Θέματα Ασφάλειας Διαδικτυακών Συναλλαγών και Προστασίας της Ιδιωτικότητας

Δ. Καραγιάννη και Γ. Σταματίου

Πάτρα, Φεβρουάριος 2021

Contents

[1 ο Κεφάλαιο – Εισαγωγικά Θέματα 4](#_Toc64708160)

[1.1 Πληροφοριακά Συστήματα 4](#_Toc64708161)

[1.1.1 Συστατικά μέρη και Τύποι Πληροφοριακών Συστημάτων 5](#_Toc64708162)

[1.1.2 Ασφάλεια Πληροφοριακών Συστημάτων 7](#_Toc64708163)

[1.2 Κρυπτογραφία 11](#_Toc64708164)

[1.2.1 Συμμετρικά και Μη Συμμετρικά Κρυπτογραφικά Συστήματα 14](#_Toc64708165)

[1.2.2 Κρυπτογραφικά Πρωτόκολλα και Αλγόριθμοι 21](#_Toc64708166)

[1.3 Προσωπικά Δεδομένα και Ιδιωτικότητα 22](#_Toc64708167)

[1.3.1 Ανωνυμία 24](#_Toc64708168)

[1.3.2 Μη–συνδεσιμότητα 26](#_Toc64708169)

[1.3.3 Ψευδωνυμία 27](#_Toc64708170)

[1.3.4 Διαχείριση Ταυτότητας 28](#_Toc64708171)

[1.4 Απαιτήσεις Ταυτοποίησης 29](#_Toc64708172)

[1.4.1 Αυθεντικοποίηση 29](#_Toc64708173)

[1.4.2 Εξουσιοδότηση 30](#_Toc64708174)

[2 ο Κεφάλαιο – Τεχνολογίες Προστασίας Ιδιωτικότητας 30](#_Toc64708175)

[2.1 Εισαγωγή 30](#_Toc64708176)

[2.1.1 Συλλογή Δεδομένων 31](#_Toc64708177)

[2.1.2 Προβλήματα και απειλές κατά της ιδιωτικότητας 32](#_Toc64708178)

[2.1.3 Κατηγορίες και Εργαλεία PETs (Privacy Enhancing Technologies) 33](#_Toc64708179)

[2.2 Διαπιστευτήρια (Credentials) 41](#_Toc64708180)

[2.2.1 Ψηφιακά Credentials (Digital Credentials) 42](#_Toc64708181)

[3 ο Κεφάλαιο – Πρωτόκολλο SSL (Secure Socket Layer) 43](#_Toc64708182)

[3.1 Γενικά 43](#_Toc64708183)

[3.2 Υπηρεσίες που προσφέρει το SSL 44](#_Toc64708184)

[3.3 Χαρακτηριστικά του SSL 44](#_Toc64708185)

[3.4 SSL Ψηφιακά Πιστοποιητικά 45](#_Toc64708186)

[3.5 Αντοχή του SSL σε γνωστές επιθέσεις 46](#_Toc64708187)

[4 ο Bitcoin 48](#_Toc64708188)

[4.1 Γενικά 48](#_Toc64708189)

[4.2 Βασικές έννοιες του bitcoin 49](#_Toc64708190)

[4.2.1 Ψηφιακά κλειδιά και ψηφιακές υπογραφές: 49](#_Toc64708191)

[4.2.2 Ιδιωτικό κλειδί (Private key) – Δημόσιο κλειδί (Public key) 50](#_Toc64708192)

[4.2.3 Κρυπογραφικές λειτουργίες κατακερματισμού (Hashing) 51](#_Toc64708193)

[4.2.4 Αλυσίδα των μπλοκ – Blockchain 51](#_Toc64708194)

[4.2.5 Τι είναι η εξόρυξη (mining) 52](#_Toc64708195)

[4.2.6 Τρόποι εξόρυξης bitcoin 54](#_Toc64708196)

[4.2.7 Άλλοι τρόποι απόκτησης bitcoin 55](#_Toc64708197)

[4.3 Συναλλαγές με bitcoin και ψηφιακά πορτοφόλια 59](#_Toc64708198)

[4.3.1 Ψηφιακά πορτοφόλια – Bitcoin wallets 60](#_Toc64708199)

