπότητα»

Helen Fisher

Η σύγχρονη έννοια της Ιδιωτικότητας όπως αυτή συγκροτείται μέσω των νέων τεχνολογιών και μορφών επικοινωνίας και συναλλαγής πληροφοριών, αποτελεί στην πραγματικότητα μια καινούρια έννοια για την ανθρωπότητα καθώς εμπεριέχει καινούριους τρόπους διάδοσης της πληροφορίας και καινούριες απειλές για τα προσωπικά δεδομένα και την Ιδιωτικότητα. Η πληροφορία πλέον αποτελεί έναν «ζωντανό» οργανισμό που διατηρείται στα πληροφοριακά συστήματα με στόχο την άμεση διαθεσιμότητα και χρήση της.

Υπό προϋποθέσεις η πληροφορία που συνδέεται με ένα άτομο, ανεξάρτητα του τι αντιπροσωπεύει, είναι δυνατόν να είναι διαθέσιμη σε ένα τεράστιο κοινό και για μεγάλο χρονικό

διάστημα. Δραστηριότητες, συναισθήματα, στοιχεία του χαρακτήρα και άλλα προσωπικά δεδομένα αποκαλύπτονται καθημερινά, συνειδητά ή μη συνειδητά, μέσω των νέων υπηρεσιών επικοινωνίας καθώς οι χρήστες τους αγνοούν τα όρια της Ιδιωτικότητας σε σχέση με αυτές τις επικοινωνίες. Η συμπεριφορά των χρηστών αντικατοπτρίζει την άγνοιά τους σχετικά με την προστασία των δεδομένων τους στην σημερινή κοινωνία της πληροφορίας, καθώς στην πλειοψηφία τους είτε αδιαφορούν και παρακάμπτουν δραστηριότητες που θα ενίσχυαν την προστασία, είτε επιδεικνύουν αποτρεπτική συμπεριφορά απέναντι στις εν λόγω υπηρεσίες δαιμονοποιώντας τες, φανταζόμενοι πως ζουν σε μια Οργουελική κοινωνία όπου όλες τους οι κινήσεις και δραστηριότητες παρακολουθούνται, καταγράφονται και αξιολογούνται από τον «Μεγάλο Αδελφό».

Που όμως τελειώνει η αλήθεια και αρχίζει ο μύθος στις απόψεις των χρηστών; Πώς κάποιος μπορεί να ισχυριστεί με σιγουριά σήμερα ότι είναι κύριος διαχειριστής των δεδομένων του; Η αλήθεια είναι πως το 2013 ήταν η ως τώρα χειρότερη χρονιά όσον αφορά τα ζητήματα της Ιδιωτικότητας, και η χρονιά που αποτέλεσε την αρχή των συζητήσεων για την προστασία της, ακόμα και μεταξύ ατόμων που μέχρι πρότινος αγνοούσαν την σύγχρονη έννοιά της. Σε αυτό συνέβαλαν γεγονότα όπως οι μεγαλύτερες μαζικές παραβιάσεις σε λογαριασμούς χρηστών που είχαν ποτέ συμβεί, η απροσδιορίστου χρόνου διατήρηση πληροφορίας στις μηχανές αναζήτησης όπου άνοιξε το θέμα του «Δικαιώματος να Ξεχνιέσαι» (υπόθεση Mario Costeja González εναντίον Google)[59], αλλά ακόμα περισσότερο οι αποκαλύψεις της υπόθεσης «Snowden»[60] όπου συντάραξαν τους χρήστες όλων των υπηρεσιών επικοινωνίας και προκάλεσαν ρήξεις και διπλωματικά επεισόδια μεταξύ χωρών. Μια υπόθεση που έφερε στο φως αποδείξεις σχετικά με το χειρότερο σενάριο, πως οι πληροφορίες όλων συλλέγονται και αξιοποιούνται στο όνομα της γενικότερης ασφάλειας των πολιτών και της διαφύλαξης της ειρήνης. Ακόμα ένα μεγάλο πλήγμα για την ασφάλεια των δεδομένων και της Ιδιωτικότητας αποτέλεσε η ανακάλυψη μιας ευπάθειας στο πρωτόκολλο SSL (HeartBleed)[61], ενός εκ των ασφαλέστερων τρόπων προστασίας δεδομένων. Συνέπεια αυτών ήταν δημιουργία αλυσιδωτών αντιδράσεων και η έναρξη συζητήσεων για την δημιουργία τρόπων ενίσχυσης της Ιδιωτικότητας.

