Πανεπιστήμιο Θεσσαλίας
Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών
Τηλεπικοινωνιών και Δικτύων

Μεταπτυχιακή Εργασία

Ιδιωτικότητα και Ασφάλεια Πληροφορίας

Επιβλέπων Καθηγητής: Βασίλειος Βερύκιος

Της
Μαρίας Παλέτσου

Νοέμβριος 2007
ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΒΙΒΛΙΟΘΗΚΗ & ΚΕΝΤΡΟ ΠΛΗΡΟΦΟΡΗΣΗΣ
ΕΙΔΙΚΗ ΣΥΛΛΟΓΗ «ΓΚΡΙΖΑ ΒΙΒΛΙΟΓΡΑΦΙΑ»

Αριθ. Εισ.: 6031/1
Ημερ. Εισ.: 08-11-2007
Δωρεά: Συγγραφέα
Ταξιθετικός Κωδικός: Δ
025.04
ΠΑΛ
ΤΜΗΜΑ Μηχανικών Ηλεκτρονικών Υπολογιστών Τηλεπικοινωνιών και Δικτύων
Πανεπιστημίου Θεσσαλίας

Μεταπτυχιακή Εργασία

Ιδιωτικότητα και Ασφάλεια Πληροφορίας
tης
Παλέτσου Μαρίας

Επιβλέπων Καθηγητής: Βασίλειος Βερύκιος

Νοέμβριος 2007
Περιεχόμενα

Λίστα Πινάκων ..............................................................................................................5
Λίστα Σχημάτων ...........................................................................................................6

Κεφάλαιο 1 ....................................................................................................................7
Εισαγωγή .......................................................................................................................7
  1.1 Γενικό Υπόβαθρο ...............................................................................7
  1.2 Βασικός Στόχος της Εργασίας ...............................................8
  1.3 Σύντομη Περιγραφή Κεφαλαίων ...........................................11

Κεφάλαιο 2...................................................................................................................14
Ιδιωτικότητα Δεδομένων ...........................................................................................14
  2.1 Μοντέλα Προστασίας της Ιδιωτικότητας Δεδομένων..........................15
  2.2 Εξέλιξη στην Προστασία Δεδομένων.............................................17
    2.2.1 Ελληνική Νομοθεσία ........................................................................19
    2.2.1.1 Νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα Γενικότερα ....................................................................20
    2.2.1.2 Νομοθεσία για την Προστασία Δεδομένων Ειδικότερα στον Τομέα των Τηλεπικοινωνιών..............................................21
    2.2.2 Ευρωπαϊκή Νομοθεσία .....................................................................23
    2.2.2.1 Νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα Γενικότερα ...................................................................24
    2.2.2.2 Νομοθεσία για την Προστασία Δεδομένων Ειδικότερα στον Τομέα των Τηλεπικοινωνιών..............................................25
    2.2.3 Διεθνής Νομοθεσία ...........................................................................32
    2.2.3.1 Νομοθεσία για την Προστασία Δεδομένων.....................................33
    2.2.3.2 Προστασία APEC ........................................................................35
    2.2.3.3 Νομοθεσία για την Προστασία Δεδομένων στον Τομέα των Τηλεπικοινωνιών .........................................................36
  2.3 Διασυνοριακή Ροή Δεδομένων Προσωπικού Χαρακτήρα ...............38
  2.4 Επίλογος ...........................................................................................40
Κεφάλαιο 3
Εποπτικοί Φορείς Ασφάλειας σε Ελλάδα και Ευρώπη
3.1 Ελληνικοί Εποπτικοί Φορείς Ασφάλειας
3.1.1 Γενικό Επιτελείο Εθνικής Άμυνας
3.1.2 Εθνική Υπηρεσία Πληροφοριών
3.1.3 Διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας
3.1.4 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
3.1.5 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
3.1.6 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομειων
3.1.7 Ελληνικός Φορέας Ασφάλειας Διασταύρωσης Τηλεπικοινωνιών
3.1.8 Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας για το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας
3.2 Ευρωπαϊκοί και Διεθνείς Εποπτικοί Φορείς Ασφάλειας
3.2.1 Ευρωπαϊκή Επιτροπή
3.2.2 Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών
3.2.3 Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών
3.2.4 Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας
3.3 Επίλογος

Κεφάλαιο 4
Δεδομένα Υπηρεσιών με Βάση τη Θέση
4.1 Υπηρεσίες με Βάση τη Θέση
4.1.1 Συστατικά ενός Συστήματος Υπηρεσιών με Βάση τη Θέση
4.1.2 Μέθοδοι Εντοπισμού Θέσης
4.1.3 Απαιτήσεις ενός Συστήματος Υπηρεσιών με Βάση τη Θέση
4.2 Χωρο-χρονικά δεδομένα
4.2.1 Ενέργειες Κινούμενων Αντικειμένων
4.2.2 Συσχετιζόμενες Καταστάσεις και Φαινόμενα
4.2.3 Θέματα Ιδιωτικότητας σε Χωρο-χρονικά Δεδομένα
4.3 Επίλογος

Κεφάλαιο 5
Τεχνικές Διασφάλισης Ιδιωτικότητας σε Χωρο-χρονικά Δεδομένα
5.1 Πολιτικές Ασφαλείας
5.2 Κρυπτογραφία
5.2.1 Ασύμμετρη Κρυπτογραφία ή Κρυπτογράφηση Δημοσίου
5.2.2 Ιεραρχική Κρυπτογράφηση Βασισμένη στην Ταυτότητα
5.2.3 Άλλες Κρυπτογραφικές Προσεγγίσεις
5.3 Κ-ανωνυμία
5.3.1 Κ-ανωνυμία Κατα τη Συλλογή της Θέσης
5.4 Επίλογος
Κεφάλαιο 6.................................................................103
Συστήματα Διασφάλισης της Ιδιωτικότητας Θέσης των Χρηστών.........103
6.1 Σύστημα Βασισμένο στην Επέκταση Χωρικών Συνιστωσών.....105
6.2 Σύστημα Βασισμένο στον Location Anonymizer...............106
6.3 Σύστημα Casper.........................................................109
6.4 Σύστημα HESTIA...........................................................112
6.5 Σύστημα Ανωνυμίας Χωρικών Ερωτήσεων.........................114
6.6 Επίλογος .....................................................................117

Κεφάλαιο 7.................................................................118
Χρηματοδότηση της Έρευνας – Ερευνητικά Προγράμματα..........118
7.1 Οργανισμοί Χρηματοδότησης της Έρευνας.........................119
7.1.1 7ο Πρόγραμμα - Πλαίσιο............................................119
7.1.2 Εθνικό Ίδρυμα Επιστημών .......................................121
7.1.3 Εθνική Υπηρεσία Ασφάλειας .......................................124
7.1.4 Εθνικό Ίδρυμα Υγείας .............................................125
7.1.5 MITRE....................................................................126
7.2 Συναφή Ερευνητικά Προγράμματα................................128
7.2.1 Πρόγραμμα GeoPKDD...............................................128
7.2.2 Πρόγραμμα iTrust.......................................................129
7.2.3 Πρόγραμμα PORTIA..................................................130
7.2.4 Πρόγραμμα KDubiq....................................................132
7.2.5 Πρόγραμμα geopriv....................................................133
7.2.6 Πρόγραμμα PRIME....................................................134
7.2.7 29ο Διεθνές Συνέδριο Προστασίας Δεδομένων...........136
7.3 Επίλογος .....................................................................137

Κεφάλαιο 8.................................................................138
Συμπεράσματα ..................................................................138
Βιβλιογραφία......................................................................140
Λίστα Πινάκων

Πίνακας 5.1 Κ-ανωνυμία με Κ = 2 και QIDs = {περιοχή, χρόνος, έτος γέννησης, γένος} ................................................................. 94

Πίνακας 5.2 Κ-ανωνυμία με Κ = 2 και QIDs = {περιοχή, χρόνος}. ................... 95

Πίνακας 5.3 Κ-ανωνυμία με Κ = 2 και QIDs = {περιοχή, χρόνος}. ................... 95
Λίστα Σχημάτων

Εικόνα 2.1 Νομική αντιμετώπιση ανά τον κόσμο για την προστασία δεδομένων..19
Εικόνα 4.1 Τυπικό σύστημα υπηρεσιών με βάση τη θέση. .................................65
Εικόνα 4.2 Τρόπος παροχής υπηρεσιών ενός συστήματος υπηρεσιών με βάση τη θέση. .................................................................67
Εικόνα 4.3 Εύρεση θέσης μέσω τηλεπικοινωνιακού δικτύου. ........................69
Εικόνα 4.4 Εύρεση θέσης απευθείας από το τερματικό. ..............................70
Εικόνα 5.1 Παράδειγμα επέκτασης περιοχής για την ανωνυμία των χρηστών. ....98
Κεφάλαιο 1

Εισαγωγή

Τα τελευταία χρόνια η εκρηκτική πρόοδος της τεχνολογίας και η ολοένα και αυξανόμενη χρήση υπολογιστών και διαδικτύου έχουν διευκολύνει τη συλλογή, διατήρηση και μεταφορά όλο και περισσότερων προσωπικών δεδομένων των ατόμων από ιδιωτικούς ή δημόσιους φορείς. Η επεξεργασία των δεδομένων αυτών από τη μία δίνει τη δυνατότητα παροχής υπηρεσιών υψηλού αντίκτυπου, αλλά από την άλλη αυξάνει τις ανησυχίες των ανθρώπων για τη μυστικότητα των καθημερινών τους δραστηριοτήτων.

1.1 Γενικό Υπόβαθρο

Οι τεχνολογικές εξελίξεις στον τομέα των δικτύων και των συστημάτων γεωγραφικού εντοπισμού επιτρέπουν την ανάπτυξη
εξατομικευμένων εφαρμογών υψηλού κοινωνικού και οικονομικού 
ενδιαφέροντος. Εντούτοις, οι υπηρεσίες αυτές είναι πολύπλοκες και 
απαιτούν τη γνώση πολλών χαρακτηριστικών των χρηστών. Πολλές από 
τις καθημερινές δραστηριότητες των ανθρώπων πραγματοποιούνται 
τα τελευταία χρόνια χρησιμοποιώντας φορητές συσκευές, όπως κινητά 
tηλέφωνα, φορητοί υπολογιστές και υπολογιστές παλάμης. Παρόλο που τα 
dεδομένα αυτά έχουν τεράστιες απαιτήσεις σε χώρο για τη συλλογή 
τους, η πρόοδος των τεχνολογιών και των βάσεων δεδομένων επιτρέπει 
τη συνεχή αποθήκευση τέτοιων πληροφοριών. Τα δεδομένα τα οποία 
συλλέγονται από 
tις φορητές συσκευές χαρακτηρίζονται ως «ευαίσθητα» εάν μπορούν να 
apokaliónoun τη θέση των χρηστών σε συγκεκριμένες χρονικές 
stigmés. 
Αυτό έχει ως αποτέλεσμα όταν συνδυάζονται με προηγούμενα 
apothēkeména αποθηκευμένα δεδομένα για κάποιο συγκεκριμένο χρήστη να δημιουργούν 
μία πλήρη ηλεκτρονική εικόνα για τις κινήσεις του. Ως εκ τούτου, η γνώση 
tétoiou eíðous πληροφοριών ελλοχεύει πολλούς κινδύνους για θεμελιώδη 
dikaiwmata και ελευθερίες της ιδιωτικότητας της προσωπικής ζωής των 
anthrṓpωn.

Η ιδιωτικότητα αποτελεί ένα μείζον θέμα στον τομέα των 
tηλεπικοινωνιών το οποίο έχει κεντρίσει την προσοχή τόσο του νομοθετικού 
όσο και του τεχνολογικού και ερευνητικού τομέα. Οι ανησυχίες για τη 
μυστικότητα των πληροφοριών σε αυτούς τους τομείς εντάθηκε κυρίως μετά 
tis trōmokratikēs enérgeies sthn Amerika kai thn Eυρώπη.

1.2 Βασικός Στόχος της Εργασίας

Η ιδιωτικότητα των προσωπικών δεδομένων αποτελεί ίσως τον πιο 
krisióμo παράγοντα τόσο για την εθνική ασφάλεια όσο και για την
προστασία της προσωπικής ζωής των ανθρώπων. Τα ερωτήματα τα οποία προκύπτουν κατά τη συλλογή και επεξεργασία δεδομένων στα σύγχρονα συστήματα είναι πολλά. Βασικός στόχος αυτής της εργασίας είναι να εξετάσει τις απαιτήσεις και τα ερωτήματα τα οποία προκύπτουν στα σύγχρονα συστήματα παροχής υπηρεσιών θέσης σε ένα συνδυασμένο κοινωνικό, νομοθετικό και τεχνικό επίπεδο.

Στην εργασία αυτή θα εστιάσουμε αρχικά στο νομοθετικό και ρυθμιστικό πλαίσιο κάθε χώρας το οποίο αποτελεί αναμφισβήτητα το ισχυρότερο μέσο για την προστασία της εθνικής ασφάλειας και των πολιτών της. Καθώς οι πολίτες δεν έχουν τη δυνατότητα να ελέγχουν κάθε φορά που χρησιμοποιούν μία υπηρεσία αν ο φορέας παροχής υπηρεσιών τηρεί τους απαραίτητους νόμους για την προστασία τους. Για τον έλεγχο αυτό, στη συνέχεια της παρούσας μελέτης θα αναφερθούμε σε δημόσιους εποπτικούς και ελεγκτικούς φορείς. Επιπλέον, καθώς στις μέρες μας δεν υπάρχει κοινή νομοθεσία προστασίας των πολιτών και των δεδομένων τους, αλλά η κάθε χώρα θεσπίζει δικούς της νόμους. Είναι πιθανό δεδομένα τα οποία συλλέγονται από κάποιον φορέα να επεξεργάζονται με αθέμιτο τρόπο σε άλλες χώρες χωρίς τη γνώση του υποκειμένου τους. Για το λόγο αυτό η κάθε χώρα συμπεριλαμβάνει στη νομοθεσία της τις προϋποθέσεις για τη διασυνοριακή ροή των δεδομένων των πολιτών, ενώ παράλληλα οι ελεγκτικές αρχές συνεργάζονται μεταξύ τους και με τους πολίτες και τις αντίστοιχες αρχές άλλων χωρών προκειμένου να παρέχουν γενική προστασία των πολιτών.

Η κινητή τηλεφωνία αποτελεί την ταχύτερα αναπτυσσόμενη τεχνολογία μετάδοσης φωνής, δεδομένων και οπτικοακουστικού περιεχομένου, παρουσιάζοντας πλεονεκτήματα έναντι των ανταγωνιστικών τεχνολογιών, κυρίως ως προς το κόστος. Η αυτοματοποιημένη συλλογή χωρο-χρονικών δεδομένων από τις φορητές συσκευές παρέχει μία πλήρη εικόνα του χρήστη αλλά και του περιβάλλοντος στο οποίο κινείται. Για την προστασία της ιδιωτικότητας των δεδομένων και τη διατήρηση της ανωνυμίας των υποκειμένων δεν αρκεί μόνο η νομοθετική προσέγγιση αλλά και η τεχνική.
Στην εργασία αυτή θα εξετάσουμε τις τεχνικές οι οποίες χρησιμοποιούνται για να καλύψουν την ανάγκη για προστασία του απορρήτου των επικοινωνιών και της ταυτότητας των χρηστών. Οι βασικότερες μέθοδοι που επιτυγχάνουν την προστασία αυτή στις υπηρεσίες θέσης είναι οι πολιτικές ασφάλειας, η κρυπτογραφία και η Κ-ανωνυμία. Οι πολιτικές ασφάλειας αποτελούν ένα απαραίτητο μέτρο για τη δημιουργία ασφαλών συστημάτων. Από τη στιγμή που τα προσωπικά δεδομένα έχουν συλλεχθεί οι φορείς παροχής υπηρεσιών θα πρέπει να εφαρμόζουν μία πολιτική ασφάλειας προκειμένου να καθορίσουν τα δικαιώματα των συμμετεχόντων μερών για την προσπέλαση στα δεδομένα. Δυστυχώς, η μέθοδος αυτή δεν είναι αρκετή για την ασφάλεια των χρηστών, δεδομένου ότι κάποιο τρίτο, μη έμπιστη, πηγή μπορεί να υποκλέσει τα δεδομένα από το σύστημα και να τα επεξεργαστεί με αθέμιτο τρόπο. Για την αντιμετώπιση αυτού του προβλήματος θα πρέπει τα δεδομένα να μετατρέπονται σε τέτοια μορφή ώστε να μη μπορούν να αναγνωριστούν από τρίτες μη συμμετέχουσες οντότητες. Η μέθοδος για να πραγματοποιηθεί αυτό είναι η κρυπτογραφία ή η Κ-ανωνυμία. Μέσω της κρυπτογραφίας, ο χρήστης μπορεί να στέλνει την ταυτότητά του, τις πληροφορίες θέσης του καθώς και να ανταλάσσει δεδομένα με τους φορείς παροχής υπηρεσιών σε μία άγνωστη προς τρίτους μορφή. Στις σύγχρονες υπηρεσίες θέσης (Location-Based Services - LBS), όμως, ο χρήστης μπορεί να θέτει ερωτήσεις στον φορέα παροχής υπηρεσιών για την εξυπηρέτηση των οποίων είναι απαραίτητη η γνώση της θέσης του. Σε αυτή την περίπτωση, δεν παρέχεται ασφάλεια στα ίδια τα δεδομένα, αλλά στην ταυτότητα το προσόπου στο οποίο ανήκουν έτσι ώστε να μη μπορεί να προσδιοριστεί. Η μέθοδος που χρησιμοποιείται για αυτό το σκοπό είναι η Κ-ανωνυμία.

Σε αυτό το πλαίσιο, διάφορα συστήματα και αλγόριθμοι έχουν προταθεί στη βιβλιογραφία για την προστασία της ανωνυμίας θέσης των χρηστών. Στην εργασία αυτή θα εξετάσουμε τα βασικότερα προτεινόμενα συστήματα τα οποία μπορούν να εφαρμοστούν στις υπάρχουσες υπηρεσίες θέσης διατηρώντας την ανωνυμία ενός μεγάλου πλήθους χρηστών σε πραγματικό χρόνο. Τέλος, τα τελευταία χρόνια όλο και περισσότεροι Ευρωπαϊκοί και διεθνείς χρηματοδοτικοί οργανισμοί καθώς και ερευνητές
ανά τον κόσμο στρέφουν την προσοχή τους στην ανάπτυξη τεχνολογικών μεθόδων και συστημάτων για την παροχή ιδιωτικότητας στα σύγχρονα συστήματα υπηρεσιών θέσης. Για το λόγο αυτό, θα αναλύσουμε τις κυριότερες ερευνητικές προσπάθειες σε αυτό το πλαίσιο.

1.3 Σύντομη Περιγραφή Κεφαλαίων

Η εργασία αυτή οργανώνεται ως εξής: αρχικά, στο κεφάλαιο 2 θα εξετάσουμε το θέμα της ιδιωτικότητας των δεδομένων όπως αντιμετωπίζεται από νομικής πλευράς. Συγκεκριμένα, στην παράγραφο 2.1 θα αναλύσουμε τα βασικότερα μοντέλα προστασίας της ιδιωτικότητας των δεδομένων, ενώ στην παράγραφο 2.2 θα εξετάσουμε το βασικότερο από αυτά τα μοντέλα, τους νόμους. Ειδικότερα, θα αναλύσουμε την Ελληνική, Ευρωπαϊκή και διεθνή νομοθετική προσέγγιση ξεχωριστά, τόσο για την προστασία της ιδιωτικότητας των δεδομένων γενικά, όσο και για την προστασία των τηλεπικοινωνιακών δεδομένων. Τέλος, στην παράγραφο 2.3 θα εξετάσουμε τον τρόπο με τον οποίο διάφορες χώρες ανά τον κόσμο ρυθμίζουν νομοθετικά τη διασυνοριακή ροή δεδομένων, γεγονός που αποτελεί ανασταλτικό παράγοντα για την ιδιωτικότητά τους.

Στη συνέχεια, στο κεφάλαιο 3 θα περιγράψουμε τους εθνικούς, Ευρωπαϊκούς και διεθνείς εποπτικούς φορείς που είναι αρμόδιοι για τον έλεγχο της εφαρμογής του νομοθετικού και ρυθμιστικού πλαισίου της κάθε χώρας. Ειδικότερα θα δοθεί στον τρόπο με τον οποίο οι φορείς αυτοί συνεργάζονται μεταξύ τους αλλά και με τους πολίτες προκειμένου να παρέχουν την απαραίτητη προστασία. Ειδικότερα, στην παράγραφο 3.1 θα αναλύσουμε τους Ελληνικούς φορείς και στην παράγραφο 3.2 θα εξετάσουμε τους βασικότερους Ευρωπαϊκούς και διεθνείς εποπτικούς
φορείς, εστιάζοντας στις αρμοδιότητές τους στον τομέα των τηλεπικοινωνιών.

Στο κεφάλαιο 4 θα εξετάσουμε τα συστήματα παροχής υπηρεσιών θέσης, καθώς και τα δεδομένα τα οποία προέρχονται από τις κινούμενες οντότητες που χρησιμοποιούν τέτοιου είδους συστήματα. Πιο συγκεκριμένα, στην παράγραφο 4.1 θα εξετάσουμε τα συστατικά των υπηρεσιών θέσης, τον τρόπο με τον οποίο παρέχουν τις υπηρεσίες στους χρήστες, τις μεθόδους εντοπισμού των θέσεων των χρηστών, καθώς και τις απαιτήσεις των συστημάτων αυτών. Εν συνεχεία, στην παράγραφο 4.2 θα ερευνήσουμε τα χαρακτηριστικά των χωρο-χρονικών δεδομένων που επηρεάζουν την ανάλυσή τους, καθώς και τα βασικότερα ζητήματα ιδιωτικότητας που προκύπτουν κατά τη συλλογή και ανάλυσή τους.

Στο κεφάλαιο 5 θα ερευνήσουμε τις βασικότερες τεχνικές διασφάλισης της ιδιωτικότητας των δεδομένων και της ανωνυμίας των χρηστών. Πιο συγκεκριμένα, στην παράγραφο 5.1 θα αναλύσουμε τις απαιτήσεις ασφαλείας των συστημάτων οι οποίες εκφράζονται μέσα από τις πολιτικές ασφαλειάς. Ο πιο κρίσιμος παράγοντας στον οποίο θα εστιάσουμε, είναι ο έλεγχος προσπέλασης στα δεδομένα. Στη συνέχεια, στην παράγραφο 5.2, θα εξετάσουμε μία μέθοδο προστασίας της ασφαλείας των χρηστών και των συστημάτων, την κρυπτογραφία, αναλύοντας τις βασικότερες κρυπτογραφικές προσεγγίσεις οι οποίες έχουν αναπτυχθεί για την προστασία των χωρο-χρονικών δεδομένων. Τέλος, στην παράγραφο 5.3 θα παρουσιάσουμε μία πολύ σημαντική τεχνική διασφάλισης της ανωνυμίας των κατόχων των δεδομένων και των περιοχών στις οποίες βρίσκονται, την Κ-ανωνυμία.

Στο κεφάλαιο 6, θα εξετάσουμε τα διάφορα συστήματα που προτείνονται στη βιβλιογραφία προκειμένου να αντιμετωπίσουν τα προβλήματα των υπαρχόντων συστημάτων παροχής υπηρεσιών θέσης. Στις παραγράφους 6.1 - 6.5 θα ερευνήσουμε τη δομή των βασικότερων προτεινόμενων συστημάτων, τους αλγόριθμους που χρησιμοποιούνται για την υλοποίησή τους καθώς και τα αποτελέσματα των πειραματικών μελετών για τη χρήση τους στις υπάρχουσες υπηρεσίες θέσης.
Τέλος, στο κεφάλαιο 7 θα αναλύσουμε τους οργανισμούς, οι οποίοι χρηματοδοτούν την έρευνα για την πρόοδο των επιστημών και της τεχνολογίας, καθώς και τα ερευνητικά προγράμματα τα οποία λαμβάνουν χώρα αυτή την περίοδο. Πιο συγκεκριμένα, στην παράγραφο 7.1 θα περιγράψουμε τον τρόπο με τον οποίο οι βασικότεροι Ευρωπαϊκοί και διεθνείς χρηματοδοτικοί οργανισμοί υποστηρίζουν τις ερευνητικές ομάδες στην έρευνα που σχετίζεται με τα ζητήματα που παρουσιάσαμε στα προηγούμενα κεφάλαια, ενώ στην παράγραφο 7.2 θα αναλύσουμε τα σημαντικότερα Ευρωπαϊκά και διεθνή προγράμματα τα οποία χρηματοδοτούνται από αυτούς τους οργανισμούς προκειμένου να παρέχουν λύσεις και μεθόδους για την προστασία της ιδιωτικότητας των χρηστών υπηρεσιών θέσης.
Κεφάλαιο 2

Ιδιωτικότητα Δεδομένων

Η ιδιωτικότητα αποτελεί ένα από τα πιο σημαντικά ζητήματα που συνδέονται με τις τεχνολογίες πληροφοριών. Κατά τη διάρκεια της συλλογής και ανταλλαγής δεδομένων προκύπτουν πολλά ερωτήματα τα οποία απαιτούν απαντήσεις. Ειδικότερα, πώς μπορούν τα ευαίσθητα προσωπικά δεδομένα να αποθηκευτούν και να υποβληθούν σε επεξεργασία χωρίς να παραβιάσουν τα προσωπικά δικαιώματα και η ελευθερία των ατόμων; Πώς μπορούν τα προσωπικά δεδομένα να χρησιμοποιούνται αποκλειστικά από εξουσιοδοτημένες οντότητες με τέτοιο τρόπο ώστε να βοηθούν τα άτομα και όχι να τα βλάπτουν, παραδείγματος χάριν στιγματίζοντας τα κοινωνικά; Αυτά τα ερωτήματα τα οποία απαιτούν απαντήσεις σε ένα συνδυασμένο τεχνικό, νομικό και κοινωνικό επίπεδο, εξετάζουν ένα πολύ κρίσιμο ζήτημα, τόσο από εθνική όσο και από κοινωνική σκοπιά.

Στο κεφάλαιο αυτό θα εξετάσουμε το θέμα της ιδιωτικότητας των δεδομένων όπως αντιμετωπίζεται κυρίως από νομικής πλευράς. Συγκεκριμένα, στην παράγραφο 2.1 θα αναλύσουμε τα βασικότερα μοντέλα
προστασίας της ιδιωτικότητας των δεδομένων. Στην παράγραφο 2.2, θα εξετάσουμε το βασικότερο από αυτά τα μοντέλα, τους νόμους και θα αναλύσουμε τη νομική προσέγγιση των Ευρωπαϊκών και μη Ευρωπαϊκών χωρών. Πιο συγκεκριμένα, στην παράγραφο 2.2.1 θα αναλύσουμε την Ελληνική νομοθεσία, τόσο για την προστασία των δεδομένων γενικότερα, όσο και για την προστασία των δεδομένων ειδικότερα στον τομέα των τηλεπικοινωνιών. Μία αντίστοιχη ανάλυση θα κάνουμε στην παράγραφο 2.2.2 για την Ευρωπαϊκή νομοθεσία περί προστασίας δεδομένων. Εν συνεχεία, στην παράγραφο 2.2.3 θα ερευνήσουμε τη διεθνή νομική προσέγγιση για την προστασία των δεδομένων ειδικότερα, ενώ θα αναλύσουμε μία πολύ σημαντική διεθνή ανάπτυξη για την προστασία της ιδιωτικότητας των δεδομένων που προέρχεται από τα κράτη του APEC. Επιπλέον, θα ερευνήσουμε τη διεθνή προσέγγιση για την προστασία των δεδομένων ειδικότερα στον τομέα των τηλεπικοινωνιών. Τέλος, στην παράγραφο 2.3 θα εξετάσουμε τη διασυνοριακή ροή δεδομένων, που αποτελεί έναν ανασταλτικό παράγοντα για την ιδιωτικότητά τους.

2.1 Μοντέλα Προστασίας της Ιδιωτικότητας Δεδομένων

Η προσπάθεια για την προστασία της ιδιωτικότητας των δεδομένων έχει γίνει στις μέρες μας ένα από τα βασικότερα ερευνητικά ζητήματα, κυρίως λόγω της ραγδαίας ανάπτυξης της τεχνολογίας. Οι περισσότερες χώρες του κόσμου αντιμετωπίζουν αυτό το καύριο ζήτημα θεσπίζοντας νέους νόμους ή ανανεώνοντας τους ήδη υπάρχοντες για την προστασία της ιδιωτικότητας των δεδομένων. Οι νόμοι αυτοί περιλαμβάνουν μέτρα για την προστασία προσωπικών δεδομένων αλλά και για την προστασία δεδομένων...
επικοινωνιών, τα οποία και αφορούν μηνύματα ηλεκτρονικού ταχυδρομείου, τηλεφωνικά δεδομένα και άλλα. Συνήθως, υπάρχει ξεχωριστή νομοθετική μνεία για τέτοιου είδους δεδομένα, όπως συμβαίνει στην Ελλάδα και γενικότερα σε όλη την Ευρώπη.

Το πρώτο και βασικότερο μοντέλο για την προστασία δεδομένων είναι οι νόμοι που αφορούν τη συλλογή και την επεξεργασία των δεδομένων από δημόσιους ή ιδιωτικούς φορείς. Θεσπίζοντας νόμους οι χώρες δεν αφήνουν την προστασία δεδομένων στην κρίση του κάθε δημόσιου ή ιδιωτικού φορέα. Σε κάθε χώρα που έχει θεσπίσει νόμους για την προστασία δεδομένων υπάρχει συνήθως κάποια δημόσια Αρχή η οποία επιτηρεί την εφαρμογή τους.

Σε κάποιες περιπτώσεις, όμως, όπως συμβαίνει στην Αμερική, δεν υπάρχει κάποιος γενικός νόμος περί προστασίας ευαίσθητων ή προσωπικών δεδομένων. Αντίθετα, για κάθε τομέα, όπως για παράδειγμα προστασία οικονομικών ή ιατρικών δεδομένων, υπάρχει ξεχωριστή νομοθεσία. Το μειονέκτημα σε αυτήν την περίπτωση είναι ότι με κάθε ξεχωριστό τομέα της ανθρώπινης δραστηριότητας ή με κάθε καινούρια τεχνολογία θα πρέπει να θεσπίζεται ξεχωριστός νόμος.

Σε πολλές περιπτώσεις, η προσπάθεια για προστασία των δεδομένων μπορεί να γίνει και από τους ιδίους τους φορείς, όπως οι εταιρείες, οι επιχειρήσεις και άλλα. Έτσι λοιπόν μπορούν να δημιουργήσουν ένα σύνολο από αρχές και οδηγίες που θα προσδιορίζουν τα δικαιώματα που έχει η κάθε συμμετέχουσα οντότητα πάνω στα προσωπικά δεδομένα. Το μοντέλο αυτό από μόνο του δεν μπορεί να προσφέρει σημαντική προστασία διότι συνήθως είναι ανεπαρκές και στερείται απόλυτου ελέγχου για την επιβολή του. Επιπρόσθετα, δεν μπορεί να υπάρχει μία κοινή πολιτική προστασίας αφού οι οδηγίες και οι αρχές αυτές βρίσκονται στην ευχέρεια του κάθε φορέα.

Τέλος, με τη ραγδαία ανάπτυξη της τεχνολογίας, η προστασία δεδομένων μπορεί να καταλήξει στα χέρια του κάθε χρήστη. Για παράδειγμα, οι χρήστες του διαδικτύου μπορούν να εγκαταστήσουν στον προσωπικό τους υπολογιστή προγράμματα ή συστήματα προκειμένου να
επιτύχουν το βαθμό ασφάλειας που επιθυμούν. Παραδείγματα αποτελούν οι τοίχοι προστασίας, οι *proxy servers* ή η κρυπτογράφηση.

Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι τα παραπάνω μοντέλα δεν είναι απαραίτητα να χρησιμοποιούνται ανεξάρτητα. Αντιθέτως, μπορούν να χρησιμοποιηθούν παράλληλα (ακόμα και όλα) προκειμένου να παρέχεται η μέγιστη προστασία των ευαίσθητων/προσωπικών δεδομένων.

2.2 Εξέλιξη στην Προστασία Δεδομένων

Ο σεβασμός και η προστασία της ανθρώπινης αξιοπρέπειας, της μυστικότητας και της ελευθερίας ανάπτυξης της προσωπικότητας, αποτελούν θεμελιώδεις αναζητήσεις για κάθε δημοκρατική κοινωνία. Η καθολική παρουσία της τεχνολογίας σε όλους τους τομείς της καθημερινής μας ζωής δε θα μπορούσε να αφήσει ανεπηρέαστη την νομική σκέψη. Οι καθημερινές δραστηριότητες και συναλλαγές των ανθρώπων γίνονται όλο και περισσότερο χρησιμοποιώντας ηλεκτρονικά δίκτυα επικοινωνιών και των παρεχόμενων από αυτά υπηρεσιών. Τα δεδομένα τα οποία παράγονται περιέχουν τόσο τις πληροφορίες των ατόμων που επικοινωνούν και της χρονικής διάρκειας των επικοινωνιών, όσο και πληροφορίες για το χρόνο και τη γεωγραφική θέση που χρησιμοποιούνται οι σταθερές και κινητές υπηρεσίες φωνής, τα fax, τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα *SMS* και το διαδίκτυο [44, 65]. Προκειμένου να προστατευθεί η ιδιωτική ζωή των ανθρώπων, οι αρχές που επιβάλλουν και ελέγχουν το νομοθετικό πλαίσιο θεωρούν ότι μερικά στοιχεία δεν πρέπει να αποθηκεύονται από όλους τους φορείς παροχής επικοινωνιών, στην έκταση που αυτό συμβαίνει και τελευταία. Από την άλλη πλευρά, αν τα συγκεκριμένα δεδομένα δεν αποθηκεύονται τότε
δε να είναι διαθέσιμα ούτε σε περιπτώσεις που οι δημόσιες αρχές τα χρειαστούν για έρευνα ή εξερεύνηση εγκλημάτων.

Τα πρώτα ίχνη της ανάγκης για την προστασία των προσωπικών δεδομένων παρατηρούνται στη Σύμβαση της Ρώμης το 1950 για την προστασία των ατομικών δικαιωμάτων. Από τότε και μέχρι σήμερα οι περισσότερες χώρες, Ευρωπαϊκές ή μη, έχουν θεσπίσει νόμους για την προστασία των δικαιωμάτων και ελευθεριών των ατόμων, καθώς και για την προστασία της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Οι νόμοι αυτοί ανανεώνονται διαρκώς κυρίως μετά τις τρομοκρατικές ενέργειες, όπως οι επιθέσεις της 11ης Σεπτεμβρίου του 2001 στην Αμερική, του 2004 στη Μαδρίτη και του 2005 στην Αγγλία. Την ίδια στιγμή, πολλοί ερευνητές αναζητούν τρόπους για την προστασία δεδομένων, όπως θα παρουσιαστεί στα επόμενα κεφάλαια.

Στον παρακάτω χάρτη παρουσιάζεται η νομική αντιμετώπιση της προστασίας δεδομένων από όλες τις χώρες του κόσμου μέχρι το Μάιο του 2007. Ο χάρτης αυτός έχει αντληθεί από τον ιστοχώρο: Privacy International [88].
Εικόνα 2.1 Νομική αντιμετώπιση ανά τον κόσμο για την προστασία δεδομένων.

2.2.1 Ελληνική Νομοθεσία

Η Ελλάδα είναι μία από τις χώρες που έχουν ξεχωριστό νόμο για την προστασία δεδομένων προσωπικού χαρακτήρα γενικότερα (Νόμος 2472/1997) και για την προστασία δεδομένων προσωπικού χαρακτήρα ειδικότερα στον τηλεπικοινωνιακό τομέα (Νόμος 2774/1999) [3]. Στις ακόλουθες ενότητες θα αναλύσουμε τις βασικές αρχές των νόμων αυτών για την προστασία των δεδομένων και των κατόχων τους.
2.2.1.1 Νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα
Γενικότερα

Στην Ελλάδα, η προστασία των πολιτών από την επεξεργασία δεδομένων προσωπικού χαρακτήρα προστατεύεται από το νόμο 2472/1997, όπως έχει τροποποιηθεί με βάση τις οδηγίες του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Ο νόμος αυτός, όπως έχει τροποποιηθεί από μεταγενέστερους νόμους, θεσπίζει τις προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προκειμένου να προστατεύονται τα δικαιώματα και οι θεμελιώδεις ελευθερίες των φυσικών προσώπων, καθώς και η ιδιωτική τους ζωή. Συγκεκριμένα, διαχωρίζει τα δεδομένα σε δεδομένα προσωπικού χαρακτήρα και σε ευαίσθητα δεδομένα [3]. Τα δεδομένα προσωπικού χαρακτήρα αναφέρονται στο υποκείμενο των δεδομένων· παραδείγματα τέτοιου είδους δεδομένων αποτελούν το όνομα, η διεύθυνση ή γενικότερα κάποιο προσδιοριστικό της οικονομικής, πολιτιστικής ή κοινωνικής ταυτότητας του ατόμου. Από την άλλη, τα ευαίσθητα δεδομένα αφορούν την φυλετική ή εθνική προέλευσή, τις θρησκευτικές πεποιθήσεις και την υγεία.

Αλλάζοντας την φύση τους, τα ευαίσθητα δεδομένα απαιτούν πιο αυστηρό τρόπο νομικής αντιμετώπισης από τα προσωπικά δεδομένα γενικά. Το ερώτημα που προκύπτει από αυτό το σημείο είναι πώς πρέπει να είναι οι προϋποθέσεις συλλογής των δεδομένων, ποιες οι συνθήκες επεξεργασίας τους και από ποιον θα χρησιμοποιηθούν. Σύμφωνα με το νόμο 2472/1997, η συλλογή δεδομένων πρέπει να είναι καθορισμένη, θεμιτή και νόμιμη, ενώ ο
κάθε πολίτης θα πρέπει να είναι σε θέση να γνωρίζει ποιος, που, πότε, πώς και γιατί επεξεργάζεται τα προσωπικά του δεδομένα. Η επεξεργασία προσωπικών δεδομένων θα πρέπει να τηρεί τις προϋποθέσεις τις οποίες αναφέρει ο νόμος. Έτσι, η συλλογή και επεξεργασία ευαισθητων δεδομένων απαγορεύεται, εκτός αν συντρέχει μία αναγκαία συνθήκη, όπως η διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, ή λόγοι εθνικής ασφάλειας, αναγκών εγκληματολογίας, προστασία δημόσιας υγείας και άλλοι. Τέλος, στο νόμο αναφέρονται τα δικαιώματα του υποκειμένου των δεδομένων, όπως το δικαίωμα ενημέρωσης, πρόσβασης, αντίρρησης, ή προσωρινής δικαστικής προστασίας του.

