ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ, ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ ΚΑΙ ΤΟ ΝΟΜΙΚΟ ΤΗΣ ΠΛΑΙΣΙΟ

ΣΙΣΜΑΝΙΔΟΥ ΧΡΥΣΑ-ΑΝΝΑ

Επιβλέπων Καθηγητής: Σταμούλης Γεώργιος

Βόλος, 2019

UNIVERSITY OF THESSALY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

DIPLOMA THESIS

PERSONAL ONLINE DATA PROTECTION, DIGITAL SIGNATURE AND ITS LEGAL FRAMEWORK

SISMANIDOU CHRYSA-ANNA

Supervisor: Stamoulis Georgios

Volos, 2019

Ευχαριστίες

Οφείλω θερμές ευχαριστίες στον επιβλέποντα Καθηγητή κ. Σταμούλη Γεώργιο για την πολυποίκιλη φροντίδα, τη συνεχή επιστημονική στήριξη αλλά και την ανθρώπινη συμπαράσταση του που αποτέλεσαν ανεκτίμητο οδηγό και συντέλεσαν στην επιτυχημένη εκτέλεση της διπλωματικής μου εργασίας.

Επίσης, ευχαριστώ θερμά την οικογένεια μου για την συνεχή ενθάρρυνση και ψυχική υποστήριξη που μου προσέφεραν κατά τη διάρκεια των σπουδών μου.

Βόλος, Μάρτιος, 2019

Αφιερωμένο

στον Ηλία, την οικογένεια μου και τους φίλους μου

ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ, ΗΛΕΚΤΡΟΝΙΚΗ ΥΠΟΓΡΑΦΗ ΚΑΙ ΤΟ ΝΟΜΙΚΟ ΤΗΣ ΠΛΑΙΣΙΟ

Περίληψη

Το πρώτο σκέλος της παρούσας διπλωματικής εργασίας επικεντρώνεται στην ανάλυση των προβλημάτων και των κινδύνων που προκύπτουν μέσω της συλλογής και επεξεργασίας προσωπικών δεδομένων κατά τη διάρκεια των ηλεκτρονικών επικοινωνιών, ενώ δίνεται ιδιαίτερη έμφαση στους τρόπους προστασίας της ιδιωτικής ζωής των υποκειμένων τους, δηλαδή των ατόμων που αφορούν τα προσωπικά δεδομένα.

Στη συνέχεια, το δεύτερο και τρίτο σκέλος αντίστοιχα, ασχολείται αναλυτικά με τα ηλεκτρονικά μέσα των ηλεκτρονικών συναλλαγών και ιδιαίτερα με την ηλεκτρονική υπογραφή ως μέσο διατυπώσεως της γνησιότητας των ηλεκτρονικών εγγράφων και το νομοθετικό πλαίσιο που έχει θεσπιστεί ή έχει τροποποιηθεί με κύριο μέλημα την κάλυψη των κενών που δημιουργήθηκαν λόγω της ραγδαίας αύξησης των τεχνολογιών της πληροφορικής.

Abstract

The first of the present thesis is mainly centered around the analysis of the risks and challenges that arise due to the gathering and processing of personal data through means of digital communications. Great emphasis will be given on the ways to securing and protecting the personal life of the ones such data belong.

On the second and third part accordingly, will be covering matters of digital transactions in detail and digital signature as a mean of certifying digitally signed documents and the legislative framework, either created or modified, concerning covering the gap that was created as a result of the breakthrough in technology.

Περιεχόμενα

1.3 Ρυθμίσεις για την προστασία των προσωπικών δεδομένων στο χώρο των ηλεκτρονικών επικοινωνιών

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

2.1 Ηλεκτρονικά Έγγραφα

2.2 Ορισμός και είδη Ηλεκτρονικής Υπογραφής

Εισαγωγή

Η συνεχής εξέλιξη και ανάπτυξη της τεχνολογίας και ειδικότερα οι τομείς που σχετίζονται με τους ηλεκτρονικούς υπολογιστές έχουν διεισδύσει σε πολλές πτυχές της καθημερινότητα μας τα τελευταία χρόνια. Κατά λογική ακολουθία, είναι αναμενόμενο η ηλεκτρονική επικοινωνία να είναι ένα από τα κυρίαρχα μέσα επικοινωνίας στη σύγχρονη κοινωνία ή όπως λέγεται αλλιώς στην Κοινωνία της Πληροφορίας. Αντικείμενο αυτών των επικοινωνιών είναι δεδομένα, πολλά από τα οποία συμπίπτουν στην έννοια των «δεδομένων προσωπικού χαρακτήρα». Ο μεγάλος όγκος δεδομένων προσωπικού χαρακτήρα που μεταδίδεται μέσω ηλεκτρονικών επικοινωνιών εγκυμονεί κινδύνους παραβίασης τους από τρίτους.

Η έλευση και η εξάπλωση του διαδικτύου έδωσε τη δυνατότητα σε οποιονδήποτε περιηγητή την ευκαιρία για μαζική άντληση δεδομένων που αφορούν συνανθρώπους του. Η επίφαση ανωνυμίας που δημιουργεί το διαδίκτυο επαναπαύει τους χρήστες νιώθοντας την φαινομενική ασφάλεια της ανωνυμίας των προσωπικών τους στοιχείων. Αυτό δημιουργεί ένα πρόσφορο πεδίο δράσης σε αυτούς που χρησιμοποιούν το διαδίκτυο ως μέσο παραβίασης, υποκλοπής και αξιοποίησης των προσωπικών δεδομένων του υποκειμένου για δικό τους όφελος.

Συνεπώς, τα δεδομένα αυτά χρήζουν ειδικής προστασίας καθώς αποτελούν ένα ιδιαίτερα ευαίσθητο κομμάτι στο χώρο των ανθρωπίνων δικαιωμάτων και της προστασίας της προσωπικότητας, το οποίο είναι αρκετά συχνό φαινόμενο στις μέρες μας καθώς οι κίνδυνοι παραβίασης τους ποικίλλουν. Από άποψη νομικής προστασίας, δημιουργήθηκε ένας αυτοτελής και αυτόνομος κλάδος, το «Δίκαιο της πληροφορικής» το οποίο προέκυψε εξαιτίας της χρήσης ηλεκτρονικής τεχνολογίας της πληροφορικής με στόχο την κάλυψη των κενών που υπάρχουν σε αυτόν τον νέο τρόπο συσσώρευσης, οργάνωσης, επεξεργασίας και διάδοσης πληροφοριών.

Μερικά από τα κυρίαρχα θέματα που διαπραγματεύεται το «Δίκαιο της Πληροφορικής» είναι η προστασία λογισμικού και λοιπών έργων (βάσεις

δεδομένων, πολυμέσα, ψηφιακά έργα στο διαδίκτυο, ιστοσελίδες κ.α.), οι συμβάσεις πληροφορικής (συμβάσεις υλικού ηλεκτρονικού υπολογιστή, λογισμικού, παραχώρησης βάσεων δεδομένων, υπηρεσιών διαδικτύου κ.α.), οι ηλεκτρονικές συναλλαγές (ηλεκτρονικό εμπόριο, προστασία καταναλωτών στις ηλεκτρονικές συναλλαγές, ηλεκτρονικά έγγραφα και ηλεκτρονικές υπογραφές), η προστασία προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες (το συνταγματικό πλαίσιο και το γενικό πλαίσιο προστασίας των δεδομένων) και η ποινική ρύθμιση εγκληματικών πράξεων που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή (απάτη υπολογιστή, παραβίαση απορρήτων, χωρίς συγκατάθεση αντιγραφή και πρόσβαση σε δεδομένα , πλαστογραφία με ηλεκτρονικό έγγραφο).

Μέσα λοιπόν από αυτό το πλέγμα, των σύνθετων σχέσεων και κινδύνων που προκύπτουν στα πλαίσια της ψηφιακής εποχής, το πρώτο μέρος της παρούσας διπλωματικής εργασίας θα αναλύσει τους πιθανούς κινδύνους που μπορούν να προκύψουν μέσω της ελεύθερης χρήσης των ηλεκτρονικών επικοινωνιών και του διαδικτύου, καθώς και τα μέτρα προστασίας που απαιτούνται για τη προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής του ατόμου.

Το δεύτερο μέρος έχει στόχο την εξοικείωση του αναγνώστη με τη τεχνολογία της ηλεκτρονικής υπογραφής καθώς θα γίνει αναλυτική περιγραφή της έννοιας, των ειδών αλλά και των εφαρμογών της στην καθημερινή ζωή. Ακόμη θα μελετηθεί αν και κατά πόσο η υπάρχουσα νομοθεσία περί ηλεκτρονικών υπογραφών ικανοποιεί το ζητούμενο της ασφάλειας των ηλεκτρονικών συναλλαγών. Στο τρίτο μέρος της διπλωματικής παρουσιάζεται λεπτομερώς το νομοθετικό πλαίσιο που υπάρχει μέχρι σήμερα για τις ηλεκτρονικές υπογραφές σε Διεθνές και Εθνικό πλαίσιο, οι νομοθετικές προσεγγίσεις των ηλεκτρονικών υπογραφών και η αναγνώριση τους ως μέσο πιστοποίησης ηλεκτρονικών συναλλαγών.

ΜΕΡΟΣ ΠΡΩΤΟ

1.1 Εννοιολογική Προσέγγιση του Δικαίου της Πληροφορικής

1.1.1 Ορισμός του Δικαίου της Πληροφορικής

Ένας από τους πιο πρόσφατους κλάδους της νομικής επιστήμης, στον οποίο εντάσσεται ένα σύνολο κανόνων που ρυθμίζει διάφορα προβλήματα και σχέσεις που προκύπτουν, λόγω των ιδιαίτερων γνωρισμάτων της ηλεκτρονικής τεχνολογίας της πληροφορικής είναι το «Δίκαιο της Πληροφορικής». Κύρια αρμοδιότητα του είναι η θέσπιση ρυθμίσεων που είναι σχετικές με τις τεχνολογίες αυτές και η επίλυση προβλημάτων που αφορούν είτε ψηφιακά αγαθά (π.χ. λογισμικό, βάσεις δεδομένων, πολυμέσα) είτε υπηρεσίες (καταχώρηση ονόματος χώρου διαδικτύου, παροχή πρόσβασης στο δίκτυο κ.α.) αλλά και σημαντικά κενά στην προστασία των προσωπικών δεδομένων και ατομικών δικαιωμάτων του ατόμου που προϋπάρχουσες νομοθεσίες δεν μπορούν να επιλύσουν.[1]

Δύο σημαντικοί παράγοντες που συνετέλεσαν στη δημιουργία του νέου αυτού κλάδου της νομικής και στην ύπαρξη του «Δικαίου της πληροφορικής» είναι η τεχνολογία της πληροφορικής και η καθεαυτό έννοια της πληροφορίας. Παρόλο που μελετά ζητήματα που προκύπτουν μέσω της λειτουργίας των εφαρμογών των τεχνολογιών της πληροφορικής και των επικοινωνιών και γενικότερα ελέγχει με νομικά μέσα τις κοινωνικές επιδράσεις τους εντάσσεται στον ευρύτερο κλάδο της νομικής και περιλαμβάνει ένα πλήθος νομικών κανόνων που ρυθμίζουν τόσο την επεξεργασία δεδομένων στο πλαίσιο τεχνολογικών εφαρμογών off-line όσο και στο πλαίσιο διαδικτυακών εφαρμογών.

Πολύ συχνά γίνεται χρήση μεθόδων και μεθοδολογικών εργαλείων του κλάδου του δικαίου που αντιστοιχούν σε κάθε πρόβλημα, σε σημείο που αυτό να ταυτίζεται σχεδόν πάντα με τον κλάδο στον οποίο αναφέρεται. Για παράδειγμα, σε

περιπτώσεις που αφορούν την προστασία των προσωπικών δεδομένων χρησιμοποιείται το συνταγματικό και διοικητικό δίκαιο ενώ για τις τηλεπικοινωνιακές και ηλεκτρονικές συναλλαγές θεσπίστηκαν νέα ειδικά νομοθετικά πλαίσια.

Εξαιτίας της συνεχούς ανάπτυξης και των ραγδαίων εξελίξεων στον τομέα της τεχνολογίας είναι αναγκαίες οι συχνές τροποποιήσεις με τη θέσπιση νέων κανόνων ή μεταβολή των υπαρχόντων. Χαρακτηριστική περίπτωση είναι η αντικατάσταση της Οδηγίας 96/66/ΕΚ με την Οδηγία 2002/58/Κ η οποία μεταφέρθηκε στο ελληνικό δίκαιο με τον νόμο 3471/2006 και αφορούσε την προστασία των προσωπικών δεδομένων στον τομέα των τηλεπικοινωνιών. Ο νέος αυτός κλάδος αναζητεί τις δυνατότητες προσαρμογής των παραδοσιακών κλάδων δικαίου με την προσαρμογή τους στα νέα δεδομένα ενώ παράλληλα εξελίσσονται νέοι κλάδοι όπως το ηλεκτρονικό εμπόριο και το δίκαιο της προστασίας των προσωπικών δεδομένων.[2]

Πολύ συχνά συναντώνται και άλλοι όροι αντί του «Δικαίου της Πληροφορικής» όπως «Δίκαιο της Πληροφορίας» (Information Law), Δίκαιο Η/Υ (Computer Law) κ.α., κυρίως σε χώρες του εξωτερικού και αναφέρονται ουσιαστικά στο ίδιο αντικείμενο.

1.1.2 Οι προκλήσεις που έχει να αντιμετωπίσει το Δίκαιο της Πληροφορικής

Η εφαρμογή κανόνων από τους εκάστοτε κλάδους δικαίου δεν αρκεί για να προσφέρει λύση σε συγκεκριμένες κατηγορίες προβλημάτων που προκύπτουν, αλλά απαιτείται γενικότερη κατανόηση των τεχνολογικών δεδομένων. Αυτό συνεπάγεται ότι νομικοί που έχουν γενική παιδεία και όχι κάποια στοιχειώδη γνώση εννοιών της τεχνολογίας της πληροφορικής θα έρθουν αντιμέτωποι με προβλήματα κατανόησης της τεχνολογικής πραγματικότητας.

Τα «ψηφιακά αγαθά» όπως χαρακτηρίζονται το λογισμικό , οι βάσεις δεδομένων, τα πολυμέσα και οι υπηρεσίες της νέας τεχνολογίας όπως η καταχώρηση ονόματος χώρου διαδικτύου, η παροχή πρόσβασης στο δίκτυο κοκ, είναι μερικά από τα προβλήματα που καλείται να αντιμετωπίσει το δίκαιο της πληροφορικής ενώ δεν παραλείπουμε να αναφέρουμε τις περιπτώσεις που σχετίζονται με τη προστασία των ατομικών δικαιωμάτων και συνταγματικών

ελευθεριών του ατόμου μέσω της χρήσης των εφαρμογών της νέας τεχνολογίας. Στην ιδιαίτερη περίπτωση της απελευθέρωσης των τηλεπικοινωνιών απαιτείται η δημιουργία ενός νέου ρυθμιστικού πλαισίου για τις τηλεπικοινωνίες και για τις ηλεκτρονικές επικοινωνίες.[3]

1.1.3 Δίκαιο της Πληροφορίας

Στη σύγχρονη εποχή, η οποία χαρακτηρίζεται και ως «εποχή της Πληροφορίας» έχει ιδιαίτερη σημασία η ελευθερία της πληροφόρησης η οποία σημείωσε ραγδαία ανάπτυξη μέσω της εξέλιξης της τεχνολογίας και του διαδικτύου. Η πληροφορία πλέον έχει τεράστια οικονομική και πολιτιστική αξία καθώς δεν αφορά μόνο περιπτώσεις προγραμμάτων Η/Υ που περιέχουν πληροφορίες, αλλά και πληροφορίες που λειτουργούν ως «πρώτη ύλη» για βάσεις δεδομένων. [4]

Για τον λόγο αυτό, θεωρείται από πολλούς συγγραφείς ότι η πληροφορία αποτελεί το γνωστικό αντικείμενο του νέου κλάδου και γίνεται αναφορά για το «Δίκαιο της Πληροφορίας» ενώ κάνουν λόγο για «πληροφοριακά αγαθά», τα οποία συμπεριλαμβάνουν πληροφορίες με προστιθέμενη αξία όπως, αξίες προστασίας από το δίκαιο (π.χ. πρωτοτυπία, πραγματοποίηση ουσιωδών επενδύσεων κ.α). [5] Με αυτό τον τρόπο η πληροφορία αποκτά μεγάλη ισχύ καθώς συμπεριλαμβάνεται στα τρία μεγαλύτερα μεγέθη ανάμεσα στην ύλη και την ενέργεια.

Παρόλα αυτά, η θεμελίωση ενός νέου κλάδου που βασίζεται στην έννοια της πληροφορίας έχει αρκετές δυσκολίες καθώς η απροσδιοριστία της έννοιας της πληροφορίας δεν βοηθά στη συγκέντρωση όλων των πιθανών κανόνων δικαίου που να καλύπτουν τον ορισμό της. Η σύνδεση των υποκειμένων που προκύπτουν από την συλλογή , την επεξεργασία και την διάδοση πληροφοριών είναι ανεδαφική, κάτι που δεν είναι επιθυμητό σε περιπτώσεις θέσπισης νέων κανόνων.

Ο διαχωρισμός μεταξύ του «Δικαίου της Πληροφορικής» και του «Δικαίου της Πληροφορίας» είναι ξεκάθαρος καθώς το δίκαιο της πληροφορικής επικεντρώνεται στην υποκείμενη τεχνολογία και στα προβλήματα που προκύπτουν από την διάδοση εφαρμογών στην κοινωνία και την οικονομία[6] και αντικείμενο της είναι η τεχνολογία της ηλεκτρονικής επεξεργασίας δεδομένων στο τομέα της

πληροφορικής και των τηλεπικοινωνιών ενώ το δίκαιο της πληροφορίας εστιάζεται κυρίως στη ρύθμιση των σχέσεων των προσώπων δικαίου με σημείο αναφοράς την πληροφορία.[7]

1.2 Προσωπικά Δεδομένα

1.2.1 Ορισμός και χαρακτηριστικά προσωπικών δεδομένων

Εξαιτίας της ραγδαίας ανάπτυξης της τεχνολογίας και του διαδικτύου, οι ηλεκτρονικές επικοινωνίες έχουν διεισδύσει σε μεγάλο βαθμό στις σύγχρονες κοινωνίες και έχουν αφήσει το στίγμα τους σε κάθε πτυχή κοινωνικής δραστηριότητας. Τα «δεδομένα» τα οποία είναι οι μεταφερόμενες πληροφορίες των ηλεκτρονικών επικοινωνιών πολύ συχνά αφορούν συγκεκριμένα πρόσωπα και για αυτό το λόγο έχουν χαρακτηριστεί και ως «δεδομένα προσωπικού χαρακτήρα» ή «προσωπικά δεδομένα» λόγω του περιεχομένου τους. Οι πρακτικά απεριόριστες δυνατότητες που προσφέρει η εν λόγω τεχνολογία, οδηγούν στη δημιουργία μιας ανάγλυφης εικόνας της προσωπικότητας κάθε ατόμου και σε συνδυασμό με την ασύλληπτη ταχύτητα διάδοσης τους καθιστούν το άτομο «διαφανές», «ελέγξιμο» αν όχι και «χειραγωγίσιμο».[8]

Η εισβολή του διαδικτύου στην καθημερινότητα των ανθρώπων οδήγησε μοιραία σε καταχωρήσεις των προσωπικών δεδομένων τους μέσα σε διάφορες υπηρεσίες, με απόρροια τη δημιουργία κινδύνων προσβολής και επεξεργασίας τους ακόμη και χωρίς τη συγκατάθεση του υποκειμένου. Ως υποκείμενο των δεδομένων, εννοείται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί (άμεσα ή έμμεσα) κυρίως βάσει ταυτότητας ή ενός ή περισσοτέρων στοιχείων που χαρακτηρίζουν την υπόσταση του.[9] Ο όρος προσωπικά δεδομένα που θα χρησιμοποιηθεί στη μελέτη αυτή αντί του όρου «δεδομένα προσωπικού χαρακτήρα» τόσο κατά τον Ν 2472/1997 όσο και κατά την Οδηγία 95/46/ΕΚ είναι εσκεμμένα ευρύς ώστε να προσφέρει όσο το δυνατόν μεγαλύτερη προστασία στο υποκείμενο των δεδομένων, και γίνεται κατανοητός με δύο έννοιες:

- Την έννοια της πληροφορίας που αποτελεί αντικείμενο προστασίας στο πλαίσιο του δικαίου των προσωπικών δεδομένων και
- Το αντικείμενο του αντίστοιχου νομικού κλάδου, δηλαδή τη σύνδεση του με την έννοια της ιδιωτικότητας.[10]

Βασικό στοιχείο των προσωπικών δεδομένων είναι η σύνδεση τους με ένα συγκεκριμένο πρόσωπο, έτσι ώστε να προκύπτει η ταυτότητα του προσώπου είτε άμεσα (αναφορά στο όνομα του) είτε έμμεσα (με τη «φωτογράφηση» του). Μέχρι να γίνει η σύνδεση ενός προσώπου με μια πληροφορία δεν γίνεται λόγος για προσωπικό δεδομένο όπως και όταν ένα προσωπικό δεδομένο αποσυνδεθεί από το πρόσωπο που το αφορά.

Από τα παραπάνω συμπεραίνουμε ότι τα δεδομένα προσωπικού χαρακτήρα είναι μια πληροφορία, η οποία μπορεί να εμπίπτει στο πεδίο των προσωπικών δεδομένων (δηλαδή σε πληροφορία συγκεκριμένη και εκμεταλλεύσιμη) ή στο πεδίο της ιδιωτικότητας (δηλαδή στην έννοια της κατάστασης, της ιδιότητας ή του συναισθήματος) ανάλογα με τη σχέση μεταξύ του υποκειμένου και του υπευθύνου επεξεργασίας (δηλαδή του χρήστη που καθορίζει το σκοπό τον τρόπο επεξεργασίας των προσωπικών δεδομένων, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός).

Τα προσωπικά δεδομένα χωρίζονται σε δύο μεγάλες κατηγορίες: α) τα απλά και β) τα ευαίσθητα δεδομένα. Απλά θεωρούνται τα δεδομένα εκείνα που περιλαμβάνουν πληροφορίες όπως: όνομα, επώνυμο, κατοικία, επάγγελμα, μορφωτικό επίπεδο, καταναλωτικές συνήθειες, ταξιδιωτική δραστηριότητα, οικογενειακή και περιουσιακή κατάσταση, μισθός, τραπεζικοί λογαριασμοί. Στα ευαίσθητα προσωπικά δεδομένα ανήκουν τα δεδομένα εκείνα που αφορούν: τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία (φυσική ή ψυχική), την κοινωνική πρόνοια, την ερωτική ζωή, τα σχετικά με ποινικές διώξεις ή καταδίκες (π.χ. ποινικό μητρώο), τα μητρώα και αρχεία της Εθνικής Αρχής Ιατρικώς Υποβοηθούμενης Αναπαραγωγής, τα γενετικά δεδομένα, τις δηλώσεις και τα στοιχεία της αίτησης του αιτούντος πολιτικό άσυλο, τη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων (π.χ. σωματείο ομοφυλοφίλων). Τα δεδομένα στην τελευταία κατηγορία δεν μπορούν να μεταβληθούν παρά μόνο με σχετικούς νόμους.

Η πρακτική σημασία της διάκρισης των δεδομένων στις κατηγορίες που αναφέρθηκαν παραπάνω έγκειται στην ενισχυμένη νομική προστασία που έχουν τα ευαίσθητα προσωπικά δεδομένα σε σχέση με τα απλά, καθώς θεσπίζονται πιο αυστηρές προϋποθέσεις για την επεξεργασία τους σε σχέση με εκείνες των απλών προσωπικών δεδομένων. Τα μέτρα που λαμβάνονται για τη πρόσβαση σε αυτά είναι α) η γραπτή συγκατάθεση του υποκειμένου σε αντίθεση με την προφορική συγκατάθεση των απλών, β) η λήψη σχετικής άδειας από την Αρχή Προστασίας Προσωπικών Δεδομένων σε σχέση με την επεξεργασία των απλών όπου αρκεί η γνωστοποίηση της επεξεργασίας στην Αρχή.

1.2.2 Προσωπικά Δεδομένα στο Διαδίκτυο και Ειδικές Διατάξεις

1.2.2.1 Εισαγωγή

Ο όρος «ηλεκτρονικές επικοινωνίες» που τείνει να αντικαταστήσει τον όρο «τηλεπικοινωνίες» καλύπτει κάθε είδους μετάδοση δεδομένων και σημάτων. Μετά την διείσδυση του διαδικτύου ως νέου παγκόσμιου επικοινωνιακού μέσου, εμφανίστηκε η ανάγκη επέκτασης της προστασίας των προσωπικών δεδομένων και στον τομέα των τηλεπικοινωνιών.

Στον τομέα των ηλεκτρονικών επικοινωνιών υπάρχουν ειδικές διατάξεις ως προς την προστασία των προσωπικών δεδομένων κυρίως βάσει του νόμου 3471/2006, ο οποίος αποτελεί την πράξη της προσαρμογής της ελληνικής νομοθεσίας προς την κοινοτική Οδηγία 2002/1958. Η συγκεκριμένη Οδηγία 2002/1958 η οποία είναι γνωστή και ως Οδηγία για την ηλεκτρονική - ιδιωτικότητα (e- Privacy Directive) εκδόθηκε με σκοπό τη διασφάλιση της προστασίας των προσωπικών δεδομένων και έθεσε τα θεμέλια για την εξασφάλιση ικανοποιητικού επιπέδου προστασίας των δεδομένων στον τηλεπικοινωνιακό τομέα.[11]

Ο νόμος αυτός βρίσκει εφαρμογή κατά την επεξεργασία των προσωπικών δεδομένων και τη διασφάλιση του απορρήτου των επικοινωνιών κατά το πλαίσιο

της παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών.[12]

1.2.2.2 Πρόσφατες νομικές ρυθμίσεις - Ο νόμος 3471/2006

Ο νόμος 3471/2006 ο οποίος αντικατέστησε τον νόμο 2774/99 καθώς με την εξέλιξη της τεχνολογίας δημιουργήθηκαν επιπλέον ανάγκες προστασίας των προσωπικών δεδομένων σε δίκτυα ηλεκτρονικών επικοινωνιών, κυρίως λόγω των εκτεταμένων φαινομένων υποκλοπών. Ο κυρίαρχος σκοπός του νόμου 3471/2006 είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και της ιδιωτικής τους ζωής, καθώς και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών (άρθρο 1 νόμος 3471/2006).[13]

Οι διατάξεις οι οποίες είναι σχετικές με την προστασία των προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα δεν είναι αυτοτελείς αλλά εντάσσονται στο γενικότερο πλαίσιο των ρυθμίσεων του νόμου 2472/97 οι οποίες εφαρμόζονται για κάθε ζήτημα που δεν ρυθμίζεται ειδικότερα από τον νόμο.

1.2.2.3 Οι κατ' ιδίαν διατάξεις του νόμου 3471/2006

Με βάση το νόμο 3471/2001 (άρθρο 4) προστατεύεται το απόρρητο των επικοινωνιών κατά τη χρήση υπηρεσιών που προσφέρονται μέσω του διαδικτύου στους χρήστες, ενώ επιβάλλονται κυρώσεις στους παραβάτες σε περίπτωση άρσης του απορρήτου όταν δεν τηρούνται συγκεκριμένοι όροι και προϋποθέσεις.

Ακόμη, καθορίζεται βάσει του προεδρικού διατάγματος 47/2005 η τεχνική μέθοδος πρόσβασης στα στοιχεία και το είδος που τεχνολογικού εξοπλισμού που χρησιμοποιείται, οι υποχρεώσεις των παρόχων υπηρεσιών επικοινωνίας ενώ ρυθμίζεται η τεχνική μέθοδος λήψης, αναπαραγωγής και μεταβίβασης των στοιχείων, όπως και εγγυήσεις για τη χρήση και καταστροφή τους, τη διασφάλιση του απορρήτου των επικοινωνιών από τεχνικής απόψεως αλλά και από άποψη αρμόδιων εξουσιοδοτημένων προσώπων.

Σε ειδικές περιπτώσεις, όπου είναι δύσκολος ο εντοπισμός στοιχείων επικοινωνίας, η αρμόδια αρχή απευθύνεται στους αρμόδιους φορείς οι οποίοι οφείλουν να παρέχουν πρόσβαση στα εκάστοτε στοιχεία που αυτή αναζητά. Εξαιτίας του νόμου 3471/2006 , ο οποίος έχει ειδικές ρυθμίσεις που εξειδικεύουν την απαγόρευση προσβολής του απορρήτου γίνεται σαφές ότι θα απαγορεύεται η χρήση λογισμικού που έχει στόχο την υποκλοπή των δεδομένων που διαβιβάζονται μέσω διαδικτύου (packet sniffing) και η αποθήκευση των δεδομένων των χρηστών με στόχο τη δημιουργία του προφίλ τους χωρίς την έγκριση τους.

Σε περιπτώσεις που χρειάζεται να αποδειχθούν στοιχεία από εμπορικές συναλλαγές ή άλλων περιπτώσεων επικοινωνίας κατά κύριο λόγο επαγγελματικής φύσεως επιτρέπεται η καταγραφή δεδομένων κίνησης όταν αυτή πραγματοποιείται κατά τη διάρκεια νόμιμης επαγγελματικής δραστηριότητας. Συνεπώς, είναι δυνατή η αυτόματη, ενδιάμεση ή παροδική αποθήκευση πληροφοριών με την προϋπόθεση οι πληροφορίες να μη φυλάσσονται για διάστημα μεγαλύτερο από εκείνο που χρειάζεται για τη μετάδοση και διαχείρισης της κίνησης.[14]

Επιπλέον, το άρθρο 4 του νόμου 3471/2006 απαγορεύει τη χρήση των δικτύων ηλεκτρονικών επικοινωνιών για την αποθήκευση πληροφοριών ή για τη πρόσβαση σε πληροφορίες οι οποίες είναι αποθηκευμένες στον τερματικό εξοπλισμό του συνδρομητή ή χρήστη, ειδικά όταν πρόκειται για την εγκατάσταση κατασκοπευτικών λογισμικών και κρυφών αναγνωριστικών στοιχείων. Ωστόσο, σε περιπτώσεις διαβίβασης μιας επικοινωνίας μέσω δικτύου με θεμιτά μέσα επιτρέπεται η αποθήκευση πληροφοριών με τις σχετικές ενημερώσεις των χρηστών. Έτσι, υιοθετείται ένα σύστημα «opt-out» ως προς τα αρχεία «cookies» στο οποίο ο χρήστης δύναται να δηλώσει τη συγκατάθεση του, αλλά μόνο εκ των υστέρων.