[4.3.2 Τύποι ψηφιακών πορτοφολιών 61](#_Toc64708200)

[4.3.3 Πως ακριβώς γίνεται η δημιουργία ενός ψηφιακού πορτοφολιού: 64](#_Toc64708201)

[4.4 Πλεονεκτήματα & Μειονεκτήματα του Bitcoin 67](#_Toc64708202)

[4.4.1 Πλεονεκτήματα του Bitcoin 67](#_Toc64708203)

[4.4.2 Μειονεκτήματα του Bitcoin 70](#_Toc64708204)

[4.5 Στατιστικά στοιχεία 72](#_Toc64708205)

[4.5.1 Πλήθος Βitcoin σε κυκλοφορία 72](#_Toc64708206)

[4.5.2 Tιμή αγοράς Bitcoin 73](#_Toc64708207)

[4.5.3 Χρόνος επιβεβαίωσης συναλλαγών 75](#_Toc64708208)

[4.5.4 Αριθμός των συναλλαγών που αναμένεται να επιβεβαιωθεί. 76](#_Toc64708209)

[4.5.5 Συνολική αξία των ανταμοιβών που καταβάλλονται στους miners 76](#_Toc64708210)

[4.5.6 Hast rate και κατανάλωση ηλεκτρικής ενέργειας (για trillions of hashes/sec) 77](#_Toc64708211)

[5 ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) 79](#_Toc64708212)

[5.1 Γενικά 79](#_Toc64708213)

[5.2 Πεδίο εφαρμογής και στόχοι της οδηγίας 80](#_Toc64708214)

[5.3 Οι βασικές αρχές της οδηγίας 82](#_Toc64708215)

[5.4 Το περιεχόμενο του κανονισμού 84](#_Toc64708216)

[5.5 Τα δικαιώματα του υποκείμενου των δεδομένων 87](#_Toc64708217)

[5.6 Ζητήματα προστασίας προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο 94](#_Toc64708218)

[5.6.1 Συγκατάθεση πελάτη 94](#_Toc64708219)

[5.6.2 Γενικοί Όροι Συναλλαγών (ΓΟΣ) 96](#_Toc64708220)

[5.6.3 Οι γενικοί όροι συναλλαγών στο ηλεκτρονικό εμπόριο 97](#_Toc64708221)

[5.7 Μέτρα συμμόρφωσης με τον κανονισμό 98](#_Toc64708222)

[5.7.1 Καταγραφή δεδομένων – ροές δεδομένων (DATA INVENTORY- FLOWS) 98](#_Toc64708223)

[5.7.2 Αρχεία καταγραφής δραστηριοτήτων επεξεργασίας και μεθοδολογία καταγραφής 99](#_Toc64708224)

[5.7.3 Εκτίμηση επιπτώσεων στην προστασία δεδομένων (DPIA) 101](#_Toc64708225)

[5.7.4 Κρυπτογράφηση δεδομένων και χρήση ψευδωνύμων 104](#_Toc64708226)

[5.7.5 Κρυπτογράφηση και ανωνυμοποίηση από την πλευρά των εταιριών 105](#_Toc64708227)

[5.8 Παραβίαση των προσωπικών δεδομένων 106](#_Toc64708228)

[6 ο Επίλογος – οι θεμέλιοι λίθοι της σύγχρονης κρυπτογραφίας 110](#_Toc64708229)

[6.1 Προβλήματα, αλγόριθμοι και τα όρια της υπολογισιμότητας 110](#_Toc64708230)

[6.2 Γρήγορα Επιλύσιμα Προβλήματα: η κλάση P και η πρακτική υπολογισιμότητα 112](#_Toc64708231)

[6.3 Συμπεράσματα και προοίμιο στην κρυπτογραφία 118](#_Toc64708232)

[6.4 Βιβλιογραφία Kεφαλαίου 5 119](#_Toc64708233)

[Βιβλιογραφικές Αναφορές 119](#_Toc64708234)