2.2.1.2 Νομοθεσία για την Προστασία Δεδομένων Ειδικότερα στον Τομέα των Τηλεπικοινωνιών

Η Ελληνική νομοθεσία περιέχει ξεχωριστό νόμο για την προστασία των θεμελιωδών δικαιωμάτων και της ιδιωτικής ζωής κατά την επεξεργασία τηλεπικοινωνιακών δεδομένων (νόμος 2774/1999 [3]). Ο νόμος αυτός βρίσκει εφαρμογή τόσο στους δημόσιους όσο και στους ιδιωτικούς φορείς τηλεπικοινωνιακών υπηρεσιών, ενώ έχει τροποποιηθεί βάσει των Οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Σύμφωνα με το νόμο 2774/1999, οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Θα πρέπει να σημειωθεί εδώ ότι για κάθε ζήτημα σχετικό με την παροχή τηλεπικοινωνιακών υπηρεσιών που δεν
ρυθμίζεται ειδικότερα από το συγκεκριμένο νόμο, εφαρμόζεται αντ’ αυτού ο νόμος 2472/1997.

Το Νομοσχέδιο του 2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, με την ενσωμάτωση των Οδηγιών 2002/19/ΕΚ, 2002/20/ΕΚ, 2002/21/ΕΚ, 2002/22/ΕΚ, 2002/58/ΕΚ και 2002/77/ΕΚ [36], ορίζει ότι τα τηλεπικοινωνιακά δεδομένα αποτελούν προσωπικά δεδομένα και θα πρέπει να προστατεύονται, κατά τη συλλογή και επεξεργασία τους. Πιο συγκεκριμένα, απαγορεύεται η ακρόαση, υποκλοπή, αποθήκευση ή οποιοδήποτε άλλο είδος παρακολούθησης ή επιτήρησης των ηλεκτρονικών επικοινωνιών και των συναφών δεδομένων κίνησης και θέσης από άλλα πρόσωπα πλην των χρηστών. Η καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης επιτρέπεται όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδείκτικων στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα, με την προϋπόθεση ότι και τα δύο μέρη παρέχουν τη συγκατάθεσή τους, εφόσον βέβαια έχουν ενημερωθεί από πριν για το σκοπό της καταγραφής αυτής.

Επιπρόσθετα, τα δεδομένα κίνησης που αφορούν συνδρομητές και χρήστες, τα οποία υποβάλλονται σε επεξεργασία για την πραγματοποίηση κλήσεων και αποθηκεύονται από το φορέα παροχής τηλεπικοινωνιακού δικτύου, πρέπει να διαγράφονται ή να καθίστανται ανώνυμα κατά τη λήξη της κλήσης. Τα δεδομένα που αφορούν τον αριθμό ή την προσωπική της συσκευής του συνδρομητή, τη διεύθυνση του συνδρομητή, το χρόνο έναρξης και τη διάρκεια κλήσεων που πραγματοποιήθηκαν, καθώς και άλλες πληροφορίες σχετικές με τους τρόπο και τη διαδικασία πληρωμής, επιτρέπεται να υποβάλλονται σε επεξεργασία μόνο για την έκδοση του λογαριασμού και μέχρι το τέλος της περιόδου εντός της οποίας μπορεί να αμφισβητηθεί νομίμως ο λογαριασμός ή να επιδιωχθεί η πληρωμή του. Η επεξεργασία δεδομένων κίνησης θα πρέπει να ανατίθεται σε πρόσωπα τα οποία ενεργούν υπό την εποπτεία των φορέων παροχής δημοσίων τηλεπικοινωνιακών δικτύων ή της διαθέσιμων τηλεπικοινωνιακών υπηρεσιών.
Τέλος, ο φορέας παροχής διαθέσιμων τηλεπικοινωνιακών υπηρεσιών προς τους χρήστες οφείλει να λαμβάνει τα απαραίτητα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των υπηρεσιών του και η ασφάλεια του δημόσιου τηλεπικοινωνιακού δικτύου.

Τα μέτρα αυτά θα πρέπει να εξασφαλίζουν ένα επίπεδο ασφάλειας ανάλογο προς τον υπάρχοντα κίνδυνο. Επιπρόσθετα, σε περίπτωση που υπάρχει κίνδυνος παραβίασης της ασφάλειας του δημόσιου τηλεπικοινωνιακού δικτύου, ο φορέας παροχής της υπηρεσίας οφείλει να ενημερώσει τους συνδρομητές για τον κίνδυνο αυτό, καθώς επίσης και για όλες τις δυνατότητες αποτροπής του.

2.2.2 Ευρωπαϊκή Νομοθεσία

Η Ευρωπαϊκή Επιτροπή θέτει το ευρύτερο θεσμικό πλαίσιο για την ασφάλεια των δεδομένων στην Ευρώπη με την έκδοση σχετικών Οδηγιών, Κανονισμών και Συστάσεων. Η Ευρωπαϊκή Ένωση έχει τους αυστηρότερους νόμους περί προστασίας δεδομένων και θεμελιωδών ελευθεριών των ανθρώπων. Η Ευρωπαϊκή νομοθεσία περιλαμβάνει έξι οδηγίες για την προστασία δεδομένων (Οδηγία 95/46/ΕΕ [26]) και για την προστασία δεδομένων ειδικότερα στον τομέα τηλεπικοινωνιών (Οδηγία 97/66/ΕΚ [36]) οι βασικές αρχές των οποίων θα παρουσιαστούν στην ακόλουθη ενότητα.
2.2.2.1 Νομοθεσία για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα
Γενικότερα

Το 1995, η Ευρωπαϊκή Ένωση θέσπισε την Οδηγία 95/46/ΕΕ [26], γνωστή και ως Οδηγία ιδιωτικότητας της ΕΕ. Στην Οδηγία αυτή η ΕΕ απαιτεί από όλα τα κράτη μέλη της να θεσπίσουν τους δικούς τους νόμους βασισμένους στους κανόνες της Οδηγίας περί προστασίας των θεμελιωδών δικαιωμάτων των άνθρωπων. Η βασικότερη αρχή της Οδηγίας είναι ότι κάθε άνθρωπος έχει το δικαίωμα της μυστικότητας της προσωπικής και οικογενειακής ζωής καθώς και της αλληλογραφίας του. Επιπλέον, η Οδηγία κατοχύρωνει σε κάθε πολίτη το δικαίωμα να γνωρίζει το που αποθηκεύονται τα δεδομένα του, από ποιον επεξεργάζονται και για ποιο λόγο. Τα δεδομένα μπορούν να συλλέγονται μόνο για συγκεκριμένους και νόμιμους λόγους. Παράλληλα, δεν πρέπει να συλλέγονται περισσότερα δεδομένα από όσα είναι απαραίτητα για να επιτευχθεί ο σκοπός συλλογής τους ή να κρατούνται για μεγαλύτερο χρονικό διάστημα από τον αρχικό λόγο συλλογής τους. Επιπρόσθετα, η Οδηγία τονίζει ότι η επεξέργασία των δεδομένων, η οποία απέχει από τον αρχικό στόχο συλλογής τους, μπορεί να πραγματοποιηθεί μόνο με τη συγκατάθεση του ατόμου στο οποίο ανήκουν τα δεδομένα. Η συλλογή και επεξέργασία των δεδομένων θα πρέπει πάντα να γίνεται με γνώμονα την προσωπική ζωή του κάθε ατόμου, ακόμα και αν στα δεδομένα αυτά δεν περιέχονται ευαίσθητα δεδομένα. Ο μόνος λόγος για να μην ασκηθούν αυτά τα δικαίωμα είναι οι περιπτώσεις εθνικής προστασίας, δημόσιας ασφάλειας και υγείας, οικονομικής ευημερίας της
κάθε χώρας ή για την πρόληψη εγκληματικών ή τρομοκρατικών ενεργειών [26, 91].

Παράλληλα, η Οδηγία, απαιτεί από κάθε μέλος της Ευρωπαϊκής Ένωσης να έχει τη δική της δημόσια Αρχή (ή τις δικές της αρμόδιες Αρχές) η/οι οποίες/οι θα ελέγχουν/ουν το κατά πόσο τηρούνται οι νόμοι του κάθε κράτους. Οι Αρχές αυτές των κρατών μελών της ΕΕ θα πρέπει να βρίσκονται σε συνεργασία μεταξύ τους, ενώ οι υπάλληλοι μιας τέτοιας Αρχής δεσμεύονται από το επαγγελματικό απόρρητο για τις εμπιστευτικές πληροφορίες στις οποίες έχουν πρόσβαση στη διάρκεια της υπηρεσίας τους αλλά και μετά από το τέλος των καθηκόντων τους (άρθρο 28 της Οδηγίας 95/46/ΕΕ).

Τέλος, λόγω της ανησυχίας της Ευρώπης για τη νομοθεσία των μη Ευρωπαϊκών χωρών και ιδιαίτερα των ΗΠΑ, η Οδηγία προστατεύει τους Ευρωπαίους πολίτες από τη μεταφορά των δεδομένων προς τις χώρες αυτές. Οι προϋποθέσεις για τη μεταφορά των δεδομένων προς τρίτες χώρες θα αναλυθούν στην παράγραφο 2.3.

### 2.2.2.2 Νομοθεσία για την Προστασία Δεδομένων Ειδικότερα στον Τομέα των Τηλεπικοινωνιών

To 1997 η Ευρωπαϊκή Κοινότητα εισήγαγε την Οδηγία 97/66/ΕΚ [36] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ού Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Η Ευρωπαϊκή Κοινότητα αποσκοπεί στην εναρμόνιση των διατάξεων των κρατών μελών της, έτσι ώστε να διασφαλίζεται ισοδύναμο επίπεδο
προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών όσον αφορά την
επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό
tομέα, καθώς και την ελευθερία κυκλοφορία των δεδομένων αυτών στην
Κοινότητα. Επιπρόσθετα, αποσκοπεί στη δημιουργία ενός κατάλληλου
περιβάλλοντος για τη μελλοντική ανάπτυξη των τηλεπικοινωνιών στην
Κοινότητα [1].

Όλα τα κράτη μέλη της Ευρωπαϊκής Κοινότητας έχουν
προσαρμόσει τη νομοθεσία τους σύμφωνα με τις Οδηγίες του Ευρωπαϊκού
Κοινοβουλίου για την προστασία προσωπικών δεδομένων και το απόρρητο
tων επικοινωνιών που διενεργούνται μέσω του δημόσιου τηλεπικοινωνιακού
dικτύου και των διαθέσιμων τηλεπικοινωνιακών υπηρεσιών. Ειδικότερα, η
Οδηγία, όπως έχει προσαρμοστεί το 2002 με την Οδηγία 2002/58/ΕΚ [36],
apagorfei tην akro Basi, upoklopη, apothkeusi ou allo eidos
parakolouthish twn epikoinwionwn apò proóspa plhwn twn chrhstwn xwris
ti sygkatasthse toun, ektois an uparchei syzetikη vomicη òdea.

H Odh gia 2002/58/ΕΚ proasarmostithke metà tηn 11η Σεπτεμβρίου
2001 kai kathoriçê toun orous kátw apò toun oposous ta krate meîh
mporôwn na egrînous twn nomothetikâ métra gia tηn epiboli nómu,
symperilambanoménwn kai twn métron diatîrēhsis dedoménnwn, dihalh tη
diagrafi toun ótan den einai pleon aparaîtita gia tōn arxikó skopó gia
ton oposoîn apothkeúthikan. Pio sygkkeirménna, ta dedoména prêphei na
svllêgonontai kai na diatprounontai me nómu tróspo kai gia sygkkeirménη
xronikí periódo. Ta dedoména ta opoia svllêgonontai kai apothkeúontai thâ
prêphei na einai mîno ta aparaîtita kai ta katalhla gia tōn arxikó skopó
svlloghs toun. Epiprostîtha, thâ prêphei na eoxasofaliizontai eparkh techniká
kai organwstiká métra asfálleias gia tηn proasstasia twn bâsewn dedoménnwn
ōi opoies periôchoun ta dedoména autâ. Sýmpfova me tηn Odh gia, ta
dedoména epikoinwionwn pou upobálloontai se epexeiragasia kai
apothkeúontai apo ton proumíthenvth enós dhimóssiou h idiótikow diktúou
epikoinwionwn prêphei na sbhstoun h na ginoun anónyma meta to peráso tωn
diasthmatos tōn arxikó skopou svlloghs toun (gía paraðeigma gia
skopous plhrwmwn h timolôghshs). Autí h epexeiragasia einai epitrepth
mîno mékhi to peráso tηs periódou kata tη diárrkeia tηs opoias o
λογαριασμός μπορεί να εκδοθεί και πληρωθεί. Εδώ θα πρέπει να σημειωθεί ότι στα δεδομένα επικοινωνιών, οι θέσεις των χρηστών κινητών υπηρεσιών αποτελούν ευαίσθητα δεδομένα, σύμφωνα με την Οδηγία, και, επομένως, αντιμετωπίζονται με τα αυστηρά νομοθετικά μέτρα για τα ευαίσθητα δεδομένα.

Επιπρόσθετα, για σκοπούς μάρκετινγκ ο φορέας παροχής ηλεκτρονικής υπηρεσίας μπορεί να επεξεργαστεί δεδομένα μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων. Σε αυτή την περίπτωση θα πρέπει να δοθεί η δυνατότητα στο υποκείμενο να αποσύρει τη συγκατάθεσή του οποιαδήποτε στιγμή. Οι φορείς παροχής υπηρεσιών οφείλουν να ενημερώσουν τον χρήστη για τον τύπο δεδομένων που υποβάλλονται σε επεξεργασία και για τη διάρκεια της επεξεργασίας πριν τη λήψη της συγκατάθεσης. Επιπρόσθετα, η συμμόρφωση των μέτρων διατήρησης δεδομένων θα πρέπει να επιτευχθεί λαμβάνοντας υπόψη τα θεμελιώδη δικαιώματα που αποτελούν αναπόσπαστο τμήμα των γενικών αρχών του κοινοτικού δικαίου, συμπεριλαμβανομένου του δικαιώματος σεβασμού της ιδιωτικής ζωής, όπως καθορίζεται στο άρθρο 8 της Ευρωπαϊκής Συνθήκης σχετικά με τα ανθρώπινα δικαιώματα.

Η επιθυμητή προσέγγιση είναι τα κράτη μέλη να διαφέρουν όσο το δυνατόν λιγότερο αναφορικά με τις περιόδους διατήρησης των δεδομένων. Με αυτό τον τρόπο αποφεύγεται η κατάσταση στην οποία παροχείς ηλεκτρονικών υπηρεσιών εκφράζουν διαφορετικές τεχνικές και νομικά περιβάλλοντα, ενώ οι Αρχές Προστασίας Δεδομένων των κρατών μπορούν να συνεργαστούν χωρίς αντιφάσεις και προβλήματα.

Στις 14/05/2003 πραγματοποιήθηκε στο Λονδίνο μία σύσκεψη στην οποία παρουσιάστηκαν στατιστικά στοιχεία τα οποία αποδείκνυαν ότι η αστυνομία και άλλες εξεταστικές αρχές του Ηνωμένου Βασιλείου δέχονται καθημερινά μία πρωτοφανή ποσότητα αναφορών από προμηθευτές επικοινωνιών [88]. Τα δεδομένα αυτά αφορούν λογαριασμούς τηλεφώνων, μηνύματα ηλεκτρονικού ταχυδρομείου, λεπτομέρειες πελατών και αρχεία που παρουσιάζουν τις θέσεις των ανθρώπων από κλήσεις που πραγματοποιήθηκαν από κινητά τηλέφωνα. Αυτές οι πληροφορίες περιέχουν...
προσωπικά δεδομένα των ατόμων. Για παράδειγμα, περιλαμβάνουν από τους αριθμούς που καλούν ή δέχονται κλήσεις, όπως και πληροφορίες που αναφέρονται κατά τη διάρκεια των τηλεφωνικών συνδιαλέξεων. Οι πληροφορίες αυτές, αν συνδυαστούν κατάλληλα μπορούν να δημιουργήσουν το προφίλ των ανθρώπων. Στο προφίλ αυτό φανερώνονται οι επαφές και οι φιλίες που έχει ο κάθε χρήστης, τα ενδιαφέροντά του, οι συναλλαγές του, οι μετακινήσεις (από τις θέσεις των φορητών συσκευών) και γενικότερα οι προσωπικές του πληροφορίες. Στο συνέδριο αυτό, το ερώτημα που προέκυψε είναι για πιο λόγο πολλές φορές δεν εφαρμόζεται ο νόμος προστασίας δεδομένων και καταπατούνται τα δικαιώματα απορρήτου επικοινωνιών και προστασίας προσωπικών δεδομένων.

Παρόλα αυτά όμως, τα κράτη μέλη, λόγω των τρομοκρατικών επιθέσεων, ανησυχούν και εξετάζουν τη διατήρηση αυτών των δεδομένων για μεγαλύτερο χρονικό διάστημα. Ορισμένα από τα κράτη μέλη έχουν υιοθετήσει ή προγραμματίζουν να υιοθετήσουν μέτρα να απαιτούν από τους περισσότερους ή όλους τους χειριστές επικοινωνιών να διατηρούν δεδομένα επικοινωνιών προκειμένου να μπορούν να χρησιμοποιηθούν από τις δημόσιες αρχές σε έκτακτες περιπτώσεις.

Στις 25 Μαρτίου 2004 το Ευρωπαϊκό Συμβούλιο εξέτασε προτάσεις για τους κανόνες διατήρησης δεδομένων επικοινωνιών από τους φορείς παροχής υπηρεσιών με στόχο την καταπολέμηση της τρομοκρατίας. Σε απάντηση, τέσσερα κράτη μέλη (Αγγλία, Ιρλανδία, Σουηδία και Γαλλία) παρουσίασαν τις προτάσεις τους σχετικά με τη διατήρηση δεδομένων παρά το γεγονός ότι η Ιρλανδία και η Σουηδία δεν είχαν μέχρι τότε τέτοιου είδους νόμους. Οι προτάσεις τους παρουσιάστηκαν ως απάντηση στην τρομοκρατία (βασισμένες στις τρομοκρατικές επιθέσεις του 2001 στις ΗΠΑ και του 2004 στην Ισπανία) καθώς και στην αντιμετώπιση άλλων εγκληματικών πράξεων. Οι χώρες αυτές θεωρούν πως είναι πολύ σημαντικό να διατηρούνται δεδομένα που υπάρχουν στα δημόσια ή ιδιωτικά δίκτυα επικοινωνιών για την πρόληψη, την έρευνα και την ανίχνευση εγκλημάτων και αδικημάτων που περιλαμβάνουν χρήση ηλεκτρονικών συστημάτων επικοινωνιών. Η πρόταση που παρουσίασαν αφορά μόνο στα δεδομένα που παράγονται από μία επικοινωνία, ενώ δεν αφορά στο περιεχόμενο των επικοινωνιών αυτών.
Για παράδειγμα, αναφέρεται σε δεδομένα απαραίτητα να προσδιορίζουν την πηγή, τη δρομολόγηση και τον προορισμό μιας επικοινωνίας, το χρόνο, την ημερομηνία, τη διάρκεια και τη γεωγραφική θέση της επικοινωνίας αυτής στην αρχή και καθ’ όλη τη διάρκειά της. Το βασικό στοιχείο που περιλαμβάνει η πρόταση είναι η ανάγκη για εναρμόνιση των μέτρων μεταξύ των κρατών μελών, αφού κάποιες χώρες έχουν περάσει νομοθεσία σχετικά με τη διατήρηση δεδομένων για σκοπούς πρόληψης, έρευνας και ανίχνευσης εγκλημάτων ή υπενθύμισης, ενώ σε άλλες χώρες η νομοθεσία είναι εν εξελίξει.

Η διατήρηση όμως των δεδομένων και η πρόσβαση σε αυτά μπορεί να προκαλέσει παρέμβαση στην ιδιωτική ζωή του ατόμου. Εντούτοις, μία τέτοια παρέμβαση δεν προκαλεί άστοχες διεθνείς νόμους όσον αφορά στο δικαίωμα να τηρηθεί η μυστικότητα. Άλλωστε, όπως αναφέραμε και παραπάνω, μια τέτοια παρέμβαση προβλέπεται από το νόμο 2002/58/ΕΚ ανατιμά για λόγο ανάλογο με τον προοριζόμενο σκοπό για τον οποίο τα δεδομένα αυτά έχουν συλλεχθεί.

Στο συμβούλιο της 25ης Μαρτίου, οι υπηρεσίες επιτροπής επεδίωξαν σχόλια από τα κράτη μέλη για ζητήματα όπως οι τρέχουσες πρακτικές πρακτικές αποθήκευσης στοιχείων επικοινωνιών για επιχειρησιακούς λόγους, καθώς και το χρονικό διάστημα για το οποίο αυτά κρατούνται ανάλογα με τις υπηρεσίες (σταθερή/κινητή τηλεφωνία, SMS, MMS, μηνύματα ηλεκτρονικού ταχυδρομείου, διαδίκτυο). Επίσης, ερεύνησαν τις τρέχουσες πρακτικές για τις δημόσιες αρχές που διατηρούν δεδομένα ή έχουν πρόσβαση σε αυτά. Ειδικότερα, εξέτασαν την εφαρμογή της διατήρησης των δεδομένων για τις αρχές του κράτους και την ανάγκη για αυτούς να τηρήσουν τις διατάξεις των νομοθετικών μέτρων. Επίσης, ερεύνησαν τις τρέχουσες πρακτικές για τις δημόσιες αρχές που διατηρούν δεδομένα ή έχουν πρόσβαση σε αυτά. Ειδικότερα, εξέτασαν την εφαρμογή της διατήρησης των δεδομένων για τις αρχές του κράτους και την ανάγκη για αυτούς να τηρήσουν τις διατάξεις των νομοθετικών μέτρων. Επίσης, ερεύνησαν τις τρέχουσες πρακτικές για τις δημόσιες αρχές που διατηρούν δεδομένα ή έχουν πρόσβαση σε αυτά. Ειδικότερα, εξέτασαν την εφαρμογή της διατήρησης των δεδομένων για τις αρχές του κράτους και την ανάγκη για αυτούς να τηρήσουν τις διατάξεις των νομοθετικών μέτρων.
έγκλημα. Το πλάνο αυτό συμπεριλαμβάνει πολλούς τομείς που παρουσιάζουν προβλήματα για την προστασία των ανθρώπων, όπως αυτός των τηλεπικοινωνιών λόγω της αυξανόμενης διεθνούς διανομής δεδομένων.

Οι τρομοκρατικές επιθέσεις όμως, συνεχίζουν να ανησυχούν τα μέλη της Ευρωπαϊκής Ένωσης. Ως τμήμα του αγώνα ενάντια στην τρομοκρατία και το οργανωμένο έγκλημα, οι Ευρωπαίοι υπουργοί δικαιοσύνης συναντήθηκαν στο Λουξεμβούργο τον Ιούνιο του 2005 στο Συμβούλιο «δικαιοσύνης και εσωτερικών υποθέσεων» προκειμένου να πετύχουν μία συμφωνία για την πολιτική που πρέπει να ακολουθηθεί σχετικά με τη διατήρηση δεδομένων που επεξεργάζονται και αποθηκεύονται από τους προμηθευτές τηλεπικοινωνιακών υπηρεσιών. Συγκεκριμένα, το βασικό ερώτημα που προέκυψε στη συζήτησή τους είναι ποιοι τύποι δεδομένων θα πρέπει να αποθηκεύονται και για πόσο χρονικό διάστημα πρέπει να διατηρούνται. Αρχικά, εξέτασαν τα δεδομένα που συλλέγονταν από τις τηλεφωνικές γραμμές και τα κινητά τηλέφωνα. Όσον αφορά στο διαδίκτυο, οι αντιπρόσωποι των κρατών μελών συμφώνησαν σε μία μεταβατική περίοδο ώστε να λάβουν υπόψη τα προβλήματα του μερικού εθνικού προμηθευτές μπορούν να αντιμετωπίσουν στην εφαρμογή αυτού του τύπου διατήρησης των δεδομένων. Τα κράτη μέλη συμφώνησαν στην ύπαρξη ενός οργάνου διατήρησης δεδομένων για να αποτραπούν και να ελεγχθούν αποτελεσματικά ορισμένοι τύποι οργανωμένου εγκλήματος [88].

Τον επόμενο μήνα όμως, οι βομβαρδισμοί στην Αγγλία (7 Ιουλίου 2005) αναστάτωσαν την Ευρωπαϊκή Κοινότητα. Αμέσως μετά τους βομβαρδισμούς, η Βρετανική κυβέρνηση απαίτησε από όλους τους φορείς παροχής υπηρεσιών επικοινωνιών να διατηρήσουν όλες τις υπάρχουσες πληροφορίες που είχαν συλλέχθει μέχρι τη στιγμή. Αυτό συμπεριλαμβάνει τα περιεχόμενα των email servers, τα SMS και MMS μηνύματα, το περιεχόμενο φωνητικών ταχυδρομείων (voicemail), τα δεδομένα επικοινωνιών (συμπεριλαμβανομένων κινητών και σταθερών τηλεφώνων καθώς και VoIP) και άλλα. Μετά το γεγονός αυτό, ο υπουργός Εσωτερικών του Ηνωμένου Βασιλείου θα προτείνει μία ανανεωμένη πολιτική διατήρησης τηλεπικοινωνιακών δεδομένων στο συμβούλιο της Ευρώπης. Θα πρέπει να σημειωθεί εδώ ότι μετά τους βομβαρδισμούς στη
Μαδρίτη το 2004 μία παρόμοια πολιτική προτάθηκε, αλλά αντιμετώπισε σημαντικές αντιδράσεις στην Ευρωπαϊκή Επιτροπή και το Ευρωπαϊκό Κοινοβούλιο.

Το Ηνωμένο Βασίλειο συνέχισε την πίεση προς την Ευρωπαϊκή Επιτροπή με στόχο την ανανέωση της πολιτικής συνέχισε την πίεση προς την Ευρωπαϊκή Επιτροπή με στόχο την ανανέωση της πολιτικής διατήρησης τηλεπικοινωνιακών δεδομένων. Αυτό είχε ως αποτέλεσμα η επιτροπή να περιγράψει διάφορα μέτρα προστασίας για οποιαδήποτε πολιτική διατήρησης δεδομένων. Πιο συγκεκριμένα, πρότεινε να υπάρχει ένα κοινό κάτω όριο της περιόδου διατήρησης δεδομένων για όλα τα κράτη μέλη, καθώς και ένα μέγιστο σύνολο δεδομένων που μπορούν να διατηρηθούν (και όχι ελάχιστο όπως ορίζεται στην Οδηγία). Παράλληλα, ο σκοπός διατήρησης δεδομένων θα πρέπει να περιοριστεί στην αντιμετώπιση της τρομοκρατίας και όχι στο σοβαρό εγκλημα που ορίζεται ως τέλος χώρα, ενώ οι τύποι των δεδομένων που συλλέγονται θα πρέπει να είναι εξετασμένοι και εγκριθεί από το Ευρωπαϊκό Κοινοβούλιο. Τέλος, η πρόσβαση στα δεδομένα θα πρέπει να γίνεται μετά από δικαστική έγκριση και να περιορίζεται μόνο σε εκείνο που είναι απαραίτητο στην πλαίσιο της εκάστοτε έρευνας. Τα δεδομένα θα διατηρούνται έξω από τις λειτουργίες των φορέων παροχής υπηρεσιών με αυστηρά μέτρα ασφάλειας (όπως παραδείγματος χάριν κρυπτογράφηση), ενώ οι δηλώσεις για τον τρόπο με τον οποίο θα χρησιμοποιούνθον θα πρέπει να είναι σαφείς. Τα μέτρα αυτά καλούνται να εφαρμοστούν μόνο για την κατάπολεμηση σοβαρών εγκλημάτων και όχι στο σοβαρό έγκλημα όπως το ερμηνεύει κάθε χώρα, ενώ οι τύποι των δεδομένων που συλλέγονται θα πρέπει να είναι εξετασμένοι και εγκριθεί από το Ευρωπαϊκό Κοινοβούλιο. Τέλος, στις 15/12/2005 το Ευρωπαϊκό Κοινοβούλιο ψήφισε την έκδοση μίας νέας Οδηγίας για να επιτρέψει τη διατήρηση των δεδομένων που παρήχθησαν από την τηλεφωνία, τα SMS και το διαδίκτυο, χωρίς το περιεχόμενο των πληροφοριών επικοινωνίας. Η Οδηγία αυτή είναι ιδιαίτερα αμφισβητούμενη λόγω του αντίκτυπου που θα έχει στην προστασία των πολιτών της Ευρωπαϊκής Ένωσης, καθώς και της ευχέρειας που αφήνει στα κράτη μέλη της. Για παράδειγμα, στα δεδομένα η πρόσβαση πρέπει να γίνει για σκοπούς καταπολέμησης σοβαρών εγκλημάτων και τρομοκρατίας, όμως
δεν υπάρχει ορισμός στην Οδηγία για τις έννοιες αυτές, με αποτέλεσμα να μπορούν τα κράτη μέλη να θέσουν ορισμούς πέρα από τους σκοπούς για τους οποίους προορίζεται η Οδηγία. Επιπλέον, το χρονικό διάστημα διατήρησης δεδομένων αφίνεται σχετικά απροσδιόριστο, ελάχιστο 6 μήνες και μέγιστο ένα χρόνο, με αποτέλεσμα κάποια κράτη μέλη να μπορούν να επεκτείνουν αυτά τα χρονικά πλαίσια. Ηδη κάποιες χώρες της Ευρώπης έχουν δείξει τέτοιες προθέσεις. Το Ηνωμένο Βασίλειο είναι ο βασικός υποκινητής των μέτρων αυτών, κυρίως μετά τους βομβαρδισμούς της 7ης Ιουλίου 2005. Η Οδηγία είναι πιθανό να ολοκληρωθεί μέσα σε 18 μήνες, ενώ μερικά κράτη μπορούν να κάνουν επεκτάσεις και για να επιτρέψουν την αποτελεσματική διατήρηση των δεδομένων διαδικτύου. Αναμένονται, όμως, αντιδράσεις από κάποια κράτη μέλη. Ήδη η Ιρλανδία έχει δηλώσει την πρόθεσή της να αναφέρει την Οδηγία στο Ευρωπαϊκό Δικαστήριο, ενώ μερικοί ευρωβουλευτές πιστεύουν ότι η Οδηγία στερείται από μερικά επαρκή μέτρα προστασίας.

2.2.3 Διεθνής Νομοθεσία

Δεδομένου ότι μέσω του διαδικτύου γίνεται καθημερινή ανταλλαγή πληροφοριών (και ειδικά προσωπικών δεδομένων) σε όλο τον κόσμο, πολλές χώρες στρέφονται σε νομοθετικές προσπάθειες για την προστασία της προσωπικής μυστικότητας. Παραδείγματος χάριν, οι κυβερνήσεις της Ασίας, της Αυστραλίας και της Νέας Ζηλανδίας, της Ιαπωνίας, του Χονγκ Κονγκ, της Αμερικής και της Νότιας Αφρικής έχουν περάσει νομοθεσία για να προστατεύσουν τα προσωπικά δεδομένα και τη μυστικότητα. Στις ακόλουθες παραγράφους θα εξετάσουμε τις νομοθετικές προσεγγίσεις των μη Ευρωπαϊκών χωρών για την προστασία των δεδομένων, καθώς και την
πιο σημαντική προσπάθεια ανάπτυξης ισοδύναμου νομοθετικού πλαισίου στις χώρες του APEC. Τέλος, θα εξετάσουμε τις διεθνείς νομοθετικές προσεγγίσεις για την προστασία ιδιωτικότητας δεδομένων στον τομέα των τηλεπικοινωνιών.

2.2.3.1 Νομοθεσία για την Προστασία Δεδομένων

Οι κυβερνήσεις της Ασίας έχουν θεσπίσει νομοθεσία για το σεβασμό των ανθρωπίνων δικαιωμάτων και ελευθεριών, καθώς επίσης και για την ιδιωτικότητα των προσωπικών δεδομένων του ατόμου. Στην Αυστραλία, η ιδιωτικότητα των δεδομένων προστατεύεται από το νόμο του 1998 που αναφέρεται στο δίκαιο χειρισμού των προσωπικών πληροφοριών των ατόμων [1]. Αυτός ο νόμος παρέχει προστασία για τα προσωπικά δεδομένα που συλλέγονται είτε από δημόσιους είτε από ιδιωτικούς φορείς [20, 21]. Επίσης, η Νέα Ζηλανδία έχει θεσπίσει νομοθεσία για την προστασία των πολιτών της, παρόμοια με τη νομοθεσία της Αυστραλίας.

Το 2005, η Ιαπωνία θέσπισε πέντε νέους νόμους για την προστασία των δεδομένων. Συγκεκριμένα, οι νόμοι αυτοί αφορούν την προστασία της ιδιωτικότητας των προσωπικών δεδομένων τα οποία χρησιμοποιούνται όχι μόνο στο δημόσιο αλλά και στον ιδιωτικό τομέα και καθορίζουν τον τρόπο με τον οποίο οι δημόσιοι ή οι ιδιωτικοί φορείς συλλέγουν, διατηρούν και επεξεργάζονται τις προσωπικές πληροφορίες [17, 117]. Αυτοί οι νόμοι περιλαμβάνουν την προστασία των δεδομένων για τους ιατρικούς και οικονομικούς τομείς, καθώς επίσης και για τους τομείς των τηλεπικοινωνιών.
Το 1996 το Χονγκ Κονγκ πέρασε το διάταγμα περί προστασίας προσωπικών δεδομένων, το οποίο έχει επηρεαστεί από την Οδηγία της Ευρωπαϊκής Ένωσης [36]. Το Χονγκ Κονγκ προστατεύει την ιδιωτικότητα των πολιτών του αποτρέποντας οποιονδήποτε συσχετισμό των δεδομένων άμεσα ή έμμεσα με κάποιο πρόσωπο και ισχύει για οποιονδήποτε χρήστη ο οποίος συλλέγει, διατηρεί, ή επεξεργάζεται τα προσωπικά δεδομένα [41, 43]. Οι ιδιοκτήτες των δεδομένων έχουν το δικαίωμα να επιβεβαιώνουν το που φυλάσσονται τα δεδομένα τους.

Θα πρέπει επίσης να αναφερθεί ότι από τις χώρες που μελετάμε, η Κίνα δεν έχει ιστορία στην προστασία των δικαιωμάτων ιδιωτικότητας των πολιτών της και παρέχει ακόμα λιγότερη προστασία μυστικότητας των δεδομένων. Όσον αφορά στους κανονισμούς που αφορούν την ασφάλεια διαδικτύου, η Κίνα παρέχει την πιο περιορισμένη προστασία των δικαιωμάτων.

Η Αμερική αποτελεί μία από τις χώρες οι οποίες έχουν θεσπίσει νόμους ανά τομέα. Δηλαδή, η νομοθεσία της δεν αποτελείται από έναν νόμο για την προστασία των προσωπικών δεδομένων γενικά, αλλά από ξεχωριστούς νόμους για κάθε είδους δεδομένων. Ετσι, για παράδειγμα, έχει ξεχωριστό νόμο για την προστασία των ιατρικών δεδομένων [113], ή των οικονομικών δεδομένων [114]. Επιπρόσθετα, ένα πολύ σημαντικό μειονέκτημα της Αμερικάνικης νομοθεσίας σε σχέση με την Ευρωπαϊκή είναι η έλλειψη νόμου προστασίας μυστικότητας για τον ιδιωτικό τομέα. Σε αυτό το σημείο, είναι σημαντικό να αναφερθεί ότι εκτός της Ευρώπης, στην Αυστραλία, την Ιαπωνία και το Χονγκ Κονγκ, η νομοθεσία για την ιδιωτικότητα δεδομένων είναι πιο αυστηρή σε σχέση με τη νομοθεσία των ΗΠΑ [70].

Τέλος, στη Νότια Αφρική, η μυστικότητα αντιμετωπίζεται ως θεμελιώδες ανθρώπινο δικαίωμα και ως εκ τούτου έχει θεσπιστεί νομοθεσία για την προστασία δεδομένων τόσο για το δημόσιο όσο και για τον ιδιωτικό τομέα. Οι νόμοι αυτοί αναγνωρίζουν τα δικαιώματα των πολιτών και προστατεύουν την ιδιωτικότητα του ατόμου σε πολλούς τομείς της καθημερινής ζωής, όπως οι ιατρικοί τομείς, οι τραπεζικές συναλλαγές, το μάρκετινγκ και άλλα [31, 99]. Σε αυτό το σημείο, είναι σημαντικό να
αναφερθεί ένα προσωπικό παράδειγμα που περιγράφει ένας Νοτιοαφρικανός, ο Martin Olivier [82]. Ο Olivier περιγράφει την προσωπική του εμπειρία όταν αποφάσισε να ταξιδέψει με τη σύζυγό του στην Ολλανδία. Όταν προσπάθησαν να ολοκληρώσουν τις διαδικασίες του ταξιδιού τους, η πρεσβεία τους ενημέρωσε ότι οι διαδικασίες θα έπαιρναν πολύ περισσότερο από τον απαιτούμενο χρόνο, επειδή η σύζυγός του είναι γιατρός και υπήρχαν φόβοι ότι θα ασκούσε το επάγγελμα της σε άλλη χώρα. Κατά συνέπεια, ακύρωσαν το ταξίδι τους. Με το παράδειγμά του, ο Olivier εξηγεί ότι τα προσωπικά δεδομένα κάθε προσώπου μπορούν να χρησιμοποιηθούν με έναν παράνομο τρόπο. Εκτός αυτού, δίνει εμφάση στην ανεπάρκεια διαχωρισμού των δεδομένων, για παράδειγμα σε προσωπικά ή ευαίσθητα δεδομένα. Τέλος, υπογραμμίζει ότι δεν δόθηκε καμία αναφορά στη σύζυγό του για το ότι τα προσωπικά της δεδομένα μπορούν να χρησιμοποιηθούν σε άλλες χώρες με αθέμιτο τρόπο χωρίς συγκατάθεσή της.