Βάσει των γενικών αρχών για την επεξεργασία δεδομένων, η συλλογή και η επεξεργασία τους πρέπει να γίνεται με θεμιτό και νόμιμο τρόπο. Ο νόμος 3471/2006 ορίζει ότι η επεξεργασία των δεδομένων πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της. Επιπλέον, τα δεδομένα πρέπει να βρίσκονται και να παραμένουν σε τέτοια μορφή που να είναι δυνατός ο προσδιορισμός της ταυτότητας των υποκειμένων τους κατά τη διάρκεια της περιόδου που απαιτείται για να γίνει η συλλογή και η επεξεργασία τους.

Ειδικότερα, η διάταξη του άρθρου 6 κάνει αναφορά στα δεδομένα κίνησης (δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς διαβίβασης ή

χρέωσης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών) ότι πρέπει να απαλείφονται ή να καθίστανται ανώνυμα κατά τη λήξη της κλήσης, ενώ για τα δεδομένα χρέωσης η επεξεργασία επιτρέπεται μόνο μέχρι το τέλος της περιόδου όπου γίνεται η συναλλαγή ενώ η συγκατάθεση του χρήστη είναι απαραίτητη προϋπόθεση για όλα τα παραπάνω. Πιο συγκεκριμένα, στα δεδομένα κίνησης, μπορεί να περιλαμβάνονται σε αυτά μεταξύ άλλων, ο αριθμός, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού, η διεύθυνση, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας και το δίκτυο από το οποίο προέρχεται ή σε αυτό που καταλήγει η επικοινωνία.

Με τη βοήθεια των πληροφοριών αυτών είναι δυνατή η δημιουργία προφίλ των χρηστών, των δικτύων ηλεκτρονικής επικοινωνίας αλλά και η παρακολούθηση της σχετικής δραστηριότητας τους οι οποίες οδηγούν στην εξαγωγή συμπερασμάτων για τους σκοπούς της άμεσης προώθησης προϊόντων και υπηρεσιών αλλά και για σκοπούς αντεγκληματικής πολιτικής. Η επεξεργασία των δεδομένων όταν ο χρήστης δεν δώσει τη συγκατάθεση του απαγορεύεται σύμφωνα με το άρθρο 5, ενώ πρέπει να προηγείται ενημέρωση του συνδρομητή με εξαίρεση τις υπηρεσίες που έχει ζητήσει ο χρήστης. Εδώ, σε αντίθεση με τα cookies υιοθετείται ένα σύστημα «opt-in».[15]

Τέλος, βασικό ρόλο στο σύστημα προστασίας του νόμου 3471/2006 έχουν τα δικαιωμάτων των χρηστών. Με ειδικές ρυθμίσεις που είναι προσαρμοσμένες στις υπηρεσίες των ηλεκτρονικών επικοινωνιών, οι συνδρομητές μπορούν να λαμβάνουν αναλυτικούς λογαριασμούς των συνδέσεων τους ενώ υπάρχει η δυνατότητα αναγνώρισης κλήσεων με τα στοιχεία της ταυτότητας της καλούσας γραμμής ενώ ένα ιδιαίτερο δικαίωμα που προβλέπεται στο άρθρο 9 είναι το δικαίωμα του συνδρομητή να εμποδίζει τις αυτόματες προωθούμενες κλήσεις από τρίτους στη τερματική του συσκευή.

Σημαντική είναι και η ρύθμιση του άρθρου 11 για τη μη ζητηθείσα επικοινωνία στην οποία περιλαμβάνεται η ηλεκτρονική αλληλογραφία και γενικώς οι επικοινωνίες με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας. Καθιερώνεται λοιπόν ένα σύστημα «opt-in» που σημαίνει ότι η πραγματοποίηση μη αιτηθείσας επικοινωνίας επιτρέπεται μόνο αν ο συνδρομητής δώσει την συγκατάθεση του εκ των προτέρων. Σε αντίθετη περίπτωση, προβλέπεται απαγόρευση της πραγματοποίησης της αιτηθείσας επικοινωνίας και η δήλωση του καταγράφεται σε

ειδικό κατάλογο (opt- out register). Στην παράγραφο 4 του άρθρου προβλέπεται η απαγόρευση της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν ως σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται με διακριτό τρόπο η ταυτότητα του αποστολέα και η διεύθυνση στην οποία μπορεί να ζητηθεί ο τερματισμός της επικοινωνίας.

Τέλος, ο νόμος 3471/2006 προβλέπει ένα σύστημα ποινικών και αστικών κυρώσεων σε περίπτωση μη εφαρμογής των διατάξεων του.

1.2.3 Οι κίνδυνοι για τα προσωπικά δεδομένα στις ηλεκτρονικές επικοινωνίες

1.2.3.1 Εξέλιξη του Διαδικτύου

Η διάδοση του διαδικτύου ανά τον κόσμο και η εισβολή του σε μεγάλο βαθμό στην καθημερινότητα των ανθρώπων, συνέβαλε στην ανάπτυξη της «Κοινωνίας της Πληροφορίας» ,όπως χαρακτηρίζεται από πολλούς η σύγχρονη εποχή και όχι άδικα, καθώς το διαδίκτυο αποτελεί έναν χώρο ελεύθερης διακίνησης ιδεών και πληροφοριών. Σημαντικός σύμμαχος αυτής της καινοτομίας υπήρξε η ραγδαία ανάπτυξη της τεχνολογίας και με αυτό τον τρόπο το διαδίκτυο κατάφερε να συνδέσει σε παγκόσμιο επίπεδο την επικοινωνία των ανθρώπων.

Αρχικά, το διαδίκτυο ξεκίνησε ως μια προσπάθεια δημιουργίας ενός πανεπιστημιακού δικτύου με το όνομα «APRANET» το 1969. Η ιδέα αυτή εξελίχθηκε από ερευνητές που ήθελαν να συνδέσουν δύο σημεία Α και Β και να μπορούν να επικοινωνούν μεταξύ τους ,ακόμη και με τη βοήθεια άλλων σημείων δικτύου σε περίπτωση που χαθεί η μεταξύ τους σύνδεση.

Για την περαιτέρω εξέλιξη του διαδικτύου σημαντικό ρόλο είχε η ανάπτυξη το 1978 των πρωτοκόλλων επικοινωνίας Transport Control Protocol/ Internet Protocol (TCP/IP) τα οποία χρησιμοποιήθηκαν στη μετάδοση δεδομένων μέσω του διαδικτύου και επέτρεπαν την επικοινωνία των υπολογιστών μέσα από

διαφορετικά δίκτυα, χωρίς να χρειάζονται επιπλέον τεχνικές πληροφορίες. Η πορεία του διαδικτύου τελικά ως ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών που επικοινωνούν μεταξύ τους και ανταλλάσσουν πληροφορίες οδήγησε στην ανάγκη να ταυτοποιούνται οι υπολογιστές με τη χρήση μιας μοναδικής αριθμητικής διεύθυνσης IP της μορφής xxx.xxx.xxx.xxx όπου xxx είναι αριθμοί από 0 έως 255 , το λεγόμενο IPv4 το οποίο δημιουργεί μέχρι και 4.294.967.296 διευθύνσεις. Οι αριθμοί αυτοί αντιστοιχίζονται στη συνέχεια σε μια ονομασία πεδίου το λεγόμενο Domain Name και έτσι δημιουργείται το λεγόμενο Σύστημα Ονομάτων Τομέα (DNS)[16] το οποίο είναι ένα είδος τηλεφωνικού καταλόγου που μεταφράζει το Domain Name σε διευθύνσεις IP.

Οι εν λόγω διευθύνσεις, χωρίζονται σε στατικές και δυναμικές ανάλογα με το είδος σύνδεσης τους, δηλαδή αν είναι μόνιμα συνδεδεμένες σε σταθερό υπολογιστή ή αν αλλάζουν κάθε φορά που κάποιος υπολογιστής συνδέεται στο διαδίκτυο ενώ με τη δημιουργία του IPv6 ο αριθμός αυτός πολλαπλασιάζεται έτσι ώστε να υπάρχουν μοναδικές διευθύνσεις ανά χρήστη.

Το 1990 αναπτύχθηκε από τον Tim Berners Lee το «World Wide Web» ή απλώς Web ενώ το 1993 αναπτύχθηκε και εδραιώθηκε παγκοσμίως το www στο εργαστήριο CERN[17] της Ελβετίας το οποίο αποτελεί το μέσο για αναζήτηση, προσπέλαση και ανεύρεση πληροφοριών στο διαδίκτυο μέσω του οποίου οι χρήστες θα μπορούν να συνδεθούν στο διαδίκτυο με τη χρήση browser (πρόγραμμα πλοήγησης).[18]

Ο θαυμαστός αυτός όμως κόσμος του διαδικτύου αποτέλεσε και έναν χώρο στον οποίο αναπτύχθηκαν δραστηριότητες ,όπως διάδοση ψευδών και δυσφημιστικών πληροφοριών, ενίσχυση τρομοκρατικών ενεργειών , κλοπή πνευματικής ιδιοκτησίας και παράνομης επεξεργασίας προσωπικών δεδομένων, από κρατικούς ή μη φορείς που χρησιμοποιούσαν τη σύγχρονη τεχνολογία των επικοινωνιών για τη θεμιτή ή αθέμιτη παρακολούθηση των δραστηριοτήτων και της επικοινωνίας των πολιτών.[19]

Μερικά χαρακτηριστικά παραδείγματα της αρνητικής επίδρασης του διαδικτύου στη ζωή μας είναι η ανησυχητική ενίσχυση των τεχνολογικών προσπαθειών παρακολούθησης των επικοινωνιών μέσω της παρακολούθησης τηλεφωνικών συνδιαλέξεων και της ηλεκτρονικής αλληλογραφίας. Ο έλεγχος των πληροφοριών των ηλεκτρονικών ταχυδρομείων από συστήματα όπως το «Carnivore» του F.B.I ή το δορυφορικό σύστημα παρακολούθησης «Echelon» το

οποίο σάρωνε τις τηλεπικοινωνίες παγκοσμίως και είχε πρόσβαση σε όλες τις ψηφιακές επικοινωνίες του πελάτη αποτελούν σημαντικά παραδείγματα έντονου προβληματισμού σχετικά με το μέγεθος και τις συνέπειες της διακινδύνευσης του ανθρώπου μέσα στο περιβάλλον της θεαματικής εξέλιξης των αποκαλούμενων «Τεχνολογιών της πληροφορίας και της επικοινωνίας» (Information and communication technologies, ICTs).

[16] Τα domain names λειτουργούν ως των διευθύνσεις των δικτυακών τόπων και έχουν δύο ή περισσότερα επίπεδα, π.χ. uom.gr όπου το «gr» θεωρείται η ευρύτερη περιοχή ονοματοδοσίας ενώ το uom εκφράζει την επωνυμία του δικτυακού τόπου. [17] Ευρωπαϊκό Κέντρο Σωματιδιακής Φυσικής

1.2.3.2 Τα «cookies»

Σε κάθε ηλεκτρονική συναλλαγή ενός ατόμου ή κατάρτιση σύμβασης στο διαδίκτυο (Internet) είναι απίθανο η ενέργεια αυτή να μην αφήσει ίχνη. Τα «cookies» όπως είναι ευρέως γνωστά αποτελούν μέρος της κυκλοφορίας H.T.T.P[20] και είναι τμήματα δεδομένων τα οποία μπορούν να αποθηκευτούν σε αρχεία κειμένου στο σκληρό δίσκο του χρήστη του διαδικτύου, κρατούν πληροφορίες για εκείνον, ενώ ταυτόχρονα ο ιστοχώρος κρατά αντίγραφο τους. Μπορούν να περιλαμβάνουν διαφόρων ειδών πληροφορίες, όπως τις σελίδες που έχει επισκεφτεί ο χρήστης, τις διαφημίσεις που επέλεξε να διαβάσει, τον αριθμό αναγνώρισης χρήστη πόση ώρα παρέμεινε σε ποιες ιστοσελίδες κ.α.

Με τον τρόπο αυτό κάθε φορά που επισκέπτεται κάποιος μια ιστοσελίδα ο δικτυακός τόπος ζητά από τον χρήστη να συμπληρώσει φόρμα με τα προσωπικά του στοιχεία και έτσι του παρέχεται η δυνατότητα να δημιουργεί cookie ώστε να είναι δυνατή η ταυτοποίηση της διεύθυνσης IP του χρήστη με τα στοιχεία της πραγματικής του διεύθυνσης. Έτσι, αναγνωρίζονται οι κινήσεις που είχε κάνει την τελευταία φορά που την είχε επισκεφθεί και αυτό έχει ως αποτέλεσμα τη δημιουργία ενός προφίλ του χρήστη το οποίο πέρα από θεμιτές πληροφορίες που μπορεί να περιέχει, όπως καταναλωτικές συνήθειες και πολιτιστικά ή άλλα ενδιαφέροντα μπορεί να περιλαμβάνει και πληροφορίες που ανήκουν σε

ευαίσθητα προσωπικά δεδομένα όπως φυλετική ή εθνική καταγωγή, πολιτικά φρονήματα, σεξουαλικές προτιμήσεις, θρησκευτική δραστηριότητα.

Η εκούσια παροχή των δεδομένων εξυπηρετεί ιδιαίτερα τα συμφέροντα επιχειρήσεων, τα οποία έχουν στόχο την εμπορική εκμετάλλευση, καθώς παρέχουν πληροφορίες για τη βελτίωση της στρατηγικής τους και του προγραμματισμού τους. Ωστόσο, η πρακτική αυτή προχώρησε σε τέτοιο βαθμό, με απόρροια την δημιουργία των συστημάτων «ψηφιακής σήμανσης» στα οποία γίνεται στοχευμένη διαφήμιση στο διαδίκτυο, που προσαρμόζεται και μεταβάλλεται ανάλογα με την ηλικία ή το φύλο του ατόμου.

Τα «cookies» ταξινομούνται σε προσωρινά (session cookies) ή μόνιμα (persistent cookies). Τα cookies της πρώτης κατηγορίας απαλείφονται αυτόματα αν ο αποδέκτης της υπηρεσίας κλείσει τον browser του, ενώ τα μόνιμα παραμένουν αποθηκευμένα στον τερματικό εξοπλισμό του, μέχρι την συμπλήρωση ενός προκαθορισμένου χρόνου ισχύος, ο οποίος μπορεί να ανέρχεται και σε έτη. [21]

[20] Το Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol), είναι ένα πρωτόκολλο για την μεταφορά υπερκειμένων (hypertext). Το πρωτόκολλο υπέρ-κειμένου (HTTP) δεν λειτουργεί με διαρκή σύνδεση, αλλά κάθε φορά που ζητάει κάποιος μια σελίδα συνδέεται με τον server, παίρνει τα δεδομένα και μετά ξεσυνδέεται. Έτσι δεν μπορεί να διατηρήσει "ζωντανή" την παραγγελία του πελάτη ενώ πηγαίνει από σελ.ίδα σε σελίδα ούτε μπορεί να αναγνωρίσει την ταυτότητα του. Τη λύση τι δίνουν τα «cookies» αυτό το αρχείο κειμένου, που αποθηκευμένο στο σκληρό δίσκο, βοηθάει, κάθε φορά που επισκεπτόμαστε μία web σελ.ίδα, στο να πιστοποιεί ότι είμαστε εμείς και όχι κάποιος άλλος.

1.2.3.3 Οι “Διαδικτυακοί κοριοί” (Web Bugs)

Τα Web Bugs παρόλο που μοιάζουν αρκετά με τα cookies, καθώς και εκείνα ταυτοποιούν τη διεύθυνση IP του χρήστη και καταγράφουν τα δεδομένα κίνησης

των χρηστών κατά την πλοήγηση τους στο διαδίκτυο, διαφοροποιούνται μόνο ως προς τη δυνατότητα του χρήστη να γνωρίζει τη σύνδεση του υπολογιστή του με κάποιο τρίτο server. Ένα web bug είναι μια εντολή προς τον browser να συνδεθεί με κάποιο τρίτο server και να δώσει κάποιες πληροφορίες. Λόγω της ενσωμάτωσης τους σε εικόνες με μέγεθος μόλις 1x1 pixel δεν είναι ορατά από τον χρήστη με γυμνό μάτι και έτσι δεν έχει τη δυνατότητα να τα απενεργοποιήσει, απορρίψει ή να τα διαγράψει. Αυτό έχει ως αποτέλεσμα να προκαλούνται μεγάλα προβλήματα γιατί τα Web Bugs μπορούν να χρησιμοποιηθούν από τρίτους για να εποπτεύουν τις σελίδες που επισκέπτονται οι χρήστες.[22]

Ένα ακόμη πρόβλημα που προκύπτει έμμεσα από τα Web Bugs είναι οι λεγόμενοι spammers, να παίρνουν το μήνυμα ότι οι ηλεκτρονικές διευθύνσεις που έστειλαν ανεπιθύμητα μηνύματα να είναι έγκυρες. Αυτό προκύπτει από το γεγονός ότι τα Web Bugs έχουν την δυνατότητα να επαληθεύουν τις ηλεκτρονικές διευθύνσεις των χρηστών του διαδικτύου και να εντοπίζουν ποιος και πότε διάβασε κάποιο mail ακόμη και να γνωστοποιήσουν την διεύθυνση IP του παραλήπτη του mail.

1.2.3.4 Το κατασκοπευτικό λογισμικό (Spyware)

Το Spyware πρόκειται για τύπο κακόβουλου λογισμικού το οποίο εγκαθίσταται στον σκληρό δίσκο του υπολογιστή χωρίς να έχει καμία γνώση ο χρήστης και εκτελείται στο παρασκήνιο χωρίς να μπορεί να απεγκατασταθεί ούτε να αντιμετωπιστεί με τη χρήση antivirus και firewalls. Ο σχεδιασμός τους βασίζεται στη μόλυνση συστημάτων υπολογιστών με σκοπό την αυθαίρετη και κρυφή ενεργοποίηση πλήθους παράνομων κατασκοπευτικών διεργασιών. Αρκετά λογισμικά κατασκοπείας χρησιμοποιούνται για κρυφή υποκλοπή προσωπικών δεδομένων του χρήστη- θύματος, όπως αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, προσωπικά στοιχεία σύνδεσης σε διαδικτυακούς λογαριασμούς, κωδικούς πρόσβασης. Σε άλλες περιπτώσεις spyware viruses μπορεί να υποκλέπτουν-καταγράφουν σε τρίτους τις προτιμήσεις και τις δραστηριότητες του χρήστη, όπως πληροφορίες για τις κινήσεις του χρήστη στο διαδίκτυο, τις ιστοσελίδες που επισκέπτεται, τα κριτήρια που εισάγει για τις διαδικτυακές του αναζητήσεις, τις αγορές που κάνει.

Κάποιοι από τους πιο γνωστούς τρόπους διαδικτυακής εξάπλωσης spyware είναι οι παρακάτω: [23]

I. Παραπλανητικό marketing: πρόκειται για έναν από τους πιο γνωστούς τρόπους παραπλάνησης των χρηστών καθώς οι δημιουργοί spyware προωθούν τα προγράμματα τους ως χρήσιμα και αξιόπιστα εργαλεία. Έτσι μεγάλος αριθμός χρηστών πέφτει θύμα τους και εγκαθιστά αυτά τα προγράμματα στον υπολογιστή του με σκοπό να τον ωφελήσουν.
II. Συνοδευτικά πακέτα λήψης (Software Bundles): οι περισσότερες δωρεάν εφαρμογές περιέχουν συνοδευτικά πακέτα λήψης στα οποία κρύβονται διαφόρων ειδών PUPs (potentially unwanted programs) τα οποία εμφανίζονται κατά τη διάρκεια λήψης της εφαρμογής. Απαιτείται ιδιαίτερη προσοχή στην απεγκατάσταση της εφαρμογής καθώς πολλές φορές δεν συνοδεύεται και με απεγκατάσταση του spyware.
III. Κενά στην ασφάλεια: τα κενά που υπάρχουν στην ασφάλεια του συστήματος και web browsers επωφελούνται οι δημιουργοί spyware καθώς με διάφορους τρόπους όπως παραπλανητικές αναδυόμενες διαφημίσεις, ύποπτους συνδέσμους ανακατεύθυνσης, κακόβουλες επισυνάψεις, συνδέσμους ανακατεύθυνσης σε mails κ.α. προσπαθούν να μολύνουν μεγάλο αριθμό συστημάτων υπολογιστών.
IV. Άλλες απειλές: αρκετά spyware εξαπλώνονται μέσω του διαδικτύου με τη βοήθεια διαφόρων ιών, Trojans , worms κ.α. κακόβουλων προγραμμάτων και αρχείων.

1.2.3.5 Ηλεκτρονικό Ταχυδρομείο

Ο κίνδυνος υποκλοπής προσωπικών δεδομένων μέσω του ηλεκτρονικού ταχυδρομείου δημιουργείται όταν συλλέγονται οι ηλεκτρονικές διευθύνσεις για

την αποστολή διαφημιστικών μηνυμάτων, καθώς το ηλεκτρονικό ταχυδρομείο επιτρέπει την αποστολή μηνυμάτων σε πολλαπλούς αποδέκτες, και όταν παρακολουθείται η κίνηση του μηνύματος. Με αυτό τον τρόπο δίνεται η δυνατότητα σε ανεπιθύμητους να αντλήσουν πληροφορίες του μηνύματος όπως και κωδικούς πρόσβασης που χρησιμοποιεί ο χρήστης και να χρησιμοποιήσουν τις πληροφορίες αυτές για κακόβουλους σκοπούς.

Το πρόβλημα ασφάλειας των ηλεκτρονικών ταχυδρομείων οφείλεται στις αδυναμίες που έχει το SMTP [24] πρωτόκολλο το οποίο αναλαμβάνει να μεταφέρει μηνύματα από τον χρήστη στον εξυπηρετητή του ηλεκτρονικού ταχυδρομείου και να τα προωθήσει σε επόμενους εξυπηρετητές καθώς τα πακέτα που δημιουργεί είναι ευαίσθητα σε υποκλοπές και δεν είναι κρυπτογραφημένα.

Συνεπώς, είναι ανάγκη οι υπηρεσίες ασφάλειας του ηλεκτρονικού ταχυδρομείου να εγγυώνται εμπιστευτικότητα, δηλαδή προστασία του μηνύματος από μη εξουσιοδοτημένους χρήστες και ασφάλεια κρυπτογραφώντας τα μηνύματα με συμμετρικούς ή ασύμμετρους αλγορίθμους.

Η πιστοποίηση της πηγής ενός μηνύματος γίνεται με τη χρήση ψηφιακών υπογραφών οι οποίες επιβεβαιώνουν την αυθεντικότητα του μηνύματος και είναι αυστηρά μοναδικές, προσωπικές και ιδιαίτερα δύσκολες στη πλαστογράφηση τους.

[24] Κύριος φορέας των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι το Πρωτόκολλο Μεταφοράς Απλού Ταχυδρομείου (SMTP - Simple Mail Transfer Protocol).

1.2.3.6 Μη ζητηθείσα ηλεκτρονική επικοινωνία (spamming)

Η ανεπιθύμητη αλληλογραφία (spam) προσεγγίζεται διαφορετικά από τις εθνικές νομοθεσίες και από διάφορους τομείς. Σε κάποιες χώρες του εξωτερικού όπως για παράδειγμα στην Γαλλία το spam σχετίζεται με την ανώνυμη και μαζική αποστολή ηλεκτρονικών μηνυμάτων προς πολλαπλούς δέκτες χωρίς να υπάρχει οποιαδήποτε σχέση μεταξύ αυτών και του αποστολέα του μηνύματος. Αποτελεί σημαντικό εμπόδιο στην ανάπτυξη του διαδικτύου καθώς υπάρχει κίνδυνος πολλοί χρήστες του ηλεκτρονικού ταχυδρομείου να σταματήσουν να χρησιμοποιούν

υπηρεσίες μέσω διαδικτύου ή και να τις περιορίσουν σε μεγάλο βαθμό καθώς τα spam αποτελούν ήδη το 70% των μηνυμάτων του ηλεκτρονικού ταχυδρομείου τους.

Η αρνητική επιρροή του spam δεν περιορίζεται μόνο στο επίπεδο των χρηστών αλλά βρίσκει αντίκτυπο και στο ηλεκτρονικό εμπόριο καθώς μειώνει την εμπιστοσύνη του καταναλωτή στις ηλεκτρονικές συναλλαγές μέσω του διαδικτύου. Σύμφωνα με τον πρώην Ευρωπαϊκό Επίτροπο, αρμόδιο σε θέματα επιχειρήσεων Errki Liikanen «επιπλέον το spam εμπεριέχει μεγαλύτερο κόστος για τις επιχειρήσεις. Μόνο με όρους χαμένης παραγωγικότητας το κόστος υπολογίζεται σε δισεκατομμύρια ευρώ μόνο στην Ευρώπη. Επικοινωνίες για νόμιμους εμπορικούς και διαφημιστικούς σκοπούς δεν αναγιγνώσκονται πια».[25]

Με βάση όλες τις παραπάνω νέες τεχνολογίες του διαδικτύου μπορεί εύκολα να αντιληφθεί κανείς ότι η ανωνυμία στο διαδίκτυο είναι μύθος και ότι ο απλός χρήστης καλείται να προστατευθεί μόνος του από τους πιθανούς κινδύνους που μπορεί να προκύψουν με την εισβολή του διαδικτύου στην ιδιωτική του ζωή.

1.3 Ρυθμίσεις για την προστασία των προσωπικών δεδομένων στο χώρο των ηλεκτρονικών επικοινωνιών

1.3.1 Εισαγωγή

Στη σημερινή εποχή, την εποχή του διαδικτύου και των μεγάλων δεδομένων (big data), τα προσωπικά δεδομένα του κάθε χρήστη μπορούν να βρίσκονται οπουδήποτε, είτε αναρτημένα σε κάποιο κοινωνικό δίκτυο είτε σε διαδικτυακά forum ή σε σελίδες εξειδικευμένων υπηρεσιών (π,χ, υπηρεσίες online αναζήτησης εργασίας) αναδεικνύοντας πολλά καινούργια θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων. Αυτό το μεγάλο εύρος διάχυσης των προσωπικών δεδομένων, αλλά και το γεγονός ότι το διαδίκτυο των πραγμάτων είναι μέρος της καθημερινότητας μας, βάσει του οποίου όλες οι συσκευές είναι

συνδεδεμένες στο διαδίκτυο και επικοινωνούν μεταξύ τους, οι κίνδυνοι ασφαλείας πολλαπλασιάζονται. Αυτό έχει επιφέρει την ασφάλεια των προσωπικών δεδομένων θέμα μείζονος σημασίας ,ενώ άμεση κρίνεται η ανάγκη για προστασία.

1.3.2 Υποχρεώσεις του Παρόχου

1.3.2.1 Τήρηση Αρχών Επεξεργασίας

Ο υπεύθυνος για την επεξεργασία των προσωπικών δεδομένων πρέπει να τηρεί όλες τις Αρχές Επεξεργασίας των Προσωπικών Δεδομένων προκειμένου να καθιστά νόμιμη τη διαδικασία επεξεργασίας. Πιο συγκεκριμένα πρέπει να τηρεί τις εξής: α) την αρχή νομιμότητας του σκοπού και του τρόπου επεξεργασίας σύμφωνα με την οποία η επεξεργασία πρέπει να εξυπηρετεί κάποιον που είναι γνωστός στο υποκείμενο και έχει δηλωθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ), β)την αρχή της αναλογικότητας η οποία βάσει των κριτηρίων που διαθέτει διακρίνει τα δεδομένα με βάση τη συνάφεια τους, γ)την αρχή της ακρίβειας σύμφωνα με την οποία τα δεδομένα πρέπει να ανταποκρίνονται στην πραγματικότητα και δ) την αρχή της χρονικής διάρκειας τήρησης των δεδομένων σύμφωνα με την οποία τα προσωπικά δεδομένα που επιτρέπουν τη σύνδεση με το υποκείμενο πρέπει να τηρούνται για καθορισμένο χρόνο ο οποίος ορίζεται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Όσον αφορά την επεξεργασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών εξειδικεύεται στην αρχή της αναλογικότητας και στην αρχή της χρονικής διάρκειας τήρησης των δεδομένων. Σύμφωνα με την αρχή της αναλογικότητας, τα υπό επεξεργασία δεδομένα πρέπει να είναι συναφή και όχι παραπάνω από όσα χρειάζονται για τους σκοπούς της επεξεργασίας.

Η αρχή της αναλογικότητας χρησιμοποιεί για το νόμιμο έλεγχο επεξεργασίας δύο κριτήρια , ένα ποιοτικό και ένα ποσοτικό, με σημείο αναφοράς το σκοπό της επεξεργασίας. Με βάση το ποιοτικό κριτήριο ελέγχεται αν το δεδομένο προς εξέταση είναι συναφές με τον επιθυμητό σκοπό. Αν η επεξεργασία δεν ικανοποιεί το ποιοτικό κριτήριο τότε είναι παράνομη και παραλείπεται η εξέταση του με το ποσοτικό κριτήριο. Σε περίπτωση που η επεξεργασία περάσει τον έλεγχο με επιτυχία με βάση το ποιοτικό κριτήριο ακολουθεί ο έλεγχος με βάση

το ποσοτικό κριτήριο. Αν και ο τελευταίος καταλήξει σε θετικό αποτέλεσμα τότε η επεξεργασία είναι σύμφωνη με την αρχή της αναλογικότητας.

Βάσει του νόμου 3471/2006, προσδιορίζονται τα όρια της αρχής αναλογικότητας ενώ γίνεται αναφορά στη διαδικασία επεξεργασίας των προσωπικών δεδομένων η οποία πρέπει να περιορίζεται στο μέτρο εξυπηρέτησης των σκοπών της. Εισάγεται ακόμη, η έννοια της «εξοικονόμησης δεδομένων» η οποία έχει στόχο την μείωση του πλήθους των προσωπικών δεδομένων που απαιτούνται κατά τη διάρκεια της επεξεργασίας τους.

Από τις εξειδικευμένες εφαρμογές της αρχής της αναλογικότητας δεν γίνεται να παραληφθεί η επιβολή στους παρόχους να δημοσιεύουν στους έντυπους ή ηλεκτρονικούς καταλόγους των συνδρομητών μόνο τα δεδομένα προσωπικού χαρακτήρα. Έτσι, σε περιπτώσεις που συμφωνεί και ο συνδρομητής για τη χρήση των προσωπικών δεδομένων του, μπορεί να γίνει εύκολα η ταυτοποίηση του. Τα στοιχεία που καταχωρούνται σε περιπτώσεις φυσικών προσώπων είναι το όνομα, το επώνυμο, το πατρώνυμο και η διεύθυνση ενώ για τα νομικά πρόσωπα είναι η επωνυμία ή διακριτικός τίτλος, η έδρα, η νομική μορφή και η διεύθυνση.[26]

Σύμφωνα με την αρχή της καθορισμένης χρονικής διάρκειας τήρησης των δεδομένων, τα δεδομένα μπορούν να παραμένουν σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων κατά τη διάρκεια της περιόδου που απαιτείται για τη συλλογή και την επεξεργασία τους. Η αρχή της χρονικής διάρκειας τήρησης των δεδομένων επιβάλλει μετά τη λήξη της επικοινωνίας τα δεδομένα να καταστρέφονται καθώς δεν έχουν κάποιο λόγο ύπαρξης. Οι περιπτώσεις στις οποίες επιτρέπεται η επεξεργασία των δεδομένων και μετά τη λήξη της επικοινωνίας είναι για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς εφόσον δεν θίγονται τα δικαιώματα των υποκειμένων τους ή τρίτων.