1. ο Κεφάλαιο – Εισαγωγικά Θέματα
   1. Πληροφοριακά Συστήματα

Πληροφοριακό Σύστημα είναι κάθε σύστημα κατάλληλα οργανωμένο το οποίο είναι υπεύθυνο για τη συλλογή, οργάνωση, αποθήκευση και διαβίβαση πληροφοριών. Από την άλλη πλευρά Πληροφοριακό Σύστημα με την καθαρά υπολογιστική ερμηνεία είναι ένα σύστημα που απαρτίζεται από ανθρώπους και υπολογιστές και μεριμνά για την επεξεργασία ή ερμηνεία διαφόρων πληροφοριών. Ο όρος Πληροφοριακό Σύστημα χρησιμοποιείται αρκετές φορές ίσως και καταχρηστικώς όταν επιθυμούμε να περιγράψουμε περιπτώσεις οι οποίες αφορούν αμιγώς το λογισμικό που χρησιμοποιείται σε μία συγκεκριμένη διαδικασία ή σε μία ηλεκτρονική βάση δεδομένων ή όταν αναφερόμαστε σε ένα μόνο προσωπικό υπολογιστή[[1]](#footnote-1).

Σύμφωνα με την [Jes08] και τη σύγχρονη ακαδημαϊκή μελέτη ένα Πληροφοριακό Σύστημα αφορά συστήματα που σχετίζονται με τις πληροφορίες και τα συμπληρωματικά δίκτυα (υλικό και λογισμικό) όπου άνθρωποι και οργανισμοί χρησιμοποιούν για τη συλλογή, διαλογή, επεξεργασία, δημιουργία και διανομή των δεδομένων. Ιδιαίτερη έμφαση δίνεται στα Πληροφοριακά Συστήματα που αποτελούνται από χρήστες, επεξεργαστές, αποθηκευτικές μονάδες, εισόδους και εξόδους καθώς και τα προαναφερθέντα δίκτυα επικοινωνίας. Επιπρόσθετα στόχος κάθε Πληροφοριακού Συστήματος είναι να μπορεί να υποστηρίζει αποτελεσματικά τις λειτουργίες, τη διαχείριση και τη λήψη αποφάσεων στο πλαίσιο ενός οργανισμού. Επιπλέον σύμφωνα με την [Bul13] και [Kro08] τα Πληροφοριακά συστήματα είναι ο συγκερασμός της τεχνολογιών της πληροφορίας και των επικοινωνιών (ΤΠΕ), συμπεριλαμβανομένου του τρόπου με τον οποίο οι άνθρωποι αλληλοεπιδρούν με αυτή την τεχνολογία, με ευρύτερο στόχο την υποστήριξη των όλων των διαδικασιών του οργανισμού στον οποίον μετέχουν. Βεβαίως, θα πρέπει να υπάρχει σαφής διάκριση μεταξύ των πληροφοριακών συστημάτων, των συστημάτων πληροφορικής και των επιχειρηματικών διαδικασιών. Τα Πληροφοριακά συστήματα περιλαμβάνουν μερικά συστατικά των ΤΠΕ και εστιάζουν στην τελική χρήση των ΤΠΕ ελέγχοντας παράλληλα την απόδοση και την ποιότητα όλων των επιχειρηματικών διαδικασιών που συμβαίνουν σε ένα οργανισμό.

Τέλος στην [Sil95] διατυπώνονται δύο εκδοχές των Πληροφοριακών συστημάτων όπου και οι δύο περιλαμβάνουν το λογισμικό, το υλικό, τα δεδομένα, τους ανθρώπους, και τις διαδικασίες. Ενίσχυση της αυτής της προσέγγισης γίνεται στην [Zhe09] εάν στις παραπάνω εκδοχές προστεθούν κάποια βασικά στοιχεία όπως το περιβάλλον, ο σκοπός, τα όρια και οι αλληλεπιδράσεις μεταξύ των χρηστών. Τέλος η *Association for Computing Machinery* στην [Acm05] υποστηρίζει ότι η επιστημονική κοινότητα θα πρέπει να εστιάσει στην ενσωμάτωση λύσεων πληροφορικής αλλά και επιχειρηματικών διαδικασιών για την πλήρη κάλυψη όλων των αναγκών πληροφορικής σε επιχειρήσεις αλλά και σε οποιουσδήποτε οργανισμούς.