Ήδη η Ιδιωτικότητα των επικοινωνιών αποτελεί μια έννοια ευρύτερα γνωστή και όλο και περισσότεροι χρήστες αναζητούν τρόπους προστασίας της. Μηχανισμοί και τεχνολογίες όπως περιγράφηκαν στην παρούσα διατριβή εξελίσσονται και αποσκοπούν στην διαφύλαξη των πληροφοριών των χρηστών. Ειδικότερα η τεχνολογία της Κρυπτογραφίας αποτελεί ένα από τα σημαντικότερα εργαλεία που συγκαταλέγονται σε αυτές τις τεχνολογίες. Μέγιστο ρόλο φυσικά καταλαμβάνουν και οι νομοθετικές ρυθμίσεις και αλλαγές που εξελίσσονται σχεδόν παράλληλα

με τις τεχνολογικές εξελίξεις έχοντας ως στόχο τον περιορισμό της κατάχρησης των δεδομένων από την πλευρά των παρόχων των ηλεκτρονικών υπηρεσιών επικοινωνίας.

Η Ιδιωτικότητα φαίνεται ότι θα συνεχίσει να αποτελεί ένα από τα μείζονα προβλήματα για το μέλλον των ηλεκτρονικών υπηρεσιών όπως επίσης και γενικότερα για το μέλλον του Διαδικτύου καθώς η αξία της πληροφορίας φαίνεται να είναι τεράστια και όχι μόνο οικονομική. Η προστασία της φυσικά δεν είναι μόνο ευθύνη των μηχανισμών ενίσχυσης, των νόμων και των πολιτικών προστασίας. Σημαντικότερο στοιχείο θωράκισης της Ιδιωτικότητας δεν μπορεί να θεωρηθεί άλλως από τον εκάστοτε χρήστη των υπηρεσιών, ο οποίος όντας γνώστης των απειλών και των αντίμετρων που σχετίζονται με την ασφάλεια των δεδομένων του μπορεί να θέσει τις βάσεις για μια ασφαλέστερη χρήση τους.

Βιβλιογραφία

[01] Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας. «Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών». Εκδόσεις Παπασωτηρίου, Αθήνα 2010.

[02] Φίλιππος Μίτλεττον. Μορφές ιδιωτικότητας. Μια κατ΄ εξοχήν πολιτική ιδιότητα και κοινωνική επιλογή. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Φεβρουάριος 2008.

[03] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Xamax Consultancy, Aug 1997.
http://www.rogerclarke.com/DV/Intro.html

[04] Rachel Finn and David Wright, Trilateral Research & Consulting, London, Michael Friedewald, Fraunhofer ISI, Karlsruhe, Seven Types of Privacy, European Data Protection: Coming of Age, Springer, January 2013.

[05] Daniel J. Solove, A Taxonomy Of Privacy, University of Pennsylvania, Law Review, January 2006.

[06] Νόμος 2472/1997, «Προστασία Του Ατόμου Από Την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα Με Ενσωματωμένες Τις Τροποποιήσεις».

[07] Δέκα Ερωτήσεις – Απαντήσεις Για Τα Προσωπικά Δεδομένα, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL

[08] Αιτιολογική Έκθεση Ν. 3917, Διατήρηση Δεδομένων που Παράγονται ή Υποβάλλονται σε Επεξεργασία σε Συνάρτηση με την Παροχή Διαθέσιμων στο Κοινό Υπηρεσιών Ηλεκτρονικών Επικοινωνιών ή Δημοσίων Δικτύων Επικοινωνιών, Αθήνα 11 Ιανουαρίου 2011.

[09] SafeLine, Ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο http://www.safeline.gr/kataggelies/statistika-stoiheia

[10] Internet Security Threat Report 2014, Symantec Corporation, April 2014.

[11] Kristina Ringland, The European Union's Data Retention Directive And The United States's Data Preservation Laws: Finding The Better Model, 5 Shidler Journal of Law, Commerce & Technology, 2009.