Με την παραπάνω ρύθμιση αντιμετωπίζεται η περίπτωση της δευτερεύουσας χρήσης των προσωπικών δεδομένων, που ναι μεν υπερβαίνει τον αρχικό σκοπό της επεξεργασίας αλλά εξυπηρετεί κάποιον άλλο σκοπό (ιστορικό ,επιστημονικό, στατιστικό) και ο οποίος δικαιολογεί τη διατήρηση του αρχείου και μετά την εκπλήρωση του αρχικού σκοπού επεξεργασίας.

Η διατήρηση των αρχείων επεξεργασίας είναι αρμοδιότητα του υπευθύνου επεξεργασίας και είναι υπεύθυνος για την καταστροφή όσων προσωπικών δεδομένων καταπατάνε τις παραπάνω αρχές.

1.3.2.2 Λήψη συγκατάθεσης του υποκειμένου

Για την νόμιμη επεξεργασία των προσωπικών δεδομένων κρίνεται αναγκαία η συγκατάθεση του προσώπου στον οποίο ανήκουν τα δεδομένα, ενώ υπάρχει η δυνατότητα να ανακαλέσει την συγκατάθεση του οποιαδήποτε στιγμή εκείνος επιθυμεί. Παρότι ο νόμος χρησιμοποιεί το γενικό όρο συγκατάθεση, που περιλαμβάνει τόσο τη συναίνεση (εκ' των προτέρων συγκατάθεση) όσο και την έγκριση (εκ των υστέρων συγκατάθεση) είναι φανερό ότι ο συνδρομητής /χρήστης απαιτεί τη συναίνεση και δεν αρκείται στην έγκριση επεξεργασίας των δεδομένων.

Βάσει νόμου ο συνδρομητής/χρήστης πρέπει να έχει πληροφόρηση σχετικά με τον σκοπό της επεξεργασίας, τα δεδομένα που αφορά η επεξεργασία καθώς και γνώση της ταυτότητας του υπευθύνου επεξεργασίας ή τυχόν εκπροσώπου του. Υπάρχουν όμως και περιπτώσεις επεξεργασίας των δεδομένων οι οποίες πραγματοποιούνται χωρίς την συγκατάθεση του υποκειμένου και αφορούν ειδικές περιπτώσεις επεξεργασίας πάντα με τη σύμφωνη γνώμη της Αρχής.

Όσον αφορά τον τρόπο με τον οποίο μπορεί να δώσει τη συγκατάθεση του ο συνδρομητής /χρήστης αυτό μπορεί να γίνει είτε με γραπτά είτε με ηλεκτρονικά μέσα. Η συγκατάθεση απαιτείται να είναι γραπτή όταν αφορά επεξεργασία ευαίσθητων δεδομένων, ενώ όταν αφορά απλά δεδομένα αρκεί να είναι προφορική αλλά ρητή. Η έγγραφη συναίνεση του ισοδυναμεί με εκείνη που διαβιβάζεται ηλεκτρονικά με προηγμένη ηλεκτρονική υπογραφή, ενώ αν δεν απαιτείται έγγραφη συγκατάθεση αυτή μπορεί να διαβιβαστεί ηλεκτρονικά με απλή ηλεκτρονική υπογραφή. Όταν η συγκατάθεση δίνεται με ηλεκτρονικά μέσα ο υπεύθυνος επεξεργασίας πρέπει να εξασφαλίζει:[27]

- Ότι ο συνδρομητής ή χρήστης ενεργεί με πλήρη επίγνωση των συνεπειών που έχει η δήλωση του η οποία καταγράφεται με ασφαλή τεχνικά τρόπο
- Ότι μπορεί να είναι ανά πάσα στιγμή προσβάσιμη στον χρήστη ή συνδρομητή
- Και ότι μπορεί να την ανακαλέσει οποιαδήποτε στιγμή

Τέλος, οι προϋποθέσεις για την ηλεκτρονική συγκατάθεση είναι οι εξής:

- Ο ασφαλής τεχνικά τρόπος: Αρκεί ένα ασφαλές έγγραφο ασύμμετρα κρυπτογραφημένο
- Άμεσα προσβάσιμη δήλωση: Η δυνατότητα του συνδρομητή ή χρήστη να μπορεί οποιαδήποτε στιγμή να ανατρέχει στη δήλωση του η οποία ως ηλεκτρονικό έγγραφο δεν θα μπορεί να μεταβληθεί παρά μόνο με τη διαδικασία της ανάκλησης

Τα παραπάνω χαρακτηριστικά αποτελούν προϋπόθεση για την εγκυρότητα της συγκατάθεσης του υποκειμένου ώστε τα προσωπικά του δεδομένα να γίνουν αντικείμενο επεξεργασίας.

Πρέπει, τέλος να τονιστεί ότι ακόμη και όταν δεν απαιτείται η συγκατάθεση του υποκειμένου για την επεξεργασία των προσωπικών δεδομένων του , ο υπεύθυνος επεξεργασίας έχει την ευθύνη να τον ενημερώσει (εκτός κι αν πρόκειται για εντελώς εξαιρετική περίπτωση και βάσει νόμου δεν χρειάζεται ενημέρωση), όπως και να γνωστοποιήσει στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα την επεξεργασία, ή να λάβει άδεια αν πρόκειται για ευαίσθητα δεδομένα.[28]

1.3.3 Δικαιώματα του υποκειμένου

1.3.3.1 Δικαίωμα στην ενημέρωση

Κατά τη διάρκεια επεξεργασίας και συλλογής των προσωπικών δεδομένων του υποκειμένου είναι υποχρέωση του υπευθύνου επεξεργασίας (και παράλληλα δικαίωμα του συνδρομητή ή χρήστη) να ενημερώνει σχετικά με την τέλεση της επεξεργασίας, καθώς και με τις συνθήκες αλλαγής των δεδομένων. Η ενημέρωση του υποκειμένου πρέπει να συμβαίνει είτε παρέχει τη συγκατάθεση του για τη συλλογή των δεδομένων είτε όχι. Σύμφωνα με τα παραπάνω, ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο και μάλιστα κατά το πρώιμο στάδιο της

συλλογής δεδομένων, με σαφή τρόπο ως προς την ταυτότητα του ή την ταυτότητα τυχόν εκπροσώπου του, το σκοπό της επεξεργασίας των προσωπικών δεδομένων του και τους αποδέκτες ή τις κατηγορίες των αποδεκτών των δεδομένων και τέλος την ύπαρξη του δικαιώματος πρόσβασης. [29]

Ως προς τον τρόπο ενημέρωσης του υποκειμένου για την επεξεργασία των δεδομένων του πρέπει να λαμβάνεται υπόψιν κατά πόσο συνδράμει στην συλλογή των δεδομένων το υποκείμενο ή όχι. Σε περιπτώσεις που συμβάλλει και το ίδιο το υποκείμενο τότε η ενημέρωση του γίνεται εγγράφως ενώ στην δεύτερη περίπτωση δίνεται με πρόσφορο τρόπο ώστε να εξασφαλίζεται η επαρκής πληροφόρηση του υποκειμένου.

Σε περιπτώσεις όπου η επεξεργασία των προσωπικών δεδομένων γίνεται για δημοσιογραφικούς σκοπούς και αφορά δημόσια πρόσωπα δεν κρίνεται αναγκαία η υποχρέωση για την ενημέρωση του υποκειμένου.

1.3.3.2 Δικαίωμα πρόσβασης

Το υποκείμενο έχει δικαίωμα πρόσβασης να γνωρίζει τις πληροφορίες που προκύπτουν από την επεξεργασία των προσωπικών του δεδομένων και για την επίτευξη αυτού του δικαιώματος υπάρχουν ειδικές νομοθεσίες που το προσφέρουν ενώ παράλληλα θέτουν προθεσμία για την ικανοποίηση του αιτήματος.

Συνεπώς από τα παραπάνω θα υπάρχει πρόσβαση του υποκειμένου στις ακόλουθες πληροφορίες: [30]

- Όλα τα προσωπικά δεδομένα που υφίστανται επεξεργασία και την προέλευση τους
- Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες των αποδεικτών
- Την εξέλιξη της επεξεργασίας για το χρονικό διάστημα από την προηγούμενη ενημέρωση του
- Τη λογική της αυτοματοποιημένης επεξεργασίας
- Τη διόρθωση, τη διαγραφή ή τη δέσμευση των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη προς τις διατάξεις του παρόντος νόμου

- Την κοινοποίηση σε τρίτους στους οποίους έχουν ανακοινωθεί τα δεδομένα, κάθε διόρθωσης, διαγραφής ή δέσμευσης εφ' όσον αυτό δεν είναι δυνατό

Το δικαίωμα πρόσβασης του υποκειμένου μπορεί να το εκφράσει με γραπτό τρόπο είτε με αυτοπρόσωπη παρουσία του ενδιαφερομένου ή του νόμιμου εκπροσώπου του είτε από απόσταση (π.χ. απλό ή ηλεκτρονικό ταχυδρομείο).

Συνεπώς , υποβάλλονται οι σχετικές αιτήσεις στον υπεύθυνο επεξεργασίας με την ταυτόχρονη καταβολή χρηματικού ποσού το οποίο ρυθμίζεται με σχετική απόφαση της Αρχής όπως και ο τρόπος καταβολής του ή οποιοδήποτε άλλο συναφές ζήτημα. Σε περίπτωση μη ανταπόκρισης του υπευθύνου στο αίτημα πρόσβασης τότε το υποκείμενο έχει τη δυνατότητα να προσφύγει στην Αρχή η οποία θα κρίνει αν πρέπει να καταβληθεί πρόστιμο.

Σε περιπτώσεις που κρίνονται ιδιαίτερα κρίσιμες από την Αρχή ή γίνεται η συλλογή των πληροφοριών για θέματα εθνικής ασφάλειας τότε είναι πιθανό να αποκλεισθεί το δικαίωμα πρόσβασης.

1.3.3.3 Δικαίωμα στην αντίρρηση

Ο νόμος παρέχει το δικαίωμα στο υποκείμενο να προβάλει αντιρρήσεις σχετικά με την επεξεργασία των προσωπικών δεδομένων που τον αφορούν. Πρόκειται για το πιο «δυναμικό» δικαίωμα του υποκειμένου καθώς περιλαμβάνει την ενεργή αντίδραση του στην επεξεργασία των προσωπικών δεδομένων του.

Το δικαίωμα αντίρρησης παρέχει δύο δυνατότητες στο φορέα του. Με βάση την πρώτη δυνατότητα μπορεί ο οποιοσδήποτε να αποκλείσει την επεξεργασία προσωπικών του δεδομένων από οποιονδήποτε για λόγους προώθησης πώλησης αγαθών ή παροχής υπηρεσιών εξ αποστάσεως. Η δεύτερη δυνατότητα είναι να προβάλει στον υπεύθυνο επεξεργασίας τις αντιρρήσεις για την επεξεργασία των δεδομένων που τον αφορούν. Και οι δύο αυτές δυνατότητες συνιστούν το περιεχόμενο των δικαιωμάτων απόλυτης και σχετικής αντίρρησης οι οποίες θα αναλυθούν παρακάτω.

Το δικαίωμα απόλυτης αντίρρησης στρέφεται ενάντια σε όλους τους υπεύθυνους επεξεργασίας οι οποίοι χρησιμοποιούν την επεξεργασία των προσωπικών δεδομένων του υποκειμένου προκειμένου να χρησιμοποιηθούν στην προώθηση πώλησης αγαθών ή παροχή υπηρεσιών από απόσταση (telemarketing, τηλεφωνικές ή με φαξ διαφημίσεις προϊόντων κ.α.). Ο τρόπος άσκησης του δικαιώματος αντίρρησης ασκείται με την υποβολή έγγραφης δήλωσης του ενδιαφερομένου προς την Αρχή Προστασίας Προσωπικών Δεδομένων ότι δεν επιθυμεί τα προσωπικά του δεδομένα να υποστούν επεξεργασία για οποιονδήποτε από τους παραπάνω λόγους.

Το δικαίωμα σχετικής αντίρρησης σε αντίθεση με το δικαίωμα απόλυτης αντίρρησης, ασκείται και αυτό εγγράφως αλλά απευθύνεται στον υπεύθυνο επεξεργασίας για συγκεκριμένα υπό επεξεργασία προσωπικά δεδομένα και ο διαμαρτυρόμενος ζητά συγκεκριμένες ενέργειες για διόρθωση, μη χρησιμοποίηση και διαβίβαση των προσωπικών δεδομένων.

1.3.4 Εποπτικές Αρχές

1.3.4.1 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Το όλο νομικό πλαίσιο προστασίας της ιδιωτικής ζωής του ατόμου από την ανεπιθύμητη επεξεργασία προσωπικών δεδομένων θα ήταν ανώφελο, αν δεν υπήρχε ένα όργανο επιφορτισμένο με την εποπτεία της εφαρμογής της σχετικής νομοθεσίας. Το όργανο αυτό ονομάζεται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, είναι ανεξάρτητη δημόσια Αρχή που δεν υπόκειται σε οποιονδήποτε διοικητικό έλεγχο.

Η Αρχή αποτελείται από επτά μέλη εκ των οποίων ένα ανώτατο δικαστικό λειτουργό, έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι σε γνωστικό αντικείμενο του δικαίου, έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι σε γνωστικό αντικείμενο της πληροφορικής, έναν καθηγητή ή αναπληρωτή καθηγητή Α.Ε.Ι και τρία πρόσωπα με κύρος και εμπειρία στον τομέα προστασίας των προσωπικών δεδομένων.

Σύμφωνα με το νόμο καθορίζονται και οι αρμοδιότητες της Αρχής οι οποίες διακρίνονται σε α) εποπτικές-ελεγκτικές, β) αποφασιστικές- κυρωτικές, γ) νομοθετικές-γνωμοδοτικές.

Οι εποπτικές-ελεγκτικές αρμοδιότητες που ασκεί η Αρχή είναι οι παρακάτω:

- Επιβλέπουν την ενιαία εφαρμογή των ρυθμίσεων σχετικά με την προστασία του ατόμου
- Ασκούν ανεξάρτητο έλεγχο στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν και τις αρμοδιότητες της εθνικής εποπτικής Αρχής που προβλέπεται στις διεθνείς συμφωνίες της Ελλάδας
- Καλούν τα επαγγελματικά σωματεία και τις λοιπές ενώσεις φυσικών προσώπων στην κατάρτιση κωδικών δεοντολογίας για αποτελεσματικότερη προστασία της ιδιωτικής ζωής
- Απευθύνουν συστάσεις και υποδείξεις στους υπευθύνους επεξεργασίας
- Ενεργούν αυτεπαγγέλτως σε διοικητικούς ελέγχους στα πλαίσια των οποίων ελέγχονται η τεχνολογική υποδομή και άλλα μέσα που υποστηρίζουν την επεξεργασία των δεδομένων.

Η Αρχή ασκεί ακόμη τις εξής αποφασιστικές και κυρωτικές αρμοδιότητες:

- Αποφασίζει για χορήγηση ή όχι αδειών επεξεργασίας όπως προβλέπονται από το νόμο και αφορούν ενδεικτικά την επεξεργασία ευαίσθητων προσωπικών δεδομένων, τη διασύνδεση αρχείων όταν αφορούν ευαίσθητα δεδομένα, τη διασυνοριακή ροή δεδομένων κ.α.
- Εκδίδει αποφάσεις μετά από καταγγελίες ατόμων για παράνομη επεξεργασία προσωπικών δεδομένων ή θέτει σε αρχείο αιτήσεις ή παράπονα που κρίνονται ως αβάσιμα, ανώνυμα, αόριστα
- Επιβάλλει τις διοικητικές κυρώσεις που προβλέπονται από τη νομοθεσία προστασίας των προσωπικών δεδομένων

Ολοκληρώνοντας, οι νομοθετικές και γνωμοδοτικές αρμοδιότητες της Αρχής είναι οι ακόλουθες:

- Εκδίδει κανονιστικές πράξεις για ρυθμίσεις ειδικών, τεχνικών και λεπτομερειακών θεμάτων σχετικών με τη προστασία των προσωπικών δεδομένων
- Γνωμοδοτεί για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία προσωπικών δεδομένων και επισημαίνει τυχόν μεταβολές στον τομέα της προστασίας του ατόμου από την επεξεργασία των προσωπικών δεδομένων
- Εξετάζει αιτήσεις υπεύθυνων επεξεργασίας με τις οποίες ζητείται ο έλεγχος και η εξακρίβωση της νομιμότητας της επεξεργασίας[31]

1.3.4.1.1 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)

Ο νεότερος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων γνωστός και ως General Data Protection Regulation (GDPR) που τέθηκε σε λειτουργία το Μάϊο του 2018 αλλάζει ριζικά τον τρόπο που οι επιχειρήσεις και οργανισμοί συλλέγουν, επεξεργάζονται και διαχειρίζονται προσωπικά δεδομένα κάθε μορφής. Πρόκειται για ένα εκσυχρονισμένο νομοθετικό πλαίσιο το οποίο καθορίζει τις περιπτώσεις στις οποίες επιτρέπεται να χρησιμοποιούνται , αποθηκεύονται, διαγράφονται, μεταβιβάζονται και εν γένει να επεξεργάζονται τα προσωπικά δεδομένα αλλά κυρίως τον τρόπο προστασίας τους.[31] Ο Κανονισμός θα επηρεάσει κάθε οργανισμό και εταιρεία στην Ευρώπη, η οποία διαχειρίζεται με οποιονδήποτε τρόπο προσωπικά δεδομένα, αλλά και κάθε εταιρεία που συναλλάσσεται στην επικράτεια της Ευρωπαϊκής Ένωσης.

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων θεσπίζει την υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων σε τρεις συγκεκριμένες περιπτώσεις:

- Όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος των δεδομένων που υφίστανται επεξεργασία)
- όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα
- όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα

Μερικές από τις αλλαγές που επέφερε η αναθεώρηση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένα είναι η αλλαγή στα θέματα προστασίας των ανηλίκων (π.χ. απαγόρευση χρήσης social media από άτομα κάτω των 16 ετών παρά μόνο με τη γονική συγκατάθεση), το δικαίωμα στη λήθη δηλαδή το δικαίωμα του υποκειμένου να ζητήσει τη άμεση διαγραφή των δεδομένων του, το δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα που αυτό σημαίνει ότι θα υπάρχει σαφέστερη ενημέρωση του πολίτη στο στάδιο συλλογής και επεξεργασίας των δεδομένων του, το δικαίωμα διόρθωσης ανακριβών στοιχείων ή τη συμπλήρωση ελλιπών από τον υπεύθυνο επεξεργασίας και τέλος, το δικαίωμα εναντίωσης στην επεξεργασία , βάσει του οποίου ο πολίτης θα φέρει αντίθεση ως προς την επεξεργασία των δεδομένων του, υπό συγκεκριμένες προϋποθέσεις (π.χ. εμπορική προώθηση).

1.3.4.2 Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε) πρόκειται για μια ανεξάρτητη Αρχή με διοικητική αυτοτέλεια και έχει βασικές αρμοδιότητες την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης και επικοινωνίας με οποιονδήποτε άλλο τρόπο όπως ορίζεται από το Σύνταγμα.[32]

Πιο συγκεκριμένα η Α.Δ.Α.Ε έχει τις ακόλουθες αρμοδιότητες:

- Διενεργεί αυτεπάγγελτα, κάνοντας τακτικούς και έκτακτους ελέγχους σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π) , δημόσιες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία
- Λαμβάνει πληροφορίες σχετικά με την εκπλήρωση της αποστολής της , από τις παραπάνω υπηρεσίες , οργανισμούς και καλεί σε ακρόαση τους εκπροσώπους ή τα στελέχη τους
- Προβαίνει σε κατάσχεση μέσων που παραβιάζουν το απόρρητο των επικοινωνιών και σε καταστροφή των στοιχείων αυτών
- Εξετάζει καταγγελίες ατόμων που θίγονται από τον τρόπο ή τη διαδικασία άρσης του απορρήτου
- Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στο ΦΕΚ καθώς και συστάσεις και υποδείξεις σχετικά με θέματα της αρμοδιότητας της [32]

1.3.4.3 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων πρόκειται για μία ανεξάρτητη Αρχή που διαθέτει ειδικά δικαιώματα από το Σύνταγμα της Ελλάδας ενώ βάσει νομοθετικών κανόνων ενισχύθηκε ο εποπτικός , ελεγκτικός και ρυθμιστικός της ρόλος. Οι κυριότερες αρμοδιότητες της είναι η ρύθμιση και η εποπτεία της αγοράς ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται εταιρείες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου, καθώς και ο έλεγχος της ταχυδρομικής αγοράς στην οποία δραστηριοποιούνται εταιρείες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς.

Ανάμεσα στις αρμοδιότητες της εντάσσονται και εκείνες της Επιτροπής Ανταγωνισμού στις εν λόγω αγορές και μαζί με αυτή συνθέτουν τον ενισχυμένο ρόλο της σε αντίθεση με τα πρώτα χρόνια ίδρυσης της όπου οι αρμοδιότητες της επικεντρωνόταν στην εποπτεία της απελευθερωμένης αγοράς των τηλεπικοινωνιών. Με την ψήφιση του Ν.2668/98 ο οποίος καθόριζε τον τρόπο οργάνωσης και λειτουργίας του τομέα των ταχυδρομικών υπηρεσιών, ανατέθηκε στην Εθνική Επιτροπή Τηλεπικοινωνιών (όπως ήταν αρχικά ονομασμένη) και η ευθύνη για την εποπτεία και ρύθμιση της αγοράς των ταχυδρομικών υπηρεσιών και μετονομάστηκε σε Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ).

1.3.5 Διακινδύνευση Προσωπικών Δεδομένων με τη χρήση μη επανδρωμένων αεροσκαφών (U.A.V- ‘drones’)

Όπως το διαδίκτυο, του οποίου οι πρώτες εφαρμογές ήταν στρατιωτικές έτσι και τα drones είχαν ως αρχικό σκοπό δημιουργίας την υλοποίηση στρατιωτικών προγραμμάτων και αποστολών, όμως πλέον χρησιμοποιούνται σε μεγάλο βαθμό στη καθημερινότητα των απλών πολιτών ως μέσο διασκέδασης, hobby, εμπορικών μεταφορών, επιτήρησης εγκαταστάσεων, καταπολέμησης της εγκληματικότητας.

Τα drones ή U.A.Vs ή R.P.A.S είναι εξ αποστάσεως κατευθυνόμενες ή αυτόματα προγραμματισμένες κατευθυνόμενες ιπτάμενες συσκευές οι οποίες στελεχώνονται συνήθως από μια κάμερα καταγραφής εικόνας ή και ήχου, χρήσιμη για το χειριστή του drone να βλέπει τη πορεία του, αλλά και ικανή να καταγράφει ό,τι βρίσκεται στο πεδίο λήψης της κάμερας.

Μερικές από τις δυνατότητες τους είναι να μπορούν να μεταφέρουν αντικείμενα, είτε να μεταδίδουν την εικόνα και τον ήχο που λαμβάνουν μέσω της κάμερας καταγραφής γεγονός που τις καθιστά εργαλείο υψηλής σημασίας. Μέσω των drones επιτυχγάνονται: ο έλεγχος των συνόρων, η διεξαγωγή αποστολών σε χώρους ατυχημάτων όπου κρίνεται επικίνδυνη η παρουσία διασωστών, οι σκοποί των Υπηρεσιών Πολιτικής Προστασίας (π.χ. επιθεωρήσεις σε χώρους φυσικών καταστροφών), η επιθεώρηση και συντήρηση υποδομών, η χαρτογράφηση, η μετεωρολογία και η προστασία του περιβάλλοντος, η χρήση τους στη γεωργία και την αλιεία, η δημοσιογραφική έρευνα και τέλος η μεταφορά εμπορευμάτων.

Βάσει των παραπάνω λόγων, τα drones είναι εξαιρετικά χρήσιμα και αναγκαία στις μέρες μας όταν χρησιμοποιούνται με σύνεση, όμως σε αντίθετη περίπτωση εγγυμωνούν σοβαρούς κινδύνους. Οι τεχνικές δυνατότητες των συσκευών δημιουργούν εύλογες ανησυχίες σε θέματα διείσδυσης τους στην ιδιωτική ζωή των ατόμων μέσω της συλλογής και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα εν αγνοία των υποκειμένων. Κατ’ επέκταση τίθεται το ζήτημα εφαρμογής νομοθετικών κανόνων καθώς τα παραπάνω συνιστούν πληροφορίες που αναφέρονται στο υποκείμενο των δεδομένων και η ταυτότητα του μπορεί να γίνει γνωστή ή να εξακριβωθεί.

Από άποψη προστασίας των προσωπικών δεδομένων το πρόβλημα δεν έγγυται στο γεγονός αποκλειστικά της χρήσης και υπερπτήσης των drones, αλλά κυριολεκτικά στη πιθανή κακόβουλη χρήση των διαθέσιμων ειδών τεχνολογιών αιχμής, με τις οποίες είναι δυνατός ο εξοπλισμός τους (π.χ. κάμερες, αισθητήρες κίνησης, εντοπιστές ip addresses κ.α.).

Στα νομικά ζητήματα που σχετίζονται με τη προστασία των προσωπικών δεδομένων προτείνεται η εισαγωγή νόμων καθώς και μιας σειράς πρακτικών για τη μείωση των κινδύνων για τα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία από τη χρήση των δυνατοτήτων των drones και αφορούν «όλη την αλυσίδα των drones» , δηλαδή από τον κατασκευαστή έως τον τελικό χρήστη και υπεύθυνο επεξεργασίας των δεδομένων, αλλά και το υποκείμενο των δεδομένων.

Πέρα των άλλων μέτρων προστασίας της ιδιωτικής ζωής του ατόμου , προτείνεται ο ορισμός μιας μορφής δεδομένων η οποία θα χρησιμοποιείται για την παροχή πληροφοριών σε μια ανοιχτή διαδικτυακή διεπαφή, ώστε οι πληροφορίες αυτές να διατίθενται μέσω παρόχων υπηρεσιών , να παρουσιάζονται μέσω εφαρμογής για έξυπνα τηλέφωνα ή να μεταφορτώνονται απευθείας στο drone.

Μέσω του πλαισίου αυτού προτείνεται η δυνατότητα ταυτοποίησης του drone και του χειριστή του μέσω ενός ηλεκτρονικού chip (I drone) ή μιας κάρτας SIM ή ακόμη και η καταγραφή τους μέσω διαδικτυακών εφαρμογών.[33]

1.3.6 Ποινικά Αδικήματα

1.3.6.1 Απάτη με ηλεκτρονικό υπολογιστή

Η ηλεκτρονική εγκληματικότητα η οποία προέκυψε τα τελευταία χρόνια μαζί με την ταυτόχρονη ανάπτυξη και εξέλιξη της τεχνολογίας οδήγησε σε νέες μορφές εγκληματικότητας, οι οποίες συνδέονται με την πληροφορική και τους Η/Υ. Χαρακτηριστικό παράδειγμα πλάνης είναι η απάτη με υπολογιστή, όπου ο δράστης εισάγει ψευδή δεδομένα σε ένα σύστημα πληροφορικής, τα οποία μπορούν με αυτοματοποιημένες διαδικασίες να υποστούν επεξεργασία, ή σε περιπτώσεις που ο δράστης παρεμβαίνει στο λογισμικό ή στο υλικό ενός υπολογιστή επηρεάζοντας με αυτό τον τρόπο το αποτέλεσμα της επεξεργασίας της πληροφορίας. Τα παραπάνω παραδείγματα δεν αποτελούν προϊόν απάτης καθώς δεν γίνεται άμεση επέμβαση του ανθρώπου, όπως θα γινόταν σε περιπτώσεις απάτης φυσικού προσώπου στις οποίες ο δράστης προβαίνει στην εν γνώση παράσταση ψευδών γεγονότων ως αληθινών ή στην απόκρυψη αληθινών γεγονότων.

Ως προς την παραβίαση των απορρήτων στοιχείων των Η/Υ, απόρρητα στοιχεία ενός Η/Υ θεωρούνται εκείνα που α) είναι προσιτά σε περιορισμένο κύκλο προσώπων χωρίς να είναι ευρέως γνωστά, β) συνδέονται με τη λειτουργία μιας επιχείρησης και γ) η πρόσβαση σε αυτά είναι δυσχερής και τηρούνται απόρρητα με τη βούληση του κατόχου τους.

Ακόμη, η εγκληματική συμπεριφορά πραγματοποιείται με την αθέμιτη αντιγραφή, χρησιμοποίηση, αποκάλυψη σε τρίτους ή παραβίαση απόρρητων στοιχείων ή προγραμμάτων Η/Υ. Η ενσωμάτωση δηλαδή του προγράμματος σε υλικό φορέα αλλά και η δημιουργία αντιγράφων στην οποία έχουν πρόσβαση τρίτοι άμεσα ή έμμεσα. Πέρα από την αντιγραφή όμως, απαγορεύεται και η χρήση ενός προγράμματος Η/Υ χωρίς δικαίωμα ενώ απόρρητα θεωρούνται και τα στοιχεία που περιέχονται σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή, τα

στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών και η επικοινωνία μέσω ηλεκτρονικών συστημάτων (π.χ. ηλεκτρονικό ταχυδρομείο).[34]

Το κενό που υπάρχει στον τομέα αυτό προσπαθεί να καλυφθεί από τη θέσπιση νέων νόμων και διατάξεων με στόχο την προστασία των προσωπικών δεδομένων και την επιβολή κυρώσεων στα άτομα που προβαίνουν σε αυτές τις αθέμιτες ενέργειες.

1.3.6.2 Πλαστογραφία σε ηλεκτρονικό έγγραφο

Σύμφωνα με το νόμο 1805/88 διευρύνθηκε ο νομοθετικός ορισμός της έννοιας του εγγράφου, καθώς με τον όρο έγγραφο νοείται οποιοδήποτε μέσο χρησιμοποιείται από Η/Υ ή περιφερειακή μνήμη υπολογιστή , με ηλεκτρονικό , μαγνητικό ή άλλο τρόπο προκειμένου να γράψει, αποθηκεύσει, παράγει ή αναπαράγει στοιχεία που δεν μπορούν να διαβαστούν άμεσα, όπως και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία , εικόνα, σύμβολο ή ήχος εφόσον τα μέσα και τα υλικά προορίζονται να αποδείξουν γεγονότα που έχουν έννομη σημασία.