2.2.3.2 Προστασία APEC

Το 2003 τα κράτη του APEC (Asia-Pacific Economic Coorporation), από τον Καναδά μέχρι την Κίνα και από την Αυστραλία ως τη Νέα Ζηλανδία, άρχισαν επίσημες διαβουλεύσεις για την ανάπτυξη ενός κοινού προτύπου προστασίας της ιδιωτικότητας μαζί με τα πρωτόκολλα για το χειρισμό ζητημάτων περιορισμού εξαγωγής δεδομένων. Είναι ίσως η σημαντικότερη διεθνής ανάπτυξη για την προστασία της ιδιωτικότητας μετά την Οδηγία προστασίας δεδομένων της Ευρωπαϊκής Ένωσης [12]. Ο βασικός στόχος είναι να προωθηθεί η ανάπτυξη αποτελεσματικών καθεστώτων ιδιωτικότητας στα κράτη του APEC που μέχρι τώρα έχουν πολύ ελαστική νομοθεσία και αδυναμία στην επιβολή της νομοθεσίας αυτής.
Η Αυστραλία πρότεινε την ανάπτυξη των αρχών ιδιωτικότητας χρησιμοποιώντας τις εδώ και 20 ετών Οδηγίες για την προστασία της ιδιωτικότητας και της διασυνοριακής ροής των προσωπικών δεδομένων του 1980. Στα μέσα του 2003 δημιουργήθηκε μία περιφερειακή ομάδα ειδικών με στόχο την ανάπτυξη ανεξάρτητα πρότυπα για την προστασία ιδιωτικότητας σε κάθε περιοχή με σκοπό να επηρεάσουν τη θέσπιση νόμων ιδιωτικότητας σύμφωνα με αυτά τα πρότυπα [12, 22].

Θα πρέπει να σημειωθεί ότι η πρωτοβουλία αυτή είναι πολύ σημαντική διότι ενθαρρύνει την ανάπτυξη ισχυρότερων νόμων για την ιδιωτικότητα των δεδομένων στις χώρες του APEC. Όπως συμβαίνει και στην Ευρώπη, έτσι και σε αυτές τις χώρες, θα μπορεί να υπάρξει ισορροπία και εναρμόνιση της προστασίας μυστικότητας των δεδομένων και της διασυνοριακής ροής τους.

2.2.3.3 Νομοθεσία για την Προστασία Δεδομένων στον Τομέα των Τηλεπικοινωνιών

Οι διεθνείς χώρες έχουν εργαστεί συστηματικά τα τελευταία χρόνια για την εκδόσεις νόμων ιδιωτικότητας των τηλεπικοινωνιακών δεδομένων και, ιδιαίτερα των δεδομένων θέσης. Οι πληροφορίες θέσης χαρακτηρίζονται ως είδος ιδιόκτητων πληροφοριών των πελατών (Customer Proprietary Network Information - CPNI) στην παράγραφο 222 του νόμου του 1934 της Αμερικής που αφορά τις επικοινωνίες. Μία τέτοιοι είδους πληροφορία αποτελεί προσωπικό δεδομένο και πρέπει να κρατηθεί εμπιστευτική και να μη χρησιμοποιηθεί ή να αποκαλυφθεί χωρίς προηγούμενως ο πελάτης να έχει δώσει την έγκρισή του [28]. Οι ακόλουθες τέσσερις βασικές αρχές
πληροφοριών συντάσσονται στον οργανισμό οικονομικής συνεργασίας και ανάπτυξης (Organization of Economic Co-operation and Development - OECD) [69], προκειμένου να διατηρηθεί η ιδιωτικότητα των πληροφοριών θέσης:

- Οι πληροφορίες θέσης ενός χρήστη πρέπει να συλλέγονται μόνο όταν είναι απαραίτητες για την παροχή μίας υπηρεσίας.
- Οι φορείς παροχής υπηρεσιών θέσης θα πρέπει να επιδιώξουν συμφωνία με το χρήστη προτού συλλέξουν τα δεδομένα θέσης του. Επιπλέον, ο κάθε χρήστης μπορεί να αποσύρει οποιαδήποτε στιγμή τη συγκατάθεσή του.
- Η χρήση και η κοινοποίηση των δεδομένων πρέπει να περιοριστούν σύμφωνα με τη συγκατάθεση που έχει δώσει ο χρήστης. Εάν οι φορείς παροχής υπηρεσιών θέσης δεν είναι απαραίτητο να γνωρίζουν την αληθινή ταυτότητα του χρήστη, τότε πρέπει να χρησιμοποιηθούν ψευδώνυμα.
- Όταν η απαιτούμενη υπηρεσία ολοκληρώνεται, τα δεδομένα θέσης πρέπει είτε να σβηστούν είτε να καταστούν ανώνυμα, δηλαδή να είναι αδύνατο από αυτά τα δεδομένα να προσδιοριστεί το πρόσωπο στο οποίο ανήκουν.

Αυτές οι αρχές είναι ίδιες με τις αντίστοιχες Ευρωπαϊκές που περιγράφαμε νωρίτερα και χρησιμούν ως βασικές οδηγίες για τους οργανισμούς και τις χώρες για τον χειρισμό των δεδομένων θέσης. Αξίζει να σημειωθεί ότι οι αρχές αυτές μπορεί να μην ισχύουν σε ειδικές περιπτώσεις, όπως οι κλήσεις έκτακτης ανάγκης.

Άλλες χώρες, όπως ο Καναδάς, η Αυστραλία, η Νέα Ζηλανδία, η Λατινική Αμερική και η Ιαπωνία έχουν εργαστεί σημαντικά στη θέσπιση νόμων περί ιδιωτικότητας των δεδομένων επικοινωνιών και θέσης [15].
2.3 Διασυνοριακή Ροή Δεδομένων Προσωπικού Χαρακτήρα

Ένας πολύ σημαντικός παράγοντας στην ιδιωτικότητα δεδομένων είναι η γνώση του ποιος θα επεξεργαστεί τα δεδομένα. Μέχρι πριν λίγα χρόνια κάθε χώρα είχε τη δυνατότητα να έχει τη δική της νομοθεσία για την προστασία των ανθρώπινων δικαιωμάτων. Πλέον, με την εκρηκτική αύξηση της χρήσης των υπολογιστών και του διαδικτύου τα προβλήματα της προστασίας των δεδομένων δεν περιορίζονται μόνο σε μία περιοχή ή μόνο σε ένα κράτος. Στις ημέρες μας, στόχος είναι να εξασφαλιστεί ο διεθνής σεβασμός των δικαιωμάτων κάθε ανθρώπου. Η δυνατότητα όλοι οι υπολογιστές σε όλο τον κόσμο να συνδέονται μεταξύ τους μέσω του διαδικτύου αυξάνει αυτήν την ανησυχία, αφού συχνά οι χώρες που λαμβάνουν τα προσωπικά δεδομένα μπορεί να μην έχουν την ιδιαίτερα, ή και καθόλου, νομοθεσία για την προστασία των ανθρώπινων δικαιωμάτων. Για το λόγο αυτό, απαιτείται μεγάλη ειδικευμένη υποστήριξη και επιθετική συντηρητική προσέγγιση. Κατά τη διασυνοριακή ροή δεδομένων πέρα από τη χώρα στην οποία έχουν συλλεχθεί, η δυνατότητα ελέγχου της επεξεργασίας τους είναι μεγάλη.

Για τους παραπάνω λόγους, στην Ελλάδα η αρμόδια Αρχή που εξετάζει και αποφαίνεται για την πραγματοποίηση ή όχι της διασυνοριακής ροής δεδομένων είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (παράγραφος 3.1.4). Η Αρχή έχει επιθετική ρόλο στη μεταφορά των δεδομένων σε κάποια άλλη χώρα εφόσον κρίνει ότι η χώρα αυτή, στην οποία θα πραγματοποιηθεί η επεξεργασία των δεδομένων, εξασφαλίζει...
ικανοποιητικό επίπεδο προστασίας τους. Ο έλεγχος γίνεται λαμβάνοντας υπόψη τη φύση των δεδομένων, καθώς και τους σκοπούς και τη διάρκεια επεξεργασίας τους. Το ιδίο, φυσικά, ισχύει και για όλες τις Ευρωπαϊκές χώρες. Στο νόμο περί προστασίας δεδομένων της Ευρωπαϊκής Ένωσης, και συγκεκριμένα στα άρθρα 25-26 [26], αναλύεται το ιδιαίτερα σημαντικό ζήτημα της διασυνοριακής ροής προσωπικών δεδομένων προς τρίτα κράτη εκτός της ΕΕ. Η ροή δεδομένων σε χώρες εντός της ΕΕ δεν απαιτεί ιδιαίτερη νομοθεσία αφού όλες οι χώρες-μέλη ακολουθούν το νομοθετικό πλαίσιο που προτείνει η ΕΕ. Για το λόγο αυτό τα δεδομένα μπορούν να μεταφέρονται ελεύθερα από το ένα κράτος-μέλος στο άλλο. Στις υπόλοιπες χώρες, όμως, η νομοθεσία για την ιδιωτικότητα δεδομένων μπορεί να είναι κατώτερη ή ακόμη και ανεπαρκής. Για το λόγο αυτό, η Οδηγία απαιτεί να μη διαβιβάζονται τα δεδομένα σε χώρες οι οποίες δεν εξασφαλίζουν την επαρκή προστασία τους. Τα κράτη μέλη οφείλουν να ελέγξουν και να μην επιτρέψουν τη ροή των προσωπικών πληροφοριών σε τρίτα κράτη που δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας, λαμβάνοντας υπόψη όλες τις σχετικές περιστάσεις και τους όρους της επεξεργασίας τους στο άλλο κράτος.

Επί παραδείγματι, μερικά κράτη, όπως οι ΗΠΑ, δεν έχουν επεκτείνει τη νομοθεσία τους για την προστασία δεδομένων στον ιδιωτικό τομέα, με αποτέλεσμα η ΕΕ να απαγορεύει σε πολλές περιπτώσεις τη διαβίβαση δεδομένων στις ΗΠΑ. Πριν την ηλεκτρονική εποχή, οι διαφορές στις πολιτικές μυστικότητας των δεδομένων μεταξύ της Ευρώπης και των ΗΠΑ ήταν ελάχιστες. Στη σημερινή εποχή, όπου το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές υπηρεσίες αποτελούν κομμάτι της καθημερινής μας ζωής, η διαφορά στις πολιτικές αυτές είναι πολύ μεγάλη. Παρόλο που σήμερα η Ευρώπη βρίσκεται πολύ πιο πίσω στη χρήση υπολογιστών και διαδικτύου σε σχέση με τις ΗΠΑ, οι νόμοι της περί προστασίας μυστικότητας των δεδομένων είναι οι πιο περιεκτικοί σε όλο τον κόσμο. Για το λόγο αυτό η ΕΕ παροτρύνει τους αγοραστές μέσω διαδικτύου να αποφεύγουν τις ηλεκτρονικές αγορές από αμερικάνικες επιχειρήσεις λόγω των ανησυχιών που αφορούν την ιδιωτικότητά τους [26, 90].
Επιπλέον, η ΕΕ έχει το δικαίωμα να ελέγξει και να αποφανθεί για το εάν τα τρίτα κράτη εξασφαλίζουν το απαραίτητο επίπεδο προστασίας της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και δικαιωμάτων του ατόμου. Η διασυνοριακή ροή δεδομένων προς τρίτες χώρες, οι οποίες μπορεί να μην παρέχουν το απαραίτητο επίπεδο προστασίας τους, επιτρέπεται μόνο στις περιπτώσεις όπου ο ιδιοκτήτης των δεδομένων δώσει τη συγκατάθεσή του ή σε περιπτώσεις έκτακτης ανάγκης, όπως η διασφάλιση εθνικής προστασίας ή η ανίχνευση τρομοκρατικών και εγκληματικών επιθέσεων. Επιπλέον, υπάρχει η δυνατότητα διασυνοριακής ροής δεδομένων προς χώρες με ανεπαρκές επίπεδο προστασίας, από τη στιγμή που η αρμόδια Αρχή παρέχει ικανοποιητική εγγύηση για την προστασία της ιδιωτικής ζωής και των δικαιωμάτων του ατόμου.

Τέλος, και οι μη Ευρωπαϊκές χώρες περιλαμβάνουν στη νομοθεσία τους νόμους για τη διασυνοριακή ροή δεδομένων σε άλλες χώρες. Το πιο σημαντικό παράδειγμα αποτελούν οι χώρες του APEC για τις οποίες υπάρχουν νόμοι οι οποίοι συγκεκριμενοποιούν το πότε επιτρέπεται και πότε απαγορεύεται η μεταφορά προσωπικών δεδομένων σε άλλες χώρες.

2.4 Επίλογος

Κατά τη διάρκεια των τελευταίων 40 περίπου ετών, η αυξανόμενη συλλογή προσωπικών δεδομένων των ατόμων από το δημόσιο και ιδιωτικό τομέα έχει αντιμετωπισθεί με ιδιαίτερο φόβο και έχει επηρεάσει σημαντικά τη νομική σκέψη. Με την ολοένα και αυξανόμενη χρήση του διαδικτύου από τους πολίτες όλου του κόσμου, τα προσωπικά δεδομένα του κάθε ανθρώπου μπορούν να ταξιδέψουν παντού. Παράλληλα, η ιδιωτικότητα αποτελεί ένα μείζον θέμα και στον τομέα των τηλεπικοινωνιών. Τα τελευταία χρόνια,
όπου οι περισσότερες δραστηριότητες των ατόμων πραγματοποιούνται χρησιμοποιώντας φορητές συσκευές, είναι δυνατή η συλλογή όλο και περισσότερων προσωπικών τηλεπικοινωνιακών δεδομένων από τις συσκευές αυτές. Τα κινούμενα αντικείμενα παράγουν ευαίσθητη δεδομένα τα οποία φανερώνουν σε ποιο σημείο βρίσκεται ο χρήστης σε συγκεκριμένες χρονικές στιγμές, με αποτέλεσμα να δημιουργούν μία πλήρη εικόνα των κινήσεών του. Παρόλο που τα δεδομένα αυτά έχουν τεράστιες απαιτήσεις σε χρόνο για τη συλλογή τους, η πρόοδος της τεχνολογίας επιτρέπει τη συνεχή αποθήκευση τέτοιων πληροφοριών.

Η νομοθεσία παρέχει αναμφισβήτητα ένα ισχυρό μέσο για την προστασία ιδιωτικότητας. Εντούτοις, κάθε χώρα καθορίζει τους δικούς της νόμους για την ιδιωτικότητα των δεδομένων με αποτέλεσμα να μην υπάρχει κοινή νομοθεσία για την προστασία των θεμελιωδών δικαιωμάτων των ανθρώπων. Αυτός είναι ο λόγος για τον οποίο τα περισσότερα κράτη οδηγήθηκαν στη θέσπιση νόμων για τον περιορισμό της διασυνοριακής ροής δεδομένων [15]. Σε αυτό το κεφάλαιο εξετάσαμε τα βασικά μοντέλα προστασίας δεδομένων και εστιάσαμε στο σημαντικότερο μοντέλο, τους νόμους. Αναλύσαμε τη νομοθεσία των Ευρωπαϊκών και μη Ευρωπαϊκών χωρών, αφενός για την προστασία των δεδομένων γενικά και, αφετέρου, για την προστασία των τηλεπικοινωνιακών δεδομένων, η οποία ιδιαίτερα μετά τις τρομοκρατικές ενέργειες στην Ευρώπη και την Αμερική έχει γίνει πολύ πιο αυστηρή. Τέλος, εξετάσαμε ξεχωριστά τη νομοθεσία για τη διασυνοριακή μεταφορά των δεδομένων σε άλλες χώρες.
Κεφάλαιο 3

Εποπτικοί Φορείς Ασφάλειας σε Ελλάδα και Ευρώπη

Ο έλεγχος και η εποπτεία της εφαρμογής του νομοθετικού και ρυθμιστικού πλαισίου ασφάλειας της κάθε χώρας απαιτεί την ύπαρξη διάφορων εποπτικών αρχών και φορέων, οι οποίοι συνεργάζονται συνήθως μεταξύ τους προκειμένου να προστατεύσουν την εθνική ασφάλεια. Στο κεφάλαιο αυτό θα εξετάσουμε τους εθνικούς, Ευρωπαϊκούς και διεθνείς εποπτικούς φορείς ασφάλειας. Ειδικότερα, στην παράγραφο 3.1 θα αναλύσουμε τους Ελληνικούς φορείς και στην παράγραφο 3.2 θα εξετάσουμε τους βασικότερους Ευρωπαϊκούς και διεθνείς εποπτικούς φορείς, εστιάζοντας στις αρμοδιότητές τους στον τομέα των επικοινωνιών.
3.1 Ελληνικοί Εποπτικοί Φορείς Ασφάλειας

Στην Ελλάδα οι βασικότεροι φορείς εποπτείας της ρύθμισης του εθνικού νομοθετικού πλαισίου είναι οκτώ. Σε αυτή την παράγραφο θα εξετάσουμε τις αρμοδιότητες των φορέων αυτών και τον τρόπο με τον οποίο ελέγχουν την εφαρμογή των εθνικών νόμων. Ιδιαίτερη έμφαση θα δώσουμε στον έλεγχο τήρησης των νόμων 2472/1997 και 2774/1999 τους οποίους παρουσιάσαμε στην παράγραφο 2.2.1. Πιο συγκεκριμένα, στις παραγράφους 3.1.1, 3.1.2 και 3.1.3 θα αναλύσουμε τις βασικότερες αρμοδιότητες του Γενικού Επιτελείου Εθνικής Άμυνας [11], της Εθνικής Υπηρεσίας Πληροφοριών [35] και της Διεύθυνσης Εγκληματολογικών Ερευνών [24], αντίστοιχα. Στις δύο επόμενες παραγράφους, 3.1.4 και 3.1.5, θα ερευνήσουμε τις δύο βασικότερες δημόσιες αρχές που είναι αρμόδιες για τον έλεγχο εφαρμογής των νόμων που περιγράψαμε στο προηγούμενο κεφάλαιο. Οι αρχές αυτές είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [3] και η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών [2]. Στη συνέχεια, στις παραγράφους 3.1.6, 3.1.7 και 3.1.8 θα αναλύσουμε άλλους φορείς προστασίας της ασφάλειας των επικοινωνιών: την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων [29], τον Φορέα Πρόληψης Τηλεπικοινωνιακής Απάτης [37] και την Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας [47], αντίστοιχα.
3.1.1 Γενικό Επιτελείο Εθνικής Άμυνας


Στον τομέα των επικοινωνιών, το ΓΕΕΘΑ είναι επιφορτισμένο με την έκδοση του νέου Εθνικού Κανονισμού Ασφαλείας Επικοινωνιών ο οποίος εχει ως στόχο την εφαρμογή του σε όλους τους δημόσιους φορείς, όπως τα υπουργεία, οι νομαρχίες και λοιπά. Για τη διαμόρφωση του κανονισμού αυτού έχουν ληφθεί υπόψη οι αντίστοιχοι κανονισμοί του NATO, ενώ την πιστοποίησή του έχει επιφορτιστεί η Εθνική Υπηρεσία Πληροφοριών (το ρόλο και τις αρμοδιότητες της οποίας θα παρουσιάσουμε στην επόμενη παράγραφο) με βάση το διεθνές πρότυπο ISO 15408.
3.1.2 Εθνική Υπηρεσία Πληροφοριών

Η Εθνική Υπηρεσία Πληροφοριών – ΕΥΠ [35] λειτουργεί εποπτικά σε εθνικό επίπεδο και ως εκ τούτου οι πολίτες δεν μπορούν να έρθουν άμεσα σε επαφή με αυτή. Αποτελεί αυτοτελή πολιτική δημόσια υπηρεσία με έργο τη συλλογή, επεξεργασία και διανομή πληροφοριών που αφορούν στην ασφάλεια της χώρας, ενώ συνεργάζεται με δημόσιους εθνικούς και Ευρωπαϊκούς φορείς, καθώς και με φορείς του NATO για θέματα ασφάλειας των επικοινωνιών. Το καθεστώς λειτουργίας της ΕΥΠ ρυθμίζεται από προεδρικά διατάγματα που εκδίδονται με εφαρμογή του ιδρυτικού της νόμου (Νόμος 1645/86 [35]). Στο άρθρο 2 του νόμου αυτού ορίζονται οι αρμοδιότητες της υπηρεσίας, οι βασικότερες από τις οποίες είναι:

- Η συλλογή, επεξεργασία και διανομή στις αρμόδιες αρχές των πληροφοριών που αφορούν στην εθνική ασφάλεια της χώρας.
- Η αντιμετώπιση της κατασκοπευτικής σε βάρος της χώρας δραστηριότητας ξένων οργάνων πληροφοριών.
- Ο συντονισμός των δραστηριοτήτων όλων των υπηρεσιών πληροφοριών και ασφάλειας του κράτους σχετικά με τη συλλογή και τη διάθεση των πληροφοριών που έχουν σχέση με τα αντικείμενα αρμοδιότητάς της.

Σύμφωνα με το Προεδρικό Διάταγμα 360/92 η Πέμπτη Διεύθυνση της ΕΥΠ είναι αρμόδια για την ασφάλεια των Εθνικών Επικοινωνιών [83]. Για το λόγο αυτό οι αρμοδιότητες της διευρύνονται με τη σύνταξη εθνικών κανονισμών και την υποστήριξή των δημόσιων φορέων στη διεξαγωγή τεχνικών ελέγχων για την ασφάλεια των επικοινωνιών. Επιπλέον, είναι
εξουσιοδοτημένη να αξιολογεί από πλευράς ασφάλειας τα κρυπτογραφικά συστήματα τα οποία προμηθεύονται οι δημόσιες υπηρεσίες.

Η Απόφαση 2001/264 του Ευρωπαϊκού Κοινοβουλίου προβλέπει τη δημιουργία μίας Εθνικής Αρχής Ασφάλειας Επικοινωνιών και Πληροφορικής (INFOSEC). Με βάση το Προεδρικό Διάταγμα 325/2003 στην Ελλάδα η ΕΥΠ είναι η αρμόδια υπηρεσία και, παράλληλα, είναι εξουσιοδοτημένη για την εκπροσώπηση της Ελλάδος στην Ευρωπαϊκή Ένωση για θέματα ασφαλείας των επικοινωνιών. Η υπηρεσία αυτή σε συνεργασία με τις αντίστοιχες αρχές της Ευρωπαϊκής Ένωσης διαδραματίζει σημαντικό ρόλο στη δημιουργία και ενεργοποίηση ελληνικών προγραμμάτων ασφαλείας και επικοινωνιών, οι οποίοι εξυπηρετούν την ανάγκη και την ανάγκη της Ελλάδας και της Ευρωπαϊκής Ένωσης. Η ΕΥΠ είναι εξουσιοδοτημένη να αξιολογεί από πλευράς ασφάλειας τα κρυπτογραφικά συστήματα τα οποία προμηθεύονται οι δημόσιες υπηρεσίες.

Η Απόφαση 2001/264 του Ευρωπαϊκού Κοινοβουλίου προβλέπει τη δημιουργία μίας Εθνικής Αρχής Ασφάλειας Επικοινωνιών και Πληροφορικής (INFOSEC). Με βάση το Προεδρικό Διάταγμα 325/2003 στην Ελλάδα η ΕΥΠ είναι η αρμόδια υπηρεσία και, παράλληλα, είναι εξουσιοδοτημένη για την εκπροσώπηση της Ελλάδος στην Ευρωπαϊκή Ένωση για θέματα ασφαλείας των επικοινωνιών. Η υπηρεσία αυτή σε συνεργασία με τις αντίστοιχες αρχές της Ευρωπαϊκής Ένωσης πιστοποιεί την ασφάλεια των συστημάτων της ΕΕ. Επιπλέον, η υπηρεσία αυτή εκπροσωπεί την Ελλάδα στον διεθνή οργανισμό Αναγνώρισης Κοινών Κριτηρίων Πιστοποιητικών (Common Criteria Recognition Arrangement – CCRA) για την αμοιβαία εφαρμογή και αναγνώριση των πιστοποιητικών για τα συστήματα ασφάλειας τεχνολογιών πληροφορικής. Όπως αναφέραμε και παραπάνω, τα πιστοποιητικά αυτά χορηγούνται με βάση τα κριτήρια και τη μεθοδολογία του διεθνούς προτύπου ISO 15408. Η αξιολόγηση αφορά διάφορα συστήματα, όπως βάσεις δεδομένων, τοίχοι προστασίας, εξυπνες κάρτες και άλλα, τα οποία ανάλογα με το βαθμό ασφαλείας που παρέχουν κατατάσσονται σε επίπεδα [83].

Θα πρέπει να σημειωθεί εδώ ότι η ΕΥΠ ελέγχεται από την Ειδική Επιτροπή Προστασίας του Απορρήτου των Επικοινωνιών καθώς και από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όπως θα περιγραφούν στις επόμενες παραγράφους.
3.1.3 Διεύθυνση Εγκληματολογικών Ερευνών της Ελληνικής Αστυνομίας

Η Διεύθυνση Εγκληματολογικών Ερευνών (ΔΕΕ) [24] της Ελληνικής Αστυνομίας (ΕΛΑΣ) αποτελεί την εθνική εγκληματολογική υπηρεσία της χώρας. Έχει ενταχθεί στο Δίκτυο Ευρωπαϊκών Ινστιτούτων Δικανικών Επιστημών (European Network of Forensic Science Institutes - ENFSI) και παρέχει σημαντική υποστήριξη και βοήθεια στο έργο όλων των διοικητικών Αρχών της χώρας.

Όσον αφορά τον τομέα των επικοινωνιών, έχει ιδρυθεί το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος το οποίο εξετάζει εγκληματικές πράξεις που πραγματοποιούνται μέσω διαδικτύου και τιμωρούνται από τη νομοθεσία. Οι πολίτες μπορούν να απευθύνονται στην υπηρεσία αυτή μέσω της Διεύθυνσης Ασφάλειας Αττικής η οποία μετά την προανάκριση στέλνει τα προς εξέταση πειστήρια στο Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος.

3.1.4 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) [3] αποτελεί έναν ανεξάρτητο δημόσιο φορέα υπεύθυνο για την
εποπτεία των νόμων 2472/1997 και 2774/1999. Η σημαντικότερη αρμοδιότητα της ΑΠΔΠΧ είναι η εξέταση ερωτήσεων, παραπόνων και καταγγελιών των πολιτών σχετικά με την εφαρμογή των παραπάνω νόμων, καθώς και η προστασία των αιτούντων όταν ζητείται έλεγχος της νομιμότητας κάποιων ενεργειών. Η ΑΠΔΠΧ παρέχει οδηγίες για το βαθμό ασφαλείας των δεδομένων καθώς και για τα μέτρα προστασίας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία δεδομένων εν όψει και των τεχνολογικών εξελίξεων. Οι Οδηγίες που εκδίδει έχουν ως σκοπό την ενιαία εφαρμογή των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επιπρόσθετα, η ΑΠΔΠΧ χορηγεί τις αδειες τήρησης αρχείων που περιέχουν ευαίσθητα δεδομένα στους υπεύθυνους επεξεργασίας, ενώ επίσης, χορηγεί αδειες διασύνδεσης αρχείων και διασυνοριακής ροής δεδομένων. Παράλληλα, η ΑΠΔΠΧ είναι αρμόδια για τη διενέργεια διοικητικών ελέγχων σε αρχεία προσωπικών δεδομένων και για την παροχή γνωμοδότησεων για τις ρυθμίσεις που αφορούν στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα. Τέλος, η ΑΠΔΠΧ οφείλει να ανακοινώνει στη Βουλή και στις Αρχές αρμοδιότητας και δικαστικές καταγγελίες των αιτούντων από την επεξεργασία δεδομένων προκειμένου να επιβληθούν διοικητικές κυρώσεις, ενώ συνεργάζεται και με τις Αρχές άλλων μελών της Ευρωπαϊκής Ένωσης για την άσκηση των αρμοδιοτήτων τους.


Η ΑΠΔΠΧ έχει δεχθεί προσφυγές και κατά εταιριών και σταθερής τηλεφωνίας και γενικότερα κατά φορέων τηλεπικοινωνιακών υπηρεσιών, μετά την εξέταση των οποίων έχει λάβει κατάλληλες Αποφάσεις. Παραδείγματα τέτοιων αποφάσεων αποτελούν η Απόφαση
120/2001 [67] και η Απόφαση 77/2001 [61]. Σύμφωνα με την Απόφαση 120/2001, ένας χρήστης τηλεπικοινωνιακών υπηρεσιών δεν δικαιούται να χρησιμοποιεί το όνομα κάποιου άλλου χρήστη χωρίς τη συγκατάθεσή του. Για το λόγο αυτό οι φορείς τηλεπικοινωνιακών υπηρεσιών θα πρέπει να διαπιστώνουν την ακρίβεια των δεδομένων πριν τη λήψή τους. Επιπρόσθετα, σύμφωνα με την Απόφαση 77/2001, μετά την αίτηση τηλεφωνικής σύνδεσης από εμπορικούς συνεργάτες των τηλεπικοινωνιακών εταιριών τα δεδομένα θα πρέπει να δίνονται στον υπεύθυνο επεξεργασίας, να καταστρέφονται ή να επιστρέφονται στον πελάτη. Επίσης, τα δικαιολογητικά τα οποία συνυποβάλλονται με την αίτηση στους εμπορικούς συνεργάτες δεν θα πρέπει να διατηρούνται και μετά την υπογραφή της σύμβασης χρήσης τηλεπικοινωνιακών υπηρεσιών. Σύμφωνα με την Απόφαση 50/2001 [3], ο χρήστης τηλεφωνικών υπηρεσιών δικαιούται να ζητά να μη συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό κατάλογο του OTE ο προσωπικός του αριθμός. Τέλος, σύμφωνα με την Απόφαση 49/2001 [61], ο φορέας παροχής τηλεπικοινωνιακών υπηρεσιών υφίσταται να ενημερώνει το συνδρομητή για τις δυνατότητες απορρήτου που προσφέρονται ώστε να έχει τη δυνατότητα επιλογής.

Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο σε έκτακτες περιπτώσεις, όπως είναι η εθνική ασφάλεια. Ένα παράδειγμα άρσης απορρήτου επικοινωνιών στις εταιρείες κινητής τηλεφωνίας και στις εταιρείες παροχής υπηρεσιών διαδικτύου αποτελεί η άρση κατόπιν εισαγγελικής ή δικαστικής παραγγελίας στα πλαίσια προκαταρκτικής εξέτασης ή προανάκρισης. Σε αυτές τις περιπτώσεις, σύμφωνα με τη γνωμοδότηση 1697/2000 της Αρχής [3], η Αρχή δεν θα πρέπει να ενημερώσει το άτομο στο οποίο ανήκουν τα δεδομένα και να ζητήσει την συγκατάθεσή του, εφόσον το άτομο θα γνώριζε ότι παρακολουθείται και ο σκοπός της Αρχής θα ήταν ανέφικτος.
3.1.5 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

Εκτός από την ΑΠΔΠΧ που περιγράψαμε παραπάνω, στην Ελλάδα λειτουργεί και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) [2]. Η ΑΔΑΕ είναι μία ανεξάρτητη Αρχή που είναι υπεύθυνη για τη διασφάλιση του απορρήτου των επιστολών και της ελεύθερης επικοινωνίας με οποιονδήποτε τρόπο, καθώς και των εφαρμογών στο διαδίκτυο και των χρηστών του. Παράλληλα, παρέχει ασφάλεια στους φορείς παροχής υπηρεσιών και θεσπίζει τις υποχρεώσεις τους αναφορικά με την ασφάλεια και το απόρρητο των εφαρμογών διαδικτύου.


Τέλος, η ΑΔΑΕ διενεργεί αυτεπάγγελτα ελέγχους στις επιχειρήσεις που έχουν γενικό αντικείμενο την επικοινωνία, ενώ παράλληλα είναι αρμόδια για την κατάσχεση ψηφιακών πειστηρίων και την καταστροφή δεδομένων που έχουν καταγραφεί παράνομα. Η ΑΔΑΕ γνωμοδοτεί σε συνεργασία με τα αρμόδια Υπουργεία σχετικά με τις διαδικασίες και τις τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των
3.1.6 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων – ΕΕΤΤ [29] αποτελεί μία εθνική ρυθμιστική αρχή η οποία ελέγχει, ρυθμίζει και εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών και την ταχυδρομική αγορά. Στην αγορά ηλεκτρονικών επικοινωνιών δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου, ενώ στην ταχυδρομική αγορά συμπεριλαμβάνονται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών μεταφοράς. Η ΕΕΤΤ ασκεί τις αρμοδιότητές της της Επιτροπής Ανταγωνισμού στις εν λόγω αγορές.

Η επιτροπή αυτή ιδρύθηκε το 1992 με τον Νόμο 2075 με την επωνυμία Εθνική Επιτροπή Τηλεπικοινωνιών – ΕΕΤ και οι αρμοδιότητές της επικεντρωνόταν στην εποπτεία της αγοράς των τηλεπικοινωνιών. Στη συνέχεια της ανατέθηκε και η ευθύνη για την εποπτεία της αγοράς των ταχυδρομικών υπηρεσιών και έτσι μετονομάστηκε σε Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων. Ο σημερινός ρόλος της ΕΕΤΤ ορίζεται βάσει του Νόμου 2867/2000, ενώ με τον ισχύοντα Νόμο 3431/2006 περί ηλεκτρονικών επικοινωνιών, καθορίζεται το πλαίσιο παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών εντός της Ελληνικής επικράτειας.

Ο βασικότερος στόχος της ΕΕΤΤ είναι η εξασφάλιση της πρόσβασης όλων των καταναλωτών σε ένα μεγάλο εύρος δικτύων και υπηρεσιών επικοινωνίας, προορίζοντας παράλληλα τα δικαιώματά τους. Παράλληλα, η ΕΕΤΤ συμβάλλει στην ανάπτυξη αγορών τηλεπικοινωνιακών
και ταχυδρομικών υπηρεσιών με τη διαμόρφωση ενός ρυθμιστικού περιβάλλοντος. Επιπλέον, μία πολύ βασική αρμοδιότητα της επιτροπής αυτής είναι η ενημέρωση των καταναλωτών σχετικά με τις υπηρεσίες τηλεπικοινωνιών και ταχυδρομειών. Οι καταναλωτές και οι επιχειρήσεις μπορούν να απευθύνονται στην ΕΕΤ και να υποβάλλουν τις ερωτήσεις ή τις καταγγελίες τους.

Τέλος, σύμφωνα με το Προεδρικό Διάταγμα 150/2001 για την προσαρμογή στην Οδηγία 99/1993 του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, η ΕΕΤ είναι η αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα φορέων παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, καθώς και για τη διαπίστωση της συμμόρφωσης προς τις διατάξεις δημιουργίας υπογραφής. Επιπρόσθετα, είναι αρμόδια για τον ορισμό και την εποπτεία των ιδιωτικών ή δημόσιων φορέων για την διαπίστευση των φορέων παροχής πιστοποίησης. Η ΕΕΤ, με την απόφαση 248/71, εξέδωσε τον Κανονισμό Αρμοδιοτήτων Πιστοποίησης Ηλεκτρονικής Υπογραφής ρυθμίζοντας θέματα σχετικά με αναγνωρισμένα πιστοποιητικά καθώς και την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα φορέων παροχής υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής.

Τέλος, με μία σειρά αποφάσεων της το 2003, η ΕΕΤ δημιούργησε ένα θεσμικό πλαίσιο σχετικά με τον ορισμό και τη λειτουργία των εντεταλμένων φορέων για την Εθελοντική Διαπίστευση και τον έλεγχο της δημιουργίας υπογραφής και ασφαλών κρυπτογραφικών μονάδων, καθώς και για την Εθελοντική Διαπίστευση των φορέων παροχής υπηρεσιών πιστοποίησης.
3.1.7 Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης

Ο Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης (ΕΦΤΑ) [37] αποτελεί μία ιδιωτική πρωτοβουλία που ακολουθεί τα πρότυπα αντίστοιχων εθνικών οργανισμών άλλων χωρών. Τα μέλη του ΕΦΤΑ είναι οι υπηρεσίες πρόληψης και αντιμετώπισης της τηλεπικοινωνιακής απάτης και του ηλεκτρονικού εγκλήματος των εταιριών που προσφέρουν τηλεπικοινωνιακές υπηρεσίες (σταθερό ή κινητό δίκτυο), όπως η Cosmote, η Vodafone και ο ΟΤΕ, καθώς και εταιρίες που δραστηριοποιούνται στο ηλεκτρονικό εμπόριο και το διαδίκτυο γενικότερα.

Η ίδρυση του ΕΦΤΑ πραγματοποιήθηκε για τους εξής σκοπούς:

- Ενημέρωση των πολιτών με στόχο την προστασία τους από την τηλεπικοινωνιακή απάτη και το ηλεκτρονικό έγκλημα.
- Προστασία των μελών του από το ηλεκτρονικό έγκλημα.
- Ανταλλαγή πληροφοριών και μεθόδων με τις οποίες διενεργούνται οι τηλεπικοινωνιακές απάτες, καθώς και την από κοινού λήψη προστατευτικών μέτρων.
- Ανταλλαγή πληροφοριών σχετικά με την απάτη που προέρχεται από τρίτους οι οποίοι χρησιμοποιούντας διάφορες μεθόδους χρεώνουν το καταναλωτικό κοινό και τις εταιρίες με μεγάλα χρηματικά ποσά.

Ο ΕΦΤΑ έχει ελεγκτικό χαρακτήρα και δεν είναι αρμόδιος να επιβάλλει κυρώσεις αλλά μόνο να προλαμβάνει και να καταγγέλλει τις απάτες. Οι πολίτες ή οι επιχειρήσεις μπορούν να ενημερώνονται ή να ζητούν υποστήριξη από τον φορέα αυτόν σε θέματα τηλεπικοινωνιακής απάτης.
ΕΦΤΑ λαμβάνει υπόψη τους περιορισμούς των νόμων 2472/1997 και 2774/1999 για την προστασία δεδομένων. Επιπρόσθετα, συνεργάζεται με άλλους σχετικούς εθνικούς, Ευρωπαϊκούς και διεθνείς φορείς που ασχολούνται με την καταπολέμηση της ηλεκτρονικής απάτης και του ηλεκτρονικού εγκλήματος. Παραδείγματα τέτοιων φορέων αποτελούν οι δύο Ελληνικές αρχές προστασίας δεδομένων που περιγράψαμε στις παραγράφους 3.1.4 και 3.1.5, η Διεθνής Ένωση Τηλεπικοινωνιών (International Tellecommunication Union - ITU) [59], το Διεθνές Φόρουμ για την Αντικανονική Πρόσβαση στα Δίκτυα (Forum for International Irregular Network Access – FIINA) [38], το Ευρωπαϊκό Ινστιτούτο Ερευσών και Στρατηγικών Μελετών στις Τηλεπικοινωνίες (European Institute for Research & Strategic Studies in Telecommunications-Eurescom) [34] και άλλα.