[12] Lilian Mitrou, Digital Privacy: Theory, Technologies, and Practices, Chapter 20 - Communications Data Retention: A Pandora's Box for Rights and Liberties?, November 2007.

[13] Marc Langheinrich, Privacy by Design - Principles of Privacy - Aware Ubiquitous Systems, UbiComp '01 Proceedings of the 3rd international conference on Ubiquitous Computing, 2001.

[14] OECD, Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, July 2011.

[15] Panayiotis Kotzanikolaou, Data Retention and Privacy in Electronic Communications, IEEE Computer Society, September/October 2008.

[16] Claire Tristram, "Data Extinction," MIT Technology Review, October 2002.

[17] Yun Shen, Siani Pearson, Privacy Enhancing Technologies: A Review, HP Laboratories http://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf

[18] Γκρίτζαλης Στέφανος, Κάτσικας Κ., Σωκράτης, Γκρίτζαλης Δημήτρης, Ασφάλεια Δικτύων Υπολογιστών , Κεφ. 9ο Τεχνολογίες Ενίσχυσης Της Ιδιωτικότητας, Εκδόσεις Παπασωτηρίου, 2003.

[19] Drs. ing. R.F. Koorn RE, White Paper Privacy-Enhancing Technologies, Netherlands, 2004.

[20] W3C. Platform for privacy preferences (P3P) project.
http://www.w3.org/P3P/

[21] Ting Yu, Ninghui Li and Annie I. Antón. ACM Workshop on Secure Web Services (SWS), Washington, D.C., October 2004.

[22] The Enterprise Privacy Authorization Language (EPAL 1.1) - Reader's Guide to the Documentation.
http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/

[23] Vincent C. Hu, Evan Martin, JeeHyun Hwang, Tao Xie, Conformance Checking of Access Control Policies Specified in XACML, 31st Annual International Computer Software and Applications Conference, 2007.

[24] Anne Anderson, XACML vs EPAL 5th Annual Privacy & Security Workshop, 29 October 2004.

[25] Anderson, A.H, An introduction to the Web Services Policy Language (WSPL), Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE International Workshop.

[26] Roberto Chinnici, Jean-Jacques Moreau, Arthur Ryman, Sanjiva Weerawarana, Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Recommendation 26 June 2007.

[27] Web Services Policy 1.2 - Framework (WSPolicy), W3C Member Submission 25 April 2006.

[28] Lorrie Faith Cranor, The Role Of Privacy Enhancing Technologies.

[29] The Tor Project, https://www.torproject.org/

[30] Nathan S. Evans, Christian Grothoff, Anonymity With Tor The Onion Router, Anonymity With Tor, Technical University Munich, July 2012.

[31] Roger Dingledine, Nick Mathewson, Paul Syverson, Tor: The Second-Generation Onion Router, Proceedings of the 13th conference on USENIX Security Symposium, 2004.

[32] Anonymizer, https://www.anonymizer.com/

[33] Peter Chow, Surfing the Web Anonymously - The Good and Evil of the Anonymizer, July 2012.

[34] Justin Boyan, The Anonymizer, Protecting User Privacy on the Web, 1997.

[35] Jyoti Attri, Aarti Devi, Ankush Sharma & Pratibha Sharma, Study on cryptographic techniques in computer network security, Asian Journal of Advanced Basic Science, May 2014.

[36] Freier, Alan O., Philip Karlton, and Paul C. Kocher. "The SSL Protocol Version 3.0." Netscape. 18 Nov. 1996. 29 Apr. 2007.

[37] J.K. Harris, Understanding SSL/TLS, Virginia Tech, Oct 2008.

[38] Blue Coat solutions, Technology Primer: Secure Sockets Layer (SSL), 2008.

[39] Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy Recommendations of the National Institute of Standards and Technology, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, September 2009.

[40] David W Chadwick, Network Firewall Technologies, Nato Science Series Sub Series III, April 2004.

[41] RPANetwork, Internet Firewall Tutorial, A White Paper, July 2002.

[42] Firewall, A newsletter for IT Professionals, Issue 7, c/o Computer Centre, The University of Hong Kong.

[43] Privacy Enhancing Technologies, Meta Group Report, Ministry of Science Technology and Innovation, March 2005.