* + 1. Συστατικά μέρη και Τύποι Πληροφοριακών Συστημάτων

Υπάρχουν πολλοί και διάφοροι τύποι των πληροφοριακών συστημάτων, όπως για παράδειγμα: συστήματα επεξεργασίας συναλλαγών, συστήματα υποστήριξης αποφάσεων, συστήματα διαχείρισης γνώσης, συστήματα διαχείρισης μάθησης, συστήματα διαχείρισης βάσεων δεδομένων, συστήματα αυτοματισμού κλπ. Ζωτικής σημασίας πάντως για τα περισσότερα πληροφοριακά συστήματα αποτελούν οι τεχνολογίες, οι οποίες συνήθως σχεδιάζονται ώστε να εκτελούν καθήκοντα για τα οποία ο ανθρώπινος εγκέφαλος δεν μπορεί να εκτελέσει, όπως: η διαχείριση μεγάλου όγκου πληροφοριών, η εκτέλεση πολύπλοκων υπολογισμών, και ο έλεγχος πολλών και ταυτόχρονων διεργασιών.

Αξίζει να αναφέρουμε ότι πολλές εταιρείες και οργανισμοί έχουν δημιουργήσει επιτελικές θέσεις Πληροφοριακών Συστημάτων και Πληροφορικής (Chief Information Officer - (CIO)) ανάλογες με αυτές του Διευθύνοντα Σύμβουλου (CEO), Οικονομικού Διευθυντή (CFO) , Τεχνικού Διευθυντή (ΚΟΤ) κ.α. Επιπλέον κατά περίπτωση υπάρχει και η θέση του Διευθυντή Ασφάλειας Πληροφοριών (CISO) η οποία επικεντρώνεται στη διαχείριση της ασφάλειας των πληροφοριών.

Τα συστατικά στοιχεία που καθορίζουν και ολοκληρώνουν ένα κλασικό Πληροφοριακό Σύστημα είναι τα εξής:

* Υλικό (hardware)
* Λογισμικό (software)
* Δεδομένα (data)
* Διαδικασίες (Procedures)
* Άνθρωποι (People)
* Ανατροφοδότηση (Feedback)

Συνοπτικά ο όρος *υλικό* αναφέρεται στα μηχανήματα, [Γκρ03] στην κεντρική μονάδα επεξεργασίας (CPU), καθώς και το σύνολο των εξοπλισμών στήριξης. Μεταξύ του εξοπλισμού στήριξης είναι συσκευές εισόδου και εξόδου, συσκευές αποθήκευσης και συσκευές επικοινωνιών. Ο όρος *λογισμικό* αναφέρεται σε προγράμματα ηλεκτρονικών υπολογιστών καθώς και στα εγχειρίδια (αν υπάρχουν) που τα υποστηρίζουν. Τα *δεδομένα* είναι γεγονότα που χρησιμοποιούνται από τα προγράμματα για την παραγωγή χρήσιμων πληροφοριών. Όπως και τα προγράμματα, έτσι και τα δεδομένα αποθηκεύονται σε διάφορες συσκευές αποθήκευσης. Οι *διαδικασίες* είναι οι πολιτικές που διέπουν τη λειτουργία ενός υπολογιστικού συστήματος. Ακόμη για να καταστεί χρήσιμο κάθε πληροφοριακό σύστημα χρειάζεται ανθρώπους. Γενικά οι *άνθρωποι* και η εμπλοκή τους στη χρήση των πληροφοριακών συστημάτων, ίσως είναι το στοιχείο που επηρεάζει περισσότερο την επιτυχία ή την αποτυχία του. Το στοιχείο αυτό δεν περιλαμβάνει μόνο τους χρήστες, αλλά και εκείνους που λειτουργούν στην εξυπηρέτηση των πληροφοριακών συστημάτων, για παράδειγμα αυτούς που συλλέγουν τα δεδομένα για να εισαχθούν αργότερα στο Πληροφοριακό Σύστημα. Τέλος η *ανατροφοδότηση* είναι ένα συστατικό του Πληροφοριακού Συστήματος, αρκετά σημαντικό για τις σύγχρονες επιχειρήσεις κατά το οποίο τα δεδομένα μετασχηματίζονται σε πληροφορίες και οι πληροφορίες δημιουργούν νέες πληροφορίες με στόχο την υποστήριξη των τελικών αποφάσεων.