3.1.8 Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας για το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας

Η ομάδα αντιμετώπισης περιστατικών ασφαλείας (Computer Emergency Response Team - CERT) λειτουργεί στα πλαίσια του Εθνικού Δικτύου Έρευνας και Τεχνολογίας – ΕΔΕΤ (Greek Research and Technology Network - GRNET) [47], το οποίο διασυνδέει τα Ελληνικά Πανεπιστήμια, τα Τεχνικά Εκπαιδευτικά Ιδρύματα και τα περισσότερα Ελληνικά Ερευνητικά Κέντρα. Η ομάδα GRNET-CERT συνεργάζεται με άλλες εθνικές, Ευρωπαϊκές και Διεθνείς ομάδες οι οποίες ασχολούνται με την αντιμετώπιση περιστατικών ασφαλείας. Επιπρόσθετα, είναι μέλος του EuroCERT του συνδέσμου των Ευρωπαϊκών Ομάδων Αντιμετώπισης
Περιστατικών Ασφαλείας, με τις οποίες βρίσκεται σε συνεχή επικοινωνία και συνεργάζεται σε κοινά ζητήματα ασφαλείας υπολογιστών.

Οι βασικότερες αρμοδιότητες της ομάδας αυτής είναι να ανταποκρίνεται, να καταγράφει και να παρακολουθεί περιστατικά τα οποία αφορούν στην ασφάλεια των πληροφοριακών συστημάτων του ΕΔΕΤ και των φορέων του, ενώ παράλληλα παρέχει τεχνική βοήθεια και πληροφορίες για την επίλυση των προβλημάτων ασφαλείας. Επιπλέον, εκπαιδεύει τους χρήστες του ΕΔΕΤ και τους παρέχει την απαραίτητη πληροφόρηση και τις έγκυρες απαντήσεις πάνω σε θέματα ασφαλείας υπολογιστών και διαφύλαξης του προσωπικού απορρήτου.

Η υπηρεσία αντιμετώπισης περιστατικών υλοποιείται από την ομάδα CERT του Πανεπιστήμιου Αιγαίου και εκδίδει συστηματικά ανακοινώσεις και ενημερωτικά δελτία προκειμένου να ενημερώσει για τα κενά ασφάλειας των συστημάτων και των εφαρμογών. Οι ενημερώσεις αυτές προωθούνται και σε εκπαιδευτικούς και ερευνητικούς φορείς οι οποίοι συνδέονται στο δίκτυο του ΕΔΕΤ. Παράλληλα, αξιολογεί τα εργαλεία που είναι σχετικά με την ασφάλεια των υπολογιστικών συστημάτων, καθώς και τα συστήματα για την ανίχνευση επιθέσεων.

3.2 Ευρωπαϊκοί και Διεθνείς Εποπτικοί Φορείς Ασφαλείας

Σε αυτή την παράγραφο θα αναλύσουμε τους βασικότερους Ευρωπαϊκούς και διεθνείς φορείς για την προστασία των πολιτών κυρίως στον τομέα των τηλεπικοινωνιών. Οι φορείς που θα εξεταστούν είναι η Ευρωπαϊκή Επιτροπή [36], ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών [31], το Ευρωπαϊκό Ινστιτούτο Προτύπων
Τηλεπικοινωνιών [33] και η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας [19], οι οποίοι περιγράφονται στις παραγράφους 3.2.1, 3.2.2, 3.2.3 και 3.2.4 αντίστοιχα.

3.2.1 Ευρωπαϊκή Επιτροπή

Η Ευρωπαϊκή Επιτροπή [36] αποτελεί θεσμικό όργανο της Ευρωπαϊκής Ένωσης με απότερο σκοπό την προστασία των κοινοτικών συμφερόντων των κρατών μελών της. Η Ευρωπαϊκή Επιτροπή είναι ένα εκτελεστικό όργανο με δικαιώματα πρωτοβουλίας, εκτέλεσης, διαχείρισης και ελέγχου που ενσαρκώνει το γενικό συμφέρον της Ευρώπης. Σε αυτό το πλαίσιο έχει το δικαίωμα να προτείνει νέες ευρωπαϊκές νομοθετικές πράξεις προκειμένου να προωθήσει τα συμφέροντα της Ένωσης ή να αντιμετωπίσει τυχόν προβλήματα.

Στον τομέα των επικοινωνιών, μία πολύ σημαντική αρμοδιότητα της Επιτροπής αποτελεί η προώθηση της έρευνας και της τεχνολογικής ανάπτυξης που βασίζεται σε πολυετή προγράμματα. Τέλος, ενθαρρύνει τη δραστηριότητα των ευρωπαϊκών ερευνητικών κέντρων τα οποία αποκτούν έτσι τεχνογνωσία και παγκοσμίως αναγνωρισμένες ικανότητες. Οι δραστηριότητες αυτές πραγματοποιούνται κυρίως μέσω της Γενικής Διεύθυνσης για την Κοινωνία της Πληροφορίας (DG Information Society), η οποία παρέχει και τις απαραίτητες πληροφορίες μέσω του Δικτυακού τόπου της Ευρωπαϊκής Επιτροπής.
3.2.2 Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Network Information Security Agency – ENISA) [31] λειτουργεί ως κέντρο εμπειρογνωμοσύνης για τα κράτη μέλη, τα θεσμικά όργανα της Ευρωπαϊκής Επιτροπής και την επιχειρηματική κοινότητα όταν χρειάζονται συμβουλές σε θέματα ασφάλειας δικτύων και πληροφοριών, όπως το ηλεκτρονικό έγκλημα και οι πολιτικές ασφαλείας. Ο κυριότερος στόχος του οργανισμού αυτού είναι να προλαμβάνει, να αντιμετωπίζει και να επιλύει τα προβλήματα ασφάλειας των πληροφοριακών συστημάτων.

Οι βασικότερες δραστηριότητες του ENISA είναι η παροχή συμβουλών στην Επιτροπή και στα κράτη μέλη σχετικά με την ασφάλεια των πληροφοριών και την αντιμετώπιση τέτοιου είδους προβλημάτων, η συλλογή και ανάλυση δεδομένων για τα περιστατικά ασφάλειας και τους μελλοντικούς κινδύνους, η προώθηση μεθόδων εκτίμησης και διαχείρισης των κινδύνων που απειλούν αυτού του είδους τα συστήματα, καθώς και η παρακολούθηση της εξέλιξης των προτύπων για προϊόντα και υπηρεσίες στην κοινωνία των δικτύων και των πληροφοριών. Επιπλέον, αναζητά να αναπτύξει μια νοοτροπία ασφάλειας στα δίκτυα και τη διακίνηση πληροφορίας προς όφελος των πολιτών, των καταναλωτών, των επιχειρήσεων και των φορέων του δημόσιου τομέα της Ευρωπαϊκής Ένωσης.

Τέλος, όσο η τεχνογνωσία του ENISA θα αυξάνεται και θα εξειδικεύεται, αναμένεται να αποτελέσει έναν φορέα ο οποίος θα λειτουργεί
και συμβουλευτικά σε οποιονδήποτε φορέα, επιχείρηση ή πολίτη της 
Ευρώπης ο οποίος θα αντιμετωπίζει παρόμοια προβλήματα ασφάλειας.

3.2.3 Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών

Το Ευρωπαϊκό Ινστιτούτο Προτύπων Τηλεπικοινωνιών (European Telecommunications Standards Institute –ETSI) [33] αποτελεί έναν ανεξάρτητο, μη κερδοσκοπικό οργανισμό ο οποίος συνεργάζεται με οργανισμούς από εξήντα χώρες διεθνώς προκειμένου να παράγει πρότυπα για τις τεχνολογίες πληροφοριών και επικοινωνιών. Τα πρότυπα αυτά αποσκοπούν στην καλύτερη λειτουργία της Ευρωπαϊκής ενιαίας αγοράς. Τα μέλη του οργανισμού ETSI αποτελούν οι χρήστες, οι οργανισμοί δημιουργίας προτύπων, οι κατασκευαστές πληροφορικών συστημάτων, οι διαχειριστές δικτύων, οι παροχείς υπηρεσιών τηλεπικοινωνιών, καθώς και άλλοι αντίστοιχοι ερευνητικοί φορείς.

Τα πρότυπα που παράγει προορίζονται για εθελοντική χρήση από την αγορά και αφορούν σε τεχνολογίες ενημέρωσης και επικοινωνιών, όπως οι τηλεπικοινωνίες, οι ραδιοτηλεπικοινωνίες, η ραδιοφωνική μετάδοση, οι κινητές και δορυφορικές υπηρεσίες, καθώς και άλλοι σχετικοί τομείς. Επιπρόσθετα, το ETSI δημιουργεί κρυπτογραφικούς αλγορίθμους και πρωτόκολλα τα οποία έχουν ως σκοπό να αποτρέψουν την απάτη και την αναρμόδια πρόσβαση στις υπηρεσίες επικοινωνιών, καθώς και να προστατεύσουν την ιδιωτικότητα των χρηστών τέτοιου είδους υπηρεσιών.
3.2.4 Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας

Η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας (Computer Emergency Response Team - CERT) [19] ιδρύθηκε στην Αμερική το 1998 ως κέντρο εξειδίκευσης της ασφάλειας των δικτύων και, ιδιαίτερα, του διαδικτύου. Οι ερευνητές του CERT μελετούν τις ευπάθειες του διαδικτύου, καθώς και διάφορες μακροπρόθεσμες αλλαγές στα συστήματα δικτύων. Παράλληλα, προσφέρουν ένα ευρύ φάσμα υπηρεσιών ασφαλείας στους χρήστες τους, όπως για παράδειγμα, προειδοποιήσεις κατά της κυκλοφορίας, παροχή συμβουλών σε θέματα κυκλοφορίας και κατάρτιση σε θέματα ασφαλείας. Τέλος, σε περίπτωση περιστατικών ασφαλείας μεγάλης κλίμακας η ομάδα συντονίζει την αντιμετώπισή τους, ενώ αναλύει τα σημαντικά σημεία σε προγράμματα και δίκτυα.

3.3 Επίλογος

Η ύπαρξη ελεγκτικών φορέων και αρχών για την εποπτεία τήρησης του νομοθετικού πλαισίου μίας χώρας αποτελεί πρωταρχικό μέλημα για την προστασία των πολιτών της και στον τομέα των τηλεπικοινωνιών. Οι φορείς αυτοί συνεργάζονται τόσο μεταξύ τους, όσο και με αντίστοιχους φορείς άλλων χωρών. Παράλληλα, σε πολλές περιπτώσεις, οι πολίτες έχουν τη δυνατότητα να επικοινωνούν οι ιδιοί με τις εποπτικές αρχές και να
εκφράζουν τις απορίες τους, να κάνουν τις καταγγελίες τους ή να ζητούν
dιευκρινήσεις για τα δικαιώματά τους. Στο κεφάλαιο αυτό παρουσιάζαμε
τους βασικότερους φορείς στην Ελλάδα, την Ευρώπη αλλά και διεθνώς,
καθώς και τις αρμοδιότητές τους και τον τρόπο με τον οποίο συνεργάζονται
με τους υπόλοιπους φορείς ή με τους ίδιους τους πολίτες.
Κεφάλαιο 4

Δεδομένα Υπηρεσιών με Βάση τη Θέση

Η αυτοματοποιημένη συλλογή ευαίσθητων προσωπικών
tηλεπικοινωνιακών δεδομένων κυρίως από κινητά τηλέφωνα και άλλες
φορητές συσκευές επιτρέπει την ύπαρξη μεγάλου πλήθους δεδομένων που
αφορούν την κίνηση των χρηστών και, συγκεκριμένα, τον τόπο στον οποίο
βρίσκονται συγκεκριμένες χρονικές στιγμές. Το γεγονός ότι το κόστος
αποθήκευσης δεδομένων συνεχίζει να μειώνεται μέρα με τη μέρα έχει ως
αποτέλεσμα οι περισσότεροι φορείς, ιδιωτικοί ή δημόσιοι, να συλλέγουν όλο
και περισσότερα ευαίσθητα προσωπικά δεδομένα, πολλές φορές χωρίς να
υπάρχει κάποιος συγκεκριμένος σκοπός για τη συλλογή τους [105, 108].
Δεδομένου ότι υπάρχουν και παλαιότερα δεδομένα αποθηκευμένα για
κάποιο συγκεκριμένο πρόσωπο, αν συνδέθονται με τα καινούρια δεδομένα
μπορούν να παρέχουν μία πλήρη ηλεκτρονική εικόνα των κινήσεών του.

Αυτό το πλήθος συλλεγόμενων δεδομένων μπορεί να βοηθήσει στη
δημιουργία νέων εφαρμογών υψηλού κοινωνικού και οικονομικού
ενδιαφέροντος, αλλά παράλληλα, ελλοχεύει πολλούς κινδύνους για την
προστασία των ανθρώπων και των οργανισμών. Για παράδειγμα, αν τα
ευαισθήτα αυτά δεδομένα ανιχνευθούν από μη-εξουσιοδοτημένες οντότητες μπορούν να τροποποιηθούν, να διαγραφούν ή να υποστούν οποιαδήποτε αλλοίωση με αποτέλεσμα να βλάψουν την προσωπική ζωή των ατόμων. Το βασικότερο ερώτημα που προκύπτει σε αυτό το σημείο είναι το πώς μπορούν οι τροχείς των ατόμων που κινούνται να αποθηκευτούν και να αναλυθούν χωρίς παραβίαση των δικαιωμάτων προσωπικής μυστικότητας [44].

Στο κεφάλαιο αυτό θα εξετάσουμε τα χαρακτηριστικά των υπηρεσιών θέσης καθώς και των δεδομένων που προέρχονται από την επικοινωνία με τέτοιου είδους υπηρεσίες. Πιο συγκεκριμένα, στην παράγραφο 4.1 θα αναλύσουμε τις υπηρεσίες με βάση τη θέση. Ειδικότερα, στην παράγραφο 4.1.1 θα εξετάσουμε τα συστατικά των συστημάτων υπηρεσιών με βάση τη θέση και τον τρόπο με τον οποίον παρέχουν τις υπηρεσίες τους στους χρήστες. Στην παράγραφο 4.1.2 θα αναλύσουμε τις χρησιμοποιούμενες μεθόδους για τον εντοπισμό της θέσης των χρηστών και στην παράγραφο 4.1.3 θα αναλύσουμε τις απαιτήσεις των συστημάτων αυτών. Εν συνεχεία, στην παράγραφο 4.2 θα ερευνήσουμε τα χρονο-χρονικά δεδομένα τα οποία προκύπτουν από τους χρήστες τέτοιου είδους συστημάτων. Συγκεκριμένα, στις παραγράφους 4.2.1 και 4.2.2 θα αναλύσουμε διάφορες ενέργειες, καταστάσεις και φαινόμενα που επηρεάζουν την ανάλυση αυτών των δεδομένων, ενώ στην παράγραφο 4.2.3 θα περιγράψουμε τα βασικότερα ζητήματα ιδιωτικότητας που προκύπτουν κατά τη συλλογή και ανάλυσή τους.

4.1 Υπηρεσίες με Βάση τη Θέση

Η αλματώδης ανάπτυξη στον τομέα των τηλεπικοινωνιών και των δικτύων τα τελευταία χρόνια έχουν επιφέρει πολλές αλλαγές στον τρόπο...
επικοινωνία των ανθρώπων. Η σημαντικότερη επίδραση των αλλαγών αυτών είναι η χρήση όλων και περισσότερων φορητών συσκευών, όπως τα κινητά τηλέφωνα, οι υπολογιστές παλάμης, οι φορητοί υπολογιστές ή οι μονάδες πλοήγησης αυτοκινήτου. Οι υπηρεσίες με βάση τη θέση (Location Based Services - LBS) αποτελούν μία οικογένεια υπηρεσιών που παρέχονται στους χρήστες μέσω των φορητών συσκευών εκμεταλλευόμενες τη δυνατότητα των συσκευών αυτών να γνωρίζουν τη θέση τους και να μπορούν να την αναφέρουν ανά πάσα στιγμή μέσω μίας ασύρματης δικτυακής υποδομής.

4.1.1 Συστατικά ενός Συστήματος Υπηρεσιών με Βάση τη Θέση

Ένα σύστημα υπηρεσιών με βάση τη θέση αποτελείται από τα ακόλουθα συστατικά στοιχεία [101]:

- **Φορητές Συσκευές**: οι συσκευές αυτές μπορεί να είναι τα κινητά τηλέφωνα, οι υπολογιστές παλάμης, οι φορητοί υπολογιστές ή οι μονάδες πλοήγησης ενός αυτοκινήτου. Αποτελούν ουσιαστικά το εργαλείο μέσω του οποίου οι χρήστες ζητούν και λαμβάνουν τις πληροφορίες που επιθυμούν.

- **Σύστημα Εντοπισμού Θέσης**: για τη λειτουργία αυτών των υπηρεσιών απαιτείται να υπάρχει κάποιο σύστημα με το οποίο ο χρήστης θα γνωρίζει τη θέση του προκειμένου να την στείλει στον φορέα παροχής υπηρεσιών και να εξυπηρετηθεί. Αυτό μπορεί να πραγματοποιηθεί είτε
υπολογίζοντας τις αποστάσεις από τους σταθμούς βάσης
tου δικτύου τηλεφωνίας είτε χρησιμοποιώντας κάποιο
dέκτη ο οποίος μπορεί να βρίσκεται εσωτερικά ή εξωτερικά
στη συσκευή. Οι μέθοδοι εντοπισμού θέσης των κινητών
συσκευών θα περιγραφούν στην παράγραφο 4.1.2.

- **Φορέας Παροχής Υπηρεσιών και Εφαρμογών:** ο φορέας
  παροχής υπηρεσιών είναι υπεύθυνος για το συντονισμό και
  τη λειτουργία του συστήματος. Η βασικότερη υπηρεσία που
  προσφέρει είναι η επεξεργασία των ερωτημάτων των
  χρηστών, όπως παραδείγματος χάριν η εύρεση ή ο
  υπολογισμός μίας ζητούμενης θέσης. Εξετάζει το είδος του
  αιτήματος και αποφασίζει για το ποιες είναι οι απαραίτητες
  πληροφορίες που απαιτούνται για να εξυπηρετηθεί η
  συγκεκριμένη αίτημα. Για το λόγο αυτό απευθύνεται στον
  φορέα παροχής περιεχομένου.

- **Φορέας Παροχής Περιεχομένου και Δεδομένων:** ο
  φορέας αυτός είναι υπεύθυνος για το περιεχόμενο το οποίο
  προσφέρεται στους χρήστες μέσω των παρεχόμενων
  υπηρεσιών, συγκεκριμένα όλες τις απαραίτητες
  πληροφορίες για την εξυπηρέτηση των ερωτήσεων των
  χρηστών του συστήματος.

- **Τηλεπικοινωνιακή Υποδομή:** το δίκτυο επικοινωνίας είναι
  ασύρματο δίκτυο το οποίο μεταφέρει τα δεδομένα και τις
  πληροφορίες που ζητά ο χρήστης από το τερματικό του
  στον φορέα παροχής υπηρεσιών και στη συνέχεια την
  απάντηση του φορέα με τις ζητούμενες πληροφορίες του
  χρήστη.
Ένα τυπικό σύστημα παροχής υπηρεσιών θέσης περιγράφεται στην παρακάτω εικόνα:

Εικόνα 4.1 Τυπικό σύστημα υπηρεσιών με βάση τη θέση.

Ο τρόπος με τον οποίον παρέχονται οι υπηρεσίες στους χρήστες από τα συστήματα που περιγράψαμε παραπάνω περιγράφεται από τα παρακάτω βήματα:

- Αρχικά, λαμβάνεται από το τερματικό του χρήστη η πληροφορία της θέσης του. Στη συνέχεια η συσκευή
στέλνει μέσω του ασύρματου δικτύου τη θέση αυτή μαζί με το αντικείμενο της αναζήτησης του χρήστη στην πύλη (gateway) του συστήματος.

- Ο ρόλος της πύλης είναι να στέλνει την αίτηση σε κάποιον κατάλληλο εξυπηρετητή που ανήκει στο φορέα παροχής υπηρεσιών. Στις περιπτώσεις που χρησιμοποιείται το διαδίκτυο για την εύρεση κατάλληλων εξυπηρετητών, η πύλη είναι αρμόδια για την ανταλλαγή μηνυμάτων μεταξύ του ασύρματου δικτύου και του διαδικτύου.

- Ο εξυπηρετητής του φορέα παροχής περιεχομένου λαμβάνει την αίτηση εξυπηρέτησης και εξετάζει το είδος των ερωτημάτων. Στη συνέχεια ενεργοποιεί την κατάλληλη υπηρεσία για την ακριβή επεξεργασία του ερωτήματος.

- Το σύστημα που αναλαμβάνει την ανάλυση του ερωτήματος αποφασίζει σχετικά με το ποιες επιπλέον πληροφορίες απαιτούνται για την εξυπηρέτηση της αίτησης του πελάτη. Για το λόγο αυτό απευθύνεται σε κάποιον φορέα παροχής περιεχομένου.

- Έχοντας συγκεντρώσει όλες τις πληροφορίες που χρειάζεται, ο εξυπηρετητής θα αποφασίζει για την κατάλληλη απάντηση που πρέπει να δώσει στο χρήστη.

- Στη συνέχεια δημιουργεί την απάντηση στη μορφή που επιθυμεί ο χρήστης, για παράδειγμα με μορφή κειμένου, βίντεο και άλλα, την αποστέλλει στην πύλη μέσω διαδικτύου και αυτή με τη σειρά της την προωθεί στο χρήστη μέσω του ασύρματου δικτύου.
Τα βήματα που περιγράψαμε για την παροχή υπηρεσιών μέσω των συστημάτων υπηρεσιών θέσης φαίνονται στην παρακάτω εικόνα:

Εικόνα 4.2 Τρόπος παροχής υπηρεσιών ενός συστήματος υπηρεσιών με βάση τη θέση.
4.1.2 Μέθοδοι Εντοπισμού Θέσης

Όπως αναφέραμε και παραπάνω για να εξυπηρετηθεί ο κάθε χρήστης ο οποίος αιτείται υπηρεσίες μέσω μίας φορητής συσκευής θα πρέπει να έχει προσδιορίσει τη θέση του. Οι βασικές μέθοδοι εντοπισμού της θέσης των χρηστών στο χώρο είναι δύο:

- **Εύρεση θέσης μέσω του τηλεπικοινωνιακού δικτύου:** Η προσέγγιση αυτή απαιτεί το τερματικό να ανιχνεύεται αυτόματα από το δίκτυο, είτε να στέλνει κάποιο σήμα που επιτρέπει στο δίκτυο να βρει τη θέση του. Πιο συγκεκριμένα, το τερματικό στέλνει ένα σήμα στους πύργους και οι πύργοι διαπραγματεύονται για το ποιος είναι ο πιο κατάλληλος για να επικοινωνήσει με το τερματικό αυτό. Δεδομένου ότι πρόκειται για μία φορητή συσκευή η οποία μπορεί να αλλάζει θέση συνεχώς, οι πύργοι ελέγχουν το σήμα διαρκώς και η συσκευή μπορεί να επικοινωνεί με διαφορετικό πύργο ανάλογα με την περίπτωση. Με τη σύγκριση της σχετικής δύναμης των σημάτων οι πύργοι μπορούν να καθορίσουν τη θέση του τερματικού. Η διαδικασία αυτή φαίνεται στην παρακάτω εικόνα.
Εικόνα 4.3 Εύρεση θέσης μέσω τηλεπικοινωνιακού δικτύου.

- Εύρεση θέσης απευθείας από το τερματικό: Η προσέγγιση αυτή απαιτεί από το ίδιο το τερματικό να υπολογίζει τη θέση του με βάση σήματα τα οποία φθάνουν σε αυτό από τους σταθμούς βάσης. Το πιο γνωστό παράδειγμα αυτής της μεθόδου εύρεσης θέσης είναι το Global Positioning System – GPS, στο οποίο οι σταθμοί βάσης είναι δορυφόροι. Οι φορητές συσκευές οι οποίες μπορεί να έχουν ενσωματωμένο κάποιο GPS δέκτη μπορούν να επιτρέψουν τον προσδιορισμό της θέσης τους με μεγαλύτερη ακρίβεια. Τα συστήματα αυτά έχουν εξελιχθεί ώστε να μην υπάρχουν προβλήματα εντοπισμού θέσης και να μην αποδυναμώνονται τα σήματα που στέλνονται από τις συσκευές στην περίπτωση που ο χρήστης με τη φορητή συσκευή περιβάλλεται από πολύ
ψηλά κτήρια, δέντρα, ή βρίσκεται σε κλειστούς χώρους. Η μέθοδος αυτή περιγράφεται στην παρακάτω εικόνα.

Εικόνα 4.4 Εύρεση θέσης απευθείας από το τερματικό.

Θα πρέπει να σημειωθεί σε αυτό το σημείο ότι έχουν προκύψει και νέες υβριδικές μέθοδοι εντοπισμού θέσης των χρηστών στο χώρο οι οποίες
συνδυάζουν τις παραπάνω μεθόδους [101]. Οι βασικές αρχές στις οποίες στηρίζονται αυτές οι μέθοδοι είναι:

- Οι σταθμοί βάσης έχουν γνωστή γωνιακή θέση.
- Η πληροφορία που προέρχεται από κάποιο τηλεπικοινωνιακό σήμα μεταφράζεται σε χωρικές αποστάσεις.
- Ο υπολογισμός της απόλυτης θέσης του χρήστη πραγματοποιείται συνδυάζοντας τις παραπάνω σχετικές χωρικές αποστάσεις με τη γνωστή απόλυτη θέση των σταθμών βάσης.

4.1.3 Απαιτήσεις ενός Συστήματος Υπηρεσιών με Βάση τη Θέση

Τα συστήματα που περιγράψαμε παραπάνω τα οποία παρέχουν υπηρεσίες με βάση τη θέση των χρηστών έχουν πολλές απαιτήσεις. Αρχικά, δεδομένου ότι οι υπηρεσίες που προσφέρουν απευθύνονται σε ένα πλήθος χρηστών θα πρέπει το σύστημα να μπορεί να λειτουργήσει εξίσου αποδοτικά με οποιοδήποτε αριθμό χρηστών. Επιπρόσθετα, λόγω του ότι οι υπηρεσίες των χρηστών θα πρέπει να παρέχονται σε πραγματικό χρόνο και δεδομένου ότι ο χρήστης μπορεί να κινείται την ώρα που αιτείται κάποιες υπηρεσίες ή πληροφορίες θα πρέπει το σύστημα να ανταποκρίνεται άμεσα και να του αποστέλλει τις εξατομικευμένες υπηρεσίες. Παράλληλα, όπως και κάθε on–line σύστημα έτσι και αυτού του είδους τα συστήματα θα πρέπει να προσφέρουν τις υπηρεσίες τους αξιόπιστα και ανά πάσα χρονική στιγμή.

Τέλος, η βασικότερη απαιτήση των συστημάτων αυτών είναι η ασφάλεια που παρέχουν. Τα συστήματα αυτά θα πρέπει να υιοθετούν
4.2 Χωρο-χρονικά δεδομένα

Τα χωρο-χρονικά δεδομένα προκύπτουν από τις κινούμενες οντότητες οι οποίες αλλάζουν θέση με την πάροδο του χρόνου και αποτελούν κρίσιμα στοιχεία σε πολλές εφαρμογές, όπως στην εθνική ασφάλεια και την έρευνα εγκλημάτων [85].

Η χωρική συνιστώσα τους μπορεί να αναπαρασταθεί ως τρισδιάστατη, δισδιάστατη ή σε ορισμένες περιπτώσεις ως μονοδιάστατη ανάλογα με το πρόβλημα [63]. Επιπρόσθετα, σε ορισμένα προβλήματα μπορεί να μας ενδιαφέρουν μόνο συγκεκριμένες τοποθεσίες οπότε να εξετάζουμε το χώρο μόνο για αυτές τις τοποθεσίες. Σε κάποιες άλλες περιπτώσεις μπορεί να μη μας ενδιαφέρουν οι ακριβείς θέσεις των κινούμενων αντικειμένων αλλά οι σχετικές τους θέσεις. Για την αναπαράσταση του χώρου χρησιμοποιούνται συνήθως καθιερωμένα συστήματα αναφοράς, όπως οι γεωγραφικές συντεταγμένες [7].

Η χρονική συνιστώσα μπορεί να αναπαρασταθεί είτε ως μία ή περισσότερες ακολουθίες από χρονικές στιγμές \((t_0, t_1, \ldots, t_x)\), είτε σαν χρονικά διαστήματα εκφράζοντας την αρχή και το τέλος μίας ενέργειας \((t_{\text{αρχή}}, t_{\text{τέλος}})\) [92]. Πολλές φορές, ανάλογα με το πρόβλημα, οι αναλυτές δεν
ενδιαφέρονται για κάποιες χρονικές στιγμές μίας ημέρας, αλλά ενδιαφέρονται να αναλύσουν τα δεδομένα για κάποιες εβδομάδες, μήνες ή έτη, ή ακόμη και για συγκεκριμένες ημέρες κάθε έτους. Για την αναπαράσταση του χρόνου χρησιμοποιείται συνήθως το τυποποιημένο ημερολογιακό σύστημα.

Στη σχεδίαση ενός συστήματος κινούμενων αντικειμένων η μοντελοποίηση της κίνησης πραγματοποιείται συνήθως με την τροχιά του αντικειμένου, δηλαδή με το μονοπάτι το οποίο διαγράφει μία οντότητα σε συνάρτηση ενός συγκεκριμένου χρόνου. Ο πιο συνηθισμένος τρόπος για την αποθήκευση χωρο-χρονικών δεδομένων είναι η μορφή μίας τρισδιάστατης τροχιάς. Οι δύο διαστάσεις χρησιμοποιούνται για την αναπαράσταση του χώρου σε μορφή ενός ζευγαριού χωρικών συντεταγμένων (x,y) και η τρίτη για την αναπαράσταση του χρόνου (t) [14, 68]. Η πληροφορία η οποία εμπεριέχεται στην τροχιά δεν αφορά μόνο πρωτογενή στοιχεία σχετικά με τη θέση που βρίσκεται κάποια οντότητα μία συγκεκριμένη χρονική στιγμή, αλλά περιέχει και πιο σύνθετες διαστάσεις που προκύπτουν από το συνδυασμό αυτών των δύο συνιστώσων, όπως για παράδειγμα η ταχύτητά του, η κατεύθυνσή του ή η διανυσματική απόστασή του. Επιπρόσθετα, μπορεί να φανερώνει την αλλαγή της ταχύτητας (για παράδειγμα την επιτάχυνση ή την επιβράδυνση της οντότητας) ή ακόμα την αλλαγή της κατεύθυνσής ή του τελικού της προορισμού.

4.2.1 Ενέργειες Κινούμενων Αντικειμένων

Όπως αναφέραμε και παραπάνω, εκτός από τη θέση και τη χρονική στιγμή που κινούνται τα αντικείμενα, υπάρχουν και κάποια άλλα χαρακτηριστικά τα οποία παίζουν σημαντικό ρόλο στην ανάλυση των
κινούμενων οντοτήτων δεδομένου ότι μπορούν να επηρεάζουν τις κινήσεις τους. Για παράδειγμα, μία οντότητα μπορεί να κινείται από μόνη της ή να βρίσκεται μέσα σε κάποιο μεταφορικό μέσο. Παραδείγματος χάριν, η γνώση του αν η κινούμενη οντότητα βρίσκεται μέσα σε ένα τρένο ή ένα λεωφορείο, θα διευκρινίζει τις πιθανές διαδρομές ή τους πιθανούς προορισμούς της. Επιπρόσθετα, θα διευκρινίζει την ταχύτητα με την οποία κινείται ή τις αλλαγές της ταχύτητάς της.

Παράλληλα, υπάρχουν και άλλα προσωπικά χαρακτηριστικά τα οποία μπορούν να διευκολύνουν την ανάλυση κινούμενων δεδομένων. Επί παραδείγματι, η γνώση της ηλικίας ή της κατάστασης της υγείας του ατόμου που κινείται θα καθιστούσε πιο εύκολο τον προσδιορισμό της ταχύτητάς του· ένα ηλικιωμένο άτομο ή ένα άτομο με κινητικά προβλήματα περιορίζει την ταχύτητα με την οποία μπορεί να κινηθεί. Τέλος, το επάγγελμα της κινούμενης οντότητας είναι ένα πολύ σημαντικό χαρακτηριστικό για την ανάλυση των κινούμενων οντοτήτων. Παραδείγματος χάριν, για ένα άτομο το οποίο δουλεύει κάποιες ώρες σε εμπόδια, οποίους δεν μπορούν να προσπελάσουν συγκεκριμένες ώρες ή γραφείο είναι πολύ περιορισμένες οι αλλαγές στην θέση στην οποία βρίσκεται.

4.2.2 Συσχετιζόμενες Καταστάσεις και Φαινόμενα

Είναι σημαντικό σε αυτό το σημείο να αναφέρουμε ότι οποιαδήποτε μετακίνηση μπορεί να επηρεαστεί από διάφορες καταστάσεις και περιβαλλοντικά φαινόμενα. Επί παραδείγματι, η ανάλυση της κίνησης μπορεί να διευκολυνθεί αν παρέχεται γνώση για την ύπαρξη θάλασσας, βουνών, δάσων, αρχαιολογικών χώρων, χώρων με εμπόδια, χώρων τους οποίους δεν μπορούν να προσπελάσουν συγκεκριμένα χώματα, δρόμων οι οποίοι είναι κλειστοί λόγω έργων ή ατυχημάτων, συγκροτημάτων
πολυκατοικιών ή καταστημάτων, πολιτιστικών κέντρων και άλλα. Επιπλέον, οι κλιματολογικές συνθήκες είναι ένα από τα βασικότερα φαινόμενα τα οποία σχετίζονται με την κίνηση [76].

Αλλάς καταστάσεις περιλαμβάνουν διάφορες πολιτιστικές ή αθλητικές εκδηλώσεις, τις εθνικές εορτές, τα οράματα λειτουργίας των διαφόρων εταιριών ή των καταστημάτων και άλλα. Τέλος, είναι χαρακτηριστικό ότι οι μετακινήσεις των ατόμων τις εργάσιμες ώρες είναι πολύ μεγαλύτερες σε σχέση με τις υπόλοιπες ώρες, όπως επίσης την ημέρα οι μετακινήσεις διαφέρουν από αυτές που πραγματοποιούνται τις βραδινές ώρες. Παράλληλα, για κάθε εποχή οι αλλαγές των μετακινήσεων ποικίλουν, όπως για παράδειγμα τους καλοκαιρινούς μήνες σε σχέση με τους χειμερινούς.

Βέβαια, προκειμένου να ληφθούν οι παραπάνω καταστάσεις υπόψη κατά την ανάλυση στοιχείων οι αναλυτές θα πρέπει να έχουν πρόσθετη γνώση όλων αυτών των πληροφοριών.

4.2.3 Θέματα Ιδιωτικότητας σε Χωρο-χρονικά Δεδομένα

Τα χωρο-χρονικά δεδομένα αποτελούν σύνθετα δεδομένα και οι υπηρεσίες που σχετίζονται με τις κινούμενες οντότητες είναι πολύπλοκες. Για την παροχή τέτοιου είδους εξατομικευμένων υπηρεσιών απαιτείται η γνώση πολλών χαρακτηριστικών των χρηστών. Εκτός από τα βασικά χαρακτηριστικά που φανερώνουν το χώρο στον οποίο βρίσκεται ο κάθε χρήστης σε συγκεκριμένες χρονικές στιγμές, πολλά είναι τα περαιτέρω χαρακτηριστικά που γνωρίζουν τα συστήματα για τους χρήστες. Τα χαρακτηριστικά αυτά θα πρέπει να είναι γνωστά μόνο σε εξουσιοδοτημένες
οντότητες οι οποίες επιθυμούν να προσφέρουν εξατομικευμένες υπηρεσίες προς τους χρήστες.

Όπως περιγράφαμε στο προηγούμενο κεφάλαιο, οι περισσότερες χώρες ανά τον κόσμο προστατεύουν νομοθετικά τα τηλεπικοινωνιακά δεδομένα των πολιτών τους. Οι φορείς παροχής υπηρεσιών θέσης, όμως, προσαρμόζονται βάσει των νόμων μίας συγκεκριμένης χώρας. Σε αυτό το σημείο, λοιπόν, προκύπτουν πολλά ερωτήματα. Για παράδειγμα, αν ο φορέας αυτός χρειαστεί να εργαστεί και σε κάποια άλλη χώρα βάσει ποιων νόμων θα πρέπει να προσαρμόσει τις υπηρεσίες του; Σε τέτοιες περιπτώσεις ένα πιθανό σενάριο θα ήταν οι υπηρεσίες θέσης να προσαρμόζονται βάσει μίας από τις ακριβέστερες οδηγίες μυστικότητας, όπως για παράδειγμα οι οδηγίες της ΕΕ. Μία άλλη σημαντική ερώτηση που προκύπτει είναι το πώς οι νόμοι διασφάλισης της ιδιωτικότητας επιδρούν στη χρήση των υπηρεσιών θέσης; Πώς οι τροχιές των χρηστών και τα άλλα χαρακτηριστικά τους μπορούν να αναλυθούν χωρίς να παραβιάζουν την προσωπική τους μυστικότητα; Πώς οι χρήστες μπορούν να διευκρινίσουν τη συγκατάθεσή τους πριν χρησιμοποιήσουν τέτοιο είδους συστημάτων υπηρεσιών; Πόσο δύσκολο και χρονοβόρο θα είναι ένας χρήστης να αξιολογήσει τις δηλώσεις ιδιωτικότητας ενός φορέα παροχής υπηρεσιών κάθε φορά προτού χρησιμοποιήσει μία τέτοια υπηρεσία; Πώς ένας χρήστης θα μπορεί να ελέγξει αν ο φορέας παροχής υπηρεσιών επεξεργάζεται τα δεδομένα του περιόντα την πολιτική ασφαλείας που έχει συμφωνηθεί και το απαραίτητο νομοθετικό πλαίσιο;

Σε πολλές περιπτώσεις οι νομοθετικές προσεγγίσεις δεν απαντούν πλήρως στα παραπάνω ερωτήματα. Προκειμένου να εξασφαλίσουμε την ασφάλεια αυτών των δεδομένων κατά την επικοινωνία των χρηστών με τους φορείς παροχής υπηρεσιών με βάση τη θέση θα πρέπει να εφαρμοστεί ένας σύνθετος μηχανισμός ασφάλειας. Για το λόγο αυτό πολλοί ερευνητές προσεγγίζουν το ζήτημα της ιδιωτικότητας τέτοιων δεδομένων από τεχνικής πλευράς. Διάφορες μέθοδοι και τεχνικές για την εξασφάλιση της ασφάλειας των χορο-χρονικών δεδομένων και των αντίστοιχων υπηρεσιών έχουν προτεθεί στην βιβλιογραφία. Τις τεχνικές αυτές θα εξετάσουμε στο επόμενο κεφάλαιο.
4.3 Επίλογος

Οι τεχνολογικές εξελίξεις στο χώρο των δικτύων και των συστημάτων γεωγραφικού εντοπισμού (GPS) έχουν επιτρέψει την ανάπτυξη εφαρμογών που βασίζονται στη θέση των κινούμενων αντικειμένων. Οι υπηρεσίες που προσφέρονται στους κινούμενους χρήστες αυξάνονται μέρα με τη μέρα διευκολύνοντας τις καθημερινές τους δραστηριότητες. Οι υπηρεσίες αυτές, όμως, είναι πολύπλοκες και απαιτούν τη γνώση πολλών χαρακτηριστικών των χρηστών. Η γνώση αυτή μπορεί να βοηθά στην εξατομίκευση των προσφερόμενων υπηρεσιών, αλλά παράλληλα, ελλοχεύει πολλούς κινδύνους για την ιδιωτικότητά τους.