[44] W. Gansterer, M. Ilger, P., Lechner, R. Neumayer, J. Strauß, Anti-spam Methods - State of the Art, Institute of Distributed and Multimedia Systems, Faculty of computer Science, University of Vienna, Austria, March 2005.

[45] Prashanth Srikanthan, An Overview of Spam Handling Techniques, Computer Science Department, George Mason University, April 2004.

[46] Sarika Choudhary, Ritika Saroha, Mrs. Sonal Beniwal, How Anti-virus Software Works??, International Journal of Advanced Research in Computer Science and Software Engineering, April 2013.

[47] Body of European Regulators for Electronic Communications (BEREC), What is BEREC? http://berec.europa.eu/

[48] Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.). http://www.eett.gr

[49] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, Α.Δ.Α.Ε. www.adae.gr

[50] Νόμος 3115/2003, Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

[51] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. http://www.dpa.gr

[52] "On the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", Directive 2006/24/EC, Official Journal of the European Union, Απρίλιος 2006.

[53] "The Court of Justice declares the Data Retention Directive to be invalid", Court of Justice of the European Union, Luxembourg, 8 April 2014

[54] Νόμος 3917/2011, «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων

επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

[55] Νόμος 3674/2008 – «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις».

[56] Νόμος 3471/2006 – «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών».

[57] Νόμος 3783/2009 – «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις».

[58] Jim Halpert, Jennifer Kashatus, Kate Lucente, Data Protection Laws of the World Handbook , United States, 2014.
www.dlapiperdataprotection.com

[59] Ashifa Kassam, Spain's everyday internet warrior who cut free from Google's tentacles, The Guardian, May 2014.
http://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez

[60] Luke Harding, The Snowden Files: The Inside Story of the World's Most Wanted Man, February 2014.

[61] The Heartbleed Bug
http://heartbleed.com/

Παράρτημα Α
Πίνακες ορισμών

Α.1 Πίνακας Αγγλικής Ορολογίας

Aggregation	Συνάθροιση Δεδομένων
Analog Backups	Αναλογικά Αντίγραφα Ασφαλείας
Antispyware	Αντι-Κατασκοπευτικό Λογισμικό
Antivirus	Αντι-Ικό Λογισμικό
Application-Level Firewall	Αναχώματα Επιπέδου Εφαρμογής
Appropriation	Οικειοποίηση
Asymmetric Encryption	Ασύμμετρη Κρυπτογραφία
Authentication	Αυθεντικοποίηση
Bayesian Filter	Bayesian Φίλτρα
BEREC (Body Of European Regulators For Electronic Communications)	Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών
Bitstream Copying	Αντιγραφή Ροής Δεδομένων
Blacklists	Μαύρες Λίστες
Blackmail	Εκβιασμός
Breach Of Confidentiality	Παραβίαση Της Εμπιστευτικότητας
Browser	Φυλλομετρητής
Browser Plug-Ins	Βοηθητικά Προγράμματα Φυλλομετρητή
Canonicalization	Κανονικοποίηση
Certificates Authorities	Αρχές Έκδοσης Πιστοποιητικών
Checksum-Based Filter	Φίλτρα Άθροισματος Ελέγχου
Circuit-Level Firewall	Αναχώματα Επιπέδου Μεταφοράς
Client	Υπολογιστής Πελάτη
Collection	Συλλογή
Communications Data	Δεδομένα Επικοινωνίας
Communications Data	Δεδομένα Επικοινωνίας
Conduct	Μεταχείριση
Consent Token	Τεχνική Συναίνεσης («Κόστους» Αποστολής Μηνύματος)
Content Data	Εσωτερικά Δεδομένα
Content Data	Εσωτερικά Δεδομένα
Context Data	Εξωτερικά Δεδομένα
Context Data	Εξωτερικά Δεδομένα
Control	Διαχείριση
Cookie Files	Αρχεία «Αναγνώρισης» Χρήστη
Cookie-Cutters	Λογισμικά Απόρριψης Των Αρχείων Cookies
CSP (Communication Service Provider)	Παροχέας Υπηρεσιών Επικοινωνίας
Data	Δεδομένα
Data Collection	Συλλογή Δεδομένων