Το έγκλημα της πλαστογραφίας διαπράττεται όταν υπάρχει παράνομη αντιγραφή δεδομένων ή λογισμικού κατά την οποία ο δράστης ενεργεί με σκοπό να παραπλανήσει κάποιον τρίτο με τη χρήση του αντιγράφου που δημιούργησε. Η παραποίηση συνεπώς του νόμιμου ηλεκτρονικού εγγράφου αποτελεί για γεγονός που έχει έννομη σημασία , ενώ η χρήση του αντιγραμμένου λογισμικού πρόκειται για επιβαρυντική περίπτωση. Επιπλέον, η αλλοίωση των δεδομένων μπορεί να πληροί την ειδική υπόσταση της πλαστογραφίας με τη μορφή της νόθευσης.[35]

ΜΕΡΟΣ ΔΕΥΤΕΡΟ

2.1 Ηλεκτρονικά Έγγραφα

2.1.1 Ορισμός Ηλεκτρονικού Εγγράφου

Το ηλεκτρονικό έγγραφο (electronic document) πρόκειται για ένα σύνολο από δεδομένα τα οποία εγγράφονται στο μαγνητικό δίσκο ενός ηλεκτρονικού υπολογιστή (Η/Υ) και μπορούν να χρησιμοποιηθούν και να αποτυπωθούν με διάφορα μέσα σε ψηφιακή (οθόνη ενός Η/Υ) ή υλική-εκτυπωμένη μορφή σαν κείμενα ή εικόνες καθώς δεν είναι από μόνα τους αναγνώσιμα. Με βάση τα παραπάνω αντιλαμβάνεται κανείς ότι ηλεκτρονικά έγγραφα μπορούν να θεωρηθούν τόσο εκείνα που έχουν εξαρχής ηλεκτρονική υπόσταση όσο εκείνα που έχουν μεν υλική υπόσταση αλλά το περιεχόμενο τους αποτυπώνεται με τη χρήση της ηλεκτρονικής τεχνολογίας.

Τα ηλεκτρονικά έγγραφα χωρίζονται σε δύο κατηγορίες: α) τα γνήσια και β) τα μη γνήσια. Γνήσια θεωρούνται τα έγγραφα που έχουν αποκλειστικά ηλεκτρονική υπόσταση , δηλαδή καταχωρήσεις ηλεκτρονικών δεδομένων σε μαγνητικό υλικό. Από την άλλη πλευρά , τα μη γνήσια ηλεκτρονικά έγγραφα είναι έγγραφα με υλική μορφή , των οποίων το περιεχόμενο αλλά και η υπογραφή είναι ηλεκτρονικά αποτυπωμένα. Χαρακτηριστικά παραδείγματα μη γνήσιων ηλεκτρονικών εγγράφων είναι η τηλεομοιοτυπία (fax) και το τηλέτυπο (telex).

Τα ηλεκτρονικά έγγραφα αποτελούν βασικό κομμάτι των ηλεκτρονικών συναλλαγών καθώς η χρήση τους θεωρείται αυτονόητη σε συμβάσεις που καταρτίζονται ηλεκτρονικά , στο ηλεκτρονικό εμπόριο και σε ηλεκτρονικές βάσεις δεδομένων. Ακόμη το ηλεκτρονικό έγγραφο κυριαρχεί και στο χώρο του διαδικτύου, με τη μορφή ηλεκτρονικών επιστολών (e-mail) , ιστοσελίδων (sites),

αρχείων που διακινούνται μέσω διαδικτύου, τηλεδιασκέψεων που πραγματοποιούνται με μαγνητικά μέσα, ακόμη και σε συζητήσεις Internet Relay Chat (IRC).

Οι πολλαπλές ιδιότητες του ηλεκτρονικού εγγράφου είχαν ως αποτέλεσμα την ραγδαία αύξηση της χρήσης του σε κάθε τομέα ηλεκτρονικών επικοινωνιών και συναλλαγών καθώς διευκόλυναν σημαντικά τη καθημερινότητα των ανθρώπων. Πέραν όμως των πολλών πλεονεκτημάτων παρουσιάζουν και μια σειρά από μειονεκτήματα όπως ότι στερούνται της σταθερότητας κατά την ενσωμάτωση τους, μπορούν να υποστούν αλλοιώσεις, μετατροπές ή διαγραφές που είναι αδύνατον να εντοπιστούν, αλλά και ότι δεν διαθέτουν την ιδιόχειρη υπογραφή που είναι απαραίτητη στα έγγραφα και είναι το αποδεικτικό μέσο γνησιότητας ενός εγγράφου. Επιπλέον, όταν διακινούνται μέσω ανοιχτών δικτύων, όπως είναι το διαδίκτυο, υπάρχει κίνδυνος να υποκλαπούν αυτά από τρίτους και να αλλοιωθεί ή να τροποποιηθεί το περιεχόμενο τους.

Όσον αφορά τα έγγραφα που διακινούνται ηλεκτρονικά, κρίνεται δυσχερής η ακριβής εξακρίβωση της ταυτότητας του αποστολέα των εγγράφων, όπως και της αυθεντικότητας και της μη αλλοίωσης τους. Για να μπορέσει να υπάρχει πλήρης αξιοποίηση των δυνατοτήτων που προσφέρει η σύγχρονη τεχνολογία απαιτείται η ενίσχυση της ασφάλειας των ηλεκτρονικών συναλλαγών και γι’ αυτό χρησιμοποιούνται μέθοδοι κρυπτογράφησης που εξασφαλίζουν την ασφαλή μεταφορά δεδομένων Η/Υ μέσω ανοιχτών δικτύων.

Η ηλεκτρονική υπογραφή αποτελεί ένα από τα πιο αξιόπιστα μέσα για την εξασφάλιση της γνησιότητας των εγγράφων που διακινούνται ηλεκτρονικά. Σύμφωνα με το άρθρο 2 παράγραφος 1 του προεδρικού διατάγματος 150/2001 ως ηλεκτρονική υπογραφή ορίζονται τα «δεδομένα σε ηλεκτρονική μορφή , τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας». Οι δύο πιο βασικοί τύποι συστημάτων κρυπτογράφησης είναι το συμμετρικό και το ασύμμετρο κρυπτογραφικό σύστημα οι οποίοι θα αναλυθούν στην πορεία της παρούσας διπλωματικής εργασίας.

2.1.2 Ηλεκτρονικό Εμπόριο

Με την πρόοδο της τεχνολογίας στον τομέα της πληροφορικής και με τις δυνατότητες που έχουν οι πληροφορίες τόσο ως προς τη συλλογή τους αλλά και ως προς τη μετάδοσης τους μέσω δικτύων δημιουργήθηκε ένα νέο πλαίσιο για τη διεξαγωγή συναλλαγών, μια «εικονική» αγορά, η οποία δεν γνωρίζει γεωγραφικούς περιορισμούς αλλά είναι παγκόσμια και χρησιμοποιεί το διαδίκτυο για τη λειτουργία της. Πιο συγκεκριμένα, το εμπόριο που βασίζεται στην ηλεκτρονική μετάδοση δεδομένων που περιέχουν εικόνες , ήχο ή κείμενο ονομάζεται «ηλεκτρονικό εμπόριο». Ο ορισμός αυτός μπορεί να επεκταθεί ώστε να περιλαμβάνει κάθε είδους συναλλαγή για την οποία χρειάζεται ψηφιακή υποδομή , όπως η Online παράδοση ψηφιακού περιεχομένου, η ηλεκτρονική μεταφορά κεφαλαίων , οι ηλεκτρονικές αγοροπωλησίες μετοχών, οι ηλεκτρονικοί πλειστηριασμοί , η διαφήμιση και η προώθηση προϊόντων , η παραχώρηση βάσεων δεδομένων κ.α.

Η νέα μορφή εμπορίου που στηρίζεται στο διαδίκτυο παρέχει πολλές δυνατότητες για τη συναλλακτική επαφή των μερών, μερικές από τις οποίες είναι το ηλεκτρονικό ταχυδρομείο (e-mail) , το τηλεομοιοτύπωμα (fax), το telex και η μέθοδος ηλεκτρονικής ανταλλαγής δεδομένων (Electronic Data Interchange) σε αντίθεση με το παραδοσιακό εμπόριο που το δίκτυο ήταν ένα μέσο διακίνησης δεδομένων, για το διαδικτυακό ηλεκτρονικό εμπόριο το ίδιο το διαδίκτυο είναι η αγορά.

Με βάση τον ορισμό της Επιτροπής της ΕΕ, ως «ηλεκτρονικό» νοείται το εμπόριο που αφορά την ηλεκτρονική διεξαγωγή συναλλαγών, δηλαδή την παροχή προϊόντων και υπηρεσιών, συνήθως έναντι αμοιβής χρησιμοποιώντας εξοπλισμό ηλεκτρονικής επεξεργασίας για την επικοινωνία από απόσταση, δηλαδή την ηλεκτρονική επεξεργασία και μεταφορά δεδομένων που περιλαμβάνουν κείμενα, ήχο και εικόνα.

Ανάλογα με τον τρόπο που διεξάγεται το ηλεκτρονικό εμπόριο μπορεί να χωριστεί στα εξής είδη: α) μεταξύ επιχειρήσεων (Business to Business,B2B), β) μεταξύ επιχειρήσεων και καταναλωτών (Business to Consumer,B2C), γ) μεταξύ επιχειρήσεων και της Διοίκησης (Business to Administration) και δ) μεταξύ χρηστών (User to User). Οι ηλεκτρονικές συναλλαγές ευρύτερα , περιλαμβάνουν και άλλες κατηγορίες συναλλαγών, οι οποίοι προκύπτουν από την αλληλεπίδραση μεταξύ των καταναλωτών, των επιχειρήσεων και της Διοίκησης. [36]

Ένα ακόμη κριτήριο με το οποίο διακρίνεται το είδος του ηλεκτρονικού εμπορίου είναι ο τρόπος που παραδίδονται στον αγοραστή τα αγαθά που αγοράζει ηλεκτρονικά. Σε περιπτώσεις αγοράς άυλων αγαθών όπως είναι το λογισμικό ή υπηρεσίες πληροφόρησης τότε το ηλεκτρονικό εμπόριο λέγεται άμεσο ενώ όταν η συναλλαγή αφορά υλικά αγαθά λέγεται έμμεσο γιατί η παράδοση γίνεται με τον παραδοσιακό τρόπο ταχυδρομικής αποστολής.

Η διόγκωση του ηλεκτρονικού εμπορίου είχε ως άμεση συνέπεια την ανάγκη για ενισχυμένη ασφάλεια των συναλλαγών για την πραγματοποίηση της οποίας απαιτούνται συγκεκριμένες μέθοδοι προστασίας ηλεκτρονικών δεδομένων , είτε αποθηκευμένων, είτε διαβιβαζομένων ηλεκτρονικά στις οποίες ο κάτοχος τους επιθυμεί να παραμείνουν κρυφές σε περιπτώσεις κλοπής ή απώλειας τους. Οι μέθοδοι που χρησιμοποιούνται για την προστασία των ηλεκτρονικών δεδομένων από υποκλοπή ή αλλοίωση τους κατά τη διάρκεια των συναλλαγών ποικίλλουν. Διάφορες μορφές προστασίας είναι η ηλεκτρονική υπογραφή, τα firewalls, τα ειδικά συστήματα τηλεπικοινωνιών μεγάλης ασφάλειας, όπως τα πρωτόκολλα επικοινωνίας OPS , SAL.

Τα συνηθέστερα προβλήματα ασφάλειας που παρουσιάζονται κατά καιρούς στις συναλλαγές στο ηλεκτρονικό εμπόριο είναι:[37]

I. Η παρακολούθηση των γραμμών επικοινωνίας. Η ευκολία παρακολούθησης και υποκλοπής δεδομένων που αποστέλλονται μέσω του τηλεφωνικού δικτύου από Η/Υ σε Η/Υ, αν η τηλεφωνική γραμμή του χρήστη συνδεθεί με Η/Υ που έχει το κατάλληλο λογισμικό πρόγραμμα παρακολούθησης.
II. Η κλοπή κλειδιών πρόσβασης ή συνθηματικών. Από τη στιγμή που είναι εύκολη η παρακολούθηση γραμμών επικοινωνίας, είναι εξίσου εύκολη διαδικασία να καταγραφούν και να υποκλαπούν ηλεκτρονικά κλειδιά ή συνθηματικά που χρησιμοποιούνται για πρόσβαση σε εμπιστευτικά αρχεία ή άλλα ευαίσθητα δεδομένα. Ειδικοί στη πρόσβαση σε δεδομένα χωρίς άδεια, στο «σπάσιμο» κωδικών και στην υποκλοπή δεδομένων , ακόμη και με τη χρήση ιών, είναι οι hackers και οι crackers.
III. Η υποκλοπή και τροποποίηση της μεταδιδόμενης πληροφορίας. Είναι μια ενέργεια η οποία επιφέρει στο παθόντες σοβαρή

οικονομική ζημιά και μπορεί να προκαλέσει ανωμαλία στην ομαλή διεξαγωγή των συναλλαγών. Αν για παράδειγμα ο υποκλοπέας διακόψει την επικοινωνία μεταξύ ενός εμπόρου και του προμηθευτή του σχετικά με τη παραγγελία συγκεκριμένης ποσότητας εμπορευμάτων , τροποποιήσει τη μεταδιδόμενη πληροφορία και την επαναδρομολογήσει προς τον ανυποψίαστο προμηθευτή, τότε ο τελευταίος, χωρίς να αντιληφθεί ότι τροποποιήθηκε η πληροφορία , θα αποστείλει λανθασμένη ποσότητα εμπορευμάτων, δημιουργώντας έτσι οικονομική ζημία τόσο στον ίδιο όσο και στον έμπορο.

IV. Η «μεταμφίεση» μέσω πλαστής ηλεκτρονικής διεύθυνσης. Κατά τις ηλεκτρονικές συναλλαγές είναι συχνό και εύκολο φαινόμενο να πέφτουν αρκετοί χρήστες του διαδικτύου θύματα παραπλάνησης από άτομα με πλαστά προσωπικά στοιχεία. Το αποτέλεσμα αυτής της ηλεκτρονικής «μεταμφίεσης» είναι να αποκτά ο δράστης πρόσβαση σε ηλεκτρονικά συστήματα ξεγελώντας τους μηχανισμούς ασφαλείας των συστημάτων αυτών.

Για όλους τους παραπάνω λόγους, είναι απαραίτητη η επίτευξη μιας ασφαλούς ηλεκτρονικής συναλλαγής η οποία είναι αναγκαία όχι μόνο για τους παρόχους, όπως είναι εταιρείες, οργανισμοί και επιχειρήσεις αλλά κυρίως για τους καταναλωτές καθώς απαιτείται ένα υψηλό επίπεδο ασφάλειας και εμπιστευτικότητας. Συνεπώς, η τεχνολογία της επικοινωνίας πρέπει να παρέχει στους συναλλασσόμενους κάποιες βασικές ιδιότητες που να καθιστούν ασφαλή την επικοινωνία, οι οποίες είναι:

I. Η πιστοποίηση της αυθεντικότητας της ταυτότητας του κάθε συναλλασσόμενου: Οι ηλεκτρονικές συναλλαγές μεταξύ δύο αγνώστων επιτάσσουν την ανάγκη για διαπίστωση της ταυτότητας των συναλλασσόμενων
II. Η διαφύλαξη της ακεραιότητας: Εξασφαλίζεται το αναλλοίωτο του περιεχομένου του μηνύματος
III. Η εξασφάλιση της εμπιστευτικότητας: Το μήνυμα να προστατεύεται κατά τη διάρκεια αποστολής του ώστε να μην έχουν πρόσβαση σε αυτό μη εξουσιοδοτημένα πρόσωπα

IV. Η εξασφάλιση της μη αποποίησης ευθύνης: Οι εμπλεκόμενοι σε μια ηλεκτρονική συναλλαγή να μην έχουν τη δυνατότητα εκ των υστέρων να αρνηθούν τη συμμετοχή τους σε αυτή τη συναλλαγή

Αυτές οι τέσσερις ιδιότητες εξασφαλίζονται με το καλύτερο τρόπο με τη χρήση της ηλεκτρονικής υπογραφής.

2.2 Ορισμός και είδη Ηλεκτρονικής υπογραφής

Η συνεχώς εξελισσόμενη τεχνολογία της πληροφορικής οδήγησε στην αυξανόμενη χρήση ηλεκτρονικών εγγράφων από φυσικά ή νομικά πρόσωπα για διάφορες διεξαγωγές καθημερινών ηλεκτρονικών συναλλαγών. Σε αντίθεση με τον συμβατικό τρόπο συναλλαγών, όπου η πιστοποίηση ενός ατόμου γινόταν με τη συγκέντρωση και διατήρηση αποδείξεων που βασίζονταν σε πρωτότυπα ενυπόγραφα έγγραφα, στις ηλεκτρονικές συναλλαγές κάτι παρόμοιο δεν είναι δυνατό. Αυτό συμβαίνει επειδή τα ψηφιακά δεδομένα τα οποία χρησιμοποιούν, δεν μπορούν να ενσωματωθούν σε ένα μόνο υλικό φορέα και αυτό έχει ως άμεση συνέπεια τον κίνδυνο αλλοίωσης ή και αντιγραφής του περιεχομένου του εγγράφου τους. Επιπλέον, η αβεβαιότητα που υπάρχει σχετικά με το πρόσωπο το οποίο έχει εκδώσει το έγγραφο καθιστά την εξασφάλιση μιας υπογραφής ανάλογη με την ιδιόχειρη η οποία θα μπορεί να χρησιμοποιηθεί για συναλλαγές σε ηλεκτρονικό περιβάλλον, δηλαδή στο διαδίκτυο ή σε συναλλαγές με ηλεκτρονικά μηχανήματα.

Η μέθοδος αυτή που επιτελεί τη λειτουργία της ιδιόχειρης υπογραφής, ονομάζεται «ηλεκτρονική υπογραφή» και αποτελείται από «δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας». Έτσι, τα έντυπα μέσα που χρησιμοποιούνται για την απόδειξη μιας συναλλαγής (π.χ. ενυπόγραφα ιδιωτικά έγγραφα, επικυρωμένα φωτοαντίγραφα ταυτοτήτων, σφραγισμένοι φάκελοι κ.α.) αντικαθίστανται με

αντίστοιχα ψηφιακά δεδομένα με κύρια προϋπόθεση την χρήση αξιόπιστων τεχνικών μεθόδων πιστοποίησης της ‘προέλευσης’ και της ‘ακεραιότητας’ των δεδομένων. Η ηλεκτρονική υπογραφή πρέπει λοιπόν να μπορεί να προσαρμόζεται στις ιδιαίτερες συνθήκες παραγωγής των ηλεκτρονικών εγγράφων, να δημιουργείται με τη βοήθεια των ηλεκτρονικών μέσων επικοινωνίας και να επικυρώνει μια ηλεκτρονική συναλλαγή. Με όλα τα παραπάνω χαρακτηριστικά θα μπορούσαμε να πούμε ότι η ηλεκτρονική υπογραφή παρέχει σε ένα ηλεκτρονικό έγγραφο την εγγύηση της αυθεντικότητας, της εμπιστευτικότητας, της γνησιότητας και της μη αλλοίωσης του. Στην έννοια της ηλεκτρονικής υπογραφής εντάσσεται και η ψηφιακή υπογραφή η οποία είναι μια ασφαλής μέθοδος διαπίστωσης τόσο του δημιουργού του ηλεκτρονικού εγγράφου όσο και της γνησιότητας του εγγράφου.

Μια έγκυρη ηλεκτρονική υπογραφή πιστοποιεί στον παραλήπτη ότι το μήνυμα που δημιουργήθηκε ανήκει στον αποστολέα που το υπέγραψε ψηφιακά και ότι δεν αλλοιώθηκε-παραποιήθηκε κατά τη μεταφορά. Οι ηλεκτρονικές υπογραφές χρησιμοποιούν συνδυασμό μιας κρυπτογραφικής συνάρτησης κατατεμαχισμού (hash function) για δημιουργία της σύνοψης (hash) σε συνδυασμό με ασύμμετρη κρυπτογραφία για κρυπτογράφηση-αποκρυπτογράφηση σύνοψης. Η ηλεκτρονική υπογραφή συνίσταται με μέθοδο κρυπτογραφήσεως του κειμένου, η οποία παρέχει κατά μία άποψη εγγύηση αυθεντικότητας και μη αλλοιώσεως του. Επίσης, θα πρέπει να καθιστά δυνατή την ανάγνωση του κειμένου από μεγάλο αριθμό αναγνωστών, χωρίς αυτοί να είναι σε θέση να γνωρίζουν το κλειδί με το οποίο κρυπτογραφήθηκε το κείμενο. Σε μερικές χώρες όπως τις ΗΠΑ και κάποιες χώρες της Ευρώπης οι ηλεκτρονικές υπογραφές έχουν και νόμιμη υπόσταση.

Υπάρχουν πολλοί τρόποι, περισσότερο ή λιγότερο ασφαλείς για να υπογράψει κανείς ηλεκτρονικά και με αυτό τον τρόπο είτε να δείξει την πρόθεσή του να δεσμευτεί από την υπογραφή του και από το περιεχόμενο του εγγράφου, είτε να επιβεβαιώσει την ταυτότητα του. Μερικά παραδείγματα ασφαλών ηλεκτρονικών υπογραφών είναι τα παρακάτω:

I. Η υπογραφή που βασίζεται στην εκ των προτέρων γνώση κάποιου κωδικού, όπως μια λέξη-κλειδί ή ένας μυστικός αριθμός
II. Η υπογραφή που βασίζεται στη συμμετρική ή στην ασύμμετρη κρυπτογραφία
III. Η υπογραφή που στηρίζεται στο βιομετρικό σύστημα πιστοποίησης της ταυτότητας

Αυτά τα τρία είδη υπογραφής θα αναλυθούν αμέσως παρακάτω.

2.2.1 Η ηλεκτρονική υπογραφή που βασίζεται στην εκ των προτέρων γνώση κωδικού

Αυτό το απλό είδος ηλεκτρονικής υπογραφής έγινε ιδιαίτερα γνωστό κυρίως λόγω της χρήσης του στο σύστημα των τραπεζών με τη μορφή μυστικού κωδικού (PIN). Η χορήγηση στον πελάτη ενός μυστικού (ακόμη και ως προς την υπηρεσία) κωδικού αριθμού , με την πληκτρολόγηση του οποίου τίθεται σε λειτουργία το σύστημα και επιτυγχάνεται η ολοκλήρωση της συναλλαγής προσφέρει ταχύτερες συναλλαγές μεταξύ χρηστών και τραπεζών. Η απλή συναλλαγή του πελάτη με μια τράπεζα με τη βοήθεια ηλεκτρονικού υπολογιστή απαιτεί αντίστοιχα απλό σύστημα για την εξασφάλιση της αξιοπιστίας της συναλλαγής και ως προς το πρόσωπο του πελάτη και ως προς το περιεχόμενο της εντολής.

Η απλοϊκή λειτουργία του είναι ιδιαίτερα επισφαλής σε θέματα προστασίας και ασφάλειας καθώς είναι πιθανό ο κωδικός να γίνει αντικείμενο απομίμησης, δηλαδή να κλαπεί ή να αντιγραφεί αν πληροφορηθεί κάποιος τρίτος τον συνδυασμό των αριθμών και το πρόσωπο στο οποίο αντιστοιχεί. Ο έλεγχος γνησιότητας του χρήστη σε αυτές τις περιπτώσεις είναι αδύνατος από την τράπεζα καθώς ο σωστός κωδικός ενεργοποιεί το ηλεκτρονικό μηχάνημα (ATM) και προβαίνει στην προγραμματισμένη συναλλαγή. Συνεπώς είναι ευθύνη του ίδιου του δικαιούχου να πραγματοποιεί συστηματικούς ελέγχους του υπολοίπου του τραπεζικού του λογαριασμού όταν παρατηρεί ύποπτες κινήσεις στον λογαριασμό του και να ειδοποιεί την τράπεζα για κλείσιμο λογαριασμών όταν εντοπίσει πρόσβαση στον λογαριασμό του από μη εξουσιοδοτημένο πρόσωπο. Σε τέτοιες περιπτώσεις παύει να ισχύει το απόρρητο της υπογραφής. [38]

2.2.2 Η Ηλεκτρονική υπογραφή που βασίζεται στην κρυπτογραφία

2.2.2.1 Εισαγωγή στην Κρυπτογραφία

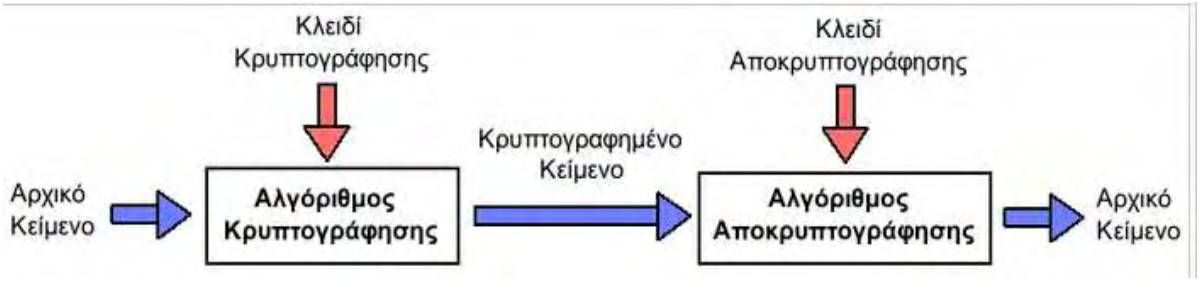
Παρόλο που διεθνώς δόθηκαν διάφοροι ορισμοί για την κρυπτογραφία ο πιο διαδεδομένος όμως είναι αυτός που αναφέρεται στο πρόβλημα της μυστικής επικοινωνίας. Με τον όρο «κρυπτογραφία» νοείται γενικά μια μέθοδος κωδικοποίησης του περιεχομένου του διαβιβαζόμενου μηνύματος σύμφωνα με ένα προκαθορισμένο μυστικό κώδικα. Κύρια αιτία ύπαρξης της κρυπτογραφίας είναι ο κίνδυνος πρόσβασης στα δεδομένα από κάποιον 'αντίπαλο' με στόχο να αλλοιώσει τα δεδομένα. Στη σύγχρονη εποχή, είναι η μετατροπή των δεδομένων ενός ηλεκτρονικού υπολογιστή με τη χρήση αλγορίθμων κρυπτογράφησης, δηλαδή ένα σύνολο από μαθηματικές συναρτήσεις, με στόχο τα δεδομένα να μπορούν να αναγνωσθούν μόνο με τη χρήση κλειδιών αποκρυπτογράφησης.

Η σημασία της κρυπτογραφίας είναι τεράστια σε τομείς που έχουν σχέση με την ασφάλεια υπολογιστικών συστημάτων και τις τηλεπικοινωνίες καθώς παρέχει ασφαλή επικοινωνία μεταξύ δύο ή περισσοτέρων άκρων επικοινωνίας (π.χ. άνθρωποι, προγράμματα υπολογιστών κ.α.) χωρίς την παρέμβαση τρίτων.

Οι βασικές έννοιες της κρυπτογραφίας είναι οι εξής:

- Αρχικό κείμενο (plaintext): αποτελείται από τα αρχικά δεδομένα τα οποία εισάγονται στον αλγόριθμο κρυπτογράφησης
- Αλγόριθμος κρυπτογράφησης (encryption algorithm): η χρήση του συγκεκριμένου αλγορίθμου πραγματοποιεί τις κατάλληλες ενέργειες για να μετασχηματίσει τα δεδομένα σε μια μορφή που να μην επιτρέπει την αποκάλυψη του περιεχομένου τους σε μη εξουσιοδοτημένα μέρη
- Μυστικό κλειδί (secret key): είναι ένας αριθμός αρκετών bits που χρησιμοποιείται ως είσοδος στον αλγόριθμο κρυπτογράφησης και η ειδοποιός διαφορά της κρυπτογραφίας με την κωδικοποίηση
- Κρυπτογραφημένο μήνυμα (ciphertext): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου στο αρχικό κείμενο
- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): πραγματοποιεί την αντίστροφη διαδικασία από τον αλγόριθμο κρυπτογράφησης, δηλαδή λαμβάνει το κρυπτογραφημένο κείμενο και με το μυστικό κλειδί που χρησιμοποιήθηκε στην διαδικασία

κρυπτογράφησης το αποκρυπτογραφεί, δηλαδή παράγει το αρχικό κείμενο



Εικόνα: Ένα τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

2.2.2.2 Αρχές μέτρησης της κρυπτογραφικής δύναμης

Το πρώτο στάδιο το οποίο αναλύει τη δύναμη ενός κρυπτογραφικού μηχανισμού είναι η υπόθεση της ικανότητας του αντιπάλου. Αυτή μπορεί να κριθεί με βάση τα μέσα που διαθέτει ο αντίπαλος, όπως είναι οι πόροι που έχει στη διάθεση του αλλά και η πρόσβαση που έχει στο κρυπτογραφημένο μήνυμα, στο απλό κείμενο και στο κρυπτοσύστημα. Με βάση αυτά έχει τις εξής δυνατότητες επίθεσης: [39]

- Επίθεση στο κρυπτογραφημένο μήνυμα: σε αυτή τη περίπτωση ο αντίπαλος έχει πρόσβαση μόνο σε συγκεκριμένα κομμάτια του κρυπτογραφημένου μηνύματος και προσπαθεί να αποκρυπτογραφήσει τα κομμάτια αυτά ή να ανακαλύψει το αντίστοιχο κλειδί. Αυτά τα συστήματα θεωρούνται ανασφαλή καθώς είναι ευάλωτα σε τέτοιου είδους επιθέσεις.
- Επίθεση με απλό γνωστό αντικείμενο: σε αυτό το είδος επίθεσης ο αντίπαλος γνωρίζει αντιστοιχίες κρυπτογραφημένου μηνύματος με απλό κείμενο και προσπαθεί να ανακαλύψει το αντίστοιχο κλειδί.

- Επίθεση με επιλεγμένο απλό κείμενο: ο αντίπαλος έχει δυνατότητα πρόσβασης στο κρυπτοσύστημα αλλά δεν γνωρίζει το κλειδί όμως ζητά την κρυπτογράφηση μηνυμάτων με απώτερο σκοπό να ανακαλύψει την αντιστοιχία του απλού κειμένου με το άγνωστο κρυπτογραφημένο μήνυμα.
- Επίθεση προσαρμόσιμου επιλεγμένου απλού κειμένου: εδώ υπάρχει η υπόθεση ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο κρυπτογράφησης και έχει στόχο να βρει το κλειδί αποκρυπτογράφησης ώστε να το χρησιμοποιήσει αργότερα για να αποκρυπτογραφεί τα νέα κρυπτοκείμενα.
- Επίθεση προσαρμόσιμου επιλεγμένου κρυπτοκειμένου: η επίθεση αυτή μοιάζει πολύ με την επίθεση του προσαρμόσιμου επιλεγμένου απλού κειμένου με τη μόνη διαφορά ότι ο αντίπαλος έχει πρόσβαση στον αλγόριθμο αποκρυπτογράφησης.