Στο κεφάλαιο αυτό εξετάσαμε τα χαρακτηριστικά των συστημάτων υπηρεσιών με βάση τη θέση, καθώς και τις απαιτήσεις που έχουν τέτοιου είδους συστήματα. Παράλληλα, ερευνήσαμε τα χαρακτηριστικά των κινούμενων οντοτήτων και των δεδομένων τα οποία προκύπτουν από αυτές, που περιλαμβάνουν τις τροχιές που ακολουθούν οι οντότητες, καθώς και άλλα χαρακτηριστικά τα οποία μπορούν να επηρεάσουν την ανάλυση τέτοιου είδους δεδομένων. Τέλος, κάναμε μία αναφορά των βασικότερων ερωτημάτων ιδιωτικότητας τα οποία προκύπτουν κατά τη χρήση υπηρεσιών με βάση τη θέση.
Κεφάλαιο 5

Τεχνικές Διασφάλισης Ιδιωτικότητας σε Χωρο-χρονικά Δεδομένα

Ποτέ άλλοτε δεν υπήρξε μεγαλύτερη ανάγκη για την προστασία του ιδιωτικού απορρήτου και της ανωνυμίας. Με τη ραγδαία ανάπτυξη των υπολογιστικών συστημάτων και των δικτύων τα υπολογιστικά συστήματα περιέχουν όλο και περισσότερα ευαίσθητα δεδομένα των χρηστών τους και οι απαιτήσεις ασφαλείας αυξάνονται εκρηκτικά. Για το λόγο αυτό είναι απαραίτητο να αναπτυχθούν τεχνικές διασφάλισης της ιδιωτικότητας, κυρίως για τα χωρο-χρονικά δεδομένα. Πολλά ερωτήματα προκύπτουν για τον τρόπο με τον οποίο μπορούν τα συστήματα να διαχειριστούν τις τροχιές των δεδομένων αυτών, για τις μεθόδους και τις αρχιτεκτονικές των συστημάτων που πρέπει να εφαρμοστούν για την προστασία τους, καθώς και για τον τρόπο που θα χρησιμοποιηθούν όλες αυτές οι μέθοδοι προκειμένου να βελτιώσουν τις εφαρμογές και να προσφέρουν καλύτερες υπηρεσίες.

Στο κεφάλαιο αυτό θα εξετάσουμε τις βασικότερες τεχνικές διασφάλισης της ιδιωτικότητας των δεδομένων και της ανωνυμίας των χρηστών. Πιο συγκεκριμένα, στην παράγραφο 5.1 θα αναλύσουμε τις
απαιτήσεις ασφαλείας των συστημάτων οι οποίες εκφράζονται μέσα από τις
πολιτικές ασφαλείας. Ο πιο κρίσιμος παράγοντας στον οποίον θα εστιάσουμε
αποτελεί ο έλεγχος προσπέλασης στα δεδομένα, δηλαδή οι περιορισμοί και οι
άδειες που δίνονται στους συμμετέχοντες για οποιαδήποτε ενέργεια πάνω στα
dεδομένα. Στη συνέχεια, στην παράγραφο 5.2, θα εξετάσουμε μία πολύ
σημαντική μέθοδο προστασίας της ασφάλειας των χρηστών και των
συστημάτων, την κρυπτογραφία. Στις παραγράφους 5.2.1, 5.2.2 και 5.2.3 θα
αναλύσουμε διάφορες κρυπτογραφικές προσεγγίσεις που έχουν αναπτυχθεί για
την προστασία των χωρο-χρονικών δεδομένων. Τέλος, στην παράγραφο 5.3 θα
παρουσιάσουμε μία πολύ σημαντική τεχνική διασφάλισης της ανωνυμίας των
υποκειμένων των δεδομένων και των περιοχών στις οποίες βρίσκονται, την Κ-
ανωνυμία, ενώ στην παράγραφο 5.3.1 θα εξετάσουμε πως εφαρμόζεται η
tεχνική αυτή κατά τη συλλογή της θέσης των χρηστών υπηρεσιών θέσης.

5.1 Πολιτικές Ασφαλείας

Υπάρχει διαφορά στο χαρακτηρισμό ενός συστήματος ως ασφαλούς
και στο χαρακτηρισμό του ως έμπιστου. Με τον όρο «έμπιστο» ("trusted")
εννοούμε ότι το σύστημα ικανοποιεί τις επιδιωκόμενες απαιτήσεις ασφαλείας
και παράλληλα έχει υψηλή ποιότητα. Προκειμένου να γνωρίζουμε το κατά
πόσον ένα υπολογιστικό σύστημα παρέχει την απαιτούμενη ασφάλεια θα
πρέπει να διατυπώσουμε το τι ακριβώς είναι αυτή η ασφάλεια.

Οι θεμελιώδεις απαιτήσεις ασφαλείας σε ένα σύστημα υπηρεσιών
θέσης είναι η εμπιστευτικότητα (confidentiality) και η ακεραιότητα (integrity)
tων δεδομένων, καθώς και η διαθεσιμότητα (availability) του συστήματος.
Εμπιστευτικότητα σημαίνει πρόληψη από μη εξουσιοδοτημένη αποκάλυψη
πληροφοριών. Επομένως, τα δεδομένα τα οποία χρησιμοποιούνται για την
παράδοση υπηρεσιών θέσης θα πρέπει να αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Η ακεραιότητα είναι η απαίτηση μη εξουσιοδοτημένης τροποποίησης και διαγραφής των δεδομένων, καθώς επίσης και δημιουργίας νέων δεδομένων, δηλαδή η διασφάλιση της εγκυρότητας, ορθότητας και πληρότητας των δεδομένων κατά τη φάση εισαγωγής, επεξεργασίας και αποτελεσμάτων της επεξεργασίας τους. Τέλος, η διαθεσιμότητα είναι η ιδιότητα ενός συστήματος να προσφέρει υπηρεσίες οι οποίες είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση. Αυτή η παράμετρος είναι πολύ σημαντική στα συστήματα παροχής υπηρεσιών θέσης, δεδομένου τού ότι είναι συστήματα πραγματικού χρόνου (real-time systems), αφού οι υπηρεσίες αλλάζουν και βελτιώνονται, ενώ οι χρήστες αυξάνονται συνεχώς.

Οι απαιτήσεις ασφάλειας που περιγράφαμε παραπάνω προσδιορίζονται διαμέσου μίας πολιτικής ασφαλείας. Η πολιτική ασφαλείας αποτελείται από ένα σύνολο από αρχές και οδηγίες που αφορούν τη διαχείριση των συστημάτων ασφαλείας. Βασικότερη ενέργεια ασφάλειας και απορρήτου πληροφοριών στις πολιτικές ασφαλείας, προκειμένου να επιτευχθεί η ακεραιότητα και η εμπιστευτικότητα των δεδομένων, αποτελεί ο προσδιορισμός των δικαιωμάτων ελέγχου προσπέλασης σε αυτά. Η μέθοδος αυτή αποτελεί την βασικότερη τεχνική που χρησιμοποιούν οι περισσότεροι φορείς υπηρεσιών για την παροχή ασφάλειας και μυστικότητας των δεδομένων. Χρησιμοποιείται από τη στιγμή που τα δεδομένα έχουν συλλέξει για να προσδιορίσει μέσω κανόνων ποια συμβαλλόμενα μέρη έχουν δικαιώματα προσπέλασης στα δεδομένα και τι είδους δικαιώματα έχουν.

Ο έλεγχος πρόσβασης στις εμπιστευτικές πληροφορίες στα συστήματα παροχής υπηρεσιών θέσης αποτελεί για διάφορους λόγους τον πιο κρίσιμο παράγοντα για την ασφάλεια τους. Αρχικά, οι χρήστες θα πρέπει να εμπιστευτούν τα συστήματα και να είναι σίγουροι ότι δε θα γίνει κακή χρήση των δεδομένων τους, δεδομένου και του ότι οι συμμετέχοντες στις νέες υπηρεσίες αυξάνονται ραγδαία και τα δεδομένα τα οποία συλλέγονται για αυτούς είναι ευαίσθητα δεδομένα με πιο σημαντικά τα δεδομένα θέσης τους. Παράλληλα, ο έλεγχος πρόσβασης θα πρέπει να υποστηρίζει ευέλικτα δικαιώματα πρόσβασης που περιλαμβάνουν περιορισμούς σε σχέση με την
προσπέλαση των ευαίσθητων δεδομένων, οι οποίοι πιθανώς να αλλάζουν
tακτικά σε κάθε σύστημα. Τέλος, τέτοιου είδους συστήματα αποτελούνται από
ένα πλήθος υπηρεσιών πληροφοριών και από ένα πλήθος διαφόρων μορφών
dεδομένων τα οποία καθιστούν την απλή διαχείριση δικαιωμάτων πρόσβασης
dύσκολη και ουσιαστική.

Τα δικαιώματα προσπέλασης αναπαρίστανται συνήθως από τριάδες
της μορφής \{S, O, AM\}, που φανερώνουν τον τρόπο προσπέλασης AM (Access
Mode) του αντικειμένου O (Object) από το υποκείμενο S (Subject) [84]. Το
αντικείμενο μπορεί να είναι οποιοδήποτε είδους δεδομένο, ενώ το υποκείμενο
μπορεί να είναι κάποιο άτομο, οργανισμός, πρόγραμμα ή οποιαδήποτε άλλη
οντότητα μπορεί να πραγματοποιήσει κάποια ενέργεια στα δεδομένα.

Υπάρχουν διάφορες προσεγγίσεις στη βιβλιογραφία για τα συστήματα
eλέγχου πρόσβασης που αφορούν στα συστήματα υπηρεσιών θέσης. Οι
περισσότερες προσεγγίσεις βασίζονται σε ένα πολύ βασικό μοντέλο σε αυτήν
την κατηγορία, τον βασισμένο-σε-ρόλους έλεγχο προσπέλασης - RBAC (Role-
Based Access Control) [95]. Σύμφωνα με αυτό το μοντέλο, κάθε χρήστης έχει
συγκεκριμένα και προσδιορισμένη πρόσβαση στα δεδομένα από το μοντέλο προνόμια για τον τρόπο προσπέλασης στα δεδομένα. Ο τρόπος προσπέλασης μπορεί να είναι
οποιαδήποτε ενέργεια που πραγματοποιείται στα δεδομένα, όπως για
παράδειγμα ανάγνωση ή εγγραφή. Παράλληλα, εκτός από τα δικαιώματα των
χρηστών προσδιορίζονται και οι κεντρικοί περιορισμοί που αφορούν στην
καταχώρηση ή χρήση τέτοιων εξουσιοδοτήσεων. Το μοντέλο αυτό ουσιαστικά
καθορίζει τον τρόπο προσπέλασης των πληροφοριών με βάση τις καθορισμένες
εργασίες και αρμοδιότητες των χρηστών στο σύστημα, οι οποίες προτείνεται να
ομαδοποιούνται και να εκφραστούν σε ρόλους. Κατόπιν, αντί να καθορίζονται
οι εξουσιοδοτήσεις προσπέλασης για κάθε χρήση έξωσηστα, καθορίζονται
πρώτα οι εξουσιοδοτήσεις για κάθε ρόλο και, εν συνεχεία, οι ρόλοι
eκφραστούν στους χρήστες [120]. Στον χρήστη που τον έχει εκφροθεί
κάποιος ρόλος του επιτρέπεται να εκτελεί όλες τις προσπέλασες για τις οποίες
έχει εξουσιοδοτηθεί ο ρόλος αυτός. Ένα πολύ ενδιαφέρον πλεονέκτημα του
μοντέλου αυτού είναι η δυνατότητα εύκολης μετατροπής της εκάστοτε
πολιτικής προσπέλασης προκειμένου να συμμορφώνεται στις ανάγκες του κάθε
οργανισμού οι οποίες μπορεί να αλλάξουν τακτικά.

81
Εντούτοις, η ιδιαίτερα δυναμική φύση των χωρο-χρονικών δεδομένων επιβάλλει πρόσθετους μηχανισμούς ασφαλείας. Για το λόγο αυτό, έχουν προταθεί διάφορες επεκτάσεις των βασικών μοντέλων για την επίλυση τέτοιων προβλημάτων. Σε πολλές περιπτώσεις, το μοντέλο RBAC επεκτείνεται για τις χωρικές συνιστώσες οι οποίες, σύμφωνα με τους περισσότερους ερευνητές, είναι το πιο σημαντικό χαρακτηριστικό των συστημάτων παροχής υπηρεσιών θέσης, το οποίο πρέπει να προστατευθεί. Σε αυτό το επίπεδο, στο [51] παρουσιάζεται ένας χωρικός βασισμένος-σε-ρόλους ελέγχος πρόσβασης (SRBAC – Spatial Role-Based Access Control). Οι Hansen και Oleshchuk βασίζονται στο γεγονός ότι στα κινητά υπολογιστικά περιβάλλοντα η διαθεσιμότητα των ρόλων και των αδειών μπορεί να εξαρτηθεί σε μεγάλο βαθμό από τη θέση των χρηστών. Για το λόγο αυτό χρησιμοποιούν πληροφορίες θέσης για τους ορισμούς πολιτικών ασφαλείας. Το μοντέλο αυτό αποτελείται από τα εξής πέντε βασικά συστατικά:

• Χρήστες, που αποτελούνται από τις κινούμενες οντότητες που μπορούν να καθιερώσουν μία ασύρματη επικοινωνία με τους πόρους των συστημάτων προκειμένου να εκτελέσουν ορισμένες δραστηριότητες.
• Ρόλους, που περιγράφονται ως το σύνολο των αδειών για την πρόσβαση στα αντικείμενα, δηλαδή στους πόρους των συστημάτων.
• Αδειες, που είναι οι εγκρίσεις για την εκτέλεση κάποιας ενέργειας σε ένα ή περισσότερα αντικείμενα και εξαρτώνται από τους ρόλους και τις χωρικές θέσεις των κατόχων των ρόλων.
• Διασύνδεση, ουσιαστικά αποτελεί μία χαρτογράφηση μεταξύ ενός χρήστη και ενός ενεργοποιημένου υποσυνόλου ρόλων που ανατίθενται σε αυτόν τον χρήστη.
• χωρικές θέσεις, οι οποίες αναπαρίστανται με συμβολικές εκφράσεις και περιγράφουν τις θέσεις που είναι προσδιορίσιμες από τα συστήματα, υποθέτοντας ότι το ασύρματο δίκτυο μπορεί να προσδιορίσει και να ελέγξει τη θέση οποιουδήποτε νόμιμου χρήστη.
Επιπρόσθετα, το μοντέλο αυτό επιτρέπει τη δημιουργία ιεραρχιών στις οποίες ένας ρόλος κληρονομεί τις άδειες ενός άλλου ρόλου για συγκεκριμένες χωρικές θέσεις, εάν όλες οι άδειες του δεύτερου ρόλου σε συγκεκριμένες θέσεις είναι οι ίδιες με τις άδειες του πρώτου ρόλου για τις ίδιες θέσεις.

Μία άλλη επέκταση του RBAC αποτελεί το γενικό χρονικό RBAC (General Temporal RBAC - GTRBAC) [60], το οποίο έχει αναπτυχθεί προκειμένου να ενσωματώσει χρονικούς περιορισμούς και να ενεργοποιήσει και να επιτρέψει νέους ρόλους. Με αυτόν τον τρόπο επιτρέπει τη δημιουργία πιο ευέλικτων πολιτικών ασφαλείας με όσο το δυνατό λιγότερα υψηλά προνόμια. Παράλληλα, απαιτείται να ενσωματωθούν στα αξιόπιστα προγράμματα εφαρμογών και άλλοι μη χρονικοί περιορισμοί όπως οι χωρικές παράμετροι και το εύρος ζώνης του δικτύου προκειμένου να διαχειριστούν εύκολα οι πολιτικές ασφαλείας.

Επιπρόσθετα, οι Fu και Xu [40] επεκτείνουν το μοντέλο RBAC για να ερευνήσουν και να επιβάλλουν χωρο-χρονικούς περιορισμούς. Προκειμένου να διευκρινιστούν οι χωρικοί περιορισμοί για τις κοινές προσβάσεις των πόρων καθορίζεται μία γλώσσα περιορισμών, ενώ για τους χρονικούς περιορισμούς εφαρμόζεται ένα μοντέλο συνεχούς χρόνου. Ο έλεγχος πρόσβασης πραγματοποιείται από μια ομάδα προσθέτων αδειών προσανατολισμένων στους πράκτορες [119]. Οι πράκτορες αποκτούν προνόμια ελέγχου πρόσβασης στους πόρους και τις υπηρεσίες των συστημάτων με έναν ευέλικτο και ασφαλή τρόπο. Το μοντέλο που προτείνεται έχει εφαρμοστεί σε ένα κινητό σύστημα πρακτόρων το οποίο μειώνει τον κινητό υπολογισμό χρησιμοποιώντας πράκτορες λογισμικού.

Τέλος, οι Cholweka et al [16] αναπτύξαν ένα context-sensitive μοντέλο ελέγχου πρόσβασης βασισμένο στο μοντέλο RBAC στο οποίο τα δικαιώματα πρόσβασης ενός υποκειμένου χορηγούνται με βάση τα πραγματικά καθήκοντα του υποκειμένου.

Οι πολιτικές ασφαλείας και οι μηχανισμοί ελέγχου πρόσβασης σε ένα σύστημα παροχής υπηρεσιών θέσης πρέπει να είναι το πρωταρχικό και βασικότερο μέλημα κάθε τέτοιου συστήματος. Αυτά τα μέτρα προστασίας αφορούν κυρίως τις συμμετέχουσες οντότητες που διαβάζουν και
επεξεργάζονται τα δεδομένα προκειμένου να παρέχουν τις εξατομικευμένες
υπηρεσίες που προσφέρουν τα συστήματα αυτά. Εντούτοις, δεν επαρκούν
ενάντια σε μία τρίτη κακόβουλη οντότητα η οποία επιθυμεί να υποκλέψει τα
dεδομένα αυτά και προορίζεται να παραβεί τους νόμους μυστικότητας που
έχουν τεθεί. Επιπλέον, ο χρήστης δεν μπορεί να έχει έλεγχο της επιβολής των
παρεχόμενων μέτρων προστασίας. Παράλληλα, ο καθορισμός των πολιτικών
ασφαλείας βρίσκεται στην ευχέρεια του κάθε φορέα παροχής υπηρεσιών με
αποτέλεσμα να μην υπάρχει μία κοινή πολιτική προστασίας και να μην είναι
dυνατός ο έλεγχος της επιβολής της. Τέλος, δεδομένου ότι οι εφαρμογές
υπηρεσιών θέσης είναι σχετικά νέες, είναι αμφισβητήσιμο το πόσο
αποτελεσματικά είναι αυτά τα μέτρα για την προστασία των χρηστών. Για το
λόγο αυτό, σε ένα τέτοιο είδους σύστημα δεν επαρκεί να ορίζονται μόνο οι
προσαναφερόμενοι μηχανισμοί, αλλά θα πρέπει να λαμβάνονται και άλλα μέτρα
προστασίας των δεδομένων που συλλέγονται, όπως θα παρουσιάσουμε στις
επόμενες παραγράφους.

5.2 Κρυπτογραφία

Η κρυπτογραφία είναι μία από τις βασικότερες τεχνικές που
χρησιμοποιείται στα συστήματα παροχής υπηρεσιών θέσης προκειμένου να
επιτευχθεί η αυθεντικοποίηση του χρήστη καθώς και η προστασία των χωρο-
χρονικών δεδομένων του από πιθανή κακόβουλη χρήση. Η μέθοδος αυτή
χρησιμοποιείται για την προστασία των καναλιών επικοινωνίας μεταξύ των
χρηστών και των φορέων παροχής υπηρεσιών κατά την αποστολή και λήψη
των χωρο-χρονικών δεδομένων, ενώ η προστασία της ταυτότητας των χρηστών
παρέχεται με τη χρήση ψευδώνυμων.
Οι φορείς παροχής υπηρεσιών θέσης θα πρέπει να εξασφαλίζουν στους χρήστες τους την εμπιστοσύνη ότι τα δεδομένα τους δε θα χρησιμοποιηθούν με κακόβουλο τρόπο. Για την επίτευξη αυτού του στόχου κρίνεται απαραίτητη η ύπαρξη ασφαλών καναλιών επικοινωνίας για την ανταλλαγή δεδομένων μεταξύ των χρηστών και των φορέων. Για το λόγο αυτό, τα τελευταία χρόνια έχουν αναπτυχθεί διάφορες προσεγγίσεις βασισμένες στην κρυπτογραφία για την προστασία των χωρο-χρονικών δεδομένων των χρηστών φορητών συσκευών.

Οι βασικότερες κρυπτογραφικές μέθοδοι όι οποίες χρησιμοποιούνται στα συστήματα παροχής υπηρεσιών θέσης αφορούν την κρυπτογράφηση της ταυτότητας του χρήστη καθώς και της θέσης του, προτού οι πληροφορίες αυτές σταλούν στον παροχέα υπηρεσιών. Με την κρυπτογράφηση της ταυτότητας των χρηστών επιδιώκεται η εξασφάλιση της αυθεντικοποίησής τους από τους παραλήπτες. Επιπρόσθετα, οι χρήστες θα πρέπει να είναι σίγουροι ότι τα δεδομένα τους δε θα υποστούν οποιαδήποτε αλλοίωση ή επεξεργασία από κάποια τρίτη, μη έμπιστη πηγή. Για το λόγο αυτό, θα πρέπει όταν συλλέγονται να κρυπτογραφούνται και από τον παραλήπτη.

5.2.1 Ασύμμετρη Κρυπτογραφία ή Κρυπτογράφηση Δημοσίου (-Ιδιωτικού) Κλειδιού

Η ασύμμετρη κρυπτογραφία είναι ένα από τα βασικότερα είδη κρυπτογράφησης το οποίο εγγυάται την αυθεντικοποίηση των χρηστών ενός συστήματος. Αυτό το είδος κρυπτογράφησης απαιτεί την ύπαρξη δύο κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας των δεδομένων πριν στείλει το μήνυμα του το κρυπτογραφεί με το δημόσιο κλειδί του
παραλήπτη. Το μήνυμα αυτό μπορεί να αποκρυπτογραφηθεί μόνο από τον παραλήπτη με τη χρήση του ιδιωτικού του κλειδιού. Από την άλλη, όμως, θα πρέπει και ο εκάστοτε αποστολέας να είναι σίγουρος ότι τα δεδομένα του δε θα υποστούν οποιαδήποτε επεξεργασία (δηλαδή ανάγνωση, τροποποίηση και άλλα), από κάποια τρίτη μη εξουσιοδοτημένη οντότητα. Για να επιτευχθεί αυτός ο σκοπός θα πρέπει όταν παραλαμβάνει ο παροχέας υπηρεσιών τα δεδομένα και πριν τα αποθηκεύσει να τα κρυπτογραφήσει και αυτός με τη σειρά του με το δημόσιο κλειδί του.

Διάφορες προσεγγίσεις σε αυτό το πλαίσιο έχουν προταθεί στη βιβλιογραφία. Για παράδειγμα, οι Hauser και Kabatnik [52] προτείνουν μία αρχιτεκτονική η οποία είναι βασισμένη στην κρυπτογραφία δημόσιου - ιδιωτικού κλειδιού προκειμένου να εξασφαλιστεί η αυθεντικοποίηση των χρηστών. Για το λόγο αυτό χρησιμοποιούνται δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Πιο συγκεκριμένα, ο χρήστης αποκτά ένα «ψευδώνυμο» στο οποίο περιέχονται όσο λιγότερες προσωπικές του πληροφορίες. Το «ψευδώνυμο» αυτό είναι το ιδιωτικό του κλειδί και το γνωρίζει μόνο ο ίδιος και ο Location Server. Με το ιδιωτικό κλειδί ο παραλήπτης (Location Server) είναι σίγουρος ότι μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα δεδομένου ότι είναι ο μόνος που γνωρίζει το κλειδί αυτό. Στη συνέχεια, όμως, προκειμένου και ο αποστολέας να είναι σίγουρος ότι κάποιος τρίτος δεν θα διαβάσει τα δεδομένα του, το «ψευδώνυμο» του κρυπτογραφείται με το δημόσιο κλειδί από τον εξυπηρετητή. Τέλος, προκειμένου να επιτευχθεί ακόμα μεγαλύτερη ασφαλεία, προστίθεται ένα μοναδικό κομμάτι πληροφοριών στο ιδιωτικό κλειδί του κάθε χρήστη, το οποίο επιλέγεται ξεχωριστά για κάθε έναν από τους χρήστες και κρυπτογραφείται και αυτό μαζί με το ιδιωτικό κλειδί.
5.2.2 Ιεραρχική Κρυπτογράφηση Βασισμένη στην Ταυτότητα

Η ιεραρχική κρυπτογράφηση βασισμένη στην ταυτότητα (Hierarchical ID-Based Encryption – HIBE) είναι μία τεχνική η οποία χρησιμοποιείται συχνά στα συστήματα παροχής υπηρεσιών θέσης. Η τεχνική αυτή είναι βασισμένη στην κρυπτογράφηση βασισμένη στην ταυτότητα (Identity-Based Encryption -IBE) [9, 42], η κύρια ιδέα της οποίας είναι να αφαιρεθεί η διαδικασία διανομής του δημόσιου κλειδιού που χρησιμοποιείται στην ασύμμετρη κρυπτογραφία και να αντικατασταθεί με μία διαδικασία κατά την οποία το δημόσιο κλειδί θα προκύπτει από κάποιο γνωστό χαρακτηριστικό της ταυτότητας του χρήστη, όπως για παράδειγμα τη διεύθυνση του ηλεκτρονικού του ταχυδρομείου. Επιπρόσθετα, στην κρυπτογράφηση βασισμένη στην ταυτότητα απαιτείται μία γεννήτρια παραγωγής ιδιωτικών κλειδιών (Private Key Generator - PKG) για την εξαγωγή του ιδιωτικού κλειδιού των χρηστών. Η γεννήτρια αυτή υπολογίζει το ιδιωτικό κλειδί ως μία συνάρτηση ενός κοινού μυστικού και της ταυτότητας του χρήστη. Παράλληλα απαιτείται ένα ασφαλές κανάλι μέσω του οποίου θα πραγματοποιηθεί η αποστολή του ιδιωτικού κλειδιού από τη γεννήτρια στο χρήστη. Επιπλέον, κάποιος ο οποίος θέλει να στείλει ένα μήνυμα στον χρήστη αυτό, θα πρέπει να αναζητήσει στη γεννήτρια τις δημόσιες πληροφορίες του προκειμένου να προκύψει το δημόσιο κλειδί. Το σημαντικότερο πρόβλημα, όμως αυτού του είδους της κρυπτογραφίας αποτελεί το γεγονός ότι η γεννήτρια ιδιωτικών κλειδιών είναι μοναδική και γνωρίζει τα ιδιωτικά κλειδιά των χρηστών. Η ύπαρξη μόνο μίας γεννήτριας παραγωγής ιδιωτικών κλειδιών είναι ανεπιθύμητη για δύο λόγους. Αρχικά, η γεννήτρια θα γνωρίζει ένα πλήθος ιδιωτικών κλειδιών και το γεγονός αυτό
αυξάνει τις ανησυχίες για την ασφάλεια των ιδιωτικών δεδομένων των χρηστών. Επιπρόσθετα, σε ένα μεγάλο δίκτυο ο φόρτος της γεννήτριας για τη δημιουργία ενός πλήθους ιδιωτικών κλειδιών θα είναι πολύ μεγάλος και παράλληλα θα πρέπει να δημιουργήσει πολλά ασφαλή κανάλια για τη διαβίβαση όλων αυτών των κλειδιών. Τα προβλήματα αυτά καλείται να επιλύσει η ιεραρχική κρυπτογράφηση βασισμένη στην ταυτότητα.

Σε αυτό το είδος κρυπτογραφίας υπάρχει μία βασική γεννήτρια παραγωγής ιδιωτικών κλειδιών, η οποία κατανέμει το φόρτο εργασίας αναθέτοντας τη δημιουργία ιδιωτικών κλειδιών και την αυθεντικοποίηση της ταυτότητας των χρηστών σε άλλες χαμηλότερου επιπέδου γεννήτριες παραγωγής ιδιωτικών κλειδιών. Στην ιεραρχική κρυπτογράφηση η βασική γεννήτρια παράγει τα ιδιωτικά κλειδιά για τις άλλες γεννήτριες οι οποίες με τη σειρά τους παράγουν τα ιδιωτικά κλειδιά των χρηστών τους. Η αυθεντικοποίηση και η μετάδοση των ιδιωτικών κλειδιών μπορούν να γίνουν τοπικά. Για να στείλει κάποιος ένα μήνυμα σε κάποιο άλλο άτομο θα πρέπει να γνωρίζει τις δημόσιες παραμέτρους από τη βασική του γεννήτρια. Ένα σημαντικό πλεονέκτημα αυτών των μοντέλων κρυπτογραφίας είναι ο έλεγχος ζημιών, αφού η αποκάλυψη ενός μυστικού από μία χαμηλότερου επιπέδου γεννήτρια δεν αποκαλύπτει μυστικά από τις υψηλότερου επιπέδου γεννήτριες.

Σε αυτό το πλαίσιο οι Horwitz και Lynn [55] παρουσιάζουν την ιεραρχική, βασισμένη στην ταυτότητα, κρυπτογράφηση και προτείνουν μία ιεραρχία 2-επιπέδων. Το μοντέλο αυτό αποτελείται από μία κύρια γεννήτρια παραγωγής ιδιωτικών κλειδιών, άλλες χαμηλότερου επιπέδου γεννήτριες και τους χρήστες. Όλοι οι χρήστες συνδέονται με κάποια αρχικά αναγνωριστικά (IDs) οποία είναι αυθαίρετα αλφαριθμητικά. Το δημόσιο κλειδί του χρήστη αποτελείται από αυτή την αρχική του ταυτότητα και το αναγνωριστικό της θέσης του, που καλείται διεύθυνση. Οι χρήστες αποκτούν το ιδιωτικό τους κλειδί από τη γεννήτρια χαμηλότερου επιπέδου στην οποία ανήκουν. Αυτές οι γεννήτριες μπορούν να υπολογίσουν το ιδιωτικό κλειδί οποιουδήποτε χρήστη ανήκει σε αυτές, εφόσον προηγουμένως έχουν ζητήσει το μυστικό κλειδί του συγκεκριμένου χρήστη από τη βασική γεννήτρια.
Οι Hengartner και Steenkiste [53] συζητούν τις ανεπάρκειες στα υπάρχοντα συστήματα ελέγχου πρόσβασης που στηρίζονται είτε στους χρήστες οι οποίοι παρουσιάζουν μία απόδειξη για την πρόσβασή τους σε κάποια υπηρεσία, είτε στις υπηρεσίες οι οποίες κρυπτογραφούν τις πληροφορίες πριν τις δώσουν σε κάποιο χρήστη. Ως λύση, προτείνουν μία αρχιτεκτονική ελέγχου πρόσβασης στις πληροφορίες η οποία υιοθετεί την ιεραρχική κρυπτογράφηση βασισμένη στην ταυτότητα. Ο βασικός στόχος της αρχιτεκτονικής αυτής είναι να ενημερώνουν οι υπηρεσίες τους χρήστες για την απαραίτητη απόδειξη της προσπέλασής τους με έναν ασφαλή τρόπο χωρίς να διαρρέουν οι πληροφορίες. Επιπλέον, οι συγγραφείς προτείνουν μία αρχιτεκτονική ελέγχου πρόσβασης η οποία είναι βασισμένη στην κρυπτογράφηση προκειμένου να εξεταστούν οι πολλαπλοί ιεραρχικοί περιορισμοί και τα δικαιώματα πρόσβασης. Στην προηγούμενη αρχιτεκτονική τα δικαιώματα πρόσβασης ενός χρήστη συγκεκριμένων ήταν απαραίτητα για την απαραίτητη απόδειξη πρόσβασης, η οποία καταδεικνύει σε μία υπηρεσία ότι ο πελάτης έχει εξουσιοδοτηθεί να έχει πρόσβαση στις πληροφορίες που ζητά. Με αυτό τον τρόπο αποφεύγεται ο «ακριβός» στόχος της δημιουργίας των δικαιωμάτων πρόσβασης των χρηστών από την κάθε υπηρεσία. Στην αρχιτεκτονική ελέγχου πρόσβασης υιοθετούνται κρυπτογραφία υπηρεσία μία υπηρεσία που τα δικαιώματα πρόσβασης είναι απλά μόνο σε κρυπτογραφημένη μορφή. Οι πελάτες οι οποίοι είναι εξουσιοδοτημένοι να έχουν πρόσβαση στις συγκεκριμένες πληροφορίες κατέχουν και τα αντίστοιχα κλειδιά αποκρυπτογράφησης και, επομένως, έχουν τη δυνατότητα να τις διαβάσουν. Οπως αναφέραμε και παραπάνω, τα δημόσια κλειδιά των πελατών αποτελούν αυθαίρετα αλφαριθμητικά και έτσι η διαχείριση και η εξατομίκευση των δικαιωμάτων προσπέλασης είναι απλές. Σε αυτή την προσέγγιση, οι συγγραφείς έχουν επεκτείνει τα ιεραρχικά σχέδια κρυπτογράφησης ώστε να υποστηρίζουν πολλαπλές ιεραρχίες.
5.2.3 Άλλες Κρυπτογραφικές Προσεγγίσεις

Διάφορες άλλες κρυπτογραφικές προσεγγίσεις για τα συστήματα παροχής υπηρεσιών θέσης έχουν προταθεί στη βιβλιογραφία. Για παράδειγμα, οι Zhu και Li [122], προτείνουν μία αρχιτεκτονική η οποία αποτελείται από τρεις συνιστώσες: τις συσκευές, τους διαμεσολαβητές και τους εξυπηρετητές. Οι συσκευές μπορεί να είναι οποιαδήποτε συσκευή με ασύρματο κανάλι επικοινωνίας και οι διαμεσολαβητές είναι προγράμματα τα οποία τρέχουν στους υπολογιστές του δικτύου. Υποθέτουμε ότι οι και οι τρεις συνιστώσες της αρχιτεκτονικής μπορούν να εκτελέσουν συμμετρικούς κρυπτογραφικούς αλγόριθμους και έχουν ενσωματωμένο ένα συμμετρικό κλειδί. Αυτό το κλειδί χρησιμοποιείται για την ασφαλή επικοινωνία των συσκευών με τους διαμεσολαβητές. Για κάθε συσκευή θα πρέπει να υπάρχει ένας διαμεσολαβητής τον οποίον να εμπιστεύεται. Τέλος, χρησιμοποιούνται πρωτόκολλα για τη δημιουργία ασφαλών καναλιών επικοινωνίας ανάμεσα σε δύο διαμεσολαβητές, δύο εξυπηρετητές, καθώς και ανάμεσα σε ένα διαμεσολαβητή και έναν εξυπηρετητή.

Μία διαφορετική προσέγγιση αποτελεί αυτή των Konidala et al [66], οι οποίοι προτείνουν ένα μοντέλο εμπιστοσύνης για τα ασύρματα υπολογιστικά συστήματα προκειμένου να παρέχονται ασφαλείς υπηρεσίες. Το πρωτόκολλο που προτείνουν αποτελείται από τρεις βασικές οντότητες: τους χρήστες, τους χειριστές κινητών υπηρεσιών (mobile operators - MO) και τους παροχείς υπηρεσιών. Αρχικά, οι χρήστες πρέπει να εγκαταστήσουν ένα απαραίτητο λογισμικό στο κινητό τους τηλέφωνο. Το λογισμικό αυτό απαιτείται για την εκτέλεση των διαδικασιών που περιλαμβάνονται στο πρωτόκολλο που προτείνεται και μπορεί να βρεθεί είτε στον ιστοχώρο είτε στο κοντινότερο κέντρο εξυπηρέτησης πελατών του MO. Το λογισμικό αυτό βοηθά στην
παραγωγή ενός κύριου μυστικού κλειδιού το οποίο είναι κοινό μεταξύ του
χρήστη και του MO. Αυτό το μυστικό κλειδί μπορεί να αποθηκεύεται στην
κάρτα SIM του κινητού προκειμένου να συμπεριλαμβάνεται στη συσκευή του
χρήστη. Παράλληλα, το κλειδί αυτό αποθηκεύεται στη βάση δεδομένων του
MO. Επομένως, ο MO παράγει για κάθε χρήστη ένα διαφορετικό κλειδί το
οποίο διατηρεί και ο ίδιος. Προκειμένου να εξασφαλίσει η επικοινωνία μεταξύ
MO και παροχέων υπηρεσιών υπάρχει μία εμπιστευτική υποδομή δημόσιου
κλειδιού (Public Key Infrastructure - PKI). O MO λαμβάνει ένα ψηφιακό
πιστοποιητικό και έναν ιδιωτικό κλειδί. Όμοια, ο παροχέας υπηρεσιών λαμβάνει
με τη σειρά του το ψηφιακό πιστοποιητικό και τον ιδιωτικό κλειδί από μία
πιστοποιημένη αρχή. O MO αποθηκεύει το ψηφιακό πιστοποιητικό το οποίο
περιλαμβάνει το δημόσιο κλειδί του παροχέα υπηρεσιών και ο παροχέας
αποθηκεύει το δικό του ψηφιακό πιστοποιητικό το οποίο περιλαμβάνει το
dημόσιο κλειδί του MO στις αντίστοιχες βάσεις δεδομένων τους. Με τον τρόπο
αυτό εξασφαλίζεται η εμπιστοσύνη μεταξύ των χρηστών και των MO, καθώς
και μεταξύ των MO και των παροχέων υπηρεσιών.