Data Processing	Επεξεργασία Δεδομένων
Data Processing	Επεξεργασία Δεδομένων
Decisional Interference	Παρεμβολές Λήψης Αποφάσεων
Digital Archaeology	Ψηφιακή Αρχαιολογία
Digital Data	Ψηφιακά Δεδομένα
Digital Data	Ψηφιακά Δεδομένα
Disclosure	Αποκάλυψη
Disposal	Διάθεση
Distortion	Στρέβλωση
DSL (Digital Subscriber Line)	Ψηφιακή Συνδρομητική Γραμμή
Dual Control	Διπλός Έλεγχος
Durable Media	Ανθεκτικότητα Των Μέσων
E-Mail	Μήνυμα Ηλεκτρονικού Ταχυδρομείου
Emulation	Εξομοίωση
Encapsulation	Ενθυλάκωση
Exclusion	Αποκλεισμός
Exposure	Έκθεση
Firewall	Ανάχωμα Ασφαλείας, Τείχος Προστασίας
FTC (Federal Trade Commission)	Ομοσπονδιακή Επιτροπή Εμπορίου
Greylisting	Γκρίζες Λίστες
Handshake	Χειραψία
Heuristic Method	Ευρετική Μέθοδος
Hoaxes	Μηνύματα Εξαπάτησης
Hybrid Encryption	Υβριδική Κρυπτογραφία
Identification	Προσδιορισμός
IMEI - International Mobile Station Equipment Identity	Διεθνής Ταυτότητα Εξοπλισμού Κινητής Τηλεφωνίας
IMSI- International Mobile Subscriber Identity	Διεθνής Ταυτότητα Συνδρομητή Κινητής Τηλεφωνίας
Increased Accessibility	Αυξημένη Προσβασιμότητα
Information Collection	Συλλογή Δεδομένων
Information Dissemination	Διάδοση Της Πληροφορίας
Information Processing	Επεξεργασία Της Πληροφορίας
Insecurity	Ανασφάλεια
Instant Messaging Spam	Spam Υπηρεσιών Άμεσων Μηνυμάτων
Internet Security Threat	Απειλή Διαδικτυακής Ασφάλειας
Interrogation	Ανάκριση
Intrusion	Παρείσφρηση
Invasion	Εισβολή
IP Address	Διεύθυνση Πρωτόκολλου Διαδικτύου
ISP (Internet Service Provider)	Παροχέας Διαδικτυακών Υπηρεσιών
Learning Content Filtering Systems	Συστήματα Μάθησης Περιεχομένου

Location Data	Δεδομένα Τοποθεσίας
Location Data	Δεδομένα Τοποθεσίας
MAC Address	Διεύθυνση Έλεγχου Πρόσβασης Σε Μέσα
Malicious Software	Κακόβουλο Λογισμικό
Mega-Breaches	Μεγάλης Έκτασης Παραβιάσεις
Metadata	Μετα-Δεδομένα
Migration	Μετανάστευση
National Regulatory Authority	Εθνική Ρυθμιστική Αρχή
Network Layer	Επίπεδο Δικτύου
Normalization	Ομαλοποίηση
One-Way Function	Μονόδρομη Συνάρτηση
OSI (Open Systems Interconnection Model)	Πρωτόκολλο Διασύνδεσης Ανοιχτών Συστημάτων
Packet Filtering	Δρομολογητές Φιλτραρίσματος
Persistent Media	Ανθεκτικότητα Των Μέσων
Personal Data	Προσωπικά Δεδομένα
Personal Data	Προσωπικά Δεδομένα
Pets (Privacy Enhancing Technologies)	Τεχνολογίες Ενίσχυσης Της Ιδιωτικότητας
Phishing	Τεχνική Διαδικτυακού «Ψαρέματος»
Phishing Host	Κακόβουλη Ιστοσελίδα
Policy Decision Point (PDP)	Σημείο Απόφασης Πολιτικής
Policy Enforcement Point (PEP)	Σημείο Επιβολής Πολιτικής
Privacy	Ιδιωτικότητα
Privacy Policy Languages	Γλώσσες Πολιτικών Ιδιωτικότητας
Proxy	Πληρεξούσιος, Μεσολαβητής
Public Key Encryption	Κρυπτογραφία Δημόσιου Κλειδιού
Quantity Method	Ποσοτική Μέθοδος
Quarantine	Καραντίνα
Rating	Αξιολόγηση
Refreshing	Ανανέωση
Reliance On Standards	Εμπιστοσύνη Στους Κανόνες Προτυποποίησης
Replication	Αναπαραγωγή
Reputation Systems	Συστήματα Φήμης
Response	Απάντηση
Retention	Διατήρηση
RFID (Radio Frequency Identification)	Αναγνώρισης Μέσω Ραδιοσυχνότητας
Scan Engine	Μηχανή Σάρωσης
Secondary Use	Δευτερεύουσα Χρήση
Secret-Key Encryption	Κρυπτογραφία Μυστικού Κλειδιού
Sensitive Personal Data	Ευαίσθητα Προσωπικά Δεδομένα