Η κλασική άποψη [Lau88] των πληροφοριακών συστημάτων και ειδικότερα τη δεκαετία του 1980, ήταν μια πυραμίδα των συστημάτων, που αντανακλούσε την ιεραρχία της οργάνωσης μίας εταιρείας ή οργανισμού, με τα συστήματα επεξεργασίας συναλλαγών στο κάτω μέρος της πυραμίδας, τα οποία ακολουθούνταν από τα πληροφοριακά συστήματα διοίκησης, έπειτα από τα συστήματα υποστήριξης αποφάσεων και τελείωναν με τα εκτελεστικά πληροφοριακά συστήματα στην κορυφή. Στο Σχήμα 1. 1 μπορούμε να παρατηρήσουμε την παραπάνω ιεραρχία:



Σχήμα 1. Πληροφοριακά Συστήματα – Μοντέλο Πυραμίδας

Το κλασικό μοντέλο πυραμίδας από τη δεκαετία του 1980 έχει υποστεί διάφορες αλλαγές και τροποποιήσεις, ωστόσο παραμένει χρήσιμο, κυρίως για εκπαιδευτικούς σκοπούς αλλά και για να τονίσει τη σημασία της ιεράρχησης τεχνολογιών, διαδικασιών και ανθρώπων μέσα σε ένα οργανισμό. Από τότε μέχρι και σήμερα έχουν αναπτυχθεί νέες τεχνολογίες και κατηγορίες πληροφοριακών συστημάτων, μερικά από τα οποία δεν μπορούν να ενσωματωθούν με ευκολία στο αρχικό μοντέλο πυραμίδας. Πολλά από τα νέα Πληροφοριακά Συστήματα, γνωστά πλέον σε εμάς, είναι τα εξής:

* Αποθήκες Δεδομένων (Data Warehouses)
* Διαχείρισης Επιχειρηματικών Πόρων (ERP)
* Έμπειρα Συστήματα (Expert Systems)
* Μηχανές Αναζήτησης (Search Engines)
* Γεωγραφικά Πληροφοριακά Συστήματα (GIS)
* κ.α
  + 1. Ασφάλεια Πληροφοριακών Συστημάτων

Στα πληροφοριακά συστήματα, στα ολοκληρωμένα πληροφοριακά συστήματα, στα συστήματα ηλεκτρονικής διακυβέρνησης (κρατικά πληροφοριακά συστήματα) καθώς και σε οποιαδήποτε άλλα συστήματα που εμπλέκονται άνθρωποι, διαδικασίες, ροή δεδομένων και πληροφοριών η συνεισφορά της ασφάλειας παίζει καθοριστικό ρόλο. Ήδη στις ημέρες μας αποτελεί γνωστικό πεδίο της επιστήμης της πληροφορικής λαμβάνοντας υπόψη στοιχεία και θεμελιώσεις από άλλες παραπλήσιες ή και μη επιστήμες. Παραπλήσιο γνωστικό πεδίο με μεγάλη συνεισφορά είναι η εφαρμοσμένη Κρυπτογραφία η οποία και αναλύεται σε επόμενες ενότητες. Εισαγωγικά θα μπορούσαμε να ορίσουμε την ασφάλεια ως την προστασία των υπολογιστικών συστημάτων και των δικτύων που διασυνδέονται με παράλληλη αποτροπή οποιασδήποτε μη εξουσιοδοτημένης πρόσβασης στη χρήσης τους.