5.3 Κ-ανωνυμία

Η ανωνυμία αποτελεί ένα από τα πιο σημαντικά χαρακτηριστικά των
υποκειμένων των δεδομένων το οποίο πρέπει να προστατεύει στα σύγχρονα
υπολογιστικά περιβάλλοντα. Ακόμα και αν πραγματοποιηθεί η μεταφορά των
dεδομένων και η χρησιμοποίησή τους για διάφορους σκοπούς (ακόμα και για
dιαφορετικούς από τους αρχικούς σκοπούς συλλογής τους), θα πρέπει να
συμβαίνει με τέτοιον τρόπο ώστε η ταυτότητα του χρήστη, η οποία περιέχεται
στα δεδομένα, να μην μπορεί να αναγνωριστεί.
Γενικά επικρατεί η λαθεμένη εντύπωση ότι τα δεδομένα τα οποία μοιάζουν ανώνυμα είναι πράγματι ανώνυμα. Δηλαδή, αν σε μία βάση δεδομένων απαλειφθούν όλα τα σαφή αναγνωριστικά από τα δεδομένα, όπως το όνομα, η διεύθυνση και ο αριθμός τηλεφώνου, ενώ οι υπόλοιπες πληροφορίες μπορούν να διαμοιραστούν ελεύθερα, δεν σημαίνει ότι η ταυτότητα του χρήστη δεν μπορεί να προσδιοριστεί. Αντίθετα, οι πληροφορίες οι οποίες δεν φανερώνουν σαφώς την ταυτότητα του χρήστη δεν εγγυώνται την ανωνυμία του. Πιο συγκεκριμένα, οι πληροφορίες αυτές ενδέχεται να περιέχουν άλλα δεδομένα, όπως η ημερομηνία γέννησης, το γένος και άλλα, τα οποία αν συνδυαστούν μπορούν να φανερώσουν την ταυτότητα των υποκειμένων τους [65, 94]

Σε μία βάση δεδομένων στην οποία συλλέγονται προσωπικές πληροφορίες των ατόμων, τα χαρακτηριστικά, των οποίων οι τιμές (σε συνδυασμό) μπορούν να συνδεθούν με εξωτερικές πληροφορίες για να αναγνωριστούν τα άτομα στα οποία αναφέρονται, ονομάζονται Quasi-identifiers – QIDs. Όταν τα χαρακτηριστικά αυτά αποτελούν συγκεκριμένες ακολουθίες χώρου και χρόνου (<τοποθεσία, χρονική στιγμή>), οι οποίες ακολουθούνται από τους χρήστες κατ’ επανάληψη (παραδείγματος χάριν για 2 εβδομάδες), ονομάζονται Location-Based QIDs – LBQIDs. Παράδειγμα ενός LBQID αποτελεί η εξής αναπαράσταση:

<Σπίτι [7 π.μ., 8 π.μ.], Γραφείο [8 π.μ., 3 μ.μ.], Σπίτι [3 μ.μ., 5 μ.μ.]

Επανάληψη: 3.μέρες * 2.εβδομάδες.

Η παραπάνω αναπαράσταση δείχνει ότι η ίδια χωρο-χρονική ακολουθία παρατηρήθηκε για τρεις μέρες της εβδομάδας και για τουλάχιστον 2 εβδομάδες [121].

Η πιο σημαντική τεχνική προστασίας της ταυτότητας των χρηστών είναι η K-ανωνυμία [18, 65, 103, 104, 106]. Στα σύγχρονα συστήματα υπηρεσιών θέσης, οι παρεχόμενες υπηρεσίες βασίζονται στην απαίτηση της γνώσης της θέσης των χρηστών. Για παράδειγμα, στην περίπτωση όπου ένας χρήστης αιτηθεί την εύρεση του κοντινότερου νοσοκομείου ως προς τη θέση και την κατεύθυνσή του, η χρήση ενός ψευδωνύμου (για παράδειγμα μίας πλαστής ταυτότητας) δεν εξασφαλίζει την ανωνυμία του, εφόσον η γνώση της θέσης του μπορεί να αποκαλύψει την πραγματική του ταυτότητα. Σε αυτή την
περίπτωση δεν επιδιώκεται να προστατευθεί ένα κομμάτι πληροφοριών από την αποκάλυψη, αλλά επιδιώκεται να προστατευθεί η αποκάλυψη του ατόμου στο οποίο αναφέρονται οι συγκεκριμένες πληροφορίες με τη μέθοδο της Κ-ανωνυμίας. Η βασική αρχή για να επιτευχθεί Κ-ανωνυμία είναι αν η χωρο-χρονική περιοχή, από την οποία έγινε η αίτηση του χρήστη και η οποία γνωστοποιείται στον παροχέα υπηρεσιών, αντιστοιχίζεται σε τουλάχιστον Κ άτομα κατά τέτοιον τρόπο ώστε να είναι αδύνατη η εύρεση της ταυτότητας του χρήστη με πιθανότητα μεγαλύτερη του 1/Κ.

Η αρχή της Κ-ανωνυμίας βρίσκει εφαρμογή και σε δεδομένα συναλλαγών. Εκεί, η βασική αρχή για να επιτευχθεί ανωνυμία είναι αν για κάθε εγγραφή υπάρχουν ακόμη τουλάχιστον Κ-1 εγγραφές των οποίων οι τιμές κάποιων χαρακτηριστικών, όπως η περιοχή που βρίσκεται, το γένος, το έτος γέννησης και άλλα, είναι ίδιες, τότε γνωρίζοντας και συνδυάζοντας όλα αυτά τα χαρακτηριστικά θα προκύπτουν Κ άτομα [4, 103, 106]. Σε αυτό το σημείο θα πρέπει να σημειωθεί ότι τα χαρακτηριστικά αυτά μπορεί να υπάρχουν και σε άλλα σύνολα δεδομένων.

Έστω ότι έχουμε ένα σύνολο από δεδομένα τα οποία αναφέρονται σε συγκεκριμένες πληροφορίες των ατόμων και περιέχουν και τις πληροφορίες θέσης τους. Τα δεδομένα αυτά οργανώνονται σε έναν πίνακα στον οποίον οι γραμμές φανερώνουν τις εγγραφές των χρηστών και οι στήλες τα χαρακτηριστικά τους τα οποία αποτελούνται από ένα σύνολο διαφόρων τιμών. Η κάθε γραμμή δεν είναι απαραίτητα μοναδική, ενώ οι στήλες δεν συσχετίζονται. Παρακάτω παραθέτουμε ένα παράδειγμα ενός πίνακα ο οποίος αποτελείται από χαρακτηριστικά στα οποία συμπεριλαμβάνονται χωρο-χρονικά δεδομένα. Υποθέτουμε ότι QIDs είναι τα χαρακτηριστικά: περιοχή (π1, π2,...), χρόνος (t1, t2...), έτος γέννησης και γένος (Α/Θ – αρσενικό/θηλυκό), όταν οι τιμές τους συνδυάζονται.
ΤιμήΣ 5.1 Κ-ανωνυμία με K = 2 και QIDs = {περιοχή, χρόνος, έτος γέννησης, γένος}.

<table>
<thead>
<tr>
<th>Περιοχή</th>
<th>Χρόνος</th>
<th>Έτος γέννησης</th>
<th>Γένος</th>
<th>Χρήστης</th>
</tr>
</thead>
<tbody>
<tr>
<td>Π1</td>
<td>t1</td>
<td>1980</td>
<td>Α</td>
<td>χ1</td>
</tr>
<tr>
<td>Π2</td>
<td>t2</td>
<td>1982</td>
<td>Α</td>
<td>χ2</td>
</tr>
<tr>
<td>Π1</td>
<td>t2</td>
<td>1983</td>
<td>Θ</td>
<td>χ3</td>
</tr>
<tr>
<td>Π1</td>
<td>t1</td>
<td>1980</td>
<td>Α</td>
<td>χ4</td>
</tr>
<tr>
<td>Π2</td>
<td>t2</td>
<td>1982</td>
<td>Α</td>
<td>χ5</td>
</tr>
<tr>
<td>Π2</td>
<td>t1</td>
<td>1981</td>
<td>Θ</td>
<td>χ6</td>
</tr>
<tr>
<td>Π1</td>
<td>t2</td>
<td>1983</td>
<td>Θ</td>
<td>χ7</td>
</tr>
<tr>
<td>Π2</td>
<td>t1</td>
<td>1981</td>
<td>Θ</td>
<td>χ8</td>
</tr>
</tbody>
</table>

Αν υποθέσουμε ότι τα χαρακτηριστικά {περιοχή, χρόνος, έτος γέννησης, γένος} μπορούν να χρησιμοποιηθούν για την ανακάλυψη της ταυτότητας των χρηστών, ο πίνακας αυτός εξασφαλίζει 2-ανωνυμία διότι κάθε ένα σύνολο αυτών των χαρακτηριστικών αντιστοιχίζεται σε δύο χρήστες. Παραδείγματος χάριν, οι χρήστες χ1 και χ4 βρίσκονται στην ίδια περιοχή (π1), την ίδια χρονική στιγμή (t1), ενώ έχουν γεννηθεί την ίδια χρονιά (1980) και είναι του ίδιου γένους (Α).

Ο στόχος, όμως, είναι να ελαχιστοποιηθεί η πιθανότητα να ανακαλυφθεί η ταυτότητα ενός χρήστη όταν συνδυαστούν οι πληροφορίες από
έναν τέτοιο πίνακα με τις πληροφορίες κάποιου άλλου. Υποθέτουμε λοιπόν, ότι έχουμε μία εταιρία κινητής τηλεφωνίας η οποία αποθηκεύει τα δεδομένα των πελατών της χρησιμοποιώντας ένα ψευδόνυμο για κάθε της χρήστη. Έστω, λοιπόν, ότι έχουμε τον παρακάτω πίνακα:

<table>
<thead>
<tr>
<th>Περιοχή</th>
<th>Χρόνος</th>
<th>Ψευδόνυμο</th>
</tr>
</thead>
<tbody>
<tr>
<td>π1</td>
<td>t1</td>
<td>ψ1</td>
</tr>
<tr>
<td>π2</td>
<td>t2</td>
<td>ψ2</td>
</tr>
<tr>
<td>π2</td>
<td>t2</td>
<td>ψ1</td>
</tr>
<tr>
<td>π1</td>
<td>t1</td>
<td>ψ3</td>
</tr>
</tbody>
</table>

Πίνακας 5.2 Κ-ανωνυμία με K = 2 και QIDs = {περιοχή, χρόνος}.

Αν θεωρήσουμε ότι τα QIDs είναι η περιοχή και ο χρόνος έχουμε πάλι 2-ανωνυμία, αφού για κάθε τέτοιο ζεύγαρι αντιστοιχούν δύο ψευδόνυμα. Έστω, όμως, ότι υπάρχει και ένας άλλος πίνακας διαθέσιμος με τον οποίον μπορούν να συνδυαστούν τα δεδομένα του προηγούμενου πίνακα:

<table>
<thead>
<tr>
<th>Περιοχή</th>
<th>Χρόνος</th>
<th>Χρήστης</th>
</tr>
</thead>
<tbody>
<tr>
<td>π1</td>
<td>t1</td>
<td>χ1</td>
</tr>
<tr>
<td>π2</td>
<td>t2</td>
<td>χ2</td>
</tr>
<tr>
<td>π2</td>
<td>t2</td>
<td>χ1</td>
</tr>
<tr>
<td>π1</td>
<td>t1</td>
<td>χ3</td>
</tr>
</tbody>
</table>

Πίνακας 5.3 Κ-ανωνυμία με K = 2 και QIDs = {περιοχή, χρόνος}.
Ο πίνακας αυτός αν θεωρήσουμε ότι έχει QIDs την περιοχή και τον χρόνο ικανοποιεί τις συνθήκες της 2-ανωνυμίας. Αν όμως συνδυαστούν οι πίνακες 4.2 και 4.3, τότε παραβιάζεται η ανωνυμία αφού αποκαλύπτεται ότι το ψευδώνυμο ψι αντιστοιχεί στον χρήστη χ1.

5.3.1 Κ-ανωνυμία Κατά τη Συλλογή της Θέσης

Γενικά, στα συστήματα παροχής υπηρεσιών θέσης υπάρχουν δύο είδη απαιτήσεων προστασίας της ιδιωτικότητας των χρηστών [118]:

Ανωνυμία θέσης: πρόκειται για την προστασία της θέσης που βρίσκεται ένας χρήστης και ειδικότερα όταν οι πληροφορίες θέσης είναι ευαίσθητες, όπως για παράδειγμα αν ο χρήστης βρίσκεται σε ένα νοσοκομείο.

Ανωνυμία προσδιοριστικών: πρόκειται για την προστασία των προσδιοριστικών των χρηστών, ειδικά όταν σε αυτά περιέχονται ευαίσθητα δεδομένα, όπως οικονομικά στοιχεία.

Μία κοινή τεχνική για την προστασία των δύο αυτών ειδών απαιτήσεων προστασίας της μυστικότητας είναι η γενικεύση των περιοχών που αναλύονται. Πιο συγκεκριμένα, η τεχνική αυτή απαιτεί την επέκταση των περιοχών που αναλύονται προκειμένου να είναι αρκετά μεγάλες ώστε στην ίδια περιοχή να βρίσκονται τουλάχιστον ακόμα K-1 χρήστες. Με αυτόν τον τρόπο επιτυγχάνουμε την ανωνυμία θέσης. Αντίστοιχα, αν οι περιοχές επεκταθούν έτσι ώστε στην περιοχή όπου βρίσκεται κάποιος χρήστης που αιτείται μία υπηρεσία βρίσκονται τουλάχιστον ακόμα K-1 χρήστες, δεν μπορεί να προσδιοριστεί ποιος από τους K χρήστες αιτήθηκε κάποια συγκεκριμένη υπηρεσία και έτσι επιτυγχάνεται ανωνυμία προσδιοριστικών.
Στην παρακάτω εικόνα φαίνεται μία περίπτωση επέκτασης μίας περιοχής προκειμένου να επιτευχθεί η ανωνυμία ενός χρήστη. Πιο συγκεκριμένα, οι χρήστες υπηρεσιών θέσης στην περιοχή της εικόνας αναπαρίστανται με χρωματιστές κουκίδες. Ας υποθέσουμε ότι ο χρήστης που αναπαρίσταται με κόκκινη κουκίδα αιτείται κάποιας υπηρεσίας. Ένας τρόπος για να επιτύχουμε K-ανωνυμία είναι να επεκτείνουμε την περιοχή του ώστε να συμπεριλαμβάνει και άλλους χρήστες, ώστε να μην μπορεί να προσδιοριστεί ποιος από τους χρήστες είναι αυτός που αιτήθηκε τη συγκεκριμένη υπηρεσία. Για παράδειγμα, στο κόκκινο πλαίσιο της εικόνας φαίνεται μία πιθανή επέκταση της περιοχής του χρήστη που αναπαρίσταται από την κόκκινη κουκίδα. Με αυτόν τον τρόπο στην περιοχή τώρα περιέχονται τρεις χρήστες και επομένως δεν μπορεί να αναγνωριστεί ποιος χρήστης έκανε την αίτηση. Άρα έχει επιτευχθεί 3-ανωνυμία.
Εικόνα 5.1 Παράδειγμα επέκτασης περιοχής για την ανωνυμία των χρηστών.

Σε αυτό το πλαίσιο, διάφορες προσεγγίσεις επέκτασης της θέσης των χρηστών προκειμένου να επιτευχθεί η ανωνυμία έχουν προταθεί στη βιβλιογραφία. Στα πλαίσια των υπηρεσιών θέσης οι Gruteser και Grunwald [48] υιοθέτησαν ένα μοντέλο βασισμένο στην Κ-ανωνυμία προτείνοντας έναν αλγόριθμο επέκτασης των περιοχών. Αρχικά, υποθέτουν ότι η υπηρεσία απαιτεί έναν ελάχιστο αριθμό K για όλους τους χρήστες. Ο αλγόριθμος λειτουργεί ως εξής: όταν στέλνεται η θέση του χρήστη, ο χώρος συνολικά υποδιαιρείται με βάση τη λογική των τετραδικών δέντρων σε τεταρτημόρια με γνώμονα κάθε τεταρτημόριο να περιέχει τον χρήστη. Η υποδιαιρέση του χώρου συνεχίζεται έως ότου λιγότεροι από Κ χρήστες βρίσκονται στην περιοχή. Ο αλγόριθμος
επιστρέφει το αμέσως προηγούμενο τεταρτημόριο και το θέτει σαν την περιοχή του χρήστη. Βέβαια, σε αυτή την προσέγγιση δεν υπάρχει κανένας περιορισμός στο πόσο μεγάλη θα είναι η περιοχή που θα επιστραφεί από τον αλγόριθμο. Το γεγονός αυτό μπορεί να οδηγήσει σε ανεπαρκή ποιότητα υπηρεσιών.

Μία άλλη προσέγγιση είναι αυτή των Gedik και Liu [41], οι οποίοι προτείνουν ένα εξατομικευμένο μοντέλο K-ανωνυμίας για την παροχή ιδιωτικότητας της χωρικής συνιστώσας των κινούμενων οντοτήτων. Το μοντέλο που προτείνουν έχει δύο χαρακτηριστικά γνωρίσματα. Αρχικά, επιτρέπει σε κάθε κινητό κόμβο να καθορίσει την ελάχιστη απαίτηση του επεξέδου ανονυμίας του, καθώς επίσης και τα ανώτερα όρια ανοχής σφαλμάτων για τις χωρικές και χρονικές διαστάσεις. Επιπρόσθετα, εφαρμόζει το μοντέλο αυτό χρησιμοποιώντας έναν χωρο-χρονικό αλγόριθμο. Ο αλγόριθμος αυτός λειτουργεί ως εξής: κάθε φορά που κάποιος χρήστης αιτείται μίας υπηρεσίας τον θέτει σαν κόμβο ενός γράφου. Λαμβάνοντας υπόψη τους περιορισμούς επέκτασης περιοχής, αναζητά αν υπάρχουν άλλοι χρήστες στην επιτρεπόμενη γενικευμένη περιοχή και, αν υπάρχουν, οι αντίστοιχοι κόμβοι του γράφου συνδέονται. Όταν ο αριθμός των χρηστών που συνδέονται γίνει K εξυπηρετούνται οι αιτήματά τους. Στην υλοποίηση του αλγορίθμου λαμβάνονται υπόψη και η μέγιστη καθυστέρηση η οποία είναι αποδεκτή από τον χρήστη για την εξυπηρέτηση των αιτημάτων του. Ο αλγόριθμος αυτός μπορεί να επιφέρει αποτελεσματικά την ανονυμία των μηνυμάτων, ενώ παράλληλα ικανοποιεί τις απαιτήσεις ανωνυμίας και ακρίβειας των μηνυμάτων.

Επίσης, ο Kido [65] προτείνει μία τεχνική ανώνυμης επικοινωνίας προκειμένου να προστατευθεί η ιδιωτικότητα της χωρικής συνιστώσας. Πιστεύει ότι η ανονυμία της θέσης είναι το πιο βασικό χαρακτηριστικό το οποίο πρέπει να προστατευθεί στα συστήματα κινητών υπηρεσιών. Για το λόγο αυτό προτείνει ένα μοντέλο το οποίο αποτελείται από δύο μέτρα. Το πρώτο μέτρο υποθέτει ότι το Κ φανερώνει τον αριθμό των περιοχών στις οποίες βρίσκονται οι χρήστες. Αν οι χρήστες ικανοποιούν την K-ανονυμία τότε ο αριθμός των περιοχών στις οποίες βρίσκονται οι χρήστες είναι αυτός του Κ. Πρώτο τρόπο, επιτυχάνεται η ανονυμία της περιοχής που βρίσκεται ο κάθε χρήστης. Το δεύτερο μέτρο, υποθέτει ότι το Κ φανερώνει τον αριθμό των
χρηστών σε μία περιοχή. Αν ένας χρήστης ο οποίος βρίσκεται σε μία συγκεκριμένη περιοχή ικανοποιεί την K-ανωνυμία, τότε ο αριθμός των χρηστών σε αυτή την περιοχή είναι τουλάχιστον K. Με τον τρόπο αυτό επιτυγχάνεται η ανωνυμία της θέσης των χρηστών μίας συγκεκριμένης περιοχής.

Τέλος, οι Xiao et al [118] παρουσιάζουν ένα μοντέλο ανωνυμίας για την προστασία ιδιωτικότητας της θέσης των χρηστών, ενώ παράλληλα ο κάθε χρήστης διευκρινίζει τις απαιτήσεις ποιότητας υπηρεσιών. Στο μοντέλο αυτό ο κινητός χρήστης μπορεί να καθορίσει τις εξής απαιτήσεις του: a) το ελάχιστο επίπεδο ανωνυμίας K, το οποίο δείχνει την απαιτούμενη επέκταση των περιοχών προκειμένου να επιτυγχάνει τόσο ανωνυμία θέσης, όσο και ανωνυμία αναγνωριστικών των χρηστών, β) τη μέγιστη καθυστέρηση για την πραγματοποίηση της επέκτασης περιοχών την οποία μπορεί να ανεχθεί, γ) τη μέγιστη επέκταση περιοχών που δείχνει το μέγιστο ανεκτό λάθος στα δεδομένα θέσης. Το K σχετίζεται με την ιδιωτικότητα της θέσης των χρηστών, ενώ οι άλλες δύο τιμές που καθορίζει ο χρήστης αντιπροσωπεύουν τις απαιτήσεις ποιότητας των παραχόμενων υπηρεσιών. Τέλος, οι τιμές αυτές μπορούν να αλλάζουν σε κάθε αίτηση του χρήστη του δεδομένου ότι οι χρήστες μπορεί να έχουν διαφορετικές απαιτήσεις ανωνυμίας και ποιότητας υπηρεσιών ανάλογα με την αίτησή τους. Για αυτούς τους λόγους αναπτύχθηκαν ένα αλγόριθμο επέκτασης των περιοχών προκειμένου να επιτύχουν ανωνυμία κατά την αίτηση των υπηρεσιών θέσης, καθώς και να προστατευθεί η ποιότητα υπηρεσιών. Επιπλέον, προτείνουν μία βελτίωση του αλγορίθμου εισάγοντας την επέκταση περιοχών σε περίπτωση αποτυχίας της επέκτασης περιοχών. Βέβαια, σε αυτή την προσέγγιση χρησιμοποιούν όσο το δυνατό λιγότερες πλαστές θέσεις προκειμένου να ελαχιστοποιήσουν τα έξοδα επικοινωνίας.
5.4 Επίλογος

Για την προστασία της ιδιωτικότητας των δεδομένων και τη διατήρηση της ανωνυμίας των χρηστών στους οποίους ανήκουν δεν αρκεί μόνο η νομοθετική προσέγγιση αλλά και η τεχνολογική. Τα τελευταία χρόνια όλο και περισσότεροι ερευνητές στρέφουν την προσοχή τους στις μεθόδους οι οποίες πρέπει να χρησιμοποιηθούν για τη δημιουργία ασφαλών και έμπιστων συστημάτων. Λόγω της ραγδαίας αύξησης της συλλογής χρω-χρονικών δεδομένων από ανθρώπους και οργανισμούς οι προσεγγίσεις των τελευταίων ετών αφορούν κυρίως στα χρω-χρονικά δεδομένα. Διάφορες μέθοδοι και αρχιτεκτονικές συστημάτων έχουν προταθεί για την προστασία αυτού του είδους πληροφοριών. Πολλοί ερευνητές υποστηρίζουν ότι ο σημαντικότερος παράγοντας που πρέπει να προστατευθεί σε αυτού του είδους τα δεδομένα αποτελεί η χωρική διάσταση. Άλλοι ερευνητές έχουν στρέψει την προσοχή τους στην προσπάθεια διατήρησης της ανωνυμίας των δεδομένων προκειμένου να αποφευχθεί η παραβίαση της ταυτότητας των υποκειμένων τους, δεδομένου ότι με την παγκόσμια αύξηση χρήσης του διαδικτύου τα δεδομένα μπορούν να μεταφέρονται ελεύθερα και να συνδυάζονται με άλλες πληροφορίες.

Σε αυτό το κεφάλαιο εξετάσαμε τις βασικότερες μεθόδους προστασίας της ιδιωτικότητας των πληροφοριών. Αρχικά αναλύσαμε μία βασική προσέγγιση για τη δημιουργία ασφαλών συστημάτων, τις πολιτικές ασφαλείας. Οι πολιτικές αυτές αποτελούνται από κανόνες που προδιδούν τα δικαιώματα των συμμετεχόντων για την προσέλαση στα δεδομένα. Τις περισσότερες φορές, όμως, αυτή η μέθοδος δεν είναι αρκετή αφού κάποια τρίτη μη-έμπιστη πηγή μπορεί να επιτεθεί στο σύστημα και να υποκλέψει τα δεδομένα. Για το λόγο αυτό τα περισσότερα συστήματα χρησιμοποιούν κρυπτογραφικές μεθόδους προκειμένου να εξασφαλίσουν την αυθεντικοποίηση...
των χρηστών τους αλλά και την εμπιστευτικότητα και ακεραιότητα των συλλεγόμενων πληροφοριών τους. Παρουσιάσαμε διάφορες κρυπτογραφικές μεθόδους που προτείνονται στην βιβλιογραφία για την προστασία, κυρίως, των χωρο-χρονικών δεδομένων.

Τέλος, εξετάσαμε μία από τις βασικότερες μεθόδους που χρησιμοποιείται στα χωρο-χρονικά δεδομένα για τη διατήρηση της ανωνυμίας των υποκειμένων τους, την Κ-ανωνυμία. Η μέθοδος αυτή δεν παρέχει ασφάλεια στα ιδία τα δεδομένα, αλλά στην ταυτότητα του προσώπου στο οποίο ανήκουν τα δεδομένα, η οποία ακόμα και αν τα δεδομένα μεταφερθούν ελεύθερα ανά τον κόσμο δεν θα πρέπει να προσδιοριστεί.
Κεφάλαιο 6

Συστήματα Διασφάλισης της Ιδιωτικότητας Θέσης των Χρηστών

Τα υπάρχοντα συστήματα παροχής υπηρεσιών θέσης προστατεύουν τους χρήστες τους χρησιμοποιώντας τεχνικές κρυπτογράφησης για την προστασία των καναλιών επικοινωνίας και ψευδώνυμα για την προστασία της ταυτότητας των χρηστών. Εντούτοις, η θέση των χρηστών μπορεί να προκύψει από το περιεχόμενο των αιτήσεών τους. Επί παραδείγματι, αν ένας χρήστης αιτηθεί την εύρεση του κοντινότερου προς αυτόν πολυκαταστήματος, μπορεί αυτόματα να αποκαλυφθεί η θέση στην οποία βρίσκεται και συνεπώς να προσδιοριστεί η ταυτότητά του. Η παραδοσιακή προσέγγιση των ψευδωνύμων των χρηστών (για παράδειγμα χρησιμοποιώντας μία πλαστή ταυτότητα) δεν βρίσκει εφαρμογή σε τέτοιου είδους υπηρεσίες αφού οι πληροφορίες θέσης γίνονται γνωστές προκειμένου να γίνει δυνατή η χρήση των προσφερόμενων υπηρεσιών από το χρήστη. Επομένως, στα υπάρχοντα συστήματα, προκειμένου κάποιος χρήστης να κρατήσει μυστικές τις πληροφορίες θέσης
του θα πρέπει να θέσει προσωρινά εκτός λειτουργίας τη φορητή συσκευή του.

Προκειμένου να αντιμετωπιστούν αυτά τα προβλήματα, διάφοροι ερευνητές έχουν προτείνει συστήματα για τη διασφάλιση της ιδιωτικότητας των πληροφοριών θέσης των χρηστών. Το βασικότερο χαρακτηριστικό των συστημάτων αυτών είναι η ύπαρξη ενός έμπιστου εξυπηρετητή ανάμεσα στους χρήστες και τους φορείς παροχής υπηρεσιών θέσης. Οι χρήστες εγκαθιστούν μία ασφαλή σύνδεση με τον έμπιστο εξυπηρετητή. Όταν ένας χρήστης αιτηθεί κάποια υπηρεσία, ο εξυπηρετητής αφαιρεί την ταυτότητά του από την αίτηση και διαβιβάζει τη μετασχηματισμένη αίτηση στον φορέα παροχής υπηρεσιών θέσης. Οι παροχείς υπηρεσιών θέσης υπολογίζουν την απάντηση βασιζόμενοι στη γενικευμένη θέση των χρηστών. Απομένοντας, η απάντηση που στέλνουν αποτελεί ένα υπερσύνολο της απάντησης που πρέπει να σταλεί πίσω στο χρήστη. Για το λόγο αυτό, η απάντηση από τον φορέα διαβιβάζεται στον εξυπηρετητή ανωνυμίας, ο οποίος με τη σειρά του φιλτράρει το αποτέλεσμα βάσει της πραγματικής θέσης και το στέλνει στο χρήστη.

Στο κεφάλαιο αυτό, θα εξετάσουμε τα βασικότερα συστήματα που προτείνονται στη βιβλιογραφία. Πιο συγκεκριμένα, στην παράγραφο 6.1 θα περιγράψουμε ένα σύστημα που βασίζεται στην επέκταση των χωρικών περιοχών για την προστασία της ανωνυμίας θέσης. Στην παράγραφο 6.2, θα εξετάσουμε ένα σύστημα το οποίο βασίζεται στην ύπαρξη ενός έμπιστου τρίτου εξυπηρετητή ανάμεσα στους χρήστες και τους φορείς παροχής υπηρεσιών, ενώ στην παράγραφο 6.3 θα αναλύσουμε το σύστημα Casper. Τέλος, στην παράγραφο 6.4 θα περιγράψουμε ένα σύστημα που προσφέρει ένα σύνολο τεχνικών ανωνυμίας μεταξύ των οποίων και τεχνικές ανωνυμίας τροχίας (trajectory K-anonymity), ενώ στην παράγραφο 6.5 θα εξετάσουμε μία προσέγγιση προστασίας της ανωνυμίας των χωρικών συνιστώσων στην περίπτωση αποστολής από τους χρήστες χωρικών επερωτήσεων.

Τα συστήματα που θα περιγραφούν παρακάτω λειτουργούν σε πειραματικό στάδιο, ενώ τα αποτελέσματα των πειραμάτων αποδεικνύουν ότι μπορούν να χρησιμοποιηθούν στους υπάρχοντες φορείς παροχής υπηρεσιών θέσης με ένα αρκετά μεγάλο αριθμό χρηστών.
6.1 Σύστημα Βασισμένο στην Επέκταση Χωρικών Συνιστωσών

Στο πλαίσιο της ανονυμίας της θέσης των χρηστών υπηρεσιών θέσης οι Gruteser και Grunwald [48] προτείνουν μία αρχιτεκτονική και τους αλγόριθμους οι οποίοι μπορούν να χρησιμοποιηθούν από ένα φορέα παροχής τέτοιου είδους υπηρεσιών. Οι αλγόριθμοι ρυθμίζουν την ανάλυση πληροφοριών θέσης προκειμένου να αντιμετωπίσουν τους περιορισμούς ανωνυμίας των οντοτήτων οι οποίες μπορεί να αιτηθούν υπηρεσίες σε μία δεδομένη περιοχή. Για το λόγο αυτό, το μοντέλο το οποίο χρησιμοποιούν βασίζεται στη μέτρηση της κυκλοφορίας πεζών και οχημάτων, καθώς και σε χαρτογραφικό υλικό υπολογίζοντας μία ρεαλιστική αναμενόμενη χωρική ανάλυση για διαφορετικούς περιορισμούς ανωνυμίας.

Για την υλοποίηση της ανονυμίας θέσης προτείνουν έναν αλγόριθμο επέκτασης των χωρικών περιοχών των χρηστών (interval cloaking algorithm). Η βασική ιδέα του αλγορίθμου αυτού είναι ότι ένας δεδομένος βαθμός ανωνυμίας μπορεί να διατηρηθεί για οποιαδήποτε περιοχή ανεξάρτητα από την πυκνότητα των χρηστών οι οποίοι βρίσκονται στην περιοχή αυτή μειώνοντας την ακρίβεια των αποκαλυφθέντων χωρικών δεδομένων. Ο αλγόριθμος δέχεται ως είσοδο την τρέχουσα θέση του αιτούντος, τις συντεταγμένες της περιοχής η οποία καλύπτεται από τον εξυπηρετητή ανωνυμίας και τις τρέχουσες θέσεις άλλων οχημάτων ή χρηστών στην περιοχή. Αρχικά επιλέγεται μία αρκετά μεγάλη περιοχή στην οποία βρίσκεται ένα πλήθος χρηστών του συστήματος. Στη συνέχεια, ελέγχεται αν ο αριθμός των κινούμενων οχημάτων στην περιοχή είναι μικρότερος του Κ. Αν ισχύει αυτή η συνθήκη τότε επιστρέφεται η περιοχή.
αυτή. Διαφορετικά, ο αλγόριθμος τρέχει επαναληπτικά διαχωρίζοντας τις περιοχές σε τεταρτημόρια. Κάθε φορά επιλέγεται το τεταρτημόριο στο οποίο περιέχεται ο χρήστης που έκανε την αίτηση. Οι περιοχές διαχωρίζονται μέχρι να μειωθεί ο αριθμός των χρηστών κάτω από τον επιθυμητό αριθμό ανωνυμίας K. Όταν επιτευχθεί αυτός ο περιορισμός επιστρέφεται η αμέσως προηγούμενη περιοχή.

Στην περίπτωση στην οποία δεν μπορεί να επιτευχθεί K-ανωνυμία επεκτείνοντας την περιοχή του χρήστη, οι ερευνητές προτείνουν μία μέθοδο επέκτασης της χρονικής συνιστώσας. Η βασική ιδέα σε αυτό το πλαίσιο είναι η καθυστέρηση εξυπηρέτησης του αιτήματος όπου υπάρχει χρήστης κάτω από τον επιθυμητό αριθμό K-1 (ώστε μαζί με τον αιτούντα να είναι K) χρήστες στην περιοχή του αιτούντα. Ο αλγόριθμος ελέγχει και τις μετακινήσεις οχημάτων προς αυτήν την περιοχή και όταν βρεθούν στην περιοχή K-1 χρήστες επιστρέφει τις γενικευμένες συνιστώσες του χώρου και του χρόνου.

6.2 Σύστημα Βασισμένο στον Location Anonymizer

Ένα διαφορετικό σύστημα προστασίας της ιδιωτικότητας της θέσης των χρηστών το οποίο διατηρεί παράλληλα την καλή λειτουργία των παρεχόμενων υπηρεσιών θέσης προτείνει ο Mokbel [74]. Η κύρια ιδέα και αυτού του συστήματος είναι η ύπαρξη μίας τρίτης έμπιστης οντότητας (Location Anonymizer) η οποία βρίσκεται μεταξύ των κινητών χρηστών και των φορέων παροχής υπηρεσιών και επιτυγχάνει την ανωνυμία θέσης. Η βασική εργασία της οντότητας αυτής είναι η επέκταση της θέσης των χρηστών σε μία χωρική περιοχή ώστε να επιτυγχάνεται K-ανωνυμία. Ουσιαστικά, το σύστημα που προτείνεται αποτελείται από τρία κύρια
συστατικά: τους χρήστες, τον εξυπηρετητή ανωνυμίας θέσης και τον
παροχέα υπηρεσιών.

Οι χρήστες κατά την εγγραφή τους στην υπηρεσία πρέπει να
υποδεικνύουν το προφίλ της ιδιωτικότητας των θέσεών τους. Το προφίλ
αυτό περιέχει τα εξής χαρακτηριστικά:

• Επίπεδο ανωνυμίας κ: το οποίο διευκρινίζει το επίπεδο
μυστικότητας. Όπως είναι φυσικό, όσο μεγαλύτερο είναι το
Κ τόσο καλύτερα προστατεύεται ο χρήστης αλλά και τόσο
περισσότερο μεγαλώνει η πιθανότητα αδυναμίας παροχής
της ζητούμενης υπηρεσίας και η καθυστέρηση
εξυπηρέτησής του. Το τελευταίο συμβαίνει καθώς ο
εξυπηρετητής ανωνυμίας θέσης επιφορτίζεται με επιπλέον
έργο, που αφορά το φιλτράρισμα των απαντήσεων που
λαμβάνονται από τον παροχέα υπηρεσιών, προκειμένου να
ανακαλύψει και να προωθήσει στο χρήστη τη σωστή
απάντηση.

• Ελάχιστη επέκταση περιοχής: καθορίζει την ελάχιστη
γενίκευση που θα πρέπει να λάβει χώρα προκειμένου ο
χρήστης να προστατεύεται επαρκώς. Η παράμετρος αυτή
είναι πολύ σημαντική σε περιοχές στις οποίες υπάρχουν
πάρα πολλοί χρήστες, όπως σε ένα γήπεδο ή ένα
πολυκατάστημα.

• Μέγιστη επέκταση περιοχής: καθορίζει το όριο πέρα από
το οποίο η γενίκευση θα οδηγήσει σε αδυναμία παροχής της
ζητούμενης υπηρεσίας. Θα υπάρχει δηλαδή υπεργενίκευση
(overgeneralization). Η παράμετρος αυτή είναι πολύ
σημαντική σε περιοχές στις οποίες δεν υπάρχουν χρήστες,
διότι σε περίπτωση που η περιοχή επεκταθεί πολύ η
ποιότητα υπηρεσιών θα μειωνείται.

• Χρονικοί περιορισμοί: ένας κινητός χρήστης μπορεί να
dιευκρινίσει πολλαπλές τιμές των παραπάνω παραμέτρων
για διαφορετικά χρονικά διαστήματα. Για παράδειγμα
κάποιος χρήστης μπορεί να έχει διαφορετικές απαιτήσεις
για τη μυστικότητα της θέσης του κατά τη διάρκεια της
ημέρας ή της νύχτας, τις καθημερινές ή τα σαββατοκύριακα
και ούτω καθεξής.