Με βάση όλα τα παραπάνω συμπεραίνουμε ότι κάθε πιθανό είδος επίθεσης βασίζεται στη γνώση του αντιπάλου του αλγορίθμου αποκρυπτογράφησης. Αυτό εκτός από διαπίστωση είναι και ένα θεμελιώδες κριτήριο στην αντικειμενική μέτρηση της δύναμης ενός κρυπτογραφικού συστήματος το οποίο είναι γνωστό ως η Αρχή του Kerchoff: «Η ασφάλεια ενός κρυπτογραφικού συστήματος δεν εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης. Η ασφάλεια του κρυπτοσυστήματος εξαρτάται μόνο από το να διατηρείται μυστικό το κλειδί».

2.2.2.3 Κρυπτογραφικές Υπηρεσίες και πρωτόκολλα

Η κρυπτογραφία έχει τέσσερις πολύ βασικές κρυπτογραφικές υπηρεσίες που στοχεύουν στην αντιμετώπιση συγκεκριμένων απειλών. Οι κρυπτογραφικές υπηρεσίες είναι οι ακόλουθες: [40]

- Εμπιστευτικότητα (confidentiality): αφορά την προστασία από τη μη εξουσιοδοτημένη κάλυψη της πληροφορίας. Η εμπιστευτικότητα θα πρέπει να προσφέρεται με τέτοιο τρόπο ώστε να είναι πολύ δύσκολη η αποκάλυψη σε τρίτους.

- Ακεραιότητα (integrity): η αλλοίωση της πληροφορίας να επιτυγχάνεται μόνο από εξουσιοδοτημένα μέρη. Μέσω της ακεραιότητας να δίνεται η δυνατότητα στον κάτοχο του μηνύματος να ανιχνεύσει πιθανές αλλαγές ή αλλοιώσεις στο μήνυμα από άτομα που δεν έχουν δικαιοδοσία.
- Μη απάρνηση (Non- repudiation): η υπηρεσία κατά την οποία τα συναλλασσόμενα μέρη δεν μπορούν να αρνηθούν την αυθεντικότητα της μετάδοσης ή της δημιουργίας του μηνύματος αντίστοιχα
- Αυθεντικότητα (authentication): μέσω της συγκεκριμένης υπηρεσίας γίνεται η εξακρίβωση της ταυτότητας του χρήστη ή γενικότερα της οντότητας με την οποία επικοινωνούμε.

Αξίζει να σημειωθεί ότι υπάρχει αλληλεξάρτηση μεταξύ της ακεραιότητας και της αυθεντικότητας ενός μηνύματος. Δεν είναι δυνατό να προσφέρεται με επιτυχία μόνο ακεραιότητα σε ένα μήνυμα χωρίς να προσφέρεται αυθεντικότητα και αντίστροφα. Στο σενάριο που προσφερθεί ακεραιότητα χωρίς αυθεντικότητα κάποιος τρίτος μπορεί να τροποποιήσει το μήνυμα και να επανυπολογίσει το κρυπτογραφικό άθροισμα ελέγχου (checksum) το οποίο προσδιορίζει την ακεραιότητα σε ένα μήνυμα.

Με τον όρο «Κρυπτογραφικό Πρωτόκολλο» προσδιορίζεται η πλήρως αποσαφηνισμένη διαδικασία που πρέπει να ακολουθηθεί από τα μέλη που επικοινωνούν μεταξύ τους προκειμένου να επιτύχουν μια συγκεκριμένη κρυπτογραφική υπηρεσία. Το πιο βασικό χαρακτηριστικό του κρυπτογραφικού πρωτοκόλλου είναι ότι κάθε μέλος πρέπει να γνωρίζει για κάθε χρονική στιγμή πιο βήμα πρέπει να εκτελεστεί αλλά και τη διαδικασία εκτέλεσης του. Αν διαπιστωθεί παρέκκλιση από τη διαδικασία τότε αυτό συνεπάγεται την κατάρρευση της επικοινωνίας ή της υποκείμενης κρυπτογραφικής υπηρεσίας.

Εικόνα: Κρυπτογραφικές πράξεις, πρωτόκολλα και υπηρεσίες

Η ανάγκη χρησιμοποίησης κρυπτογραφικών πρωτοκόλλων κρίνεται απαραίτητη καθώς ο χρήστης αντιλαμβάνεται την ασφάλεια του συστήματος με τη μορφή των κρυπτογραφικών υπηρεσιών οι οποίες προσφέρονται με την υλοποίηση των κρυπτογραφικών πράξεων. Προκειμένου οι κρυπτογραφικές πράξεις να προσφέρουν τα επιθυμητά αποτελέσματα πρέπει να εκτελεσθούν με συγκεκριμένο τρόπο και η περιγραφή δράσης τους βρίσκεται στο κρυπτογραφικό πρωτόκολλο. Συνεπώς ένα κρυπτογραφικό πρωτόκολλο είναι αναγκαίο καθώς περιγράφει τη λειτουργία και τη δράση των κρυπτογραφικών πράξεων.

Ένα πρωτόκολλο έχει τα εξής χαρακτηριστικά:

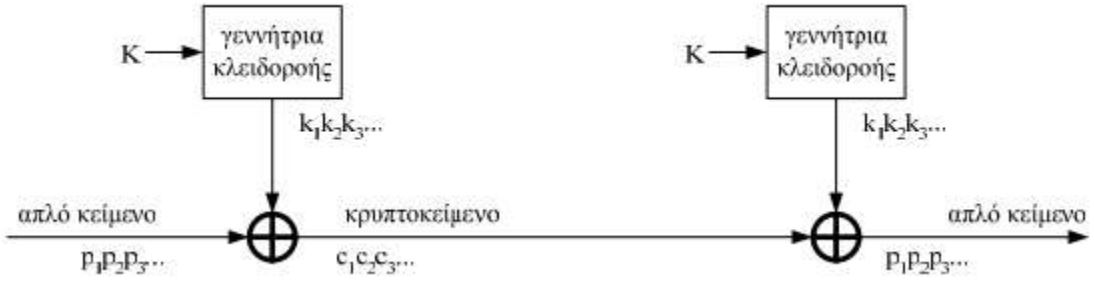
- έχει καθοριστεί εκ των προτέρων
- έχει αμοιβαία συμφωνία των μελών
- έχει σαφήνεια ως προς την εκτέλεση των βημάτων του
- έχει πληρότητα δηλαδή να υπάρχουν προκαθορισμένες ενέργειες για τα μέλη του

2.2.2.1.2 Κρυπταλγόριθμοι ροής και τμήματος

Δύο βασικές κατηγορίες κρυπταλγορίθμων είναι οι κρυπταλγόριθμοι ροής (stream cipher) και οι κρυπταλγόριθμοι τμήματος (block cipher). Στη πρώτη κατηγορία κρυπταλγορίθμων ανήκουν εκείνη που κρυπτογραφούν μια ροή

μηνύματος χωρίς να τη χωρίζουν σε κομμάτια (blocks) και η λειτουργία τους βασίζεται σε μια γεννήτρια κλειδοροής, η οποία είναι μια περιοδική ακολουθία κλειδιών. Η περιοδική ακολουθία της κλειδοροής βασίζεται σε δύο πολύ σημαντικούς λόγους. Πρώτον, θα πρέπει να έχει τη δυνατότητα να παράγει την ίδια ακολουθία κλειδιών σε δύο διαφορετικές τοποθεσίες την ίδια χρονική στιγμή το οποίο συνεπάγεται τη χρήση αξιόπιστων συσκευών. Δεύτερον, οι μηχανές πεπερασμένων καταστάσεων, στην οποία κατηγορία ανήκουν και οι ηλεκτρονικοί υπολογιστές, έχουν τη δυνατότητα αυτή. Σε περίπτωση που δεν ήταν αναγκαία συνθήκη η ασφαλής αναπαραγωγή της κλειδοροής θα μπορούσε να χρησιμοποιηθεί ένα αξιόπιστο κανάλι για τη μετάδοση ενώ από την άλλη πλευρά ως γεννήτρια κλειδοροής θα μπορούσε να ήταν μια πηγή τυχαίας ακολουθίας αριθμών ή συμβόλων.

Το βασικό πλεονέκτημα του αλγόριθμου ροής είναι η μεγάλη ταχύτητα κρυπτογράφησης και για το λόγο αυτό χρησιμοποιούνται ιδιαίτερα σε περιπτώσεις κρυπτογράφησης τηλεφωνικών συνδιαλέξεων και γενικότερα σε δεδομένα τηλεσυνδυάσκεψης. Στα αρνητικά τους είναι η χαμηλή διάχυση η οποία όμως λειτουργεί σαν πλεονέκτημα από άποψη κωδικοποίησης της πληροφορίας.



Εικόνα: Αρχή λειτουργίας κρυπταλγόριθμου ροής

Από την άλλη πλευρά, οι κρυπταλγόριθμοι τμήματος ενεργούν σε κομμάτια (blocks) του μηνύματος και κρυπτογραφούν κάθε κομμάτι (block) χωριστά. Τις περισσότερες φορές το μήκος του τμήματος είναι σταθερό και συγκεκριμένο για τον κρυπταλγόριθμο και υπάρχει περίπτωση να γεμίσει με μηδενικά σύμβολα το τελευταίο μέρος του τμήματος προκειμένου να έχει το ίδιο μήκος. Τα μειονεκτήματα του συγκεκριμένου κρυπταλγόριθμου είναι τα πλεονεκτήματα του κρυπταλγόριθμου ροής και το αντίστροφο. Για την ακρίβεια, ο κρυπταλγόριθμος τμήματος έχει υψηλή διάχυση, λόγω του ομαδικού χειρισμού των συμβόλων, και

δεν είναι εύκολη η παρέμβαση κάποιου τρίτου με παρεμβολές επιπλέον συμβόλων καθώς ελέγχεται το μέγεθος του τμήματος. Στα μειονεκτήματα τους ανήκουν η χαμηλή ταχύτητα και η διάδοση σφαλμάτων.[41]

2.2.2.2 Συμμετρική κρυπτογραφία

Με σημείο αναφοράς το κλειδί υπάρχουν δύο μεγάλες κατηγορίες κρυπτογραφίας: η «συμμετρική» ή «κρυπτογραφία ιδιωτικού κλειδιού» και η «ασύμμετρη» ή «κρυπτογραφία δημοσίου κλειδιού».

Τα συμμετρικά συστήματα κρυπτογράφησης ήταν τα πιο διαδεδομένα χρονικά συστήματα κρυπτογράφησης παρόλο που τα ασύμμετρα συστήματα είχαν εμφανιστεί επίσημα από το 1976. Η λειτουργία τους βασίζεται σε ένα κοινό κλειδί το οποίο γνωρίζει μόνο ο αποστολέας και ο παραλήπτης του μηνύματος και το οποίο χρησιμοποιούν για τη κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Η διαμοίραση του κλειδιού προϋποθέτει τα συναλλασσόμενα μέρη να είναι γνωστά και να υπάρχει αμοιβαία εμπιστοσύνη στις μεταξύ τους συναλλακτικές σχέσεις. Όποιος αποφασίζει να στείλει μήνυμα με αυτή τη μέθοδο πρέπει να γνωρίζει ότι το κρυπτογραφικό κλειδί που χρησιμοποιεί, θα πρέπει να γίνει γνωστό στον αποδέκτη του μηνύματος.

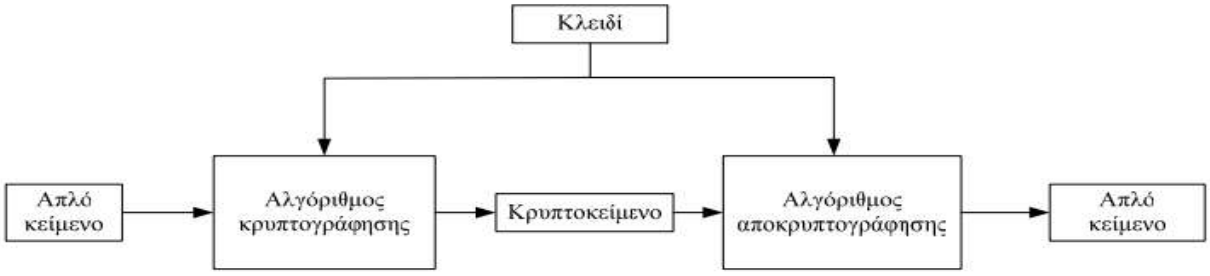
Οι πιο γνωστοί συμμετρικοί αλγόριθμοι που χρησιμοποιούνται και ανήκουν στους αλγορίθμους τμήματος είναι οι: DES (Data Encryption Standard) ο οποίος είναι ο πιο γνωστός παγκοσμίως συμμετρικός αλγόριθμος, 3-way , Blowfish, CAST, CMEA, Triple-DES ο οποίος είναι παραλλαγή του DES, DEAL FEAL, GOST, IDEA, LOKI, Lucifer κ.α. ενώ μερικά παραδείγματα συμμετρικών αλγορίθμων ροής είναι: ORYX, RC4, SEAL.

Τα βασικά χαρακτηριστικά της συμμετρικής κρυπτογραφίας είναι τα εξής:[42]

- χρησιμοποιείται το ίδιο μοναδικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση

- το κλειδί πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη, δηλαδή στον αποστολέα και στον παραλήπτη των μηνυμάτων, διαφορετικά δεν διασφαλίζεται η ακεραιότητα του μηνύματος
- προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών διαφορετικά δεν είναι αποτελεσματική η κρυπτογραφία.
- στη συμμετρική κρυπτογραφία ο αποστολέας και ο παραλήπτης του μηνύματος χρησιμοποιούν το ίδιο κοινό κλειδί. Δηλαδή ο αποστολέας κρυπτογραφεί το μήνυμα με βάση αυτό το κλειδί και ο παραλήπτης το αποκρυπτογραφεί με βάση το ίδιο κλειδί
- στη κρυπτογραφία αυτού του τύπου, θα πρέπει όλα τα κλειδιά που χρησιμοποιούνται να παραμένουν κρυφά, κάτι που είναι εξαιρετικά δύσκολο στο διαδίκτυο
- η συμμετρική κρυπτογραφία έχει ως μοναδικό σκοπό τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών και είναι κατάλληλη για μετατροπές μεγάλου όγκου δεδομένων επειδή οι υπολογισμοί που απαιτεί εκτελούνται πολύ γρήγορα από τις πιο γνωστές μεθόδους συμμετρικής κρυπτογράφησης είναι ο αλγόριθμος DES που υιοθετήθηκε από την Αμερική και το σύστημα Kerberos του γνωστού Πανεπιστημίου MIT, το οποίο αποτελεί το πιο διαδεδομένο σύστημα υποστήριξης της ασφαλούς μεταφοράς κλειδιών μέσω δημόσιων δικτύων

Τα βήματα της συμμετρικής κρυπτογραφίας φαίνονται στο παρακάτω σχήμα. Αρχικά, το απλό κείμενο εισάγεται μαζί με το κλειδί στον αλγόριθμο κρυπτογράφησης με αποτέλεσμα τη δημιουργία του κρυπτογραφημένου μηνύματος το οποίο στη συνέχεια περνάει ως είσοδος μαζί με το κοινό κλειδί στον αλγόριθμο αποκρυπτογράφησης. Ο αλγόριθμος αποκρυπτογράφησης εφαρμόζει τους αντίστροφους μετασχηματισμούς από αυτούς του αλγορίθμου κρυπτογράφησης και επαναφέρει το κείμενο στην αρχική αναγνώσιμη του κατάσταση.



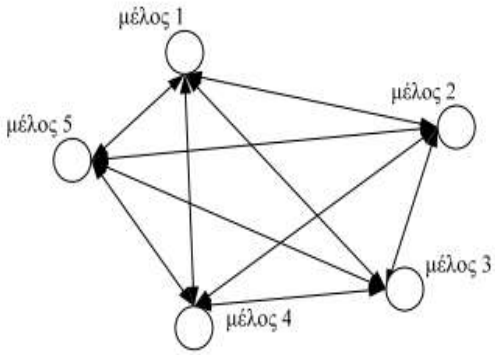
Εικόνα: Συμμετρικό σύστημα κρυπτογράφησης

Το σύστημα αυτό λόγω της απλοϊκότητας του είναι και το πιο οικονομικό σε σχέση με άλλα συστήματα κρυπτογράφησης, όμως είναι αρκετά επισφαλές καθώς ενδέχεται ο κίνδυνος προσβολής του κοινού μυστικού κλειδιού που συμπεριλαμβάνεται στο μεταδιδόμενο μήνυμα και απαιτείται για την αποκρυπτογράφηση του. Αυτό δημιουργεί την ανάγκη ο αποστολέας και ο παραλήπτης του μηνύματος να βρουν έναν ασφαλή τρόπο μετάδοσης της πληροφορίας. Η κρυπτογραφία συνεπώς δεν λύνει το πρόβλημα που υπάρχει αλλά απλώς το μετασχηματίζει σε μορφές που είναι πιο εύκολο να ελεγχθούν. Τα ασφαλή κανάλια επικοινωνίας δεν είναι πάντα διαθέσιμα, απαιτούν σχετικά μεγάλη προσπάθεια για να δημιουργηθούν και η μορφή τους είναι ανάλογη με τη περίσταση. Ένα παράδειγμα είναι η περίπτωση που ο αποστολέας και ο παραλήπτης είχαν συναντηθεί στο παρελθόν και είχαν μοιραστεί το κλειδί με σκοπό να το επαναχρησιμοποιήσουν στο μέλλον. Το ασφαλές κανάλι τους ήταν η επαφή τους χωρίς την μεσολάβηση κάποιου τρίτου. Ένας άλλος τρόπος για τη δημιουργία ασφαλούς καναλιού είναι ο τεμαχισμός του μυστικού κλειδιού και η διαβίβαση του μέσω διαφορετικών καναλιών επικοινωνίας έτσι ώστε να μην είναι δυνατός ο εντοπισμός του κλειδιού από μη εξουσιοδοτημένα άτομα.

Μια ακόμη σημαντική αδυναμία αυτού του τρόπου κρυπτογραφίας είναι η λεγόμενη «το πρόβλημα του τετραγώνου». Αν υπάρχουν n μέλη τα οποία θέλουν να επικοινωνήσουν μεταξύ τους με συμμετρική κρυπτογραφία τότε θα πρέπει ανά ζεύγη των δύο ατόμων να μοιράζονται κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Αυτό σημαίνει ότι κάθε μέλος πρέπει να αποθηκεύσει n-1 διαφορετικά κλειδιά ώστε να είναι σε θέση να επικοινωνήσει με οποιοδήποτε από τα άλλα μέλη. Συνεπώς θα πρέπει να μοιραστούν

$$\frac{n(n-1)}{2} = \frac{n^2 - n}{2}$$

κλειδιά. Το τετράγωνο στον αριθμητή υποδηλώνει τον ρυθμό αύξησης των κλειδιών με την αύξηση των μελών. Για παράδειγμα αν το n=5 τότε τα κλειδιά που χρειάζονται είναι 10. Αν εμφανιστεί ένα ακόμα μέλος ο αριθμός των κλειδιών θα γίνει 15. Για μια μικρή λίστα αποδεκτών στο διαδίκτυο με 1000 μέλη ο αριθμός των κλειδιών είναι 499.500. Αυτό έχει ως αποτέλεσμα να μην μπορεί να ανταποκριθεί στις σύγχρονες ανάγκες που προκύπτουν για την ασφαλή διακίνηση ηλεκτρονικών δεδομένων στα πλαίσια του διαδικτύου στα οποία μετέχει ένας μεγάλος αριθμός συναλλασσόμενων καθώς έχει πολύ μεγάλο οικονομικό κόστος.



	μέλος 1	μέλος 2	μέλος 3	μέλος 4	μέλος 5
μέλος 1		K_{12}	K_{13}	K_{14}	K_{15}
μέλος 2	K_{12}		K_{23}	K_{24}	K_{25}
μέλος 3	K_{13}	K_{23}		K_{34}	K_{35}
μέλος 4	K_{14}	K_{24}	K_{34}		K_{45}
μέλος 5	K_{15}	K_{25}	K_{35}	K_{45}	

Εικόνα: Πλήθος κλειδιών για n=5 μέλη

Γίνεται εύκολα κατανοητό από τα παραπάνω ότι η συμμετρική κρυπτογραφία είναι αποτελεσματική μόνο στις περιπτώσεις που τα συναλλασσόμενα μέρη είναι λίγα στον αριθμό και υπάρχει εκ των προτέρων αμοιβαία εμπιστοσύνη μεταξύ τους, ενώ αντίθετα είναι εντελώς ακατάλληλα για μεγάλα τηλεπικοινωνιακά συστήματα όπως το διαδίκτυο, όπου οι χρήστες είναι γεωμετρικά απομακρυσμένοι και άγνωστοι μεταξύ τους. Κάποια βασικά μειονεκτήματα της συμμετρικής κρυπτογραφίας που καθιστούν ακατάλληλη τη χρήση της στο διαδίκτυο είναι τα εξής:[43]

- Το βασικό πρόβλημα της διανομής και της διαχείρισης των απαιτούμενων κλειδιών (key distribution – management). Σε μια επικοινωνία δύο μερών τα συναλλασσόμενα μέρη πρέπει πριν αρχίσουν τις διαδικασίες αποστολής και λήψης μηνυμάτων, να

χρησιμοποιήσουν ένα ασφαλές κανάλι για τον προσδιορισμό του κλειδιού που θα χρησιμοποιήσουν. Πολλές φορές η διάρκεια ισχύος των κλειδιών περιορίζεται στο διάστημα μιας συνεδρίας επικοινωνίας (communication session).

- Η ανάγκη που υπάρχει για γνώση από τα συμβαλλόμενα μέρη του κλειδιού κρυπτογράφησης και αποκρυπτογράφησης πριν από την συναλλαγή, έχει ως αποτέλεσμα τη χρονική καθυστέρηση που ακυρώνει εκ των πραγμάτων ένα από τα μεγαλύτερα πλεονεκτήματα που έχουν οι ηλεκτρονικές συναλλαγές, δηλαδή την ταχύτητα διεξαγωγής τους.
- Εκτός από την εμπιστευτικότητα των μηνυμάτων υπάρχουν και άλλες απαιτήσεις ασφάλειας (ακεραιότητα, αυθεντικότητα, μη – αποποίηση ευθύνης) στα ανοιχτά και μεγάλης κλίμακας δίκτυα, όπως το διαδίκτυο, για τις οποίες η συμμετρική κρυπτογραφία δεν προσφέρει λύσεις.
- Η κάθε δημόσια υπηρεσία, οργανισμός, εταιρία ή εναλλασσόμενος ιδιώτης θα πρέπει να κατέχει και από ένα διαφορετικό κλειδί κρυπτογράφησης και αποκρυπτογράφησης για κάθε δημόσια υπηρεσία, οργανισμό, εταιρία ή ιδιώτη με τον οποίο θα συναλλασσόταν. Κάτι τέτοιο είναι εξαιρετικά δαπανηρό και ανεφάρμοστο.
- Δεν παρέχει δυνατότητα χρήσης ηλεκτρονικής υπογραφής. Στα ζητήματα αυτά , η σχετικά πρόσφατη ανεπτυγμένη κρυπτογραφία δημοσίου κλειδιού προσφέρει ικανοποιητικές διεξόδους.

Από τις παραπάνω κυριότερες αδυναμίες της συμμετρικής κρυπτογραφίας , δηλαδή να εξαρτώνται από ασφαλές κανάλι επικοινωνίας καθώς και το πρόβλημα του τετραγώνου υπήρξε η ανάγκη της ανακάλυψης της ασύμμετρης κρυπτογραφίας.

2.2.2.2 Ασύμμετρη Κρυπτογραφία

Μια άλλη μέθοδος για τη δημιουργία ηλεκτρονικής υπογραφής αποτελούν οι ασύμμετροι αλγόριθμοι (asymmetric) που λέγονται αλλιώς και αλγόριθμοι κρυπτογράφησης με δημόσιο κλειδί (public key cryptography). Το 1976 οι Whitfield Diffie και Martin Hellman, ερευνητές του Πανεπιστημίου του Stanford , εισήγαγαν μια νέα μαθηματική ανάπτυξη της μεθόδου με στόχο να μη γίνεται εκ των προτέρων η διανομή του κλειδιού αλλά κάθε συναλλασσόμενος να έχει το δικό του ζεύγος κλειδιών. Το χαρακτηριστικό αυτό αποτελεί και την βασική διαφορά μεταξύ της ασύμμετρης και της συμμετρικής κρυπτογραφίας.

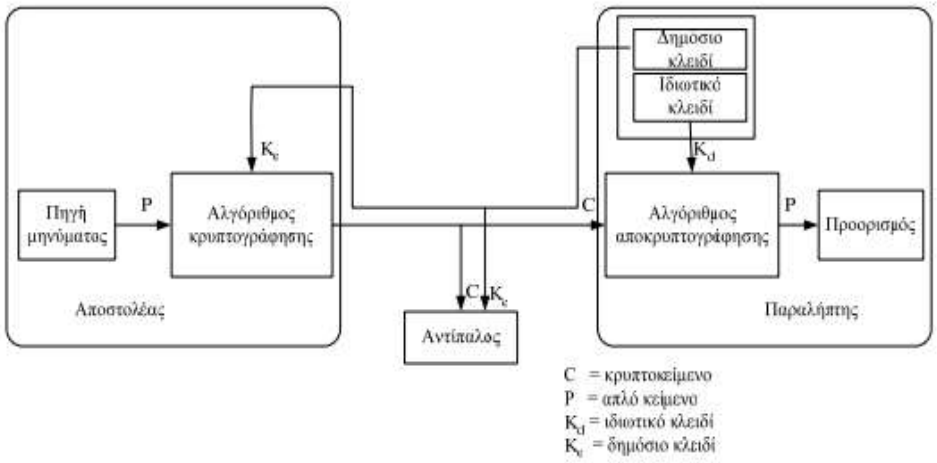
Τα συστήματα που χρησιμοποιούν ασύμμετρους αλγορίθμους για τη θέση της ηλεκτρονικής υπογραφής χρησιμοποιούν ένα συνδυασμό δημοσίου και ιδιωτικού κλειδιού. Σύμφωνα με την ασύμμετρη κρυπτογραφία το κλειδί κρυπτογράφησης δεν μπορεί να χρησιμοποιηθεί για να αποκρυπτογραφεί ή ακόμη καλύτερα, αν χρησιμοποιηθεί για αποκρυπτογράφηση να μη παράγει το ίδιο αρχικό απλό κείμενο. Καθένα από αυτά τα κλειδιά είναι ένας αλγόριθμος, ο οποίος όσο πιο πολλά ψηφία bits περιέχει τόσο πιο ισχυρή κρυπτογράφηση προσφέρει. Τα μέρη, χρησιμοποιούν ένα συνδυασμό δημόσιου και μυστικού κλειδιού τα οποία λειτουργούν πάντα ως ζεύγος με την έννοια ό,τι κρυπτογραφεί το ένα αποκρυπτογραφείται από το άλλο και αντιστρόφως.[44]

Πιο συγκεκριμένα, το μυστικό κλειδί είναι γνωστό μόνο στον κάτοχο του. Το δημόσιο κλειδί δημοσιοποιείται , ενώ αντίθετα το ιδιωτικό κλειδί είναι μυστικό και δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Το ιδιωτικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση του ηλεκτρονικού μηνύματος και είναι απόρρητο το γνωρίζει μόνο ο αποστολέας του μηνύματος και μόνο με αυτό μπορεί να επέμβει στο μήνυμα. Γίνεται αντιληπτό ότι με την χρήση των δύο κλειδιών παύει να υφίσταται η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί.

Ο αποστολέας ενός μηνύματος κατά τη διαδικασία κρυπτογραφήσεως του χρησιμοποιεί το μυστικό κλειδί (private key). Ο συνδυασμός του μηνύματος με το μυστικό κλειδί αποτελεί την ηλεκτρονική ή ψηφιακή όπως έχει επικρατήσει, υπογραφή του αποστολέα. Το κρυπτογραφημένο κείμενο μεταδίδεται στον αποδέκτη, ο οποίος το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο του κλειδί (public key). Η διαδικασία αυτή είναι πιο πρόσφορη για ανοιχτά δίκτυα, όπως

είναι το Internet αλλά δεν είναι κατάλληλη για την μεταβίβαση εκτενών μηνυμάτων λόγω του ότι είναι χρονοβόρα (τα συστήματα DES χρησιμοποιούν κλειδιά με μήκος 56 bits, ενώ τα συστήματα RES χρησιμοποιούν κλειδιά με μήκος 1024 bits). Με τη χρήση της τεχνολογίας της ασύμμετρης κρυπτογραφίας, διατηρώντας μυστικό το ένα κλειδί ως «ιδιωτικό» και διανέμοντας ελεύθερα το άλλο κλειδί ως «δημόσιο» εξασφαλίζεται ότι όλοι όσοι γνωρίζουν το «δημόσιο κλειδί» μπορούν να επαληθεύσουν μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του «ιδιωτικού» κλειδιού. Η χρησιμοποίηση ασύμμετρων αλγορίθμων για τη θέση της ηλεκτρονικής υπογραφής, η οποία και καλείται και διαδικασία RSA δεν είναι κατάλληλη για τη μεταβίβαση εκτενούς περιεχομένου μηνυμάτων, διότι είναι πολύ χρονοβόρα και για τον λόγο αυτό χρησιμοποιείται σε μεγάλη έκταση.

Ο κάθε αλγόριθμος δημοσίου κλειδιού έχει τις δικές του ιδιαιτερότητες, η πλειονότητα όμως αυτών χρησιμοποιεί ζεύγος κλειδιών και βασίζεται στο ότι όποιο από τα κλειδιά δημοσιευθεί, δεν εκθέτει πληροφορίες σχετικά με το άλλο κλειδί. Οι χρήστες λοιπόν του διαδικτύου μπορούν ελεύθερα να συμπεριλάβουν στις ιστοσελίδες τους ή σε ειδικούς καταλόγους -ευρετήρια , τα δημόσια κλειδιά τους, οπότε και παύει να υφίσταται το βασικό πρόβλημα διαχείρισης των κλειδιών της κρυπτογραφίας μυστικού κλειδιού. Τα δημόσια κλειδιά δεν χρειάζονται για τη διανομή τους έναν ασφαλή δίαυλο. Έτσι το μοντέλο επικοινωνίας ενός ασύμμετρου κρυπτοσυστήματος δεν απαιτεί ασφαλές κανάλι διανομής των δημοσίων κλειδιών αφού αυτά είναι προσπελάσιμα και ανοιχτά προς όλους τους ενδιαφερομένους χρήστες. Παρόλα αυτά, ένας αξιόπιστος δίαυλος διανομής κρίνεται απαραίτητος, ορίζοντας με αυτό τον τρόπο ένα μέσο που θα υποστηρίζει την ακεραιότητα της προέλευσης τους. Οι μικρότερες απαιτήσεις ασφάλειας για την διανομή των κλειδιών της, κάνουν την κρυπτογραφία δημοσίου κλειδιού ιδανική για ένα εκ φύσεως δημόσιο δίκτυο, το διαδίκτυο, στο οποίο πολλές φορές χρειάζεται να αποκαθίσταται η εμπιστοσύνη ανάμεσα σε δύο απομακρυσμένους χρήστες χωρίς αυτοί να συναντηθούν ή χωρίς να μεσολαβήσει κάποιο έμπιστο τρίτο μέρος. Σε αυτό το σημείο χρήζει άξιο αναφοράς ότι η αναπαραγωγή του ενός κλειδιού από το άλλο είναι πρακτικά αδύνατη.