Sensitive Personal Data	Ευαίσθητα Προσωπικά Δεδομένα
Separation Of Duties	Διαχωρισμός Των Καθηκόντων
Server	Υπολογιστής Εξυπηρετητή
Socket	Κανάλι Σύνδεσης
Spam	Αυτόκλητο Μήνυμα
Spamdexing	Spam Μηχανών Αναζήτησης
Spammer	Αποστολέας Αυτόκλητων Μηνυμάτων
SSL (Secure Sockets Layer)	Πρωτόκολλο Δημιουργίας Ασφαλούς Καναλιού Διασύνδεσης
Stateful Packet Inspection	Αναχώματα Ελέγχου Κατάστασης
Static Content Filtering Lists	Λίστες Στατικού Περιεχομένου
Surveillance	Παρακολούθηση
Symmetric-Key Cryptography	Συμμετρική Κρυπτογραφία
TCP (Telecommunication Service Provider)	Παροχέας Υπηρεσιών Τηλεπικοινωνίας
TCP (Transmission Control Protocol)	Πρωτόκολλο Ελέγχου Μετάδοσης
Technology Preservation	Διατήρηση Της Τεχνολογίας
TLS (Transport Layer Security)	Πρωτόκολλο Δημιουργίας Ασφαλούς Διασύνδεσης Στο Επίπεδο Μεταφοράς
Traffic Data	Δεδομένα Κίνησης
Traffic Data	Δεδομένα Κίνησης
Transport Layer	Επίπεδο Μεταφοράς
UDP (User Datagram Protocol)	Πρωτόκολλο Αυτοδύναμων Πακέτων
User Agents	Πράκτορες Χρήστη
Virus	Ιός
Virus Signature	Υπογραφή Ιού
Voip (Voice Over IP)	Τηλεφωνία Μέσω IP
Web Content Filtering Tools	Εργαλεία Φιλτραρίσματος Περιεχομένου
Web Domain	Όνομα Διαδικτυακού Τομέα
Web-Based Attacks	Επιθέσεις Μέσω Του Ιστοχώρου
Whitelists	Λευκές Λίστες
XML (Extensible Markup Language)	Εκτεταμένη Γλώσσα Σήμανσης
Zero-Day Vulnerabilities	Άγνωστες Ως Την Μέρα Παραβίασης Ευπάθειες Του Συστήματος

A.2 Πίνακας Ελληνικής Ορολογίας

Άγνωστες Ως Την Μέρα Παραβίασης Ευπάθειες Του Συστήματος	Zero-Day Vulnerabilities
Αναγνώριση Μέσω Ραδιοσυχνότητας	RFID (Radio Frequency Identification)