Οι χρήστες στέλνουν στον εξυπηρετητή ανωνυμίας θέσης την
ακριβή τους θέση, ενώ κατά τη συνεχή κίνησή τους στέλνουν τις
eνημερώσεις της νέας τους θέσης. Όταν ο εξυπηρετητής λάβει τις
πληροφορίες θέσης από κάποιο χρήστη ελέγχει το προφίλ του και επεκτείνει
tην περιοχή στην οποία βρίσκεται ανάλογα με τις απαιτήσεις που έχει
dιευκρινίσει κατά την εγγραφή του. Η θέση του επεκτείνεται βάσει των
παραμέτρων του προφίλ ώστε να επιτευχθεί Κ-ανωνυμία. Στη συνέχεια,
στέλνει τη γενικευμένη περιοχή στον παροχέα υπηρεσιών. Θα πρέπει να
σημειωθεί εδώ ότι ο εξυπηρετητής ανωνυμίας δε χρειάζεται να αποθηκεύει
tα ακριβή δεδομένα θέσης. Στη συνέχεια, στέλνει τη γενικευμένη περιοχή στον
παροχέα υπηρεσιών. Θα πρέπει να σημειωθεί εδώ ότι ο εξυπηρετητής ανωνυμίας δε
χρειάζεται να αποθηκεύει τα ακριβή δεδομένα θέσης. Αντίθετα, η γενικευμένη περιοχή μπορεί να
υπολογιστεί μέσω μετα-δεδομένων ή στατιστικών που διατηρούνται μέσω
tης πορείας της εκτέλεσης.

Στο προτεινόμενο σύστημα, οι παραδοσιακοί φορείς παροχής
υπηρεσιών επεκτείνονται με νέες πρόσθετες λειτουργίες οι οποίες
υποστηρίζουν χωρικές ερωτήσεις των χρηστών που βασίζονται στη χωρική
συνιστώσα. Παράδειγμα τέτοιου είδους ερωτήσεων, αποτελεί η εύρεση
tου κοντινότερου εστιατόριου ως προς τη θέση και την κατεύθυνση
tου χρήστη. Τέλος, τα δεδομένα που διατηρούνται στις
βάσεις δεδομένων χωρίζονται σε δημόσια ή ιδιωτικά δεδομένα. Τα
δημόσια δεδομένα περιλαμβάνουν στατικά αντικείμενα, όπως τα
κινούμενα αντικείμενα, όπως τα αυτοκίνητα και εστιατόρια, ή
κινούμενα αντικείμενα, όπως τα αυτοκίνητα της αστυνομίας. Η
θέση αυτού του είδους των δεδομένων είναι γνωστή και δε
χρειάζεται να κρατείται μυστική. Τα ιδιωτικά αντικείμενα είναι, κυρίως,
tοις προσωπικές πληροφορίες που
tης κινούμενων χρηστών.
6.3 Σύστημα Casper

Οι Mokbel et al [73] προτείνουν το σύστημα Casper. Το σύστημα αυτό αποτελείται από τρία κύρια συστατικά: τους χρήστες, τον εξυπηρετητή ανωνυμίας θέσης και τον επεξεργαστή αιτημάτων. Στην προσέγγιση αυτή η Κ-ανωνυμία είναι μία καθορισμένη ως προς τον χρήστη απαιτηση μυστικότητας η οποία μπορεί να έχει διαφορετική αξία για κάθε χρήστη.

Κατά την εγγραφή τους στο σύστημα οι χρήστες διευκρινίζουν το επίπεδο μυστικότητάς τους μέσω του καθορισμού του δικού τους προφίλ μυστικότητας. Το προφίλ αυτό περιλαμβάνει δύο παραμέτρους. Η πρώτη παράμετρος είναι ο βαθμός της αγαπημένης θέσης τους, δηλαδή ο χρήστης προσανατολίζει τον αριθμό Κ ο οποίος δηλώνει την επιθυμία του να μην μπορεί να προσδιοριστεί ανάμεσα σε Κ χρήστες. Η δεύτερη παράμετρος είναι ο ελάχιστος αριθμός αποδεκτού διαχωρισμού μίας περιοχής (Amin), η οποία φανερώνει ότι ο χρήστης θέλει να κρύψει τις πληροφορίες θέσης του σε μία περιοχή τουλάχιστον Amin. Η τιμή αυτή είναι χρήσιμη στις πυκνές περιοχές στις οποίες και ένα μεγάλο Κ δε θα επιτύχει υψηλότερες απαιτήσεις ασφάλειας. Ουσιαστικά η τιμή αυτή και ο Κ έχουν παρόμοια λειτουργία. Όσο μεγαλύτερη είναι η τιμή του Κ τόσο μεγαλύτερη είναι η επέκταση μίας περιοχής. Ως εκ τούτου, οι μεγάλες τιμές του Κ και του Amin δηλώνουν πολύ ανοιχτές απαιτήσεις μυστικότητας.

Ο εξυπηρετητής ανωνυμίας λαμβάνει τις ακριβείς πληροφορίες θέσης από τους κινούμενους χρήστες μαζί με το αντίστοιχο προφίλ μυστικότητας τους. Στη συνέχεια, μετατρέπει τις πληροφορίες θέσης επεκτείνοντας την περιοχή στην οποία βρίσκεται ο κάθε χρήστης βάσει του αντίστοιχου προφίλ του και, τέλος, στέλνει τις πληροφορίες θέσης, τις
οποίες έχει μετατρέψει έτσι ώστε να ικανοποιούν το απαιτούμενο από το χρήστη επίπεδο μυστικότητας, στον παροχέα υπηρεσιών θέσης.

Ένας επεξεργαστής αιτημάτων ενσωματώνεται στον παροχέα υπηρεσιών θέσης με στόχο να εξετάζει τα αιτήματα των χρηστών με βάση τις γενικευμένες και όχι τις πραγματικές πληροφορίες θέσης. Η κύρια εργασία του είναι να παρέχει ιδιαίτερα αποδοτικές, ακριβείς και ανώνυμες υπηρεσίες θέσης παρόλο που δε λαμβάνει τις πραγματικές θέσεις των χρηστών.

Στον παροχέα υπηρεσιών θέσης αποθηκεύονται δύο τύποι δεδομένων, τα δημόσια και τα ιδιωτικά. Τα δημόσια δεδομένα περιλαμβάνουν στατικά αντικείμενα των οποίων η θέση είναι γνωστή, ενώ τα ιδιωτικά δεδομένα περιέχουν κυρίως προσωπικές πληροφορίες των κινητών ή στατικών χρηστών οι οποίοι στο προφίλ τους έχουν μη μηδενικό K ή Amin. Επιπρόσθετα, ορίζονται τρεις τύποι ερωτήσεων: οι ιδιωτικές ερωτήσεις για δημόσια δεδομένα, οι δημόσιες ερωτήσεις για ιδιωτικά δεδομένα και οι ιδιωτικές ερωτήσεις για ιδιωτικά δεδομένα, όπως περιγράφονται παρακάτω.

Ιδιωτικές ερωτήσεις για δημόσια δεδομένα. Παράδειγμα μίας τέτοιας ερώτησης αποτελεί η εύρεση του κοντινότερου πρατηρίου βενζίνης σε σχέση με τη θέση και την κατεύθυνση του χρήστη. Σε αυτού του είδους την ερώτηση, ο χρήστης ο οποίος θέτει το ερώτημα είναι ιδιωτική οντότητα, ενώ οι περιοχές στις οποίες βρίσκονται τα πρατήρια είναι δημόσιες.

Δημόσιες ερωτήσεις για ιδιωτικά δεδομένα. Παράδειγμα ενός τέτοιου είδους ερώτησης αποτελεί η εύρεση του αριθμού των αυτοκινήτων που βρίσκονται σε μία συγκεκριμένη περιοχή. Σε αυτήν την περίπτωση μία δημόσια οντότητα θέτει μία ερώτηση για ιδιωτικές πληροφορίες.

Ιδιωτικές ερωτήσεις για ιδιωτικά δεδομένα. Ένα παράδειγμα μίας τέτοιας ερώτησης είναι η εύρεση κάποιου φίλου του χρήστη ο οποίος βρίσκεται πιο κοντά στην περιοχή στην οποία βρίσκεται και ο ίδιος. Σε αυτή την περίπτωση, τόσο η ερώτηση όσο και οι ζητούμενες πληροφορίες αποτελούν ιδιωτικά δεδομένα.

Για την αναπαράσταση των περιοχών στις οποίες βρίσκονται οι χρήστες οι ερευνητές προτείνουν τη χρήση μίας πυραμίδας, κάθε επίπεδο της
οποίας αποτελείται από ένα πλέγμα (grid) που δίνει το συνολικό χώρο διαιρεμένο σε κελιά με διαφορετική ανάλυση. Ετσι, στο ανώτερο επίπεδο όλος ο χώρος απεικονίζεται ως ένα κελι, ενώ στο κατώτατο επίπεδο ο χώρος είναι διαιρεμένος στο μεγαλύτερο πλήθος κελιών, σε μορφή πλέγματος. Όλα τα κελιά έχουν το ίδιο εμβαδό. Η δομή πυραμίδων χρησιμοποιείται για να παρακολουθεί δυναμικά τον τρέχοντα αριθμό των χρηστών μέσα σε κάθε κελι. Προκειμένου να επιτευχθεί η ανωνυμία των χρηστών, οι ερευνητές προτείνουν όταν από κάτω προς τα πάνω αλγόριθμο επέκτασης των περιοχών ο οποίος επαναλαμβάνεται για τα διαφορετικά επίπεδα της πυραμίδας. Ο αλγόριθμος αυτός προσδιορίζει τα κελιά τα οποία περιέχουν τον αιτούντα χρήστη μαζί με τους κοντινότερους γείτονές του και ικανοποιούν τις απαιτήσεις του προφίλ του για K-ανωνυμία και ελάχιστη περιοχή κάλυψης περιοχή Amin.

Το γεγονός ότι χρησιμοποιείται μία δομή διαχωρισμού των περιοχών όπως η πυραμίδα, παρέχει ποιότητα στις υπηρεσίες, δεδομένου ότι η γενικευμένη χωρική περιοχή δίνει ανεξάρτητη μορφή στα δεδομένα. Η αποδοτικότητα της χρήσης αυτής της δομής για ένα μεγάλο αριθμό χρηστών βασίζεται στο γεγονός ότι ο χρόνος επέκτασης περιοχών είναι αρκετά χαμηλός, οι περιοχές είναι χρησιμοποιούνται τη δομή, ενώ ο χρόνος για ενημέρωση της νέας θέσης των χρηστών βελτιστοποιείται χρησιμοποιώντας τη δομή πλέγματος.

Τέλος, οι ερευνητές παρουσιάζουν τα πειραματικά τους αποτελέσματα, τα οποία δείχνουν ότι το σύστημα που προτείνουν είναι αποδοτικό από την άποψη του χρόνου επεξεργασίας των αιτημάτων και του χρόνου επέκτασης των περιοχών. Επιπλέον, μπορεί να υποστηρίζει ένα μεγάλο αριθμό κινητών χρηστών παρέχοντας, παράλληλα, υψηλής ποιότητας υπηρεσίες χωρίς την ανάγκη γνώσης της ακριβούς πληροφορίας θέσης τους.
6.4 Σύστημα HESTIA

Οι Γκουλαλάς-Διβάνης και Βερύκιος [46] προτείνουν ένα μοντέλο μυστικότητας και ένα σύνολο από αλγορίθμους για την επίτευξη της ανωνυμίας των χρηστών υπηρεσιών με βάση τη θέση. Το μοντέλο που προτείνουν χρησιμοποιεί ένα πρότυπο K-ανωνυμίας το οποίο προσαρμόζεται στο χειρισμό χωρο-χρονικών δεδομένων επεκτείνοντας την έννοια της K-ανωνυμίας από τη χωρική ανωνυμία στην ανωνυμία των τροχιών. Επιπλέον, δημιουργούν ένα πρότυπο το οποίο υλοποιεί την προσέγγιση αυτή και χρησιμοποιείται κυρίως για λόγους πειραματισμού και αξιολόγησης.

Το προτεινόμενο σύστημα αποτελείται από τα εξής συστατικά στοιχεία:

- Ένα σύνολο χρηστών, οι οποίοι αιτούνται κάποιων υπηρεσιών θέσης.
- Μία τηλεπικοινωνιακή υποδομή, μέσω της οποίας καθίσταται εφικτή η επικοινωνία ανάμεσα στους χρήστες και τους παροχείς των υπηρεσιών θέσης.
- Ένας ασφαλής εξυπηρετητής, ο οποίος χρησιμοποιείται για τη διατήρηση της μυστικότητας των δεδομένων τροχιών σε πραγματικό χρόνο.
- Ένα σύνολο παροχέων υπηρεσιών θέσης, που προσφέρουν στους χρήστες υπηρεσίες βασισμένες στη θέση τους.

Ο πρώτος στόχος για την παροχή ανωνυμίας τροχιάς είναι να χρησιμοποιηθούν οι συλλεγόμενες τροχιές των χρηστών προκειμένου να προσδιοριστούν για κάθε χρήστη οι περιοχές στις οποίες κινδυνεύει η ιδιωτικότητά του. Αυτό γίνεται με την εύρεση συχνά χρησιμοποιούμενων περιοχών στην τροχιά κάθε χρήστη, οι οποίες είναι μια συχνές για τους
περισσότερους από τους υπόλοιπους χρήστες στο σύστημα. Οι τροχιές αυτές δεν είναι ασφαλείς εφόσον μπορούν να προσδιορίσουν ένα άλλον χρήστη του συστήματος. Μετά τον προσδιορισμό αυτών των τροχιών, ο δεύτερος στόχος του προτεινόμενου συστήματος είναι να προστατεύει την πορεία των χρηστών κατά τη διάρκεια εξυπηρέτησης τους από το σύστημα. Ετσι, όταν ο εξυπηρετητής HESTIA λάβει μία νέα αίτηση προστατεύει το χρήστη με την παροχή K-ανωνυμίας. Αν ένας χρήστης βρίσκεται σε κάποια από αυτές τις περιοχές και η προσφερθείσα υπηρεσία βρίσκεται υπό εξέλιξη, το σύστημα προχωρά προκειμένου να προστατεύσει τη μυστικότητα του μέσω της K-ανωνυμίας. Σε αυτό το πλαίσιο, το σύστημα λαμβάνει υπόψη και την παράμετρο Amin, η οποία καθορίζει τον ελάχιστο αποδεκτό διαχωρισμό της περιοχής που βρίσκεται ο χρήστη.

Βασικό ρόλο στο προτεινόμενο σύστημα έχει ο εξυπηρετητής ανωνυμίας HESTIA. Όταν δέχεται κάποιο αίτημα, ο εξυπηρετητής HESTIA εξετάζει εάν η περιοχή στην οποία βρίσκεται ο χρήστης είναι ασφαλής. Εάν δεν είναι ασφαλής, η περιοχή του επεκτείνεται έτσι ώστε να επιτυγχάνεται K-ανωνυμία. Ο εξυπηρετητής HESTIA καθορίζει αυτόματα και τη μέγιστη περιοχή γενίκευσης με βάση τις ανάγκες της ζητούμενης υπηρεσίας θέσης. Όπως και στα υπόλοιπα συστήματα, ο εξυπηρετητής ανωνυμίας αφού μετασχηματίσει τα αίτημα τα διαβιβάζει στον παροχέα υπηρεσιών προκειμένου να εξυπηρετηθούν. Ο παροχέας υπηρεσιών υπολογίζει το αποτέλεσμα με βάση τις γενικευμένες περιοχές και το στέλνει πίσω στον εξυπηρετητή HESTIA. Ο εξυπηρετητής φιλτράρει κατάλληλα τα αποτελέσματα και τα επιστρέφει στο χρήστη.

Στη βάση δεδομένων αποθηκεύονται οι απαιτήσεις μυστικότητας του κάθε χρήστη για κάθε υπηρεσία, προκειμένου να προσφέρεται η μυστικότητα των χρηστών με εξατομικευμένο τρόπο. Εππλήως, η υλοποίηση του συστήματος στηρίζεται σε ένα χωρικό πρόγραμμα διαχείρισης βάσεων δεδομένων το οποίο πραγματοποιεί ένα μέρος της απαραίτητης ανάλυσης. Για το λόγο αυτό χρησιμοποιείται μία χωρική βάση δεδομένων για τη διατήρηση του ιστορικού μετακίνησης κάθε χρήστη στο σύστημα.
Στα πλαίσια του ασφαλούς εξυπηρετητή HESTIA, υλοποιείται ένας αλγόριθμος για τον προσδιορισμό των συχνότερα ακολουθούμενων τροχιών του κάθε χρήστη προκειμένου να προσδιοριστούν οι περιοχές στις οποίες είναι ανασφαλής. Επιπρόσθετα, υλοποιούνται αλγόριθμοι για τον προσδιορισμό και τη δημιουργία των τροχιών που ακολουθούν οι χρήστες και για την παροχή της K-ανωνυμίας.

Τέλος, οι ερευνητές μέσω ενός συνόλου πειραμάτων καταδεικνύουν την αποτελεσματικότητα της προτεινόμενης προσέγγισης για τη διατήρηση της ανωνυμίας των χρηστών. Παράλληλα, συζητούν τις λεπτομέρειες εκτέλεσης που επιτρέπουν τη λειτουργία του προτεινόμενου συστήματος σε πραγματικό χρόνο, καθώς και τη δοκιμαστική λειτουργία του με διαφορετικά χωρικά προγράμματα διαχείρισης βάσεων δεδομένων.

6.5 Σύστημα Ανωνυμίας Χωρικών Ερωτήσεων

Οι Καλνής et al [62] προτείνουν ένα μοντέλο για την προστασία των χωρικών πληροφοριών των χρηστών οι οποίες προκύπτουν από τις επερωτήσεις του χρήστη στον παροχέα υπηρεσιών θέσης. Για το λόγο αυτό μετασχηματίζουν το υπάρχον μοντέλο K-ανωνυμίας έτσι ώστε να υπολογίζουν τις απαντήσεις στις επερωτήσεις των χρηστών χρησιμοποιώντας την αναζήτηση κοντινότερων γειτόνων.

Το σύστημα που προτείνεται βασίζεται στην ύπαρξη ενός εξυπηρετητή ανωνυμίας. Κάθε αίτηση που λαμβάνει ο εξυπηρετητής αυτός από τους χρήστες έχει έναν απαραίτητο βαθμό ανωνυμίας K, ο οποίος κυμαίνεται μεταξύ του 1 (καμία απαίτηση μυστικότητας) και του αριθμού του συνόλου των χρηστών (μέγιστη απαίτηση μυστικότητας). Η γενίκευση της περιοχής, πριν σταλεί το μετασχηματισμένο αίτημα στον παροχέα
υπηρεσιών θέσης, πραγματοποιείται από τον εξυπηρετητή λαμβάνοντας υπόψη αυτόν τον αριθμό Κ.

Για τη δημιουργία του συστήματος οι ερευνητές εξετάζουν την υπόθεση ότι ένας επιτιθέμενος έχει την πλήρη γνώση:

- Όλων των γενικευμένων περιοχών που λαμβάνονται από τους παροχείς υπηρεσιών.
- Των αλγόριθμων γενικευσης περιοχών που χρησιμοποιούνται από τον εξυπηρετητή ανωνυμίας.
- Τις πιθανές θέσεις όλων των χρηστών.

Η πρώτη υπόθεση δηλώνει ότι είτε οι φορείς παροχής υπηρεσιών δεν είναι έμπιστοι (για παράδειγμα μία εμπορική υπηρεσία συλλέγει πληροφορίες χωρίς την εξουσιοδότηση των χρηστών) ή το κανάλι επικοινωνίας μεταξύ του εξυπηρετητή ανωνυμίας και των φορέων παροχής υπηρεσιών θέσης δεν είναι ασφαλές. Η δεύτερη υπόθεση είναι αναμενόμενη δεδομένου ότι οι αλγόριθμοι ιδιωτικότητας των δεδομένων είναι συνήθως δημόσιοι. Η τρίτη υπόθεση παρακινείται από το γεγονός ότι οι χρήστες μπορούν συχνά (ή πάντα) να θέτουν τις επερωτήσεις τους από τις ίδιες θέσεις (επί παραδείγματι από το σπίτι ή το γραφείο), οι οποίες μπορούν να προσδιορίζονται εύκολα μέσω των δημόσιων βάσεων δεδομένων, όπως οι τηλεφωνικοί κατάλογοι.

Η βασική ιδέα του προτεινόμενου συστήματος είναι να διατηρηθεί η ανωνυμία των πληροφοριών θέσης με την αντικατάσταση των συντεταγμένων των χρηστών με μία χωρική περιοχή, ένα κύκλο ή ένα ορθογώνιο. Αυτή η περιοχή πρέπει να καλύπτει τουλάχιστον ακόμα Κ-1 χρήστες. Για το λόγο αυτό οι ερευνητές προτείνουν μεθόδους οι οποίες κατασκευάζουν αυτές τις κατάλληλες περιοχές που διατηρούν την ανωνυμία των χρηστών. Για την επέκταση των περιοχών προτείνονται δύο αλγόριθμοι: επέκταση Hilbert και επέκταση βασισμένη στους κοντινότερους γείτονες.

Ο αλγόριθμος Hilbert αποτελεί μία αποδοτική μέθοδο ανωνυμίας της θέσης των χρηστών. Βασίζεται στο διαχωρισμό των περιοχών ώστε να συγκεντρώνονται γρήγορα οι κατάλληλες περιοχές οι οποίες επιτυγχάνουν χωρική Κ-ανωνυμία, ενώ παράλληλα ελαχιστοποιείται το κόστος των υπηρεσιών και το απαραίτητο εύρος ζώνης μεταξύ των υπηρεσιών θέσης και
του εξυπηρετητή ανωνυμίας. Ο αλγόριθμος αυτός εγγυάται ότι η πιθανότητα
tου προσδιορισμού ενός χρήστη είναι πάντα οριακή στο 1/Κ
dεδομένου ότι χρησιμοποιεί ένα σταθερό σχέδιο διαχωρισμού των περιοχών. Επιπλέον, οι
συντεταγμένες του χρήστη μετασχηματίζονται σε ένα μονοδιάστατο σημείο,
dεδομένου ότι αν δύο χρήστες βρίσκονται κοντά στη δισδιάστατη
αναπαράσταση το πιθανότερο είναι να βρίσκονται κοντά και στη
μονοδιάστατη. Χρησιμοποιώντας το μετασχηματισμό αυτό το κόστος
επεξεργασίας μειώνεται. Τέλος, οι περιοχές ταξινομούνται σε ορθογώνια σε
κάθε ένα από τα οποία περιέχεται ο ίδιος αριθμός χρηστών (κ), εκτός από το
tελευταίο ορθογώνιο που διευρύνεται ώστε να περιέχει τουλάχιστον K
χρήστες. Θα πρέπει να σημειωθεί εδώ ότι ο αλγόριθμος αναζήτησης
κοντινότερων γειτόνων είναι πιο πολύπλοκος από τον αλγόριθμο Hilbert.

Οι πειραματικές μελέτες των ερευνητών του συγκεκριμένου
συστήματος δείχνουν ότι αυτό το σύστημα μπορεί να χρησιμοποιηθεί στις
υπάρχουσες υπηρεσίες παροχής υπηρεσιών θέσης με έναν μεγάλο αριθμό
χρηστών. Τέλος, τα αποτελέσματα της αποδοτικότητας του συστήματος
συγκρίνονται με τα αποτελέσματα άλλων προσεγγίσεων, όπως το σύστημα
Casper και το Interval Cloak. Παραδείγματος χάριν, ο αλγόριθμος Hilbert
παρέχει εγγύηση της μυστικότητας με τη δημιουργία των γενικευμένων
περιοχών, το κόστος επεξεργασίας επερωτήσεων και το κόστος
επικοινωνιών, το οποίο είναι ίδιο με τον Casper. Ο δεύτερος αλγόριθμος
είναι πιο αποδοτικός από τον Casper από την άποψη του κόστους
επικοινωνιών και επεξεργασίας προσφέροντας ίδιο επίπεδο διατήρησης της
ανωνυμίας. Ο πρώτος αλγόριθμος εφαρμόζεται σε περίπτωση που
επιθυμούμε τη μέγιστη εγγύηση ανωνυμίας ενώ ο δεύτερος υπερτερεί στο
υπολογιστικό κόστος. Εντούτοις και ο αλγόριθμος κοντινότερων γειτόνων
επιτυγχάνει ισχυρή ανωνυμία στις περισσότερες περιπτώσεις, ενώ μπορεί να
εφαρμοστεί στην περίπτωση που οι χρήστες δε συνηθίζουν να αιτούνται των
υπηρεσιών από συγκεκριμένες περιοχές όπως το σπίτι ή το γραφείο, αλλά
μετακινούνται συχνά και η αποδοτικότητα σε αυτήν την περίπτωση είναι
πολύ κρίσιμος παράγοντας.
6.6 Επίλογος

Στο κεφάλαιο αυτό εξετάσαμε διάφορα προτεινόμενα συστήματα για την προστασία της ανωνυμίας θέσης των χρηστών. Τα συστήματα αυτά έχουν προταθεί προκειμένου να αντιμετωπίσουν την κατάσταση κατά την οποία όταν ένας χρήστης επιθυμεί να κρατήσει ανώνυμη τη θέση του θα πρέπει να απενεργοποιήσει τη φορητή συσκευή του.

Τα περισσότερα συστήματα που προτείνονται στη βιβλιογραφία βασίζονται στην ύπαρξη ενός έμπιστου εξυπηρετητή ανωνυμίας θέσης ο οποίος βρίσκεται ανάμεσα στους χρήστες και τους φορείς παροχής υπηρεσιών και διαχειρίζεται την μεταξύ τους επικοινωνία. Οι ερευνητές προτείνουν διάφορους αλγόριθμους οι οποίοι τρέχουν στον εξυπηρετητή προκειμένου να επιτευχθεί η ανωνυμία, προτού τα αιτήματα των χρηστών σταλούν στο φορέα παροχής υπηρεσιών.

Οι πειραματικές μελέτες των ερευνητών φανερώνουν ότι τα περισσότερα από τα προτεινόμενα συστήματα μπορούν να υφίστανται στις υπάρχουσες υπηρεσίες με έναν αρκετά μεγάλο αριθμό χρηστών.
Κεφάλαιο 7

Χρηματοδότηση της Έρευνας - Ερευνητικά Προγράμματα

Η χρηματοδότηση της έρευνας αποτελεί ίσως τον πιο ανασταλτικό παράγοντα στην πρόοδο των επιστημών και της τεχνολογίας. Ο κατάλληλος εξοπλισμός, όπως οι υψηλού επιπέδου εγκαταστάσεις υπολογιστών ή τα δίκτυα υψηλής ταχύτητας, έχουν συνήθως πολύ υψηλό κόστος στο οποίο δύσκολα μπορεί να αντεπεξέλθει μία ερευνητική ομάδα. Για το λόγο αυτό, διάφοροι Ευρωπαϊκοί και διεθνείς οργανισμοί χρηματοδοτούν την επιστημονική έρευνα. Οι βασικότεροι οργανισμοί χρηματοδότησης θα παρουσιαστούν στην παράγραφο 7.1.

Παράλληλα, πολλά Ευρωπαϊκά και διεθνή ερευνητικά προγράμματα τρέχουν αυτή την περίοδο και εξετάζουν ζητήματα σχετικά με αυτά που παρουσιάσαμε στα προηγούμενα κεφάλαια. Τα προγράμματα αυτά χρηματοδοτούνται από τους οργανισμούς που θα εξετάσουμε παρακάτω και περιγράφονται στην παράγραφο 7.2.
7.1 Οργανισμοί Χρηματοδότησης της Έρευνας

Σε αυτή την παράγραφο θα παρουσιάσουμε τους πιο σημαντικούς οργανισμούς χρηματοδότησης. Πιο συγκεκριμένα, στην παράγραφο 7.1.1 θα περιγράψουμε τον βασικότερο Ευρωπαϊκό χρηματοδοτικό οργανισμό της έρευνας, το 7ο Πρόγραμμα-Πλαίσιο [39]. Στη συνέχεια, στις παραγράφους 7.1.2, 7.1.3 και 7.1.4 θα αναλυθούν οι βασικότεροι οργανισμοί χρηματοδότησης των ΗΠΑ, οι οποίοι περιλαμβάνουν το Εθνικό Ίδρυμα Επιστημών [80], την Εθνική Υπηρεσία Ασφάλειας [79] και το Εθνικό Ίδρυμα Υγείας [77]. Τέλος, στην παράγραφο 7.1.5 θα περιγράψουμε τον οργανισμό MITRE [72], ο οποίος αποτελεί μία ιδιωτική, μη κερδοσκοπική πρωτοβουλία υποστήριξης της επιστημονικής έρευνας.

7.1.1 7ο Πρόγραμμα - Πλαίσιο

Το 7ο Πρόγραμμα-Πλαίσιο - 7ο ΠΠ (Framework Programme 7 – FP7) [39] αποτελεί το κυριότερο οικονομικό εργαλείο μέσω του οποίου η Ευρωπαϊκή Ένωση υποστηρίζει την έρευνα και την τεχνολογική ανάπτυξη, καλύπτοντας σχεδόν όλους τους επιστημονικούς τομείς. Τα ΠΠ έχουν ενεργοποιηθεί από το 1984 και το κάθε ένα διαρκείες πέντε έτη. Το 7ο ΠΠ έχει διάρκεια επτά ετών, ξεκίνησε το 2007 και θα ολοκληρωθεί το 2013. Ο σχεδιασμός του βασίστηκε στα αποτελέσματα των προηγούμενων
προγραμμάτων για τη δημιουργία του Ευρωπαϊκού τομέα έρευνας με σκοπό την προώθηση της γνώσης για την οικονομική και κοινωνική ανάπτυξη στην Ευρώπη.

Για τον προσδιορισμό των επιστημονικών τομέων οι οποίοι θα χρηματοδοτηθούν από το 7ο ΠΠ η Επιτροπή έλαβε υπόψη της τις απόψεις του Ευρωπαϊκού Κοινοβουλίου, των κρατών-μελών της, της επιστημονικής κοινότητας, της βιομηχανίας και όλων των συμμετεχόντων στην Ευρωπαϊκή Έρευνα. Το 7ο ΠΠ αποτελείται από τέσσερις βασικές κατηγορίες δραστηριοτήτων οι οποίες διαμορφώνουν τέσσερα ειδικά προγράμματα: Συνεργασία, Ιδέες, Άνθρωποι και Ικανότητες, ενώ παράλληλα περιλαμβάνεται και ένα ειδικό πρόγραμμα για την πυρηνική έρευνα:

- **Συνεργασία**: περιλαμβάνει την έρευνα σε διάφορους επιστημονικούς τομείς, όπως η υγεία, η γεωργία και η βιοτεχνολογία, οι τεχνολογίες πληροφοριών και επικοινωνιών, οι νανο-επιστήμες, η ενέργεια, το περιβάλλον, το διάστημα, οι μεταφορές, οι κοινωνικο-οικονομικές και ανθρωπιστικές επιστήμες και η ασφάλεια.

- **Ιδέες**: το πρόγραμμα αυτό υποστηρίζει δράσεις έρευνας αιχμής.

- **Άνθρωποι**: περιλαμβάνει την κατάρτιση των ερευνητών και την επαγγελματική εξέλιξη, ενώ προσφέρει υποτροφίες εσωτερικού και εξωτερικού, εταιρικές σχέσεις και επικοινωνία μεταξύ Πανεπιστημίων και επιχειρήσεων και διεθνή εταιρικά σχήματα.

- **Ικανότητες**: προσφέρει υποδομές στην έρευνα, ενασχόληση της επιστήμης στον κοινωνικό ιστό, ειδικές δραστηριότητες διεθνούς συνεργασίας, έρευνα προς όφελος των μέσων μαζικής ενημέρωσης και άλλα.

Στο πρώτο πρόγραμμα, δηλαδή στη συνεργασία, κατανέμεται το μεγαλύτερο μέρος της χρηματοδότησης της έρευνας. Παράλληλα, τη μεγαλύτερη χρηματοδότηση των επιστημονικών τομέων στο πρώτο πρόγραμμα λαμβάνουν οι τεχνολογίες πληροφοριών και επικοινωνιών με σκοπό την ταχύτερη εξέλιξη των προϊόντων, τη μείωση του κόστους των
νέων τεχνολογιών, τις ταχύτερες και ασφαλέστερες συναλλαγές, την αναβάθμιση της εξυπηρέτησης και στήριξης των πελατών, καθώς και την αναβάθμιση των διαδραστικών συστημάτων.

Επιπλέον, ένα σημαντικό ποσοστό της χρηματοδότησης του 7ου ΠΠ παρέχεται στον τομέα της ασφάλειας. Η έρευνα στον τομέα προγραμματοποιείται προκειμένου να καλυφθεί η ανάγκη μίας σφαιρικής στρατηγικής για την προστασία των πολιτών από απειλές όπως η τρομοκρατία, οι φυσικές καταστροφές και η εγκληματικότητα, σεβόμενοι πάντα την ιδιωτική ζωή και διαφυλάσσοντας τα θεμελιώδη δικαιώματα των πολιτών. Σε αυτό το πλαίσιο, η έρευνα της ασφάλειας περιλαμβάνει πολλούς τομείς, όπως η ανάπτυξη τεχνολογικών λύσεων για την πολιτική προστασία, η βιοασφάλεια, η προστασία κατά της εγκληματικότητας και της τρομοκρατίας, η προστασία των πολιτών κατά τη συλλογή δεδομένων τους και η προστασία της εμπιστευτικότητας τους δεδομένων αυτών, η ανάλυση κοινωνικο-οικονομικών, πολιτικών και πολιτιστικών διαστάσεων της ασφάλειας, το κοινωνικό περιβάλλον και οι αντιλήψεις των πολιτών για την ασφάλεια, καθώς επίσης και ο συντονισμός των Ευρωπαϊκών και διεθνών προσπαθειών για την ασφάλεια στους τομείς της έρευνας.

7.1.2 Εθνικό Ίδρυμα Επιστημών

Το εθνικό ίδρυμα επιστημών (National Science Foundation - NSF) [80] αποτελεί μια ανεξάρτητη ομοσπονδιακή υπηρεσία που δημιουργήθηκε από το 1950 για να προωθήσει την πρόοδο των επιστημών και να υποστηρίξει τη γνώση και την ευημερία. Το ίδρυμα αυτό προωθεί την επιστημονική πρόοδο στις ΗΠΑ με τη χρηματοδότηση της έρευνας και της εκπαίδευσης στους περισσότερους τομείς της επιστήμης και της
εφαρμοσμένης μηχανικής μέσω επιχορηγήσεων και συνεταιρικών συμφωνιών σε κολέγια, Πανεπιστήμια, επιχειρήσεις, οργανισμούς και άλλες ερευνητικές οργανώσεις στις ΗΠΑ. Πιο συγκεκριμένα, το NSF χρηματοδοτεί περίπου το 20% της έρευνας που πραγματοποιείται από τα κολέγια και Πανεπιστήμια της Αμερικής, ενώ σε επιστήμες όπως τα μαθηματικά, η πληροφορική και οι κοινωνικές επιστήμες αποτελεί τη σημαντικότερη πηγή ομοσπονδιακής υποστήριξης και χρηματοδότησης.

Το NSF δημοσιεύει ανακοινώσεις για χρηματοδοτήσεις και οι ενδιαφερόμενοι στέλνουν τις προτάσεις τους περιγράφοντας τις ιδέες και ζητώντας ένα συγκεκριμένο ποσό υποστήριξης για κάποιο πρόγραμμα. Η κάθε πρόταση αξιολογείται και επεξεργάζεται από μία επιτροπή εμπειρογνωμόνων για κάθε τομέα. Θα πρέπει να σημειωθεί εδώ ότι το ίδρυμα αυτό λαμβάνει επίσης περίπου 40.000 προτάσεις εκπαίδευσης και κατάρτισης από τον οποίον χρηματοδοτεί περίπου τις 11.000. Πολλές από τις έρευνες τις οποίες έχει χρηματοδοτήσει έχουν κερδίσει βραβείο Νόμπελ καθώς και άλλα βραβεία.

Οι βασικότεροι τομείς των επιστημών που συμπεριλαμβάνονται στην έρευνα του ιδρύματος είναι επτά: οι βιολογικές επιστήμες, η επιστήμη υπολογιστών και πληροφοριών, η εφαρμοσμένη μηχανική, οι γεωγραφικές επιστήμες, τα μαθηματικά και οι φυσικές επιστήμες, οι κοινωνικές, οικονομικές και ανθρωπιστικές επιστήμες, καθώς και οι επιστήμες συμπεριφοράς.

Οι στόχοι του NSF είναι η ανακάλυψη και διαχείριση της γνώσης και η υποστήριξη της εκμάθησης και της ερευνητικής υποδομής. Στα πλαίσια αυτά, οι βασικότερες δραστηριότητες του ιδρύματος είναι οι εξής:

- Η ενίσχυση και η υποστήριξη της επιστημονικής έρευνας και των προγραμμάτων εφαρμοσμένης μηχανικής μέσω επιχορηγήσεων, καθώς και η αξιολόγηση του αντίκτυπου της έρευνας στη βιομηχανική ανάπτυξη και τη γενική ευημερία.
- Η παροχή υποτροφιών στις επιστήμες και την εφαρμοσμένη μηχανική, καθώς και η ενθάρρυνση της ανταλλαγής των
επιστημονικών πληροφοριών μεταξύ των ΗΠΑ και των άλλων χωρών.

- Η ενθάρρυνση και υποστήριξη της ανάπτυξης και χρήσης υπολογιστών και άλλων επιστημονικών μεθόδων και τεχνολογιών τόσο στον τομέα της έρευνας όσο και της εκπαίδευσης.

- Η αξιολόγηση των αναγκών διάφορων επιστημών και ο συσχετισμός της έρευνας και των εκπαιδευτικών προγραμμάτων στα πλαίσια αυτών των αναγκών.

- Η παροχή μίας κεντρικής πηγής πληροφοριών για τη σύλλογη, ερμηνεία και ανάλυση των δεδομένων που αφορούν τους επιστημονικούς και τεχνικούς πόρους των ΗΠΑ.

- Ο καθορισμός του συνολικού χρηματικού ποσού που παραλαμβάνεται ομοσπονδιακά από τα πανεπιστήμια και τις αρμόδιες οργανώσεις για τη συμπεριφορά της έρευνας.

- Η υποστήριξη συγκεκριμένων επιστημονικών δραστηριοτήτων σε θέματα σχετικά με τη διεθνή συνεργασία, την εθνική ασφάλεια και τα αποτελέσματα των επιστημονικών και τεχνολογικών εφαρμογών στην κοινωνία.

- Η υποστήριξη της ατομικής έρευνας από ερευνητές των ΗΠΑ.

- Η υποστήριξη δραστηριοτήτων με σκοπό την αύξηση της συμμετοχής μειονοτήτων στην επιστήμη και την τεχνολογία.