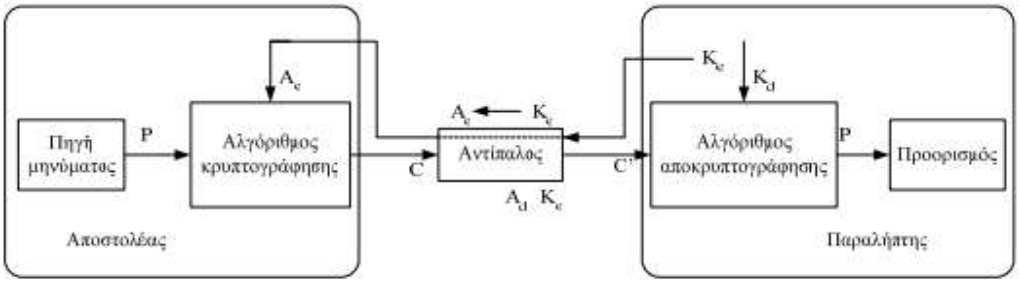
Εικόνα: Μοντέλο επικοινωνίας ασύμμετρης κρυπτογραφίας

Αυτή η αλληλεξάρτηση των κλειδιών στηρίζεται στις μαθηματικές ιδιότητες των πρώτων αριθμών, δηλαδή αριθμών που μόνο όταν διαιρούνται με τον εαυτό τους και με τον αριθμό ένα, δίνουν πηλίκο έναν ακέραιο αριθμό. Όταν οι πρώτοι αριθμοί πολλαπλασιάζονται μεταξύ τους δημιουργούν έναν τρίτο αριθμό, ο οποίος μόνο όταν διαιρείται με τους αρχικούς πρώτους αριθμούς και τον αριθμό ένα δίνει πηλίκο έναν ακέραιο αριθμό. Η μαθηματική δυσκολία εύρεσης των δύο αρχικών πρώτων αριθμών, όταν μόνο το γινόμενο αυτών των αριθμών είναι γνωστό, είναι η μαθηματική βάση της σύγχρονης ασύμμετρης κρυπτογραφίας.

Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το αντίστοιχο δημόσιο κλειδί. Ο τρίτος αριθμός που προκύπτει από τον πολλαπλασιασμό είναι το δημόσιο κλειδί, ενώ οι δύο αριθμοί που πολλαπλασιάζονται μεταξύ τους και δημιουργούν τον τρίτο αριθμό είναι το ιδιωτικό κλειδί. Ένα τέτοιο σύστημα μπορεί να νικηθεί αν ανακτηθεί το ιδιωτικό κλειδί από το δημόσιο. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Το σύστημα με το δημόσιο και το ιδιωτικό κλειδί προσφέρει όλες τις απαραίτητες ιδιότητες μιας ασφαλούς ηλεκτρονικής συναλλαγής, εξασφαλίζοντας συνθήκες που διέπονται από την αυθεντικότητα, την ακεραιότητα, την εμπιστευτικότητα και την μη αποποίηση ευθύνης.

Το σύστημα της ασύμμετρης κρυπτογραφίας αναγνωρίζεται διεθνώς ως το πλέον ασφαλές και πρακτικό σύστημα διασφάλισης της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας των ηλεκτρονικών εγγράφων. Εκτός από την

κρυπτογραφία των κειμένων, μπορεί να χρησιμοποιηθεί και για την πιστοποίηση της ταυτότητας του εκδότη τους και της ακεραιότητας του περιεχομένου του. Παρόλα αυτά όμως δεν έχουν αντιμετωπιστεί εξ ολοκλήρου οι κίνδυνοι που απειλούν την προστασία μιας ηλεκτρονικής επικοινωνίας. Για ακόμα μία φορά η κρυπτογραφία δεν έχει λύσει το πρόβλημα αλλά το έχει μετασχηματίσει. Στην περίπτωση της ασύμμετρης επικοινωνίας δεν τίθεται θέμα ασφαλούς καναλιού διανομής αλλά το πρόβλημα του «ενδιάμεσου ατόμου» (man in the middle). Η επίθεση του ενδιάμεσου ατόμου φαίνεται στο παρακάτω σχήμα στο οποίο ο αντίπαλος παρεμβάλλεται μεταξύ του αποστολέα και του παραλήπτη. Στη περίπτωση αυτή, μπορεί να αντικαταστήσει κατά τη διάρκεια αποστολής του δημοσίου κλειδιού το δημόσιο κλειδί του παραλήπτη K_C με το δικό του δημόσιο κλειδί A_c εφόσον γνωρίζει το ιδιωτικό του κλειδί $A_{d.}$ Έτσι ο αποστολέας σχηματίζει λάθος εντύπωση σχετικά με το κλειδί που έλαβε από τον παραλήπτη πιστεύοντας ότι είναι δικό του. Συνεπώς το μήνυμα κρυπτογραφείται με (C) με το δημόσιο κλειδί του αντιπάλου και έτσι ο αντίπαλος έχει τη δυνατότητα να αποκρυπτογραφήσει το μήνυμα με το ιδιωτικό του κλειδί και στη συνέχεια να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη και να μεταβιβάσει το νέο κρυπτοκείμενο στον παραλήπτη.[45] Με αυτό τον τρόπο δεν γίνεται αντιληπτή από κανένα από τα συναλλασσόμενα μέρη η παρεμβολή κάποιου τρίτου ατόμου.



Εικόνα: Επίθεση του «ενδιάμεσου ατόμου»

Συνεπώς, προκειμένου να εξασφαλιστεί ότι το εκάστοτε ιδιωτικό κλειδί χρησιμοποιείται από τον πραγματικό δικαιούχο του, μπορούν να υιοθετηθούν και κάποια πρόσθετα μέτρα ασφαλείας, τα οποία αφορούν κυρίως την χρήση τεχνικών

μεθόδων αναγνώρισης της ταυτότητας του μέσω μυστικών αριθμών (PIN) ή βιομετρικών συσκευών αναγνώρισης των δακτυλικών αποτυπωμάτων ή της ίριδας των ματιών του δικαιούχου.

2.2.2.3 Ηλεκτρονική Υπογραφή που βασίζεται στην τριμερή ασύμμετρη κρυπτογραφία

΄Ενα από τα μειονεκτήματα της ασύμμετρης κρυπτογραφίας είναι η αβεβαιότητα που υπάρχει σε σχέση με την αυθεντικότητα ή μη του δημοσίου κλειδιού, δηλαδή σε ποιο βαθμό συνδέεται αυτό με τον νόμιμο κάτοχο του. Συνεπώς, κρίνεται αναγκαία η ύπαρξη ενός τρίτου φορέα ο οποίος θα πιστοποιεί και ταυτόχρονα θα εγγυάται σε οποιονδήποτε τρίτο -αποδέκτη της ηλεκτρονικής υπογραφής ότι το δημόσιο κλειδί που χρησιμοποιεί ο συναλλασσόμενος για την αποκρυπτογράφηση του ηλεκτρονικού μηνύματος ανήκει πραγματικά στον αντισυμβαλλόμενο του και άρα είναι και ο νόμιμος κάτοχος του καθώς και τη σύνδεση του ιδιωτικού κλειδιού με τον κάτοχο του πιστοποιητικού.

Ο αναγκαίος αυτός φορέας ονομάζεται «Πάροχος Υπηρεσιών Πιστοποίησης» (εν συντομία ΠΥΠ) και η συμβολή του στην ύπαρξη ασφάλειας και εμπιστοσύνης στις συναλλαγές που πραγματοποιούνται στο περιβάλλον ανωνυμίας του διαδικτύου είναι πολύτιμη.

Οι υπηρεσίες που προσφέρει ο ΠΥΠ διακρίνονται σε ξεχωριστές λειτουργικές οντότητες και συγκεκριμένα σε:[46]

- Υπηρεσία Εγγραφής/ Καταχώρησης (Registration Authority - RA): είναι υπεύθυνη για τον έλεγχο της ταυτότητας των ενώ συλλέγει τα απαραίτητα αποδεικτικά στοιχεία πριν δώσει την έγκριση της για έκδοση σχετικών πιστοποιητικών
- Υπηρεσία Έκδοσης Πιστοποιητικών (Certification Authority- CA): η οποία είναι υπεύθυνη για την έκδοση και την υπογραφή των τελικών πιστοποιητικών των υποκειμένων
- Υπηρεσία Διαχείρισης Αιτημάτων Ανάκλησης (Revocation Management Service): η οποία υποδέχεται , ελέγχει και

διεκπεραιώνει αιτήματα για ανάκληση, παύση ή επανενεργοποίηση πιστοποιητικών σε συνεργασία με την Υπηρεσία Έκδοσης Πιστοποιητικών

- Υπηρεσία Δημοσίευσης (Dissemination & Revocation Status Service): είναι υπεύθυνη για την δημοσίευση των κειμένων τεκμηρίωσης και των υπηρεσιών των ΠΥΠ , την δημοσίευση καταλόγων και λιστών από ανακληθέντα πιστοποιητικά και σχετικών ενημερώσεων προς τους συνδρομητές των ΠΥΠ

Το ηλεκτρονικό πιστοποιητικό που εκδίδει ο ΠΥΠ αποτελεί ηλεκτρονικό αντικείμενο συσχέτισης ενός δημόσιου κλειδιού, όπως και το αντίστοιχο ιδιωτικό κλειδί του, με πληροφορίες όπως ταυτότητα του κατόχου ή περιγραφές αδειών και το δημόσιο κλειδί του. Το ηλεκτρονικό πιστοποιητικό που εκδίδεται εγγυάται για τα στοιχεία του κατόχου του. Διαφορετικά η δημιουργία ενός ζευγαριού δημοσίου-ιδιωτικού κλειδιού στο όνομα κάποιου άλλου προσώπου είναι εφικτή και θα έχει ως αποτέλεσμα την εξαπάτηση όσων συναλλάσσονται μαζί του μέσω διαδικτύου.

Τα «Πιστοποιητικά Δημοσίου Κλειδιού» (Public Key Certificates-PKC) είναι τυποποιημένα ηλεκτρονικά έγγραφα τα οποία εκδίδονται και υπογράφονται από έναν ΠΥΠ με σκοπό να πιστοποιήσουν την κατοχή συγκεκριμένου ζεύγους κρυπτογραφικών κλειδιών από ένα υποκείμενο και να περιγράψουν στοιχεία ταυτοποίησης του υποκειμένου αυτού. Τα Πιστοποιητικά Δημοσίου Κλειδιού μπορούν να χωριστούν σε ‘επώνυμα’ και ‘ψευδώνυμα’ ανάλογα με τη δημοσιοποίηση του πραγματικού ονόματος του υποκειμένου στο οποίο αναφέρονται. Επιπλέον μπορούν να εκδοθούν και ‘ανώνυμα’ πιστοποιητικά όταν πιστοποιείται η χρήση ενός λογαριασμού ηλεκτρονικού ταχυδρομείου από το υποκείμενο. Εκτός από το όνομα σε ένα πιστοποιητικό δημοσίου κλειδιού μπορεί να περιλαμβάνονται και κάποιες ιδιότητες του υποκειμένου (π.χ. επάγγελμα) ενώ δίνεται η δυνατότητα χρήσης κάποιων άλλων ειδικών πιστοποιητικών ιδιοτήτων (attribute certificate) τα οποία χρησιμοποιούνται παράλληλα με τα ‘βασικά πιστοποιητικά δημοσίου κλειδιού’ και τα οποία μπορούν να εκδίδονται από την Αρχή Πιστοποίησης Ιδιοτήτων (Attribute Authority-AA).

Πέρα από τα πιστοποιητικά για φυσικά πρόσωπα υπάρχει και άλλη μια κατηγορία πιστοποιητικών δημοσίων κλειδιών η οποία εκδίδεται έχοντας ως υποκείμενο τηλεπικοινωνιακά ή πληροφοριακά συστήματα και συσκευές (web servers, routers, client devices κ.α.) στα οποία η χρήση των κρυπτογραφικών

κλειδιών περιορίζεται σε α) υπογραφές ταυτοποίησης των συσκευών αυτών και β) σε κρυπτογράφηση άλλων συμμετρικών κλειδιών τα οποία χρησιμοποιούνται για κρυπτογράφηση διακινούμενων δεδομένων.

Η τελευταία κατηγορία ηλεκτρονικών πιστοποιητικών είναι τα «πιστοποιητικά χρονοσφραγίδας» (time-stamping certificates) τα οποία εκδίδονται ad hoc σε ηλεκτρονικά έγγραφα συγκεκριμένου σκοπού και περιλαμβάνουν στοιχεία του εκδότη τους , σύνοψη του συγκεκριμένου εγγράφου στο οποίο αναφέρονται και ακριβής ημερομηνία και ώρα αποστολής και λήψης του ηλεκτρονικά υπογεγραμμένου εγγράφου στα πλαίσια μια εμπορικής και όχι μόνο συναλλαγής. Η ανάγκη για «πιστοποιημένη» χρονοσήμανση καθίσταται ακόμη πιο σημαντική από το γεγονός ότι είναι τεχνικά δυνατή και εύκολη η τροποποίηση της ημερομηνίας του ίδιου του Η/Υ ή άλλης συσκευής που χρησιμοποιεί το συμβαλλόμενο μέρος για να αποστείλει ή να λάβει ηλεκτρονικά μηνύματα.[47] Τα πιστοποιητικά χρονοσφραγίδας εκδίδονται σε συγκεκριμένα ηλεκτρονικά έγγραφα ύστερα από αίτημα είτε του υπογράφοντα είτε του αποδέκτη τους. Ακόμη, η χρήση τους εξασφαλίζει αποδείξεις για την ύπαρξη μιας ηλεκτρονικής υπογραφής σε ένα συγκεκριμένο ηλεκτρονικό έγγραφο μια συγκεκριμένη χρονική στιγμή. Τέλος, αξίζει να αναφερθεί ότι προκειμένου να επωφεληθούν οι συναλλασσόμενοι από τα πλεονεκτήματα της χρονοσήμανσης και της αποθήκευσης, το μήνυμα πρέπει να αποσταλεί από τον αποστολέα στον παραλήπτη μόνο μέσω του ΠΥΠ.

Ο Πάροχος δημοσιεύει ψηφιακά υπογεγραμμένες δηλώσεις που εκδίδονται και υπογράφονται ηλεκτρονικά από έναν ΠΥΠ και ονομάζουν την αρχή πιστοποίησης που τα εξέδωσε, περιέχοντας τα προσωπικά στοιχεία του εγγεγραμμένου χρήστη καθώς και το δημόσιο κλειδί του, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή της πιστοποίησης που το εξέδωσε. Το δημόσιο κλειδί του ΠΥΠ είναι ελεύθερα προσβάσιμο στο διαδίκτυο. Ο ΠΥΠ εξασφαλίζει στα συμβαλλόμενα μέρη την τεχνολογία που χρειάζεται, δηλαδή το λογισμικό και το υλικό προκειμένου να δημιουργηθεί και να επαληθευτεί μια ηλεκτρονική υπογραφή. Η ηλεκτρονική υπογραφή δημιουργείται με βάση τα δεδομένα αποκλειστικής κατοχής (ιδιωτικό κλειδί) και τα προς υπογραφή δεδομένα και αποτελεί μια ψηφιακή «ετικέτα» η οποία επισυνάπτεται στα προς υπογραφή δεδομένα. Με αυτό τον τρόπο πιστοποιείται η μοναδική σχέση του δημοσίου κλειδιού με τον ιδιοκτήτη του και αποφεύγεται η οποιαδήποτε μορφή εξαπάτησης εκ μέρους κάποιου κακόβουλου τρίτου. [48]

Ένα από τα βασικότερα πλεονεκτήματα των ηλεκτρονικών πιστοποιητικών είναι το γεγονός ότι υπάρχει η δυνατότητα να ελεγχθούν χρησιμοποιώντας το δημόσιο κλειδί της αρχής πιστοποίησης. Η χρήση των ηλεκτρονικών πιστοποιητικών γίνεται κυρίως με τα HTTPS για την επαλήθευση των ασφαλών εξυπηρετητών διαδικτύου. Σε αυτή την περίπτωση, η ταυτότητα που συνδέεται με το δημόσιο κλειδί, ελέγχει ότι το domain ανήκει στο πρόσωπο ή την οντότητα, συνήθως εταιρία που έχει αιτηθεί του πιστοποιητικού.

2.2.3 Ηλεκτρονική Υπογραφή που βασίζεται σε Βιομετρικό σύστημα

Η Βιομετρική είναι η επιστήμη η οποία μελετά και αναλύει στατιστικά τα χαρακτηριστικά ενός ατόμου. Η τεχνολογία της έχει στόχο τον αυτόματο έλεγχο της ταυτότητας, δηλαδή την αναγνώριση ενός ανθρώπινου χαρακτηριστικού μέσα σε μερικά δευτερόλεπτα. Η συλλογή των βιομετρικών δεδομένων γίνεται κατά την διαδικασία εγγραφής του ατόμου στο βιομετρικό σύστημα. Με τη χρήση ειδικού αισθητήρα μετατρέπεται το συγκεκριμένο βιομετρικό χαρακτηριστικό σε ηλεκτρονικό κώδικα (λεγόμενο πρότυπο) τον οποίο αποθηκεύει και αντιστοιχίζει με το αντίστοιχο φυσικό πρόσωπο. Κάθε φορά που το άτομο προσπαθεί να αποκτήσει πρόσβαση στο συγκεκριμένο σύστημα, γίνεται έλεγχος της ταυτότητας του, ο οποίος επιτυγχάνεται με σάρωση και εκ νέου υπολογισμό του ηλεκτρονικού κώδικα σε σύγκριση με το αποθηκευμένο πρότυπο.

Σύμφωνα με τις γενικές αρχές προστασίας των προσωπικών δεδομένων είναι σημαντικός ο τόπος αποθήκευσης των «προτύπων». Τα πρότυπα μπορούν να αποθηκευτούν στη μνήμη της βιομετρικής συσκευής, σε κεντρική βάση δεδομένων, σε πλαστικές ή έξυπνες κάρτες. Τα συστήματα που επιτρέπουν την αποθήκευση των προτύπων σε μονάδες που είναι υπό πλήρη έλεγχο είναι περισσότερο φιλικά ως προς την προστασία των ανθρωπίνων δικαιωμάτων.

Η βιομετρική υπογραφή θεωρείται ότι παρέχει το υψηλότερο επίπεδο ασφαλείας στις ηλεκτρονικές συναλλαγές ενώ η διαδικασία λειτουργίας της περιλαμβάνει τέσσερα στάδια τα οποία είναι τα ακόλουθα:[49]

- Καταγραφή δείγματος κατά τη διάρκεια της εκμάθησης
- Εξαγωγή μοναδικών γνωρισμάτων και δημιουργία προτύπου
- Σύγκριση του προτύπου με το νέο δείγμα
- Αποδοχή ή μη αποδοχή του νέου δείγματος

Στον κλάδο των τηλεπικοινωνιών η βιομετρική υπογραφή προσέφερε συναλλακτική ασφάλεια καθώς οι τηλεπικοινωνίες είναι ευάλωτες σε διαφόρων ειδών επιθέσεις , όπως τρομοκρατικές ή επιθέσεις από hackers και crackers. Με τη χρήση τους λοιπόν πιστοποιείται η ταυτότητα του συναλλασσόμενου και εξασφαλίζεται η ασφαλής και αξιόπιστη τηλεπικοινωνία.

Εξαιτίας του γεγονότος ότι τα φυσικά χαρακτηριστικά και η συμπεριφορά ενός ατόμου μπορούν να αλλάξουν με την πάροδο του χρόνου ένα βιομετρικό σύστημα πρέπει να έχει τη δυνατότητα να αποδέχεται και να προσαρμόζεται σε αυτές τις αλλαγές. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από βιομετρικά συστήματα έχουν ιδιαιτερότητες καθώς αφορούν είτε τα φυσικά χαρακτηριστικά ενός ατόμου (όπως τα δακτυλικά αποτυπώματα, η γεωμετρία της παλάμης, η ανάλυση της κόρης του ματιού , τα χαρακτηριστικά του προσώπου, το DNA) είτε στοιχεία συμπεριφοράς του (όπως η χειρόγραφη υπογραφή, φωνή, ο ρυθμός πληκτρολόγησης, τρόπος βαδίσματος) και τα οποία αποτελούν μοναδικά χαρακτηριστικά.[50]

- <u>Δακτυλικό Αποτύπωμα</u>: Η αναγνώριση δακτυλικών αποτυπωμάτων είναι ένα από τα πιο γνωστά και διάσημα βιομετρικά στοιχεία. Η ευκολία χρήσης του και η αξιοπιστία του είναι μερικά από τα πλεονεκτήματα αυτής της μεθόδου ενώ απαιτείται ελάχιστος χρόνος για να αποθηκευτεί ένα αποτύπωμα. Επιπλέον, η πιστοποίηση της γνησιότητας του είναι γρήγορη και αξιόπιστη ενώ βασικό μειονέκτημα αποτελεί η δυνατότητα αντιγραφής του ίχνους του δακτυλικού αποτυπώματος που μένει πάνω στο γυαλί του σαρωτή.
- <u>Γεωμετρία χεριού</u>: Το σύστημα αυτό βασίζεται σε μια σειρά από μετρήσεις που γίνονται στο ανθρώπινο χέρι, από το σχήμα, το μέγεθος της παλάμης καθώς και από τα μήκη και πλάτη των δακτύλων. Τα πλεονεκτήματα της μεθόδου αυτής είναι ίδια με του δακτυλικού αποτυπώματος όμως ένα σημαντικό μειονέκτημα είναι ότι οι σαρωτές παλάμης χρειάζονται περισσότερη ώρα προκειμένου να

τοποθετηθούν και για το λόγο αυτό δεν είναι τόσο διαδεδομένοι στη χρήση τους.

- Ανάλυση ίριδας και αμφιβληστροειδούς του ματιού: στη βιομετρική αυτή μέθοδο δεν απαιτείται από τον χρήστη να εστιάσει το βλέμμα του σε συγκεκριμένο σημείο επειδή τα σημάδια της ίριδας είναι απλωμένα σε όλη την επιφάνεια του ματιού. Με αυτό τον τρόπο η σάρωση μπορεί να γίνει από απόσταση μερικών μέτρων κάτι που ενδείκνυται για άτομα με πρόβλημα όρασης. Όμως το κόστος του σαρωτή είναι ένα βασικό μειονέκτημα καθώς για τη σάρωση του αμφιβληστροειδούς απαιτείται μια χαμηλής ισχύος υπέρυθρη δέσμη φωτός μέσω της κόρης του ματιού, στο πλέγμα των αιμοφόρων αγγείων στο πίσω μέρος του ματιού. Αυτό εξασφαλίζει πολύ χαμηλά ποσοστά λάθους όμως επηρεάζεται αρνητικά από περιπτώσεις παθήσεων όπως ο καταρράκτης ή γλαύκωμα γιατί απαιτείται καθαρή εικόνα του πίσω μέρος του ματιού
- Χαρακτηριστικά προσώπου: Η βιομετρική ηλεκτρονική υπογραφή μέσω των χαρακτηριστικών του προσώπου πλησιάζει πολύ στο φυσικό τρόπο που οι άνθρωποι αναγνωρίζουν ο ένας τον άλλον, γεγονός που βοηθά στο να θεωρείται γενικά η μέθοδος αυτή ότι δεν προσβάλλει την προσωπικότητα του χρήστη. Ευνοείται αρκετά από την ανάπτυξη των τεχνολογιών βίντεο όμως ένα βασικό μειονέκτημα είναι ότι το πρόσωπο αλλάζει με τη πάροδο του χρόνου
- Ρυθμός πληκτρολόγησης: Η τεχνική αυτή ελέγχει το ρυθμό με τον οποίο ο χρήστης πληκτρολογεί κάτι σε τερματικό Η/Υ παρακολουθώντας το πληκτρολόγιο ανά χιλιοστό του δευτερολέπτου. Το πλεονέκτημα αυτής της διαδικασίας είναι ότι η αναγνώριση του χρήστη δεν διαφοροποιείται από την καθημερινή ρουτίνα όταν ο χρήστης βρίσκεται σε περιβάλλον όπου υπάρχουν Η/Υ. Το κόστος όμως αυτής της εφαρμογής είναι υψηλό
- Ηλεκτρονική καταγραφή της χειρόγραφης υπογραφής: Οι συσκευές ηλεκτρονικής καταγραφής της υπογραφής χρησιμοποιούν ηλεκτρονικά στυλό , επιφάνειες ευαίσθητες σε πίεση ή συνδυασμό των δύο, είναι οικονομικές αλλά έχουν μικρή διάρκεια ζωής

2.3 Ψηφιακή Υπογραφή

2.3.1 Ορισμός της ψηφιακής υπογραφής

Η ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα το οποίο βασίζεται στην τριμερή ασύμμετρη κρυπτογραφία και παρέχει όλα τα πλεονεκτήματα που εκείνη προσφέρει στους συναλλασσόμενους καθιστώντας την τη πιο άρτια και ασφαλή τεχνολογικά μέθοδο. Με τη χρήση της ψηφιακής υπογραφής σε μια ηλεκτρονική συναλλαγή διαπιστώνεται η γνησιότητα των ψηφιακών δεδομένων καθώς και η ταυτότητα του εναλλασσόμενου. Η λειτουργία της βασίζεται στο ιδιωτικό κλειδί κρυπτογράφησης το οποίο είναι υπεύθυνο για τη δημιουργία της ενώ το δημόσιο κλειδί χρησιμοποιείται για να επαληθεύει ότι η υπογραφή δημιουργήθηκε με το αντίστοιχο ιδιωτικό κλειδί.

Η ψηφιακή υπογραφή βασίζεται στις κρυπτογραφικές υπηρεσίες της αυθεντικότητας και της μη απάρνησης. Όπως έχει αναφερθεί και παραπάνω η αυθεντικότητα είναι η ταυτοποίηση ενός ατόμου ή η αυθεντικότητα ενός μηνύματος ενώ με τον όρο μη απάρνηση νοείται η υπηρεσία εκείνη κατά την οποία τα συναλλασσόμενα μέρη δεν μπορούν να αρνηθούν την αυθεντικότητα της μετάδοσης ή της δημιουργίας του μηνύματος αντίστοιχα.

Συνοψίζοντας, οι απαιτήσεις ασφάλειας της ψηφιακής υπογραφής είναι:

- Αυθεντικότητα της πηγής του μηνύματος. Κατά την επικοινωνία των μελών πρέπει να υπάρχει η δυνατότητα στον παραλήπτη να επιβεβαιώνει τη ταυτότητα του αποστολέα
- Μη απάρνηση πηγής. Αν ο αποστολέας αρνηθεί ότι έστειλε το μήνυμα πρέπει ο παραλήπτης να μπορεί να αποδείξει ότι το μήνυμα στάλθηκε από τον αποστολέα
- Μη απάρνηση προορισμού. Αν ο παραλήπτης αρνηθεί ότι έλαβε το μήνυμα πρέπει να υπάρχει η δυνατότητα να αποδειχθεί ότι το μήνυμα το έλαβε ο παραλήπτης.

Στην Ελλάδα το προεδρικό διάταγμα 150/2001 όρισε την «ψηφιακή υπογραφή» ή αλλιώς «προηγμένη ηλεκτρονική υπογραφή» αντί του όρου

ηλεκτρονική υπογραφή. Πιο συγκεκριμένα δίνεται ο ορισμός της ψηφιακής υπογραφής ως εξής: « Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή:[51]

- συνδέεται μονοσήμαντα με τον υπογράφοντα
- ταυτοποιεί τον υπογράφοντα, δηλαδή να είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος
- δημιουργείται με τα μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό έλεγχο του και
- συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων».

Από τα παραπάνω γίνεται σαφές ότι μόνο τεχνολογίες ηλεκτρονικής υπογραφής που βασίζονται στο ασύμμετρο σύστημα κρυπτογράφησης πληρούν τις προϋποθέσεις για να θεωρηθούν ως ψηφιακές υπογραφές, ενώ σαφώς δεν τις πληρούν τα συμμετρικά συστήματα που χρησιμοποιούν ένα μόνο κλειδί, το οποίο δεν μπορεί να παραμείνει μυστικό.

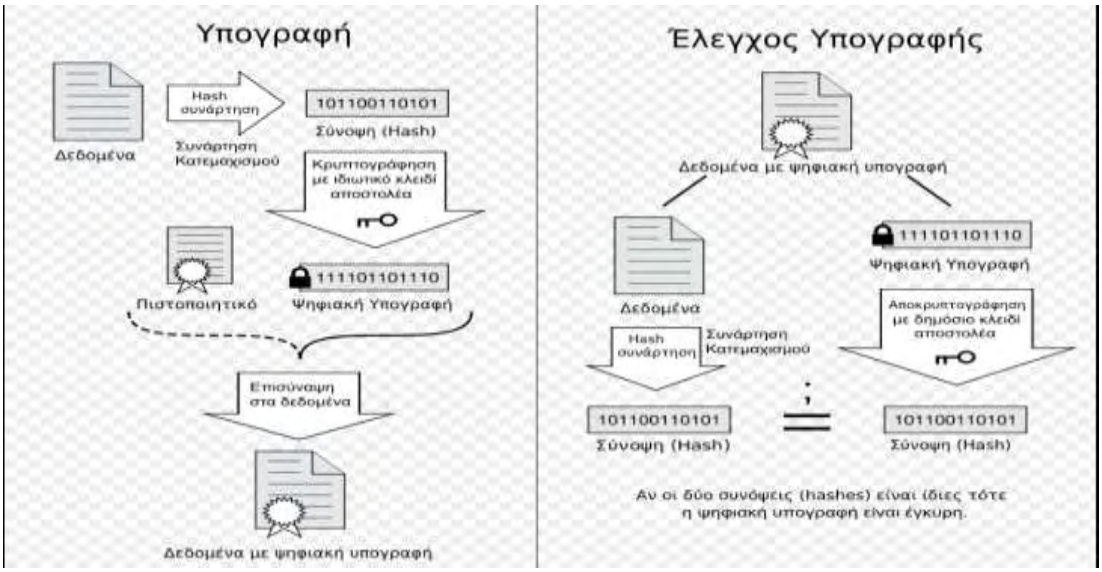
2.3.2 Τεχνολογικές μέθοδοι δημιουργίας ψηφιακής υπογραφής

Υπάρχουν διάφορες τεχνολογικές μέθοδοι δημιουργίας μιας ψηφιακής υπογραφής με την πιο συνηθισμένη και εύχρηστη μέθοδο αυτή του «δακτυλικού αποτυπώματος» δηλαδή της σύντμησης του αρχείου που πρόκειται να κρυπτογραφηθεί. Στη συγκεκριμένη μέθοδο δημιουργείται πρώτα το άθροισμα των bits, δηλαδή το «δακτυλικό αποτύπωμα» του κειμένου σύμφωνα με το οποίο συγκροτείται το περιεχόμενο του κειμένου. Όλο το κείμενο μετατρέπεται σε ένα άθροισμα από bits. Αυτό το «δακτυλικό αποτύπωμα» του κειμένου υπογράφεται στη συνέχεια, δηλαδή κρυπτογραφείται με διαδικασία RSA.[52] Στη συνέχεια αποστέλλεται στον παραλήπτη το μήνυμα με την ψηφιακή υπογραφή. Συνεπώς, ο

αποστολέας του ηλεκτρονικού κειμένου, αρχείου ή οτιδήποτε άλλου, το «σφραγίζει» δηλαδή παράγει μια σύντμηση (message digest) του μεταβιβαζόμενου κειμένου με τη βοήθεια ενός αλγορίθμου (hashing algorithm), ο οποίος δεν έχει καμία σχέση με άλλο αλγόριθμο. Ο αλγόριθμος αυτός παράγει πάντα το ίδιο συντμημένο κείμενο (hash result) για το ίδιο κείμενο, ενώ δεν ισχύει το αντίστροφο.