Ιστορικά η ασφάλεια των πληροφοριακών συστημάτων μελετήθηκε στις αρχές της δεκαετίας τους 1970 από το στρατό. Πιο συγκεκριμένα και στη σχετική δημοσίευση [War70] εξετάστηκε το πρόβλημα χρήσης και επικοινωνίας των υπολογιστών εξ αποστάσεως. Προηγουμένως η πρόσβαση σε υπηρεσίες αφορούσε τη φυσική παρουσία του χρήστη στον κεντρικό υπολογιστή. Από τις σχετικές μελέτες προέκυψαν διάφορες καινοτόμες ιδέες (ειδικά για εκείνη την εποχή) οι οποίες αποτελούν μέχρι και σήμερα θεμελιώδη ζητήματα στην εφαρμογή των πολιτικών ασφαλείας. Μία τέτοια ιδέα ήταν η εύρεση κατάλληλης ισορροπίας μεταξύ της προστασίας των πληροφορίων και της ευκολίας στην εργασία του χρήστη. Εκείνη τη δεκαετία εμφανίστηκε και ο πρώτο ιός με ονομασία Creeper στο στρατιωτικό δίκτυο ARPANET. Στη συγκεκριμένη δημοσίευση γίνεται επίσης λόγος για ύπαρξη κωδικών ασφαλείας για όλους τους χρήστες των πληροφοριακών συστημάτων και υποσυστημάτων μια ιδέα που υιοθετείται πλήρως αργότερα από τους δημιουργούς του Unix[[2]](#footnote-2). Βέβαια ένα από τα πιο σημαντικά ζητήματα που αντιμετωπίζει η επιστημονική κοινότητα και δη αυτής της κρυπτογραφίας είναι η χρήση αδύναμων κωδικών πρόσβασης. Η ευκολία χρήσης υπαγορεύει αδύναμους κωδικούς ενώ η προστασία της πληροφορίας υπαγορεύει μεγάλους και δύσκολους κωδικούς πρόσβασης. Με λίγα λόγια οδηγούμαστε στον κλονισμό της ισορροπίας που αναφέρθηκε παραπάνω.

Κατά το σχεδιασμό ασφαλών πολιτικών στα πληροφοριακά συστήματα ενσωματώνονται διαδικασίες όχι μόνο τεχνικής φύσης αλλά κυρίως διοικητικές οι οποίες και θα πρέπει να συμβαδίζουν κάθε φορά με τις τρέχουσες ηθικές και κοινωνικές αντιλήψεις. Οι πολιτικές αυτές έχουν μοναδικό στόχο την προφύλαξη του πληροφοριακού συστήματος αλλά και ολόκληρου του οργανισμού από κάθε σκόπιμη ή τυχαία απειλή. Βασικό σημείο κατά τον παραπάνω σχεδιασμό είναι ο εντοπισμός και η κατηγοριοποίηση των πληροφοριών σε εμπιστευτικές ή μη εμπιστευτικές και οι οποίες πρόκειται να χρησιμοποιηθούν στο ευρύ ή σε ένα πιο συγκεκριμένο κοινό. Όλα τα παραπάνω προϋποθέτουν την ύπαρξη μίας ευρύτερης αντίληψης και βασικών αρχών που θα πρέπει να διέπουν τους σχεδιαστικούς στόχους των πληροφοριακών συστημάτων. Ειδικότερα, κάθε αντικείμενο του συστήματος θα πρέπει να αναγνωρίζεται και να αποτυπώνεται σε αυτό μία ένδειξη του βαθμού εμπιστευτικότητας [Γκρ03].

Η πολιτική ασφάλειας που διέπει τον οργανισμό θα πρέπει να μεριμνά αποτελεσματικά για όλους τους εμπλεκόμενους στη χρήση και τη λειτουργία του Πληροφοριακού Συστήματος. Οι εμπλεκόμενοι συνήθως είναι οι χρήστες και διαχειριστές, τα διευθυντικά στελέχη και οι πελάτες του οργανισμού. Επιπρόσθετα οι νομικές και κανονιστικές διατάξεις του οργανισμού θα πρέπει να είναι ρητώς διατυπωμένες ούτως ώστε όλοι οι παραπάνω εμπλεκόμενοι να κινούνται σε συγκεκριμένο πλαίσιο αρμοδιοτήτων.

Όταν εφαρμόζεται μία πολιτική ασφάλειας είθισται να συμπεριλαμβάνουμε τα εξής:

* Εφαρμογή πληρότητας όσον αφορά τις οδηγίες και τα μέτρα προστασίας των υπηρεσιών που προσφέρουμε και των λειτουργιών που εκτελούνται.
* Εφαρμογή επικαιρότητας όσον αφορά τις τρέχουσες τεχνολογικές εξελίξεις
* Εφαρμογή γενικευσιμότητας όσον αφορά τις επιπρόσθετες παρεμβάσεις, τροποποιήσεις ή προσθήκες που μπορεί να γίνουν στο πληροφοριακό σύστημα.