Τέλος, το NSF δε λειτουργεί από μόνο του κάποιο ερευνητικό εργαστήριο αλλά υποστηρίζει τα διάφορα ερευνητικά κέντρα παρέχοντας επιχορηγήσεις για τις εγκαταστάσεις και τον εξοπλισμό που επιτρέπουν στους ερευνητές να εργαστούν σε καλύτερες συνθήκες.
7.1.3 Εθνική Υπηρεσία Ασφάλειας

Η Εθνική Υπηρεσία Ασφάλειας (National Security Agency - NSA) [79] αποτελεί έναν οργανισμό των ΗΠΑ ο οποίος έχει ιδρυθεί από το 1952 και βασικός του στόχος είναι η συλλογή και η ανάλυση δεδομένων επικοινωνιών. Παράλληλα, κατευθύνει και εκτελεί ιδιαίτερα εξειδικευμένες δραστηριότητες που βασίζονται στην παραγωγή πληροφοριών σημάτων οι οποίες περιλαμβάνουν κρυπτογραφική ανάλυση. Ουσιαστικά, η υπηρεσία αυτή είναι αρμόδια για την προστασία των πληροφοριακών συστημάτων, καθώς και για την ασφαλή διεκπεραίωση οποιουδήποτε είδους επικοινωνίας στις ΗΠΑ. Για το λόγο αυτό, σκοπός της είναι να παρέχει λύσεις, προϊόντα και υπηρεσίες προκειμένου να προστατεύσει την εθνική ασφάλεια.

Σε αυτό το πλαίσιο, λειτουργεί ένα ερευνητικό εργαστήριο ασφάλειας πληροφοριών, το οποίο διευθύνει και χρηματοδοτεί την ακαδημαϊκή έρευνα των τεχνολογιών και των τεχνικών που θα προστατεύσουν την ασφάλεια των πληροφοριακών συστημάτων. Τα βασικότερα ερευνητικά πεδία του εργαστηρίου ασφάλειας πληροφοριών περιλαμβάνουν κρυπτογραφικά συστήματα και πρότυπα, τεχνικές αυθεντικοποίησης, καθώς και διαχείριση δικτύων, λειτουργικών συστημάτων και συστημάτων επικοινωνιών. Επιπλέον, η υπηρεσία συνεργάζεται με τη βιομηχανία, τον ακαδημαϊκό τομέα, την κυβέρνηση και διάφορους ερευνητές ανά τον κόσμο προκειμένου να ανακαλύψουν μεθόδους και προϊόντα ασφάλειας των πληροφοριακών συστημάτων.

Τέλος, το NSA συνεργάζεται με υπηρεσίες προστασίας των επικοινωνιών άλλων χωρών, όπως τις υπηρεσίες της Αγγλίας, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας για την λειτουργία του συστήματος ECHELON. Το σύστημα ECHELON περιλαμβάνει τη δυνατότητα ελέγχου
ενός μεγάλου ποσοστού τηλεφωνικών, διαδικτυακών και άλλου είδους επικοινωνιών κυρίως για την πρόληψη τρομοκρατικών ενεργειών. Λόγω της παρακολούθησης διαφόρων μορφών επικοινωνιών, ο βασικότερος τομέας έρευνας του NSA αφορά την κρυπτανάλυση. Η κρυπτανάλυση είναι η μελέτη για την ανεύρεση των μεθόδων που εξασφαλίζουν την κατανόηση του νοήματος των κρυπτογραφημένων πληροφοριών έχοντας άγνωστο τον αλγόριθμο κρυπτογράφησης, το κλειδί και το αρχικό μήνυμα.

7.1.4 Εθνικό Ίδρυμα Υγείας

Το Εθνικό Ίδρυμα Υγείας (National Institutes of Health - NIH) [77] αποτελεί έναν οργανισμό των ΗΠΑ ο οποίος χρηματοδοτεί την έρευνα που είναι σχετικά κυρίως με τα ιατρικά δεδομένα και τη βελτίωση της ανθρώπινης υγείας. Σε αυτόν τον τομέα συμπεριλαμβάνεται η υποστήριξη της ιατρικής έρευνας για την επέκταση της γνώσης, καθώς και η εφαρμογή της γνώσης αυτής για την προώθηση της δημόσιας υγείας και ευημερίας.

Η χρηματοδότηση των προγραμμάτων του NIH αφορά την ενθάρρυνση των καινοτόμων ανακαλύψεων και ερευνών που σχετίζονται με τα ιατρικά δεδομένα, τη διατήρηση και ανανέωση ανθρωπίνων πόρων που είναι ζωτικής σημασίας για την αποτροπή ασθενειών, τη βελτίωση της υγείας και της ποιότητας ζωής, καθώς και την υποστήριξη γνώσης που βασίζεται στη βιοϊατρική, την επιστήμη συμπεριφοράς και σε άλλες σχετικές επιστήμες.

Μία πολύ σημαντική κατεύθυνση της έρευνας του ιδρύματος υγείας αποτελεί η ανάπτυξη συστημάτων και προγραμμάτων για τη σύλληψη, χρήση και ανταλλαγή των ιατρικών πληροφοριών και πληροφοριών υγείας συμπεριλαμβανομένων και των συστημάτων υποστήριξης της προστασίας τέτοιου είδους πληροφοριών.
7.1.5 MITRE

Το MITRE [72] ιδρύθηκε το 1958 ως ένας ιδιωτικός, μη κερδοσκοπικός οργανισμός για να παρέχει τεχνική και μηχανική υποστήριξη στην κυβέρνηση των ΗΠΑ. Κατά τη διάρκεια των σχεδόν πέντε δεκαετιών από την ιδρυσή του έχει κερδίσει τη διεθνή φήμη για την τεχνολογική καινοτομία που προσφέρει.

Το MITRE διαχειρίζεται τρία ομοσπονδιακά χρηματοδοτούμενα κέντρα έρευνας και ανάπτυξης (Federally Funded Research and Development Center - FFRDCs), με σκοπό να υποστηρίζει τις κρίσιμες αποστολές του και να αντιμετωπίσει ζητήματα εθνικής σπουδαίοτητας. Τα FFRDCs αποτελούν οργανώσεις που βοηθούν την κυβέρνηση των ΗΠΑ στην επιστημονική έρευνα και την ανάπτυξη εφαρμοσμένων συστημάτων. Οι οργανώσεις αυτές εξετάζουν μακροπρόθεσμα προβλήματα ιδιαίτερης πολυπλοκότητας, αναλύουν τεχνικές με υψηλό βαθμό αντικειμενικότητας και παρέχουν δημιουργικές και αποδοτικές λύσεις στα κυβερνητικά προβλήματα.

Ερευνητικοί τομείς στους οποίους συμμετέχει το MITRE αποτελούν η ανάλυση συστημάτων, οι επικοινωνίες και η δικτύωση, οι τεχνολογίες πληροφοριών, οι αισθητήρες, η εφαρμοσμένη μηχανική συστημάτων και άλλοι τομείς έρευνας και ανάπτυξης.

Πιο συγκεκριμένα, από την αρχή λειτουργίας του το MITRE συνεισφέρει στην έρευνα και την ανάπτυξη ευφυών και σύνθετων συστημάτων, καθώς και εργαλείων για την λειτουργία τους. Στον τομέα των επικοινωνιών και των δικτύων η συμβολή τους αφορά την έρευνα στον τομέα των δικτύων και των πρωτοκόλλων που χρησιμοποιούνται, στις
ασύρματες τεχνολογίες, τις δορυφορικές επικοινωνίες, την επεξεργασία σημάτων και τις ψηφιακές επικοινωνίες, τις ραδιοεπικοινωνίες και άλλα.

Παράλληλα, ο τομέας των τεχνολογιών πληροφοριών αποτελεί έναν από τους κυριότερους ερευνητικούς τομείς στους οποίους εργάζεται το MITRE. Σε αυτόν τον τομέα οι έρευνες περιλαμβάνουν την ασφάλεια των πληροφοριών, τις προηγμένες τεχνολογίες βάσεων δεδομένων, τη διαχείριση και επεξεργασία πληροφοριών, τις τεχνολογίες διαδικτύου και την ανάπτυξη συστημάτων που χρησιμοποιούν κρυπτογραφία για την ασφάλεια των χρηστών των πληροφοριακών συστημάτων.

Στον τομέα των αισθητήρων και της ανάλυσης σημάτων η έρευνα εστιάζει σε συστήματα αισθητήρων, σε γεωγραφικά πληροφοριακά συστήματα, σε ασύρματα δίκτυα, σε κεραίες, ραντάρ και άλλα. Τα συναφή ερευνητικά προγράμματα εξετάζουν τα κινούμενα αντικείμενα που προκύπτουν από τη δορυφορική λήψη δεδομένων, την ανάπτυξη αλγορίθμων για τη βελτιστοποίηση των σημάτων που προέρχονται από δορυφόρους προσδιορισμού θέσης και άλλα.

Τέλος, στον τομέα έρευνας και τεχνολογίας συμπεριλαμβάνονται διάφοροι ερευνητικοί τομείς, όπως η τεχνητή νοημοσύνη, η βιοτεχνολογία, οι επικοινωνίες και τα δίκτυα, η ασφάλεια και η διαχείριση πληροφοριών, καθώς και διάφορες κοινωνικές επιστήμες και επιστήμες συμπεριφοράς. Στον τομέα των επικοινωνιών και των δικτύων η έρευνα εστιάζει στα ασύρματα δίκτυα, στις επικοινωνίες μέσω δορυφόρων και την ασφάλεια των δικτύων.
7.2 Συναφή Ερευνητικά Προγράμματα

Σε αυτή την παράγραφο θα παρουσιάσουμε τα σημαντικότερα ερευνητικά προγράμματα που συνδέονται με τα ζητήματα που εξετάσαμε στα προηγούμενα κεφάλαια. Παραδείγματα τέτοιων προγραμμάτων αποτελούν το GeoPKDD [44], το iTrust [58], το PORTIA [10], το KDubiq [64], το geopriv [56] και το PRIME [86] τα οποία θα παρουσιάσουμε περιληπτικά στις παραγράφους 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5 και 7.2.6 αντίστοιχα. Τέλος, στην παράγραφο 7.2.7 θα περιγράψουμε ένα πολύ σημαντικό συνέδριο που πραγματοποιήθηκε αυτή τη χρονιά για την προστασία δεδομένων, στο οποίο ιδιαίτερη έμφαση δόθηκε στα δεδομένα που συλλέγονται από τις υπηρεσίες θέσης.

7.2.1 Πρόγραμμα GeoPKDD

Το GeoPKDD (Geographic Privacy-aware Knowledge Discovery and Delivery) [44] αποτελεί ένα πολύ σημαντικό ερευνητικό πρόγραμμα συναφές με τα ζητήματα που αναλύσαμε στα προηγούμενα κεφάλαια και χρηματοδοτείται από το 6ο Πρόγραμμα-Πλαίσιο της Ευρωπαϊκής Επιτροπής. Το πρόγραμμα αυτό εξετάζει κυρίως την ιδιωτικότητα των χωρο-χρονικών δεδομένων, όπως τα τηλεπικοινωνιακά δεδομένα τα οποία παράγονται από διάφορες φορητές συσκευές. Απότερος στόχος του GeoPKDD είναι να
αναπτύξει τη θεωρία, τις τεχνικές και τα συστήματα για την ανακάλυψη και την παράδοση γνώσης με τέτοιο τρόπο ώστε να διατηρείται η μυστικότητα των ευαίσθητων αυτών δεδομένων. Ειδικότερα, οι ερευνητές του συγκεκριμένου προγράμματος εξετάζουν μεθόδους για την αναπαράσταση, την αποθήκευση και τη διαχείριση των κινούμενων αντικειμένων. Παράλληλα, επινοούν αλγορίθμους για την προστασία της ευαίσθητης χωρο-χρονικής γνώσης έτσι ώστε να διατηρείται η ιδιωτικότητα των χρηστών. Στο πρόγραμμα ιδιαίτερη έμφαση δίνεται στην αναπαράσταση, την αποθήκευση και την διαχείριση των κινούμενων αντικειμένων και την ανωνυμία των χρηστών, όπως ο έλεγχος πρόσβασης, η κρυπτογραφία και η K-ανωνυμία.

7.2.2 Πρόγραμμα iTrust

Το πρόγραμμα iTrust [58] χρηματοδοτείται από τη μονάδα χρηματοδότησης Μελλοντικών και Αναδυόμενων Τεχνολογιών της Ευρωπαϊκής Επιτροπής (FET/IST) και εξετάζει τη διαχείριση της εμπιστοσύνης στα δυναμικά ανοικτά συστήματα. Σύμφωνα με τους ερευνητές του συγκεκριμένου προγράμματος, η επικυρωμένη ταυτότητα σε τέτοιου είδους συστήματα δεν είναι αρκετή για τη λήψη αποφάσεων σχετικά με τους περιορισμούς πρόσβασης και τον έλεγχο της απόδοσης και της αξιοπιστίας των οντοτήτων για τις οποίες δεν είναι διαθέσιμη προγενέστερη γνώση. Το πρόγραμμα αυτό χρησιμοποιεί ένα μοντέλο ασφαλείας βασισμένο στην εμπιστοσύνη και τη μυστικότητα για να αντιμετωπίσει την ανάλυση των δύσκολων αυτών παραμέτρων στα ανοικτά συστήματα. Τα συστήματα αυτά είναι ιδιαίτερα δυναμικά δεδομένου ότι οι οντότητες και οι υπηρεσίες μπορεί να αλλάζουν συνεχώς. Για το λόγο αυτό το σχετικό υπολογιστικό πρότυπο
εμπιστοσύνης θα πρέπει να προσαρμόζεται στις αλλαγές αυτές και να ενσωματώνει τα νομοθετικά πλαίσια που προκύπτουν.

Βασικότερος στόχος αυτού του προγράμματος είναι η συγκέντρωση της πείρας από τις προσανατολισμένες στην τεχνολογία επιστήμες, τους νόμους, τη φιλοσοφία και τις κοινωνικές επιστήμες για την εμπιστοσύνη και την ασφάλεια. Για το σκοπό αυτό αναλύεται η ηθική, η κοινωνιολογία και η ψυχολογία της εμπιστοσύνης, τα νομικά ζητήματα τα οποία υποστηρίζουν τη διαχείριση της καθώς και τα πρότυπα και η σημασιολογία της εμπιστοσύνης. Επιπρόσθετα, οι ερευνητές αναλύουν την τρέχουσα Ευρωπαϊκή και διεθνή νομοθεσία προκειμένου να διευκολύνουν την εναρμόνιση των ρυθμιστικών και νομοθετικών πλαισίων και την εξέλιξη τους, ώστε να υποστηριχθεί η γρήγορη λήψη των νέων τεχνολογιών στον τομέα των συστημάτων αυτών.

Τέλος, βασικός στόχος των ερευνητών είναι να διευκολύνουν την εμφάνιση μίας ευρέως αποδεκτής διοικητικής διαδικασίας εμπιστοσύνης για τα δυναμικά ανοικτά συστήματα, καθώς και την ανάπτυξη νέων παραδειγμάτων στον τομέα των συστημάτων αυτών που χρησιμοποιούν αποτελεσματικά τα υπολογιστικά πρότυπα εμπιστοσύνης.

7.2.3 Πρόγραμμα PORTIA

Η ανησυχία που προκύπτει τα τελευταία χρόνια για την ιδιοκτησία, τον έλεγχο, τη μυστικότητα και την ακρίβεια των δεδομένων που συλλέγονται από τους δημόσιους και ιδιωτικούς φορείς έχει γίνει μία κορυφαία προτεραιότητα για τους ερευνητές του προγράμματος PORTIA - Privacy, Obligations, and Rights in Technologies of Information Assessment [10]. Το πρόγραμμα αυτό χρηματοδοτείται από το Εθνικό Ίδρυμα Επιστημών των ΗΠΑ και εστιάζει τόσο στις τεχνικές προκλήσεις του χειρισμού ευαίσθητων
δεδομένων, όσο και στις πολιτικές και τα νομικά ζητήματα που αντιμετωπίζουν
tα υποκείμενα των συλλεγόμενων δεδομένων, τον κατόχου των δεδομένων
cαθώς και των χρηστών τους. Οι στόχοι του PORTIA είναι να σχεδιαστεί και
να αναπτυχθεί μία τεχνολογία επόμενης γενιάς για το χειρισμό των ευαίσθητων
δεδομένων των ατόμων που να είναι ποιοτικά καλύτερες από τις προηγούμενες
technologies, καθώς και η δημιουργία ενός εννοιολογικού πλαισίου για τη
χάραξη πολιτικής και φιλοσοφικής έρευνας στα δικαιώματα και τις ευθύνες
tων υποκειμένων των δεδομένων, των κατόχων και των χρηστών τους.

Το πρόγραμμα PORTIA ερευνά το σχεδιασμό και την ανάπτυξη μιας
υποδομής για τη διαχείριση και τη συντήρηση των ευαίσθητων
dedomenon για τη διάρκεια ζωής τους. Αρχικός σκοπός του προγράμματος αυτού είναι να
ισορροπηθούν οι πολλές forbes επικροούμενοι παράμετροι ενός asfalioús
systimatos, όπως η μυστικότητα, η ανωνυμία, η αναδεικνυμική και η
ακεραιότητα. Για το λόγο αυτό στο πρόγραμμα τονίζεται η σημαντικότητα της
βαθύτερης κατανόησης και της διευκρίνισης των δικαιωμάτων όλων των
συμμετεχόντων oντοτήτων, όπως τα υποκειμένα, οι κάτοχοι και οι χρήστες των
dedomenon.

Προκειμένου να επιτευχθεί η ασφάλεια των βάσεων δεδομένων,
pioptarixikós stóxos eínai h dhmiourgyia mekaniasmón elégχou prósbashης που
na epitrépouν tη riθή dhílsw twn dikanwmátwn twn chrístówn páno sta
dedomena. To prógrámma PORTIA smmplhronve autés tis prospátheiēes
uionthénta mebððous ois oipois eπiknerónontai stous chrístes kai ta
dedomena gia tin astfáleia ton básewn dedomenon. Parállella, oi erewnhtés
exestáçoun trópous kai mebððous gia tin próstasía tis taustótptas twn
chrístówn kai protéinovn néous orísmou tis μυστικότητας που παρέχουν
megálh próstasía. Metá apó autó to polú sηmanistikí bhìma, oi erewnhtés
esstáçoun stin anáptuxi technikon gia tì diatírsh tis μυστικότηtaς ois
oipois na einai parállela upologistikà apoðotikèes.

Idiáiterh eύfmasia dínetai sti diatírsh tis μυστικότηtaς tis thèsis
sthn oipoiá brísketai kápoioi chrísthès. Súmfwona me tous erewnhtés, ta
systímatasa eπitírshès dein thà prepei na apokalúspoun tin taustótpta toun
chrísth týmeta tis thèsis sthn oipoiá brískountan kápoia sýgkekriwménh xronikh
stigmì. Parállella, oi foréies oi oipoioi sunevgerázontai kai échovn kápoia koiná
ευαίσθητα δεδομένα θα πρέπει να εξασφαλίζουν ότι δεν θα αποκαλύπτονται ολόκληρες οι βάσεις δεδομένων από τον ένα φορέα στον άλλον, ούτε θα προκύπτουν όλες οι πληροφορίες από αντιστοιχίσεις των δεδομένων τους. Τέλος, κατά τη συνεργασία των διαφόρων φορέων θα πρέπει να παρέχεται η μέγιστη ασφάλεια χρησιμοποιώντας κρυπτογραφικά πρωτόκολλα τα οποία θα καθορίζουν την πρόσβαση στα κοινά δεδομένα.

7.2.4 Πρόγραμμα KDubiq

Το KDubiq (Knowledge Discovery in Ubiquitous Environments) [64] αποτελεί ένα χρηματοδοτούμενο πρόγραμμα από το 6ο Πρόγραμμα-Πλαίσιο της Ευρωπαϊκή Επιτροπής το οποίο έχει ως σκοπό την υποστήριξη ερευνητικών δραστηριοτήτων για την ανακάλυψη γνώσης στα σύγχρονα συστήματα. Προκειμένου να δημιουργηθεί μία ομοιογενής πλατφόρμα για την οικοδόμηση ευφυών συστημάτων ανακάλυψης γνώσης το πρόγραμμα υποστηρίζει πολλές δραστηριότητες, όπως εργαστήρια, θερινά σχολεία, forums και άλλα, στα οποία εμπειρογνώμονες από την έρευνα και τους ιδιωτικούς και δημόσιους φορείς μπορούν να προτείνουν τις μεθοδολογίες και τις προσεγγίσεις τους. Ένα από τα θέματα έρευνας του συγκεκριμένου προγράμματος είναι τα χωρο-χρονικά δεδομένα. Ιδιαίτερη εμφάση δίνεται στον τρόπο με τον οποίο μπορεί να γίνει ανακάλυψη γνώσης σε τέτοιου είδους δεδομένα, στα βασικά χαρακτηριστικά των συστημάτων παροχής υπηρεσιών θέσης, καθώς και στην ανάλυση των δεδομένων σε διάφορα κατανεμημένα περιβάλλοντα και σε φορητές συσκευές.
7.2.5 Πρόγραμμα geopriv

Το Geographic Location/Privacy (geopriv) [56] αφορά τα συστήματα παροχής υπηρεσιών θέσης. Ο αρχικός σκοπός του προγράμματος geopriv είναι να αξιολογήσει τις απαιτήσεις μυστικότητας και ακεραιότητας των δεδομένων θέσης προκειμένου να μεταδίδονται με ελεγχόμενο και ασφαλή τρόπο.

Πιο συγκεκριμένα, οι ερευνητές του προγράμματος εξετάζουν τα ζητήματα ασφαλείας (και ιδιαίτερα τη μυστικότητα) κατά την απόκτηση και μετάδοση των γεωγραφικών πληροφοριών θέσης για οποιαδήποτε μέθοδο εντοπισμού των φορητών συσκευών και αν χρησιμοποιείται. Το πρόγραμμα αυτό εστιάζει στον προσδιορισμό των απαιτήσεων ασφάλειας, καθώς και ενός επιλεγμένου σχήματος μετάδοσης προκειμένου να ικανοποιηθούν οι απαιτήσεις αυτές. Οι κανόνες ασφάλειας για τα δεδομένα θέσης εκτός από τη μετάδοση της θέσης αφορούν και τη συλλογή, χρήση, επεξεργασία, διατήρηση και μεταφορά τους. Οι πολιτικές μυστικότητας που προτείνονται για τη μεταβίβαση των ευαίσθητων δεδομένων θέσης μπορούν να χρησιμοποιηθούν και για υπηρεσίες έκτακτης ανάγκης. Επιπλέον, οι ερευνητές εξετάζουν και άλλες κρίσιμες παραμέτρους ασφάλειας σε τέτοιου είδους συστήματα, όπως η ανωνυμία και η αυθεντικοποίηση των χρηστών.

Τέλος, η ομάδα εργασίας αυτού του προγράμματος προτείνει ένα μοντέλο ασφάλειας το οποίο αποτελείται από τέσσερις βασικές οντότητες: τη γεννήτρια θέσης, τον εξυπηρετητή θέσης, τον παραλήπτη θέσης και τον κάτοχο κανόνων μυστικότητας. Οι οντότητες αυτές συνεργάζονται μεταξύ τους για την ασφαλή δημιουργία και μεταφορά των χωρικών δεδομένων. Η συνεργασία τους βασίζεται στους κανόνες μυστικότητας που διατηρεί η τελευταία οντότητα (δηλαδή ο κάτοχος κανόνων μυστικότητας). Τους
κανόνες αυτούς τους καθορίζουν οι χρήστες και πρέπει και αυτοί να επικυρώνουνται και να προστατεύονται. Θα πρέπει να σημειωθεί εδώ ότι στόχος των ερευνητών είναι να επεκταθεί η χρήση του μοντέλου που προτείνουν και σε άλλου είδους δεδομένων, εφόσον τα αποτελέσματά τους κρίθον επιτυχή.

7.2.6 Πρόγραμμα PRIME

Το πρόγραμμα PRIME (Privacy and Identity Management of Europe) [86] αποτελεί ένα Ευρωπαϊκό ερευνητικό πρόγραμμα το οποίο χρηματοδοτείται από το 6ο Πρόγραμμα-Πλαίσιο της Ευρωπαϊκής Επιτροπής. Μέλη της ερευνητικής ομάδας αυτού του προγράμματος αποτελούν Πανεπιστήμια, ερευνητικά κέντρα και εταιρείες από Ευρωπαϊκές και διεθνείς χώρες, όπως το Βέλγιο, η Γαλλία, η Γερμανία, η Ιταλία, η Ολλανδία, η Σουηδία, η Ελβετία, το Ηνωμένο Βασίλειο και οι ΗΠΑ.

Ο βασικότερος στόχος των ερευνητών του προγράμματος είναι η δημιουργία ενός λειτουργικού συστήματος προάσπισης της ιδιωτικότητας των χρηστών. Το πρότυπο αυτό παρουσιάζεται μέσα από σύγχρονα συστήματα παροχής υπηρεσιών, όπως οι επικοινωνίες μέσω διαδικτύου και οι υπηρεσίες που βασίζονται στη θέση των χρηστών.

Στα πλαίσια του PRIME οι ερευνητές περιγράφουν και αναλύουν εφαρμογές λύσεις για την ενίσχυση της διασφάλισης ιδιωτικότητας, δημιουργώντας ένα μοντέλο και προτείνοντας μία αρχιτεκτονική για τη διασφάλιση των απαιτήσεων αυτών. Επιπρόσθετα περιγράφουν τις οδηγίες σχεδιασμού και τα απαραίτητα πρωτόκολλα για τη λειτουργία του προτεινόμενου συστήματος. Τέλος, αξιολογούν την εφαρμογή του προτεινόμενου συστήματος.
Οι τρέχουσες πολιτικές μυστικότητας δίνουν στους χρήστες περιορισμένα δικαιώματα. Οι χρήστες δε μπορούν να ελέγξουν αν ο φορέας παροχής υπηρεσιών εμμένει στην πολιτική ασφάλειας η οποία συμφωνήθηκε αρχικά, ούτε μπορούν να δουν αν τηρεί τις νομικές του υποχρεώσεις. Για την αντιμετώπιση αυτών των προβλημάτων το σύστημα που προτείνουν θέτει τον χρήστη επικεφαλής στη διαχείριση ιδιωτικότητα της ταυτότητας. Σε αυτό το πλαίσιο οι χρήστες ενθαρρύνονται να αξιολογούν τις πολιτικές μυστικότητας και την εμπιστοσύνη των συμβαλλόμενων μερών. Επιπρόσθετα, θα πρέπει να συλλέγονται όσο το δυνατό λιγότερα προσωπικά δεδομένα. Αυτό από την πλευρά των φορέων παροχής υπηρεσιών σημαίνει να διατηρούν μόνο τα απαραίτητα για τη συγκεκριμένη υπηρεσία δεδομένα ή τα προσωπικά δεδομένα να καθίστανται ανώνυμα. Επίσης ο χρήστης πρέπει να γνωρίζει πως μπορεί να ελέγχει τα προσωπικά του δεδομένα.

Τέλος, για την αντιμετώπιση αυτών των προβλημάτων το PRIME θέτει τον χρήστη επικεφαλής στη προάσπιση ιδιωτικότητάς του και προτείνει μία διεπαφή με το σύστημα διαχείρισης της ταυτότητας του χρήστη, η οποία επιτρέπει στους χρήστες να δημιουργήσουν ψευδώνυμα, να συνδέσουν τα προσωπικά τους δεδομένα με τα ψευδώνυμα αυτά, να βοηθήσουν το χρήστη στην κατανόηση των πολιτικών μυστικότητας και άλλα.
7.2.7 29ο Διεθνές Συνέδριο Προστασίας Δεδομένων

Το 29ο διεθνές συνέδριο για την προστασία δεδομένων (29th International Conference of Data Protection and Privacy Commissioners) [87] πραγματοποιήθηκε φέτος στον Καναδά στα πλαίσια του Privacy Horizons: Terra Incognita με την υποστήριξη διαφόρων διεθνών εταιρειών και οργανισμών, όπως η Microsoft, IBM, iapp, symantec, Google και Oracle. Στα πλαίσια αυτά έχουν πραγματοποιηθεί στο παρελθόν συνέδρια τα οποία αφορούσαν ζητήματα εθνικής ασφάλειας, ασφάλειας στα σύγχρονα υπολογιστικά συστήματα καθώς και προστασία διαφόρων ειδών δεδομένων (ιατρικά δεδομένα, δεδομένα που συλλέγονται από τα σύγχρονα υπολογιστικά συστήματα, δεδομένα που συλλέγονται από τις φορητές συσκευές και άλλα).

Η συνεχής πρόοδος της τεχνολογίας και η εκθετική αύξηση διασυνοριακής ροής δεδομένων και παράνομης συλλογής προσωπικών δεδομένων είναι το βασικότερο έναυσμα για το αντικείμενο έρευνας του 29ου συνεδρίου για την προστασία δεδομένων. Ο βασικότερος στόχος του συνεδρίου αυτού είναι να ενθαρρύνει την ανταλλαγή ιδεών μεταξύ ερευνητών από όλο τον κόσμο, καθώς και να δημιουργήσει τις ευκαιρίες για την προώθηση αυτών των ιδεών. Για το λόγο αυτό οι συμμετέχοντες ερευνητές εξελίσσουν νομοθετικές και τεχνικές προσεγγίσεις για την αυξημένη προστασία των δεδομένων, ενώ παράλληλα προτείνουν νέες λύσεις για την αντιμετώπιση αυτών των προκλήσεων, καθώς και τις επιπτώσεις στους ανθρώπους, τους οργανισμούς και την εθνική ασφάλεια. Στο φετινό συνέδριο ιδιαίτερη έμφαση από τους ερευνητές δόθηκε στην ασφάλεια των πληροφοριών οι οποίες προκύπτουν από τις υπηρεσίες θέσης, την προστασία
δεδομένων θέσης καθώς και τη νομοθεσία η οποία αφορά τις πληροφορίες αυτές. Επίσης, ιδιαίτερη έμφαση δόθηκε από τους ερευνητές στην ασφάλεια πληροφοριών που προκύπτουν από τις υπηρεσίες θέσης, την προστασία χωρο-χρονικών δεδομένων, καθώς και τη νομοθεσία που αφορά τα δεδομένα αυτά.

7.3 Επίλογος

Η εκρηκτική αύξηση χρήσης φορητών συσκευών και των υπηρεσιών που προσφέρουν έχει κεντρίσει το ενδιαφέρον και στον τομέα της έρευνας. Οι μεγαλύτεροι Ευρωπαϊκοί και διεθνείς φορείς χρηματοδότησης της έρευνας κατανέμουν το μεγαλύτερο ποσοστό χρηματοδότησης στον τομέα των τεχνολογιών και των επικοινωνιών με σκοπό να υποστηρίζουν τις εγκαταστάσεις και τον εξοπλισμό που απαιτούνται για την ανάπτυξη καλύτερων συνθηκών γνώσης στους ερευνητές. Τέλος, διάφορα ερευνητικά προγράμματα τρέχουν αυτή την περίοδο με σκοπό την ανάπτυξη των απαιτήσεων και την ανάπτυξη τεχνολογικών λύσεων στα σύγχρονα υπολογιστικά συστήματα. Στο κεφάλαιο αυτό περιγράψαμε τον τρόπο με τον οποίο οι διάφοροι οργανισμοί χρηματοδοτούν την έρευνα κυρίως στον τομέα της ασφάλειας των επικοινωνιών, καθώς και τον τρόπο με τον οποίο οι ερευνητές προσεγγίζουν λύσεις και μεθόδους για την επίτευξη αυτών των στόχων στα σύγχρονα συστήματα.
Κεφάλαιο 8

Συμπεράσματα

Τα συστήματα παροχής υπηρεσιών θέσης αποτελούν ίσως την πιο συναρπαστική εξέλιξη των τεχνολογικών επιστημών σήμερα. Οι υπηρεσίες που προσφέρονται από τα συστήματα αυτά είναι πολύπλοκες, ενώ προκειμένου να είναι και εξατομικευμένες για τον κάθε χρήστη απαιτούν τη γνώση πολλών προσωπικών δεδομένων των χρηστών, καθώς και παραμέτρων του περιβάλλοντος στο οποίο αυτοί κινούνται. Η αλματώδης αύξηση της χρήσης τέτοιων είδους συστημάτων, καθώς και τα ερωτήματα ιδιωτικότητας τα οποία προκύπτουν από τη χρήση τους, αποτελούν ζητήματα τα οποία έχουν αντιμετωπιστεί με αμέριστο ενδιαφέρον από πολλούς τομείς της επιστημονικής κοινότητας.

Το πρώτο και βασικότερο βήμα για την εξασφάλιση της προστασίας της ιδιωτικότητας των ανθρώπων είναι η θέσπιση νόμων και η ύπαρξη εποπτικών αρχών για τον έλεγχο της τήρησής τους. Οι περισσότεροι χώρες ανά τον κόσμο έχουν θεσπίσει νόμους για την προστασία των δεδομένων τηλεπικοινωνιών, ενώ παρατηρείται η διάθεση να υπάρξει μία όσο το δυνατόν πιο κοινή πολιτική προστασίας των ανθρώπων και της
προσωπικής τους ζωής, όπως συμβαίνει με τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και τις χώρες του APEC.

Παρά ταύτα, ένα πολύ σημαντικό μέρος της προστασίας αυτής προκύπτει από τη δημιουργία συστημάτων και μεθόδων ασφάλειας και ανωνυμίας. Τα υπάρχοντα συστήματα χρησιμοποιούν μεθόδους, όπως οι πολιτικές ασφαλείας, η κρυπτογραφία και η Κ-ανωνυμία. Παρόλα αυτά, η διαρκής βελτίωση και η δημιουργία νέων, ολοένα και πιο εξατομικευμένων υπηρεσιών, απαιτεί τη βελτίωση των υπαρχόντων μεθόδων ασφάλειας. Για το λόγο αυτό, ερευνητές από όλο τον κόσμο έχουν στρέψει την προσοχή τους στην ανάπτυξη νέων και συστημάτων τα οποία είναι αποδοτικά, ενώ παράλληλα, διατηρούν τη μυστικότητα των προσωπικών δεδομένων και την ανωνυμία των χρηστών τους.
Βιβλιογραφία


URL: http://www.adae.gr

URL: http://www.dpa.gr


URL: http://www.galecia.com/weblog/mt/archives/Ayre_DataMining.pdf


URL: http://www.jisc.ac.uk/uploaded_documents/archiving_legal.pdf


[18] Clifton Ch., Kantarcioglu M. and Vaidya J. Defining Privacy for Data Mining.
URL: http://www.cimic.rutgers.edu/~jsvaidya/pub-papers/ngdm-privacy.pdf

[19] Computer Emergency Response Team – CERT.
URL: http://www.cert.org


URL: http://www.iispartners.com/china.pdf

URL: http://www.bakercyberlawcentre.org
URL: http://www.dagstuhl.de/Reports/98471.pdf

URL: http://www.ydt.gr


[27] EDPS - European Data Protection Supervisor.
URL: http://www.edps.eu.int/legislation/Opinions_A/05-09-26_Opinion_data_retention_EN.pdf

URL: http://www.techlawjournal.com/cong107/privacy_/location/s1164is.asp

[29] EETT - Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων.
URL: http://www.eett.gr

URL: http://www.enisa.europa.eu

[32] Ernst and Young. Data Protection in the European Union and other Selected Countries.

URL: http://www.etsi.org

[34] Eurescom - The European Institute for Research and Strategic Studies in Telecommunications.
URL: http://www.eurescom.de

[35] ΕΥΠ - Εθνική Υπηρεσία Πληροφοριών.
URL: http://www.nis.gr

[36] Ευρωπαϊκή Επιτροπή
URL: http://www.europa.eu

[37] ΕΦΤΑ - Ελληνικός Φορέας Πρόληψης Τηλεπικοινωνιακής Απάτης
URL: http://www.ote.gr/efta

[38] FIINA- Forum for International Irregular Network Access.
URL: http://www.fiina.org

URL: http://www.cordis.europa.eu/fp7


URL: http://www-kdd.isti.cnr.it/chiara/elencopubbl/acmgis05.pdf

URL: http://www.di.uniba.it/~malerba/activities/mstd/1.pdf


[47] Greek Research and Technology Network/Computer Emergency Response Team – GRNET/CERT.
URL: http://cert.grnet.gr


[58] iTrust project. URL: http://www.itrust.uoc.gr

[59] ITU - International Telecommunication Union. URL: http://www.itu.int


[64] KDubiq project. URL: http://www.kdubiq.org


[67] LawNet. URL: http://www.lawnet.gr


[72] MITRE. URL: http://www.mitre.org


URL:  http://www.old.netobjectdays.org/pdf/03/papers/industry/555.pdf

[77] NIH - National Institutes of Health.
URL: http://www.nih.gov

[78] Nissenbaum H. Privacy as Contextual Integrity.

URL: http://www.nsa.gov

[80] NSF - National Science Foundation.
URL: http://www.nsf.gov

[81] Oliveira St. and Zaiane O. Toward Standardization in Privacy-Preserving Data Mining.
URL:  http://www.cs.ualberta.ca/~zaiane/postscript/dm-ssp04.pdf

[82] Olivier M. Database Privacy. Balancing Confidentiality, Integrity and Availability.

URL:  http://www.ebusinessforum.gr

URL: http://knoesis.wright.edu/students/mperrv/knoesis-tr-2007-01.pdf

[86] PRIME project - Privacy and Identity Management of Europe.
URL: https://www.prime-project.eu

[87] Privacy Horizons: Terra Incognita. 29th International Conference of Data Protection and Privacy Commissioners.

[88] Privacy International.
URL: http://www.privacyinternational.org

[89] Privacy issues in Hong Kong, Japan and Australia. Hong Kong, April 2002.
URL: https://www.whitecase.com/files/Publication

URL: http://www.dir.state.tx.us/taskforce/report/privacy.pdf


[98] Spatio-temporal Data Mining for Location-based Services. URL: http://gyozo.gidofalvi.net/docs/STDM.PDF


[102] Su Ch. and Sakurai K. Secure Computation Over Distributed Databases.

URL: http://www.privacy.cs.cmu.edu/people/sweeney/kanonymity2.pdf


URL: http://www.privacy.cs.cmu.edu/people/sweeney/explosion2.pdf

URL: http://www.privacy.cs.cmu.edu/people/sweeney/kanonymity.pdf

URL: http://www.privacy.cs.cmu.edu/dataprivacy/projects/pel/pel.pdf


[111] Trajectory Data Warehousing Project.

[112] Τράπεζα Νομικών Πληροφοριών.
URL: http://www.dsanet.gr

URL: http://www.hhs.gov

URL: http://www.ftc.gov

URL: http://www.cs.uic.edu/~wolfson/mobile_ps/ngits02.pdf

URL: http://www.whitecase.com


URL: http://dpse.eas.asu.edu/tdsm/papers/JSPE05.pdf


URL: http://icsd.i2r.a-star.edu.sg/publications/ZhuHuaFei_2004_VTC_0406_05.pdf