Το συντμημένο κείμενο που προκύπτει από την παραπάνω διαδικασία στη συνέχεια κρυπτογραφείται με τη χρήση του ιδιωτικού κλειδιού του αποστολέα-υπογράφοντα. Το κρυπτογραφημένο και συντμημένο πλέον κείμενο αποτελεί την ψηφιακή υπογραφή. Η ψηφιακή υπογραφή προσαρτάται στο πρωτότυπο ηλεκτρονικό μήνυμα που είναι μη κρυπτογραφημένο. Τα δύο αυτά μέρη αποστέλλονται ως ενιαίο μήνυμα μέσω του διαδικτύου στον παραλήπτη.

[52] Το κρυπτοσύστημα RSA μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός συστήματος ψηφιακών υπογραφών. Το σύστημα ψηφιακών υπογραφών RSA απαιτεί ότι όλες οι οντότητες έχουν στην κατοχή τους αντίστοιχα ζεύγη δημόσιου και ιδιωτικού κλειδιού.



Εικόνα: Διάγραμμα χρήσης ψηφιακής υπογραφής

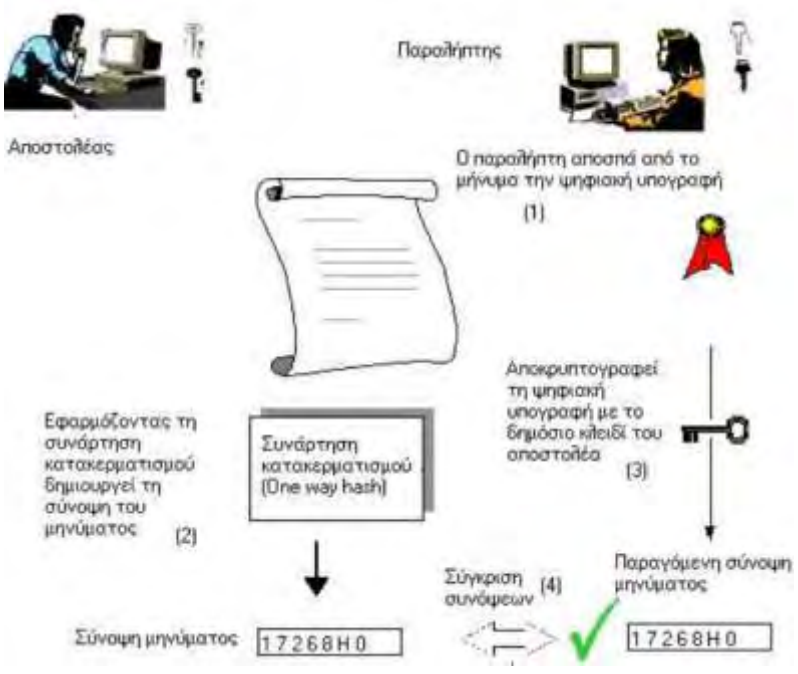
Μια ακόμη μέθοδος δημιουργίας ψηφιακής υπογραφής είναι αυτή του «ψηφιακού φακέλου» (digital envelope) η οποία επιτυγχάνει τον συνδυασμό των συστημάτων συμμετρικών και ασύμμετρων αλγορίθμων με αποτέλεσμα να μειώνει το χρόνο κρυπτογράφησης του μηνύματος. Η μέθοδος αυτή αποκαλείται διεθνώς « Υβριδικό σύστημα κρυπτογραφίας» (hybrid crypto system) γιατί το μήνυμα κρυπτογραφείται συμμετρικά από τον αποστολέα με τη χρήση ενός ασφαλούς κλειδιού μήκους 128 bits το οποίο καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και ονομάζεται «κλειδί συνεδρίας» (session key). Στην συνέχεια και για περισσότερη ασφάλεια το κλειδί αυτό κρυπτογραφείται με ασύμμετρη κρυπτογραφία, δηλαδή με το δημόσιο κλειδί του παραλήπτη. Έτσι ο παραλήπτης του εγγράφου θα πρέπει πρώτα να χρησιμοποιήσει το δικό του ιδιωτικό κλειδί για να βρει το «κλειδί συνεδρίας» του αποστολέα και στη συνέχεια, μέσω αυτού του κλειδιού και το αρχικό μήνυμα. Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Ακόμη, οι ψηφιακοί φάκελοι πέρα από ότι λύνουν το πρόβλημα της ανταλλαγής κλειδιών, βελτιώνουν και την απόδοση καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της αποτελεί εξαιρετικά χρονοβόρα διαδικασία. [53]

2.3.2 Η διαδικασία επαλήθευσης της ψηφιακής υπογραφής

Το στάδιο επαλήθευσης της ψηφιακής υπογραφής πραγματοποιείται όταν το κρυπτογραφημένο αρχείο φτάσει στον παραλήπτη. Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή, δηλαδή την κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύντμηση του μηνύματος και την αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα. Το δημόσιο αυτό κλειδί του αποστολέα είτε αποστέλλεται στον παραλήπτη μαζί με το κρυπτογραφημένο κείμενο, είτε γίνεται γνωστό μέσω δημοσίευσης σε ειδικό δημόσιο κατάλογο που τηρεί ο ΠΥΠ. Με την αποκρυπτογράφηση αυτή ο παραλήπτης επαληθεύει την ταυτότητα του αποστολέα. Μια ψηφιακή υπογραφή η οποία επαληθεύτηκε με το δημόσιο κλειδί του αποστολέα θεωρείται έγκυρη και καθιστά το μήνυμα γνήσιο δεσμεύοντας τον

αποστολέα με το περιεχόμενο του εφόσον το σχετικό πιστοποιητικό δεν έχει λήξει ή δεν έχει ανακληθεί.

Σύμφωνα με την παραπάνω διαδικασία ο παραλήπτης δημιουργεί το δικό του «δακτυλικό αποτύπωμα» του κειμένου που έλαβε, εφαρμόζοντας στο πρωτότυπο μήνυμα τον ίδιο αλγόριθμο κατακερματισμού (hash algorithm) που χρησιμοποιήθηκε κατά την υπογραφή του από τον αποστολέα και δημιουργείται κατά αυτόν τον τρόπο μια νέα σύνοψη. Ο αλγόριθμος παράγει απ' την αρχή μια σύντμηση του μεταβιβαζόμενου ηλεκτρονικού κειμένου την οποία συγκρίνει ο παραλήπτης με βάση τη σύντμηση που έλαβε (επαλήθευση ψηφιακής υπογραφής). Αν οι δύο συντμήσεις είναι ίδιες τότε η υπογραφή επαληθεύεται και επίσης πιστοποιείται ότι το απεσταλμένο μήνυμα δεν αλλοιώθηκε μέχρι να φτάσει στον προορισμό του. Σε περίπτωση που η σύνοψη που παράγει ο παραλήπτης κατά την διαδικασία της επαλήθευσης είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί τότε το ηλεκτρονικό μήνυμα έχει υποστεί αλλοίωση κατά τη μεταφορά του.



Εικόνα: Επαλήθευση ψηφιακής υπογραφής

Στο σημείο αυτό, αξίζει να αναφερθεί ότι το προεδρικό διάταγμα 150/2001 προβαίνει σε συστάσεις στις οποίες αναφέρεται ότι για μια ασφαλή διαδικασία επαλήθευσης μιας ψηφιακής υπογραφής είναι αναγκαία η τήρηση κάποιων κριτηρίων, όπως είναι τα παρακάτω: [54]

- Τα δεδομένα που χρησιμοποιούνται προς επαλήθευση της υπογραφής αντιστοιχούν στα δεδομένα που εμφανίζονται στον επαληθεύοντα
- Η υπογραφή επαληθεύεται με αξιοπιστία και το αποτέλεσμα της επαλήθευσης εμφανίζεται με ορθό τρόπο
- Ο επαληθεύων μπορεί ενδεχομένως να ορίσει με βεβαιότητα τα περιεχόμενα των δεδομένων που υπογράφονται
- Η γνησιότητα και η εγκυρότητα του πιστοποιητικού που απαιτείται κατά τη στιγμή της επαλήθευσης της υπογραφής έχουν ελεγχθεί με αξιοπιστία
- Το αποτέλεσμα της επαλήθευσης όπως και η ταυτότητα του υπογράφοντος εμφανίζεται με τον ορθό τρόπο
- Η χρησιμοποίηση ψευδωνύμου δηλώνεται εμφανώς
- Μπορούν να εντοπιστούν τυχόν τροποποιήσεις απτόμενες της ασφάλειας

Ακόμη, η Οδηγία του προεδρικού διατάγματος προβλέπει τη σύσταση ειδικής «Επιτροπής Ηλεκτρονικής Υπογραφής» η ευθύνη της οποίας είναι να διευκρινίζει τις λεπτομέρειες που υπάρχουν σε κριτήρια που σχετίζονται με την εφαρμογή της αλλά και να επανεξετάζει την εφαρμογή της Οδηγίας ανά τακτά χρονικά διαστήματα (συνήθως ανά τρία έτη).

2.3.3 Εφαρμογές ψηφιακής υπογραφής

Στις μέρες μας η ψηφιακή υπογραφή έχει εφαρμογή σε πάρα πολλούς τομείς που αφορούν τις ηλεκτρονικές συναλλαγές. Η χρήση της ψηφιακής υπογραφής μπορεί να βρίσκεται στην καθημερινότητα των απλών χρηστών ηλεκτρονικών υπηρεσιών πολλές φορές και εν αγνοία του καθώς υπάρχει ένα αρκετά μεγάλο ποσοστό άτυπων εφαρμογών ηλεκτρονικής υπογραφής τόσο σε τηλεπικοινωνίες όσο και σε τραπεζικές συναλλαγές.

Σε παγκόσμιο επίπεδο, η χρήση των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών ήδη πλαισιώνει και παρέχει υψηλότερα επίπεδα ασφαλείας σε συναλλαγές διαφόρων τύπων όπως:[55]

- Υπηρεσίες ασφαλούς ταχυδρομείου (S/MIME)
- Συστήματα υπογραφής αυθεντικότητας διακινούμενου λογισμικού (π.χ. Microsoft, Authenticode)
- Ηλεκτρονικά διαβατήρια και ηλεκτρονικές ταυτότητες (γενικής ή ειδικής χρήσης)
- Ηλεκτρονικά έγγραφα και τιμολόγια
- Ηλεκτρονική ψηφοφορία
- Συστήματα ηλεκτρονικών πληρωμών
- Κλειστές υποδομές PKI για εφαρμογές ασφαλείας μεγάλων οργανισμών (π.χ. NATO)

Σε Ευρωπαϊκό Επίπεδο σημαντικός τομέας που χρησιμοποιούνται οι ηλεκτρονικές υπογραφές είναι τα ηλεκτρονικά τιμολόγια καθώς τα τυποποιημένα συστήματα EDI (Electronic Data Interchange) υποχρεώνουν τις αρχές των κρατών μελών να εκδίδουν ηλεκτρονικά τιμολόγια καθώς είναι πολύ εύκολα στη χρήση και την ανάκτηση τους. Σε αρκετά μέλη κράτη της Ευρωπαϊκής Ένωσης έχει ήδη θεσμοθετηθεί η χρήση των ηλεκτρονικών υπογραφών στις ηλεκτρονικές ταυτότητες και διαβατήρια όπου το σύστημα βασίζεται στη χρήση δύο ή τριών ζευγών κλειδιών και πιστοποιητικών τα οποία χρησιμοποιούνται στην ταυτοποίηση, στις αναγνωρισμένες ηλεκτρονικές υπογραφές και στη κρυπτογράφηση των δεδομένων. Παρόμοια λογική έχει και η Ευρωπαϊκή Κάρτα Υγείας με την οποία ο κάτοχος της θα μπορεί να έχει πρόσβαση σε όλα τα συστήματα υγειονομικής περίθαλψης των κρατών μελών.

Στην περίπτωση της Ιταλίας έχει καθοριστεί ειδικός τύπος ηλεκτρονικής υπογραφής ο οποίος χρησιμοποιείται αποκλειστικά ως μέσο επικύρωσης δημόσιων ηλεκτρονικών εγγράφων («Firme Sicure»). Η Γερμανική νομοθεσία επιτρέπει τη χρήση ενός πιο βελτιωμένου τύπου ηλεκτρονικών υπογραφών («enhanced signatures» σε σχέση με τις «αναγνωρισμένες ηλεκτρονικές υπογραφές» ο οποίος προβλέπει την υποχρεωτική χρήση χρονοσήμανσης στα υπογεγραμμένα έγγραφα ώστε να υπάρχει δυνατότητα επανεξέτασης τους μετά την λήξη του

πιστοποιητικού που υποστήριξε την ηλεκτρονική υπογραφή τους. Επίσης, στην Γαλλία υπάρχει η δυνατότητα ηλεκτρονικής κατάθεσης διαφόρων τύπων δικογράφων με τη χρήση της ηλεκτρονικής υπογραφής τους , ενώ στην Εσθονία σε συνδυασμό με την ηλεκτρονική ταυτότητα που είναι υποχρεωτική για όλους τους πολίτες έχει καθιερωθεί ένα ολόκληρο σύστημα ηλεκτρονικής ταυτοποίησης και υπογραφής εγγράφων, το λεγόμενο «DigiDoc».

Στη περίπτωση της Ελλάδας, μια από τις πρώτες εφαρμογές νομικά έγκυρης ψηφιακής υπογραφής επίσημων εγγράφων, η οποία λειτουργεί από το 2002, είναι το σύστημα ασφαλούς ηλεκτρονικής επικοινωνίας του Χρηματιστηρίου Αξιών Αθηνών (ΧΑΑ) με τις εισηγμένες σε αυτό εταιρείες. Το σύστημα αυτό που ονομάζεται ΕΡΜΗΣ (H.E.R.M.E.S- Hellenic Exchanges Remote Messaging Services) βασίζει τη λειτουργία του στις ψηφιακές υπογραφές εξουσιοδοτημένων φυσικών προσώπων στους οποίους παρέχονται δύο διαφορετικά ζευγάρια κλειδιών και πιστοποιητικών, το ένα χρησιμοποιείται για την ταυτοποίηση τους στο σύστημα και το άλλο για την αναγνωρισμένη ηλεκτρονική υπογραφή τους στις υποβαλλόμενες ηλεκτρονικά δηλώσεις τους, που τοποθετούνται σε μια προσωποποιημένη έξυπνη κάρτα. Το σύστημα ΕΡΜΗΣ επιτρέπει την αποστολή πληροφοριών μέσω ενός περιβάλλοντος που εξασφαλίζει αξιοπιστία και ακεραιότητα δεδομένων κατά τη διάρκεια μιας ηλεκτρονικής επικοινωνίας στα πλαίσια του νομικού ενδιαφέροντος που υπάρχει για τις ψηφιακές υπογραφές.

Στο μέλλον αναμένεται ραγδαία αύξηση των περιπτώσεων χρήσης της ηλεκτρονικής υπογραφής και των εφαρμογών της τόσο σε Ευρωπαϊκό όσο και σε Διεθνές επίπεδο καθώς τα οφέλη της είναι πάρα πολλά στις ηλεκτρονικές συναλλαγές και επίσης αποτελεί ένα από τα βασικότερα αν όχι το σημαντικότερο μέσο απόδειξης της γνησιότητας των ηλεκτρονικών εγγράφων.

2.3.4 Διαφορές μεταξύ ψηφιακής και Ιδιόχειρης Υπογραφής

Όπως γίνεται αντιληπτό από τα παραπάνω, η ηλεκτρονική υπογραφή αποτελεί ψηφιακό ισοδύναμο των χειρόγραφων υπογραφών. Από νομικής πλευράς, η ηλεκτρονική υπογραφή που βασίζεται σε «αναγνωρισμένο πιστοποιητικό» και δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφής»,

κατέχει θέση ιδιόχειρης υπογραφής και αποκαλείται «προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή». Σύμφωνα με την Ευρωπαϊκή Οδηγία αλλά και με το σχετικό Ελληνικό προεδρικό διάταγμα 150/2001 (άρθρο 3) η ηλεκτρονική υπογραφή εξομοιώνεται με την ιδιόχειρη.

Παρά τη νομική εξομοίωση της προηγμένης ηλεκτρονικής υπογραφής με την ιδιόχειρη υπάρχουν μεταξύ τους κάποιες βασικές διαφορές κυρίως ως προς τη χρήση και τη λειτουργία τους. Σε αντιδιαστολή με την ιδιόχειρη υπογραφή η οποία είναι ενσωματωμένη στο μήνυμα και είναι εύκολα ορατή, η ηλεκτρονική υπογραφή δεν προσαρτάται φυσικά στο μήνυμα που υπογράφεται και απαιτεί ειδικό λογισμικό για να δημιουργηθεί και κατά συνέπεια να είναι ορατή. Επιπλέον, μια σημαντική παράμετρος που πρέπει να ληφθεί υπόψιν είναι ο σκοπός χρήσης των υπογραφών καθώς στην περίπτωση της ιδιόχειρης υπογραφής δεν είναι αναγκαία η μεταβολή της ανάλογα με το σκοπό που χρησιμοποιείται όπως συμβαίνει στη περίπτωση της ηλεκτρονικής υπογραφής.

Ακόμη ένα ζήτημα που προκύπτει είναι το ζήτημα της επαλήθευσης. Η χειρόγραφη υπογραφή, δηλαδή η γραφή του ονόματος και του επωνύμου με το χέρι, παρουσιάζει τα χαρακτηριστικά που εξατομικεύουν τη γραφή του εκδότη και ο γραφικός χαρακτήρας αποτελεί ασφαλή ένδειξη για το πρόσωπο το οποίο έχει υπογράψει ένα έγγραφο και έτσι η διαδικασία επαλήθευσης γίνεται με τη σύγκριση της με άλλες αυθεντικές υπογραφές. Από την άλλη πλευρά, οι ηλεκτρονικές υπογραφές μπορούν να επαληθευτούν χρησιμοποιώντας έναν δημόσιο γνωστό αλγόριθμο επαλήθευσης με κίνδυνο να μπορεί ο οποιοσδήποτε να επαληθεύσει μια ηλεκτρονική υπογραφή.

Τέλος, μια ακόμη ουσιαστική διαφορά μεταξύ των δύο υπογραφών είναι η προστασία που προσφέρουν στα ψηφιακά δεδομένα. Σε αντίθεση με την ιδιόχειρη η ηλεκτρονική υπογραφή παρέχει ισχυρό μηχανισμό προστασίας καθώς είναι πολύ δύσκολη έως αδύνατη η πλαστογράφηση της ενώ παράλληλα είναι σε θέση να πιστοποιήσει τόσο τη γνησιότητα του εγγράφου όσο και την ταυτότητα του αποστολέα.

ΜΕΡΟΣ ΤΡΙΤΟ

3.1 Νομικό πλαίσιο για τις Ηλεκτρονικές Υπογραφές

3.1.1 Νομικό πλαίσιο σε Διεθνές Επίπεδο

Η ανάγκη για κατοχύρωση της ασφάλειας των συναλλασσόμενων κατά τη διάρκεια μιας ηλεκτρονικής συναλλαγής μέσω διαδικτύου, οδήγησε στη θέσπιση ενός νέου νομοθετικού πλαισίου σε παγκόσμιο επίπεδο. Η πρώτη θεσμική αναγνώριση των ηλεκτρονικών υπογραφών παγκοσμίως έγινε με νομοθέτημα της Αμερικανικής Πολιτείας της Utah το 1995 οι οποίοι θέσπισαν ότι η γνησιότητα της ψηφιακής υπογραφής μπορεί να αποδειχθεί έμμεσα, καθιερώνοντας νόμιμο τεκμήριο την αποκρυπτογράφηση ενός μηνύματος με την χρησιμοποίηση του δημοσίου κλειδιού, όπως αυτή είναι καταχωρημένη στο πιστοποιητικό και η οποία θα βεβαιώνει την αντιστοιχία του συγκεκριμένου δημοσίου κλειδιού με τον συνδρομητή και συγχρόνως αποστολέα του μηνύματος θεωρώντας ως αναγνώριση της ψηφιακής υπογραφής. Έκτοτε άρχισαν να εκδίδονται ανάλογοι νόμοι και σε άλλες Πολιτείες των ΗΠΑ αλλά και σε άλλα κράτη του κόσμου, όπως η Μαλαισία και η Σιγκαπούρη.

Στον Ευρωπαϊκό χώρο, ο πρώτος σχετικός νόμος περί θεσμοθέτησης της χρήσης ψηφιακών υπογραφών και όχι γενικά περί ηλεκτρονικής υπογραφής ψηφίστηκε στην Ιταλία το 1997 και παρείχε πλήρη νομική αναγνώριση σε ηλεκτρονικές πράξεις , δεδομένα και έγγραφα, ιδιωτικά και δημόσια καθώς και αρχειοθέτηση, διαβίβαση και αναπαραγωγής τους με ηλεκτρονικά μέσα και μάλιστα όχι μόνο στις συναλλακτικές σχέσεις μεταξύ ιδιωτών αλλά και στις σχέσεις πολιτών με τις δημόσιες αρχές. Ακόμη, σύμφωνα με τον νόμο αυτό ήταν δυνατή η έκδοση πιστοποιητικών με σκοπό την επιβεβαίωση της ταυτότητας των ηλεκτρονικά συναλλασσόμενων. Στη συνέχεια ακολούθησαν η Γαλλία και η Γερμανία οι οποίες έκαναν ικανοποιητικές νομοθετικές προσπάθειες το 1996 και το 1997 αντίστοιχα, προσθέτοντας μερικές διατάξεις, διατηρώντας όμως την

ιδιόχειρη υπογραφή του αστικού Δικαίου ως μεγαλύτερης σημασίας σε σχέση με την ψηφιακή υπογραφή.[56]

Οι παραπάνω πρωτοβουλίες σε Ιταλία, Γερμανία, Γαλλία ήταν οι πρώτες στον ευρωπαϊκό χώρο όσον αφορά τις ηλεκτρονικές υπογραφές. Εκείνη την περίοδο (1996-1998) τα περισσότερα κράτη ανά τον κόσμο δεν είχαν νομοθεσία σχετικά με την ηλεκτρονική υπογραφή , ενώ ακόμη και αυτά που είχαν έπρεπε να αντιμετωπίσουν το πρόβλημα της μεταξύ τους νομοθετικής ανομοιομορφίας.

Με βάση τα παραπάνω, συμπεραίνεται ότι δεν υπάρχει ένας κοινός συντονισμός ανάμεσα στα κράτη για ένα κοινό πεδίο νομοθετικής θέσπισης των ηλεκτρονικών υπογραφών. Αυτό έχει ως αποτέλεσμα η νομική ισχύς της ηλεκτρονικής υπογραφής να διαφέρει από κράτος σε κράτος, με άμεση συνέπεια να υπάρχουν διαφορετικές απαιτήσεις σε σχέση με τον τύπο του ηλεκτρονικού υπογεγραμμένου εγγράφου. Συνεπώς, είναι επιτακτική ανάγκη η θέσπιση «κοινών κανόνων» τόσο από τεχνολογική όσο και από νομική άποψη ώστε να επιτευχθεί σταδιακά μια «διαλειτουργικότητα» στην δημιουργία, στην χρήση αλλά και στην αναγνώριση των ηλεκτρονικών υπογραφών σε κοινοτικό επίπεδο.

Για το λόγο αυτό η Ευρωπαϊκή Επιτροπή πρότεινε την συγκεκριμένη οδηγία «σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές» η οποία εγκρίθηκε και ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις 13 Δεκεμβρίου του 1999 (Επίσημη Εφημερίδα Ε.Ε. αριθ. L 013 της 19/01/2000 σ. 0012-0020). Πιο συγκεκριμένα, το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο Υπουργών αρμόδιων για θέματα τηλεπικοινωνιών υιοθέτησαν στις 13 Δεκεμβρίου 1999 την οδηγία 1999/93/ΕΚ , σε στόχο και σκοπό να δημιουργήσουν ένα σαφές κοινοτικό νομικό πλαίσιο σχετικά με τις ηλεκτρονικές υπογραφές, το οποίο θα ενισχύσει την εμπιστοσύνη στις νέες τεχνολογίες και θα συμβάλει στη γενική αποδοχή τους.

Η Ελλάδα ενσωμάτωσε στο εθνικό της δίκαιο την οδηγία 1999/93 με το προεδρικό διάταγμα 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές».

3.1.2 Νομοθετικές προσεγγίσεις της τεχνολογίας των ηλεκτρονικών υπογραφών

Η νομοθεσία περί ηλεκτρονικών υπογραφών ανήκει αναμφίβολα σε αυτές που περιέχουν πολλούς και δύσκολους τεχνικούς όρους, οι οποίοι έγιναν αντικείμενο νομοθετικής επεξεργασίας μόλις τα τελευταία χρόνια. Στις μέρες μας ο τρόπος που γίνεται η νομοθετική προσέγγιση της τεχνολογίας των ηλεκτρονικών υπογραφών χωρίζεται διεθνώς σε δύο κατηγορίες: Στην τεχνολογικά ουδέτερη (technology-neutral) προσέγγιση και στην τεχνολογικά εξειδικευμένη (technology-specific) προσέγγιση.[57]

Με τον όρο τεχνολογικά ουδέτερη νομοθεσία αντιλαμβανόμαστε ότι πρέπει να είναι προσανατολισμένη τεχνολογικά προς το μέλλον, να προνοεί δηλαδή για τη χρήση ηλεκτρονικών υπογραφών με διαφορετικά μεταξύ τους τεχνικά χαρακτηριστικά που δεν έχουν έως σήμερα εφευρεθεί. Σε μια νομοθεσία σαν και αυτήν πρέπει να προβλεφθούν οι συγκεκριμένες νομικές συνέπειες της χρήσης των ηλεκτρονικών υπογραφών, για τις οποίες σημαντικό θετικό στοιχείο είναι η προσαρμοστικότητα της νομοθεσίας στις προκλήσεις των καιρών και σε κάθε νέα τεχνολογική καινοτομία. Σε περίπτωση τροποποίησης της νομοθεσίας στο μέλλον περί ηλεκτρονικών υπογραφών, η τροποποίηση μιας τεχνολογικά ουδέτερης νομοθεσίας είναι σαφώς πιο εύκολη από αυτή της εξειδικευμένης νομοθεσίας, η οποία θα έχει ήδη δημιουργήσει ισχυρό προηγούμενο στη νομολογία και τις συναλλαγές.

Από την άλλη πλευρά, η τεχνολογικά εξειδικευμένη νομοθεσία για τις ηλεκτρονικές υπογραφές επικεντρώνεται αποκλειστικά στην τεχνολογία που υπάρχει διαθέσιμη στην αγορά προς το παρόν, ενώ είναι στενά προσκολλημένη στις τεχνικές ορολογίες του σήμερα. Με τον τρόπο αυτό, ο νομοθέτης προσπαθεί να δώσει έμφαση στην ασφάλεια , στην βεβαιότητα και στην αξιοπιστία των ήδη γνωστών και δοκιμασμένων στο εμπόριο τεχνολογιών, θωρακίζοντας με νομική ισχύ μόνο αυτές, με τη σκέψη ότι δεν είναι δυνατόν να αναγνωρίσει νομικά άγνωστης τεχνολογίας ηλεκτρονικές υπογραφές, που δεν έχουν δοκιμαστεί στη πράξη και δεν έχουν γίνει αποδεκτές ακόμη στην αγορά. Όμως η εξειδικευμένη τεχνολογικά νομοθεσία χρειάζεται συνεχή τροποποίηση και προσαρμογή στα νέα τεχνολογικά δεδομένα.

Η επιλογή της Ευρωπαϊκής Επιτροπής και του Συμβουλίου Υπουργών να υιοθετήσουν νομοθετική διατύπωση τεχνολογικά ουδέτερη και ευέλικτη, με δεδομένη την αλματώδη ανάπτυξη και τεχνολογική πρόοδο που αναμένεται να γνωρίσουν οι ηλεκτρονικές υπογραφές τα επόμενα χρόνια, κάτι που άλλωστε αναγνωρίζεται και στην αιτιολογική σκέψη του προοιμίου της οδηγίας 1999/93: «η ταχεία τεχνολογική ανάπτυξη και ο παγκόσμιος χαρακτήρας του διαδικτύου επιβάλλουν προσέγγιση που θα είναι ανοιχτή σε διάφορες τεχνολογίες και υπηρεσίες ηλεκτρονικής αναγνώρισης της γνησιότητας δεδομένων». Εξάλλου, η επιλογή μιας τεχνολογικά εξειδικευμένης νομοθεσίας θα σήμαινε διαρκή ανάγκη τροποποίησης της οδηγίας 1999/93, κάτι εξ ορισμού πολύ δύσκολο για μια ένωση διαρκώς αυξανόμενου αριθμού κρατών.

[57]Είναι αξιοσημείωτο, ότι η τεχνολογικά ουδέτερη προσέγγιση της οδηγίας 1999/93 είναι αντίθετη με την ιταλική και τη γερμανική νομοθεσία που ίσχυαν πριν την υιοθέτηση της οδηγίας 1999/93 από την ΕΕ. Η υιοθέτηση της οδηγίας 1999/93 σήμανε την τροποποίηση των δύο αυτών πρωτοποριακών νομοθεσιών, οι οποίες, ωστόσο, θα μπορούσαν να διατηρηθούν, αν θεωρούνταν ως ειδικοί κανόνες δικαίου σε σχέση με το γενικό κανόνα δικαίου περί ηλεκτρονικών υπογραφών που εισάγει η οδηγία 1999/93. Βλ. *Julià-Barcelo*/*Vinje*, «Electronic Signatures, another step towards a European framework for electronic signatures: the Commission's Directive proposal», CL&SR 14 (5) 1998, σελ. 303.