Ανάκριση	Interrogation
Αναλογικά Αντίγραφα Ασφαλείας	Analog Backups
Ανανέωση	Refreshing
Αναπαραγωγή	Replication
Ανασφάλεια	Insecurity
Ανάχωμα Ασφαλείας, Τείχος Προστασίας	Firewall
Αναχώματα Ελέγχου Κατάστασης	Stateful Packet Inspection
Αναχώματα Επιπέδου Εφαρμογής	Application-Level Firewall
Αναχώματα Επιπέδου Μεταφοράς	Circuit-Level Firewall
Ανθεκτικότητα Των Μέσων	Durable Media
Ανθεκτικότητα Των Μέσων	Persistent Media
Αντιγραφή Ροής Δεδομένων	Bitstream Copying
Αντι-Ιικό Λογισμικό	Antivirus
Αντι-Κατασκοπευτικό Λογισμικό	Antispyware
Αξιολόγηση	Rating
Απάντηση	Response
Απειλή Διαδικτυακής Ασφάλειας	Internet Security Threat
Αποκάλυψη	Disclosure
Αποκλεισμός	Exclusion
Αποστολέας Αυτόκλητων Μηνυμάτων	Spammer
Αρχεία «Αναγνώρισης» Χρήστη	Cookie Files
Αρχές Έκδοσης Πιστοποιητικών	Certificates Authorities
Ασύμμετρη Κρυπτογραφία	Asymmetric Encryption
Αυθεντικοποίηση	Authentication
Αυξημένη Προσβασιμότητα	Increased Accessibility
Αυτόκλητα μηνύματα Μηχανών Αναζήτησης	Spamdexing
Αυτόκλητα μηνύματα Υπηρεσιών Άμεσων Μηνυμάτων	Instant Messaging Spam
Αυτόκλητο Μήνυμα	Spam
Βοηθητικά Προγράμματα Φυλλομετρητή	Browser Plug-Ins
Γκρίζες Λίστες	Greylisting
Γλώσσες Πολιτικών Ιδιωτικότητας	Privacy Policy Languages
Δεδομένα	Data
Δεδομένα Επικοινωνίας	Communications Data
Δεδομένα Επικοινωνίας	Communications Data
Δεδομένα Κίνησης	Traffic Data
Δεδομένα Κίνησης	Traffic Data
Δεδομένα Τοποθεσίας	Location Data
Δεδομένα Τοποθεσίας	Location Data
Δευτερεύουσα Χρήση	Secondary Use

Διάδοση Της Πληροφορίας	Information Dissemination
Διάθεση	Disposal
Διατήρηση	Retention
Διατήρηση Της Τεχνολογίας	Technology Preservation
Διαχείριση	Control
Διαχωρισμός Των Καθηκόντων	Separation Of Duties
Διεθνής Ταυτότητα Εξοπλισμού Κινητής Τηλεφωνίας	IMEI - International Mobile Station Equipment Identity
Διεθνής Ταυτότητα Συνδρομητή Κινητής Τηλεφωνίας	IMSI- International Mobile Subscriber Identity
Διεύθυνση Έλεγχου Πρόσβασης Σε Μέσα	MAC Address
Διεύθυνση Πρωτόκολλου Διαδικτύου	IP Address
Διπλός Έλεγχος	Dual Control
Δρομολογητές Φιλτραρίσματος	Packet Filtering
Εθνική Ρυθμιστική Αρχή	National Regulatory Authority
Εισβολή	Invasion
Εκβιασμός	Blackmail
Έκθεση	Exposure
Εκτεταμένη Γλώσσα Σήμανσης	XML (Extensible Markup Language)
Εμπιστοσύνη Στους Κανόνες Προτυποποίησης	Reliance On Standards
Ενθυλάκωση	Encapsulation
Εξομοίωση	Emulation
Εξωτερικά Δεδομένα	Context Data
Εξωτερικά Δεδομένα	Context Data
Επεξεργασία Δεδομένων	Data Processing
Επεξεργασία Δεδομένων	Data Processing
Επεξεργασία Της Πληροφορίας	Information Processing
Επιθέσεις Μέσω Του Ιστοχώρου	Web-Based Attacks
Επίπεδο Δικτύου	Network Layer
Επίπεδο Μεταφοράς	Transport Layer
Εργαλεία Φιλτραρίσματος Περιεχομένου	Web Content Filtering Tools
Εσωτερικά Δεδομένα	Content Data
Εσωτερικά Δεδομένα	Content Data
Ευαίσθητα Προσωπικά Δεδομένα	Sensitive Personal Data
Ευαίσθητα Προσωπικά Δεδομένα	Sensitive Personal Data
Ευρετική Μέθοδος	Heuristic Method
Ιδιωτικότητα	Privacy
Ιός	Virus
Κακόβουλη Ιστοσελίδα	Phishing Host
Κακόβουλο Λογισμικό	Malicious Software