3.1.3 Η νομική αναγνώριση των ηλεκτρονικών υπογραφών – «Μινιμαλιστική» και «Μαξιμαλιστική» προσέγγιση

Σε διεθνές επίπεδο δημιουργήθηκε ένα σημαντικό θέμα που έπρεπε να διευθετηθεί σχετικά με το θεσμικό πλαίσιο και τη «νομική αναγνώριση» των ηλεκτρονικών υπογραφών, έτσι ώστε να είναι νομικά ισότιμες με τις ιδιόχειρες όλες οι ηλεκτρονικές υπογραφές, ανεξαρτήτως των τεχνολογικών προτύπων στα οποία θα βασίζονταν. Το ζήτημα που θα έχει η νομική αναγνώριση των ηλεκτρονικών υπογραφών είναι πολύ σημαντικό και έχει απασχολήσει αρκετά τα τελευταία χρόνια. Στο Ευρωπαϊκό Δίκαιο και κατ' επέκταση και στο Εθνικό ακολουθείται μια μικτή προσέγγιση στο θέμα της νομικής αναγνώρισης των ηλεκτρονικών υπογραφών, δηλαδή την προσέγγιση των δύο επιπέδων, η οποία διακρίνεται σε δύο διαφορετικές νομικές προσεγγίσεις: α) την «μινιμαλιστική»[58] και β) την «μαξιμαλιστική».

Στο πρώτο επίπεδο ακολουθείται η «μινιμαλιστική» προσέγγιση κατά την οποία παρέχεται πλήρης και χωρίς όρους νομική αναγνώριση σε όλες τις ηλεκτρονικές υπογραφές, ανεξάρτητα από τις τεχνολογικές προδιαγραφές. Η νομική εξίσωση των ηλεκτρονικών υπογραφών με τις ιδιόχειρες, λόγω της τεχνολογικής ουδετερότητας που επιτυγχάνει, ενθαρρύνει τους καταναλωτές να χρησιμοποιήσουν ηλεκτρονικές υπογραφές, καθώς γνωρίζουν εκ των προτέρων ότι, όποιων τεχνικών προδιαγραφών ηλεκτρονική υπογραφή κι αν χρησιμοποιήσουν, αυτή θα παράγει πλήρη αποτελέσματα, όπως και η ιδιόχειρη υπογραφή.

Η προσέγγιση αυτή είναι πολύ σημαντική στον τεχνολογικό τομέα καθώς ευνοεί την ανάπτυξη νέων τεχνολογιών ηλεκτρονικής υπογραφής. Αυτό συμβαίνει επειδή δεν προκρίνει κάποια συγκεκριμένη υπάρχουσα τεχνολογία με αποτέλεσμα να ενισχύει την ομοιόμορφη σε διεθνές επίπεδο νομοθετική αντιμετώπιση της ηλεκτρονικής υπογραφής, παρακάμπτοντας τα εμπόδια που θα δημιουργούσε η πρόκριση κάποιας συγκεκριμένης τεχνολογίας από χώρα σε χώρα.

[58]Η μινιμαλιστική προσέγγιση γενικά προτιμάται περισσότερο σε χώρες των οποίων τα δικαιϊκά συστήματα βασίζονται στο αστικό εθιμικό δίκαιο (common law) ή στη νομολογία (case law), όπως π.χ.η Μεγάλη Βρετανία, οι ΗΠΑ ή η Αυστραλία. Αυτό, γιατί στα συστήματα αυτά τα αποδεικτικά στοιχεία παίζουν πολύ πιο σημαντικό ρόλο από τη συγκεκριμένη μορφή που έχει μια ηλεκτρονική υπογραφή προκειμένου να διαπιστωθεί ποια η πρόθεση του συμβαλλομένου όταν υπογράφει. Η έμφαση, δηλαδή, δίδεται στην καταλληλότητα ή μη της μεθόδου ηλεκτρονικής υπογραφής που χρησιμοποιεί ο υπογράφων για να δηλώσει την πρόθεσή του, επομένως, ανάλογα με το είδος της συναλλαγής, μπορεί να αποδεικνύεται ότι ο υπογράφων χρησιμοποιεί ως ιδιόχειρη υπογραφή ακόμη και μια απλή τεχνολογικά ηλεκτρονική υπογραφή. Βλέπε *Mason*, «The international implications of using electronic signatures», CTLR (5) 2005, σελ. 161, *Lincoln*, ό.π., σσ. 77 – 78, *Barofsky*, «The European Commission's Directive on electronic signatures: technological "favoritism" towards digital signatures», BCI&CLR (4) 2000, σσ. 156 – 157, *Koger*, «You sign, E-sign, we all fall down: why the United States should not crown the marketplace as primary legislator of electronic signatures», TL&CP

Κάποια μειονεκτήματα της προσέγγισης αυτής είναι ότι δεν υπάρχει σαφής ορισμός ενός συγκεκριμένου είδους ηλεκτρονικής υπογραφής, η οποία θα δεσμεύει τον υπογράφοντα όπως η χειρόγραφη υπογραφή με αποτέλεσμα να καθιστά κάθε μέθοδο ηλεκτρονικής υπογραφής από την πιο απλή μέχρι την πιο περίπλοκη αρκετά δεσμευτική. Αυτή η εξίσωση «προς τα κάτω» του επιπέδου των ηλεκτρονικών υπογραφών μπορεί να αποβεί σε βάρος του υπογράφοντα, γιατί ενδέχεται να βρεθεί δεσμευμένος ακόμη κι αν δεν έχει τέτοια πρόθεση. Το σημαντικότερο όμως μειονέκτημα είναι ο κίνδυνος τεχνολογικά επισφαλών

ηλεκτρονικών υπογραφών καθώς ορίζονται βάσει υψηλών τεχνικών στάνταρ, με αποτέλεσμα να δημιουργείται ο κίνδυνος εξαπάτησης των καταναλωτών από επιτήδειους που εμπορεύονται ελαττωματικής τεχνολογίας ηλεκτρονικές υπογραφές.

Αντιθέτως, στο δεύτερο επίπεδο, η «μαξιμαλιστική»[59] προσέγγιση είναι νομικά πιο περίπλοκη , δηλαδή σύμφωνα με την προσέγγιση αυτή «μόνο συγκεκριμένες τεχνολογικοί μέθοδοι, οι οποίες ικανοποιούν συγκεκριμένα κριτήρια ασφαλείας και αξιοπιστίας, αναγνωρίζονται άμεσα ως νομικά ισότιμες με τις ιδιόχειρες υπογραφές». Η συγκεκριμένη προσέγγιση προσδίδει έννομα αποτελέσματα μόνο σε ορισμένα είδη ηλεκτρονικών υπογραφών ανάλογα με το αν αυτές συμμορφώνονται ή όχι σε συγκεκριμένα τεχνικά πρότυπα. Η νομοθετική αυτή προσέγγιση προσδίδει ειδικά νομικά προνόμια μόνο σε εγκεκριμένες ηλεκτρονικές υπογραφές. Συνήθως αυτό το ειδικό προνόμιο είναι η πλήρης νομική εξίσωση αυτών των ηλεκτρονικών υπογραφών με τις ιδιόχειρες. Παρότι αυτή η προσέγγιση είναι κατά κάποιο τρόπο τροχοπέδη στην ελεύθερη ανάπτυξη της αγοράς των ηλεκτρονικών υπογραφών υπάρχει το θετικό στοιχείο ότι η προσέγγιση αυτή προστατεύει τον καταναλωτή από αναξιόπιστες τεχνολογικές εφαρμογές της ηλεκτρονικής υπογραφής που διατίθενται στην αγορά.

[59]Ημαξιμαλιστική προσέγγιση, λόγωακριβώς του γεγονότος ότι είναι πιο περίπλοκη νομικά και τεχνολογικά από τη μινιμαλιστική, έχει προτιμηθεί περισσότερο σε χώρες των οποίων τα διοικητικά συστήματα διέπονται από νόμους με περισσότερο λεπτομερειακές από τεχνική άποψη ρυθμίσεις, όπως είναι τα συστήματα πολλών χωρών της ηπειρωτικής Ευρώπης. Τέτοιοι ήταν και οι πρώτοι νόμοι περί ψηφιακής υπογραφής που ψηφίστηκαν το 1996 και 1997 σε Ιταλία, Γερμανία και Γαλλία, όπως αναλύθηκε παραπάνω

3.2 Το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές στην Ελλάδα

3.2.1 Το προεδρικό διάταγμα 150/2001 και η Οδηγία 1999/93/ΕΚ

Στην Ελλάδα η πρώτη προσπάθεια ρύθμισης ζητημάτων ψηφιακής υπογραφής (η οποία ταυτίζεται εννοιολογικά με τις προηγμένες ηλεκτρονικές υπογραφές) και συναφών υπηρεσιών πιστοποίησης έγινε με το άρθρο 14 του νόμου 2672/1998 με τίτλο «Διακίνηση εγγράφων με ηλεκτρονικά μέσα» βάσει του οποίου τέθηκαν οι πρώτες βάσεις για την χρήση των ηλεκτρονικών υπογραφών στην ελληνική δημόσια Διοίκηση.

Ακολούθησε το προεδρικό διάταγμα 150/2001 (ΦΕΚ Α'/125 25-6-2001) το οποίο έθεσε τα θεμέλια για τη συμμόρφωση και προσαρμογή της ελληνικής νομοθεσίας σχετικά με την «χρήση της ηλεκτρονικής υπογραφής και την νομική αναγνώριση της». Σύμφωνα με το προεδρικό διάταγμα 150/2001 αναγνωρίζονται οι τεχνολογίες ηλεκτρονικής υπογραφής και ρυθμίζεται η παροχή υπηρεσιών πιστοποίησης ηλεκτρονικών εγγραφών. Η ρύθμιση τους μπορεί να γίνει με σχετική διάταξη βάσει της οποίας επαληθεύεται ή γίνεται έλεγχος εγκυρότητας του αναγνωρισμένου πιστοποιητικού μέσω της δυνατότητας πρόσβασης (είτε μέσω off-line ενημερώσεων είτε με on-line σύνδεση) σε επικαιροποιημένες πληροφορίες εγκυρότητας ή και ανάκλησης πιστοποιητικών από τον ΠΥΠ.

Στην Οδηγία 1999/93/ΕΚ ρυθμίζεται και η παροχή υπηρεσιών πιστοποίησης την οποία απαρέχουν κατ' αποκλειστικότητα οι Πάροχοι Υπηρεσιών Πιστοποίησης (ΠΥΠ) οι οποίοι εκδίδουν πιστοποιητικά ή άλλες υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές προς το κοινό. Επιπλέον οι ιδιαίτερες ευθύνες που αναλαμβάνει εκ του νόμου ο ΠΥΠ είναι :[60]

- Η ακρίβεια των στοιχείων που αναφέρονται στο πιστοποιημένο αναγνωριστικό και η πληρότητά τους
- Την διαβεβαίωση ότι ο υπογράφων που ταυτοποιείται στο αναγνωρισμένο πιστοποιητικό είναι και ο κάτοχος του (τουλάχιστον μέχρι εκείνη τη στιγμή) των δεδομένων δημιουργίας υπογραφής, τα ιδιωτικό κλειδί , που αντιστοιχούν στα δεδομένα επαλήθευσης, δημόσιο κλειδί
- Την διαβεβαίωση ότι τα ιδιωτικό κλειδί του συνδρομητή που παράγει ο ΠΥΠ μπορεί να χρησιμοποιηθεί 'συμπληρωματικά' με το δημόσιο κλειδί του σχετικού πιστοποιητικού που του εκδίδει

Βάσει της Οδηγίας προσδιορίζονται ακόμη και τα περιεχόμενα των αναγνωρισμένων πιστοποιητικών που εκδίδει ο ΠΥΠ τα οποία πρέπει να περιλαμβάνουν τουλάχιστον τα εξής στοιχεία:

- Ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό
- Τα στοιχεία αναγνώρισης του παρόχου υπηρεσιών πιστοποίησης και το κράτος στο οποίο ανήκει
- Το όνομα του υπογράφοντος ή το ψευδώνυμο με το οποίο υπογράφει
- Πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, το οποίο περιλαμβάνεται μόνο αν σημαντικό σε σχέση με το σκοπό για τον οποίο προορίζεται το πιστοποιητικό
- Δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής
- Ένδειξη της αρχής και του τέλους της περιόδου ισχύος του πιστοποιητικού
- Τον κωδικό ταυτοποίησης του πιστοποιητικού
- Την προηγμένη ηλεκτρονική υπογραφή του ΠΥΠ που την εκδίδει
- Τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού
- Τυχόν όρια στο ύψος των συναλλαγών για τις οποίες μπορεί να χρησιμοποιηθεί το πιστοποιητικό

Ακόμη, ως προς τις αρμοδιότητες της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) θα είναι υπεύθυνη για την εποπτεία των ΠΥΠ οι οποίοι θα πρέπει να συμμορφώνονται με τους όρους της απόφασης του ΕΕΤΤ, ενώ θα πρέπει να αποδεικνύουν αξιοπιστία για τη παροχή υπηρεσιών πιστοποίησης. Επιπλέον, η συγκέντρωση προσωπικών στοιχείων από τους ΠΥΠ θα γίνεται μόνο από το ενδιαφερόμενο πρόσωπο ή μόνο με ρητή συγκατάθεση του. Σε περιπτώσεις χρήσης των προσωπικών δεδομένων του ατόμου για διαφορετικούς σκοπούς θα απαιτείται η σύμφωνη γνώμη του ενδιαφερομένου προσώπου.

3.2.2 Νομοθετικοί ορισμοί για τις απλές και τις προηγμένες ηλεκτρονικές υπογραφές

Το προεδρικό διάταγμα 150/2001 (άρθρο 2 παρ. 4) ορίζει με απόλυτη σαφήνεια την «απλή ηλεκτρονική υπογραφή» ως τα δεδομένα τα οποία βρίσκονται σε ηλεκτρονική μορφή και είναι συνημμένα με άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με αυτά και χρησιμεύουν ως μέθοδος απόδειξης γνησιότητας.

Από τον ορισμό αυτό γίνεται αντιληπτό ότι οι τεχνικές κρυπτογράφησης οι οποίες βοηθούν στην κρυπτογράφηση ολόκληρου ή ενός μέρους του ηλεκτρονικού εγγράφου εμπίπτουν στον ορισμό της ηλεκτρονικής υπογραφής. Για το σκοπό αυτό ορίζονται ως δεδομένα επαλήθευσης υπογραφής κλειδιά κρυπτογραφίας και κατάλληλο λογισμικό τα οποία είναι γνωστά ως διάταξη δημιουργίας υπογραφής (άρθρο 2 αριθμός 5).

Αντίστοιχα, ως «προηγμένη ηλεκτρονική υπογραφή» ή «ψηφιακή υπογραφή» σύμφωνα με το προεδρικό διάταγμα ορίζεται η υπογραφή η οποία:[61]

- Συνδέεται μονοσήμαντα με τον υπογράφοντα
- Καθορίζει αποκλειστικά και ειδικά την ταυτότητα του υπογράφοντα
- Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο
- Συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε να μπορεί να εντοπισθεί οποιαδήποτε αλλοίωση των δεδομένων

Η προηγμένη ηλεκτρονική υπογραφή πρέπει να βασίζεται σε «αναγνωρισμένο πιστοποιητικό» και να δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφής» χαρακτηριστικά τα οποία θα αναλυθούν λεπτομερώς στη συνέχεια.

3.2.3 Η νομική προσέγγιση της προηγμένης ηλεκτρονικής υπογραφής

Όπως έχει ήδη αναλυθεί , σύμφωνα με το άρθρο 3 του προεδρικού διατάγματος 150/2001 (αντίστοιχο άρθρο 5 παρ. 1 της Οδηγίας 1999/93), η προηγμένη ηλεκτρονική υπογραφή μπορεί να είναι ισότιμη με την ιδιόχειρη υπογραφή, τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, μόνο όμως όταν πληροί δύο συγκεκριμένες τεχνικές προϋποθέσεις, δηλαδή α) βασίζεται σε «αναγνωρισμένο πιστοποιητικό» και β) δημιουργείται από «ασφαλή διάταξη δημιουργίας υπογραφής».

Βάσει της πρώτης προϋπόθεσης, η προηγμένη ηλεκτρονική υπογραφή προκειμένου να είναι ικανή να εξομοιωθεί με μια χειρόγραφη υπογραφή απαραίτητη προϋπόθεση είναι να βασίζεται σε «αναγνωρισμένο πιστοποιητικό», όπου ως πιστοποιητικό αναγνωρίζεται μια ηλεκτρονική βεβαίωση η οποία χορηγείται από τον ΓΥΠ και συνδέει μονοσήμαντα τα δεδομένα επαλήθευσης μιας υπογραφής ή δημόσιο κλειδί με ένα άτομο επιβεβαιώνοντας την ταυτότητα του, ενώ σύμφωνα με το άρθρο 2 «αναγνωρισμένο πιστοποιητικό» είναι ένα πιστοποιητικό που περιλαμβάνει : α) ένδειξη ότι εκδίδεται ως αναγνωρισμένο πιστοποιητικό, β) τα στοιχεία του ΓΥΠ και το κράτος, στο οποίο είναι εγκατεστημένος, γ) το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, δ) πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί εφόσον είναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, ε) δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος, στ) ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, ζ) τον κωδικό ταυτοποίησης του πιστοποιητικού, η) την προηγμένη ηλεκτρονική υπογραφή του ΓΥΠ που το εκδίδει , θ) τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού και ι) τυχόν όρια στο ύψος των συναλλαγών για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί .[62]

Όσον αφορά την δεύτερη προϋπόθεση που πρέπει να πληροί μια προηγμένη ηλεκτρονική μορφή το άρθρο 2 του προεδρικού διατάγματος 150/2001 ορίζει ότι «διάταξη δημιουργίας υπογραφής» είναι το διατεταγμένο υλικό ή λογισμικό που χρησιμοποιείται για την εφαρμογή των «δεδομένων δημιουργίας της υπογραφής», δηλαδή των δεδομένων, όπως κώδικες ή ιδιωτικά κλειδιά

κρυπτογραφίας, που χρησιμοποιούνται από τον υπογράφοντα για τη δημιουργία ηλεκτρονικής υπογραφής ενώ σύμφωνα με το άρθρο 2, «ασφαλής διάταξη δημιουργίας υπογραφής» είναι η διάταξη δημιουργίας υπογραφής που πληροί τους όρους που αναλύονται παρακάτω:

- Τα κρυπτογραφικά κλειδιά πρέπει να δημιουργούνται με τους κατάλληλους αλγορίθμους δημιουργίας τυχαίων αριθμών, είτε μέσω της συσκευής του χρήστη, είτε από κατάλληλες κρυπτογραφικές μονάδες του ΠΥΠ όπου μεταφέρουν άμεσα τα ιδιωτικά κλειδιά σε προσωπικές συσκευές του χρήστη
- Η υπογραφή προστατεύεται από πλαστογραφία με τα μέσα της σύγχρονης τεχνολογίας, δηλαδή απαγορεύει τη διατήρηση αντιγράφου του ιδιωτικού κλειδιού και στην ουσία επιβάλλει τη χρήση ασύμμετρης κρυπτογραφίας
- Τα ιδιωτικά κλειδιά δεν μπορούν να αντιγραφούν από τον φορέα τους , ούτε να ενεργοποιηθούν χωρίς τη χρήση επιβεβαίωσης της ταυτότητας του χρήστη

Συνεπώς, από τα παραπάνω γίνεται σαφές ότι η προηγμένη ηλεκτρονική υπογραφή που βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής έχει την ίδια αποδεικτική δύναμη με την ιδιόχειρη υπογραφή. Κατ' αντιστοιχία, όλα τα ηλεκτρονικά έγγραφα που φέρουν προηγμένη ηλεκτρονική υπογραφή η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται βάσει ασφαλούς διάταξης δημιουργίας υπογραφής εξομοιώνονται με τα παραδοσιακά υπογεγραμμένα ιδιωτικά έγγραφα. Με βάση τα παραπάνω αναγνωρίζεται ότι η προηγμένη ηλεκτρονική υπογραφή παρέχει υψηλό επίπεδο ασφαλείας και μπορεί να αντικαταστήσει την ιδιόχειρη υπογραφή.

3.2.4 Νομική αναγνώριση όλων των ηλεκτρονικών υπογραφών

Σύμφωνα με το άρθρο 3 του προεδρικό διάταγμα 150/2001 όταν η ηλεκτρονική υπογραφή δεν είναι προηγμένη ή δεν βασίζεται σε κάποιο

αναγνωρισμένο πιστοποιητικό ή δεν δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής τότε δεν εξομοιώνονται ως ισότιμες με τις ιδιόχειρες υπογραφές παρόλο που έχουν νομική ισχύ.

Για την νομική ισχύ μιας ηλεκτρονικής υπογραφής όπως αναφέρεται στο άρθρο 3 του προεδρικού διατάγματος 150/2001 δεν απαιτείται αναγκαία και ικανή συνθήκη η κατοχή ενός αναγνωρισμένου πιστοποιητικού που εκδίδεται από τον ΓΜΠούτε από την ασφαλή διάταξη δημιουργίας υπογραφής. Συνεπώς μια απλή ηλεκτρονική υπογραφή δεν είναι αναγκαίο να πληροί συγκεκριμένες τεχνικές προϋποθέσεις για να έχει νομική αναγνώριση.

Όσον αφορά τα ηλεκτρονικά έγγραφα τα οποία δεν έχουν κανενός είδος ηλεκτρονικής υπογραφής, η γνησιότητα τους αποδεικνύεται μέσω διδαγμάτων των κοινής πείρας κατά την εφαρμογή της μεθόδου της έμμεσης διατεκμηρίωσης απόδειξης (άρθρο 36).

3.3 Κατηγορίες νομικά αναγνωρισμένων ηλεκτρονικών υπογραφών

Ανακεφαλαιώνοντας, υπάρχουν τεσσάρων ειδών κατηγορίες ηλεκτρονικών υπογραφών που έχουν κατοχυρωθεί νομικά από το προεδρικό διάταγμα 150/2001 και οι οποίες περιγράφονται παρακάτω: [63]

- Απλές ηλεκτρονικές υπογραφές: στις οποίες ανήκουν κάθε μορφής ηλεκτρονικά δεδομένα τα οποία σχετίζονται με άλλα ηλεκτρονικά δεδομένα ώστε να αποτελούν μέθοδο απόδειξης της γνησιότητας τους
- Προηγμένες ηλεκτρονικές υπογραφές: στην κατηγορία αυτή ανήκουν οι ηλεκτρονικές υπογραφές οι οποίες έχουν συγκεκριμένες ιδιότητες οι οποίες αναλύθηκαν παραπάνω και στην οποία κατηγορία ανήκουν οι ψηφιακές υπογραφές εξαιτίας της ασύμμετρης κρυπτογραφίας με δημόσιο και ιδιωτικό κλειδί
- Προηγμένες ηλεκτρονικές υπογραφές που είναι αναγνωρισμένες ως ισότιμες με τις ιδιόχειρες: η κύρια διαφορά τους από τις προηγμένες ηλεκτρονικές υπογραφές έγκειται στο γεγονός ότι χρειάζονται κάποιοι πρόσθετοι όροι για τη δημιουργία τους όπως α) η υποστήριξη τους

από αναγνωρισμένο πιστοποιητικό, β) η χρήση ασφαλούς διάταξης δημιουργίας υπογραφής

- Προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε αναγνωρισμένο πιστοποιητικό (αλλά δεν παράγονται με «ασφαλή διάταξη δημιουργίας υπογραφής» όπως απαιτείται για τις ηλεκτρονικές υπογραφές που είναι ισότιμες με τις ιδιόχειρες: για τη συγκεκριμένη υποκατηγορία αξίζει να αναφέρουμε ότι στόχο έχει το υψηλό επίπεδο ασφαλείας και αξιοπιστίας που έχουν τη δυνατότητα να παρέχουν στο καταναλωτικό κοινό οι ΠΥΠ

Ως προς τα συγκεκριμένα είδη ηλεκτρονικών υπογραφών έχουν ασκηθεί αυστηρές κριτικές καθώς θεωρούνται από πολλούς ένα αρκετά πολύπλοκο σύστημα αναγνώρισης ηλεκτρονικών υπογραφών. Υπάρχουν όμως και αρκετοί υποστηρικτές αυτού του συστήματος καθώς θεωρούν ότι έχει δύο πολύ βασικά πλεονεκτήματα πάνω στα οποία στηρίζουν τις εξής απόψεις τους:

- Μόνο με αυστηρή προδιαγραφή και προτυτοποίηση των διαφορετικών ειδών ηλεκτρονικών πιστοποιητικών υπογραφής είναι δυνατή η διασυνοριακή αξιοπιστία των προϊόντων
- Μόνο με το συγκεκριμένο διαχωρισμό στα χρησιμοποιούμενα είδη ηλεκτρονικών πιστοποιητικών και υπογραφών μπορεί να προστατευθεί ο χρήστης-υπογράφων.

Είναι εύκολο να αντιληφθεί κανείς την ορθότητα των παραπάνω επιχειρημάτων, ωστόσο είναι βέβαιο ότι η θεσμοθέτηση των τεσσάρων ειδών ηλεκτρονικών υπογραφών θα είναι μια αρκετά περίπλοκη διαδικασία όχι μόνο για τους ΠΥΠ ,καθώς θα είναι αναγκασμένος να ανταποκρίνεται επιτυχώς στη ταυτόχρονη ζήτηση διαφορετικών ειδών ηλεκτρονικών υπογραφών, αλλά και για τους καταναλωτές και για το νομικό κόσμο. Από την πλευρά του καταναλωτή θα δυσκολεύεται στη σωστή επιλογή της ηλεκτρονικής υπογραφής που τον ενδιαφέρει. Ένα ακόμη κύριο πρόβλημα είναι το οικονομικό καθώς δεν αποτελεί ελκυστικό οικονομικό μοντέλο ούτε για τους ΠΥΠ αλλά ούτε και για τους καταναλωτές. Από την μεριά των ΠΥΠ θα χρειαστεί να δαπανηθούν μεγάλα ποσά προκειμένου να διαθέτουν υπογραφές διαφορετικής τεχνολογίας ενώ θα υπάρξει και επιπλέον οικονομική επιβάρυνση για την εκπαίδευση ενός πολυάριθμου και

εξειδικευμένου τεχνικού προσωπικού. Οι καταναλωτές αφετέρου, θα πρέπει να ανταποκριθούν στο αυξημένο κόστος των διαφορετικών ειδών ηλεκτρονικών υπογραφών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1.Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.1-2

2. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.5

3. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.4

4. Ιγγλεζάκης, « Οικονομική αξία των πληροφοριών του δημοσίου τομέα», Οδηγία 2003/98 με προοπτικές ενσωμάτωσης στο ελληνικό δίκαιο ΕΕΕυΔ 2005, σελ. 221

5. Κανελλοπούλου-Μπότση, 2004, «Δίκαιο της πληροφορίας», σελ.20-21

6. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.8

7. Κανελλοπούλου-Μπότση, 2004, «Δίκαιο της πληροφορίας», σελ.23

8. Κοτσαλής, «Προσωπικά Δεδομένα»,2016, σελ.22

9. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.41

10. Κοτσαλής, «Προσωπικά Δεδομένα»,2016, σελ.7

11. Τουντόπουλου, «Η προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιών», σελ.47

12. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.197

13. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.197

14. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.200-201

15. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.204-205

18. Κίτσος, «Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011, σελ.57-58

19. Κίτσος, «Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011, σελ.51

21. Μοσχίδου, «Ηλεκτρονικές συναλλαγές και προσωπικά δεδομένα με έμφαση στη νομική προστασία του Καταναλωτή στο διαδίκτυο (internet), 2015, σελ. 266

22. Κίτσος, «Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011, σελ.62

23. ΠΛΗΡΟΦΟΡΙΕΣ ΣΧΕΤΙΚΑ ΜΕ SPYWARE (ΛΟΓΙΣΜΙΚΑ ΚΑΤΑΣΚΟΠΕΙΑΣ) ΚΑΙ ΤΡΟΠΟΙ ΑΦΑΙΡΕΣΗΣ
http://ioys.gr/spyware-%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CE%BC%CE%B9%CE%BA%CE%AC-%CE%BA%CE%B1%CF%84%CE%B1%CF%83%CE%BA%CE%BF%CF%80%CE%B5%CE%AF%CE%B1%CF%82/

25. Κίτσος, «Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011, σελ.68

26. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.55-56

27. Κίτσος, «Το νομικό πλαίσιο προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής με έμφαση στον τομέα των ηλεκτρονικών επικοινωνιών», 2011, σελ.216

28. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.63

29. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.86-87

30. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.90

31. Αλεξανδροπούλου-Αιγυπτιάδου, « Προσωπικά Δεδομένα», 2007, σελ.107-108

32. ιστοσελίδα «www.adae.gr» για πληροφορίες σχετικά με δράσεις της ΑΔΑΕ, Κίτσος, σελ.283-284

33. Κοτσαλής , «Προσωπικά Δεδομένα», 2016,σελ.364-366

34. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.215-217

35. Ιγγλεζάκης, «Εισαγωγή στο Δίκαιο της Πληροφορικής», σελ.221

36. Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο»,2008, σελ.70

37. Σιδηρόπουλος, «Το δίκαιο της πληροφορικής», 2003

39. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

40. Κάτος, «Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης», 2003

41. Κάτος, «Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης», 2003

42. Νικλιτσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011, σελ.34-35

43. Κάτος, «Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης», 2003

44. Κάτος, «Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης», 2003

45. Κάτος, «Τεχνικές Κρυπτογραφίας και κρυπτανάλυσης», 2003

46.Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

47. *Ομάδα εργασίας Ε2 του ebusinessforum*, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά
ταυτοποίησης (τεχνική και νομική προσέγγιση)», 2004, σελ. 23, διαθέσιμο στην ηλεκτρονική
διεύθυνση http://www.ebusinessforum.gr/content/downloads/Paradoteo_E2-Teliko.doc

48. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

49. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

50. Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο»,2008

51.Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο»,2008

53. Μανιώτης, «Η ηλεκτρονική υπογραφή ως μέσο διαπιστώσεως της γνησιότητας των ηλεκτρονικών εγγράφων στο Αστικό Δικονομικό Δίκαιο»

54. Καραδημητρίου, «Η ηλεκτρονική υπογραφή ως μέσο ασφάλειας των συναλλαγών στο ηλεκτρονικό εμπόριο»,2008

55. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

56. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

60. Νικόλαος Βολακάκης ,«ΗΛΕΚΤΡΟΝΙΚΕΣ ΥΠΟΓΡΑΦΕΣ & ΗΛΕΚΤΡΟΝΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΤΑΥΤΟΠΟΙΗΣΗΣ(ΤΕΧΝΙΚΗ & ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ)»

61. Νικλητσιώτης, «Μέθοδοι δημιουργίας, εφαρμογές στις ηλεκτρονικές συναλλαγές, νομικό πλαίσιο και πιστοποίηση ηλεκτρονικής υπογραφής», 2011

62. Ομάδα Ε2, «Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά Ταυτοποίησης»

63. Σιούλης,«Η Ευρωπαϊκή Νομοθεσία για τις ηλεκτρονικές υπογραφές»