Κανάλι Σύνδεσης	Socket
Κανονικοποίηση	Canonicalization
Καραντίνα	Quarantine
Κρυπτογραφία Δημόσιου Κλειδιού	Public Key Encryption
Κρυπτογραφία Μυστικού Κλειδιού	Secret-Key Encryption
Λευκές Λίστες	Whitelists
Λίστες Στατικού Περιεχομένου	Static Content Filtering Lists
Λογισμικά Απόρριψης Των Αρχείων Cookies	Cookie-Cutters
Μαύρες Λίστες	Blacklists
Μεγάλης Έκτασης Παραβιάσεις	Mega-Breaches
Μετα-Δεδομένα	Metadata
Μετανάστευση	Migration
Μεταχείριση	Conduct
Μήνυμα Ηλεκτρονικού Ταχυδρομείου	E-Mail
Μηνύματα Εξαπάτησης	Hoaxes
Μηχανή Σάρωσης	Scan Engine
Μονόδρομη Συνάρτηση	One-Way Function
Μπεϋζιανά Φίλτρα	Bayesian Filter
Οικειοποίηση	Appropriation
Ομαλοποίηση	Normalization
Ομοσπονδιακή Επιτροπή Εμπορίου	FTC (Federal Trade Commission)
Όνομα Διαδικτυακού Τομέα	Web Domain
Παραβίαση Της Εμπιστευτικότητας	Breach Of Confidentiality
Παρακολούθηση	Surveillance
Παρείσφρηση	Intrusion
Παρεμβολές Λήψης Αποφάσεων	Decisional Interference
Παροχέας Διαδικτυακών Υπηρεσιών	ISP (Internet Service Provider)
Παροχέας Υπηρεσιών Επικοινωνίας	CSP (Communication Service Provider)
Παροχέας Υπηρεσιών Τηλεπικοινωνίας	TCP (Telecommunication Service Provider)
Πληρεξούσιος, Μεσολαβητής	Proxy
Ποσοτική Μέθοδος	Quantity Method
Πράκτορες Χρήστη	User Agents
Προσδιορισμός	Identification
Προσωπικά Δεδομένα	Personal Data
Προσωπικά Δεδομένα	Personal Data
Πρωτόκολλο Αυτοδύναμων Πακέτων	UDP (User Datagram Protocol)
Πρωτόκολλο Δημιουργίας Ασφαλούς Διασύνδεσης Στο Επίπεδο Μεταφοράς	TLS (Transport Layer Security)
Πρωτόκολλο Δημιουργίας Ασφαλούς Καναλιού Διασύνδεσης	SSL (Secure Sockets Layer)

Πρωτόκολλο Διασύνδεσης Ανοιχτών Συστημάτων	OSI (Open Systems Interconnection Model)
Πρωτόκολλο Ελέγχου Μετάδοσης	TCP (Transmission Control Protocol)
Σημείο Απόφασης Πολιτικής	Policy Decision Point (PDP)
Σημείο Επιβολής Πολιτικής	Policy Enforcement Point (PEP)
Στρέβλωση	Distortion
Συλλογή	Collection
Συλλογή Δεδομένων	Data Collection
Συλλογή Δεδομένων	Information Collection
Συμμετρική Κρυπτογραφία	Symmetric-Key Cryptography
Συνάθροιση Δεδομένων	Aggregation
Συστήματα Μάθησης Περιεχομένου	Learning Content Filtering Systems
Συστήματα Φήμης	Reputation Systems
Σώμα Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών	BEREC (Body Of European Regulators For Electronic Communications)
Τεχνική Διαδικτυακού «Ψαρέματος»	Phishing
Τεχνική Συναίνεσης («Κόστους» Αποστολής Μηνύματος)	Consent Token
Τεχνολογίες Ενίσχυσης Της Ιδιωτικότητας	Pets (Privacy Enhancing Technologies)
Τηλεφωνία Μέσω IP	Voip (Voice Over IP)
Υβριδική Κρυπτογραφία	Hybrid Encryption
Υπογραφή Ιού	Virus Signature
Υπολογιστής Εξυπηρετητή	Server
Υπολογιστής Πελάτη	Client
Φίλτρα Άθροισματος Ελέγχου	Checksum-Based Filter
Φυλλομετρητής	Browser
Χειραψία	Handshake
Ψηφιακά Δεδομένα	Digital Data
Ψηφιακή Αρχαιολογία	Digital Archaeology
Ψηφιακή Συνδρομητική Γραμμή	DSL (Digital Subscriber Line)