Η επιτυχία μιας πολιτικής ασφάλειας εξαρτάται, επίσης, και από τη διάθεση τήρησής της και τη συμμετοχή των εμπλεκόμενων φορέων. Με λίγα λόγια θα πρέπει να υπάρχει συνεχής και αδιάλειπτη εκπαίδευση των χρηστών, να αξιολογείται η πρόσβαση, η αμεσότητα και η ευκολία αυτής και να διενεργούνται τακτικά τεστ αντοχής (stress tests) ώστε να διαπιστώνεται το επίπεδο ετοιμότητας για την αντιμετώπιση και εξουδετέρωση οποιασδήποτε απειλής.

Σύμφωνα με την [Kra98] οι βασικοί άξονες στους οποίους στηρίζεται η ασφάλεια των πληροφοριακών συστημάτων είναι οι παρακάτω:

* **Ακεραιότητα (Integrity):** Είναι πολύ σημαντικό τα δεδομένα του πληροφοριακού συστήματος να διατηρούνται σε μία γνώριμη κατάσταση, αναλλοίωτα, χωρίς να υποστούν οποιουδήποτε είδους τροποποίηση, αφαίρεση ή προσθήκη από άτομα εντός και εκτός του οργανισμού. Συνεπώς θα πρέπει να αποτρέπεται αυστηρώς η πρόσβαση στη χρήση μη εξουσιοδοτημένων ατόμων. *Παράδειγμα ακεραιότητας θα μπορούσε να αποτελέσει ένας εκδοτικός οργανισμός μέσων μαζικής ενημέρωσης όπου θα πρέπει τα άρθρα που δημοσιεύονται στο διαδίκτυο να είναι ασφαλή από οποιαδήποτε τροποποίηση και εισαγωγή λανθασμένων πληροφοριών.*
* **Διαθεσιμότητα (Availability):** Τα δεδομένα, τα πληροφοριακά υποσυστήματα, τα δίκτυα και οι υπολογιστικοί πόροι θα πρέπει να είναι στη διάθεση των χρηστών όποτε και για όσο απαιτείται η χρήση τους. Τα τελευταία χρόνια και εξαιτίας της αύξησης της χρήσης των διαδικτυακών υπηρεσιών συχνά παρατηρούνται φαινόμενα μη διαθεσιμότητας δεδομένων. *Οι πιο συχνές περιπτώσεις είναι επιθέσεις τύπου DDOS attack. Τέτοιες επιθέσεις έχουν στόχο την υπερφόρτωση των υπολογιστικών πόρων (από τους επιτιθέμενους) με σκοπό να τεθούν εκτός λειτουργίας διάφορες υπηρεσίες ενός οργανισμού.* *Βέβαια υπο φυσιολογικές συνθήκες παρατηρείται και το φαινόμενο Slashdot όπου εξαιτίας της υπερφόρτωσης από υψηλή επισκεψιμότητα και χαμηλού transfer bandwidth ενός διαδικτυακού ιστότοπου οι υπηρεσίες βρίσκονται προσωρινά εκτός λειτουργίας.* Σε κάθε περίπτωση όμως (κακόβουλη και μη) η διαθεσιμότητα παραβιάζεται και θα πρέπει να ληφθούν άμεσα μέτρα και νέες πολιτικές ασφάλειας.
* **Εμπιστευτικότητα (Privacy ή Confidentiality):** Κάθε πληροφορία που ανταλλάσσεται στο σύστημα και ειδικά αν είναι ευαίσθητη, δεν θα πρέπει να αποκαλύπτεται σε μη εξουσιοδοτημένα άτομα. Απώλεια πληροφοριών θα μπορούσε να γίνει από τις πιο παραδοσιακές μεθόδους μέχρι τις πιο προηγμένες (πχ ψηφιακές υποκλοπές). *Μία παραδοσιακή μέθοδος θα ήταν η φυσική κλοπή hardware από το κατάλληλο τμήμα μίας εταιρείας.*
* **Πιστοποίηση και Αυθεντικότητα (authentication):** Στην περίπτωση αυτή υπάρχουν δύο βασικοί πυλώνες στους οποίους στηρίζεται η πιστοποίηση: την πιστοποίηση οντοτήτων (entity authentication ή identification) και την πιστοποίηση δεδομένων (data authentication). Με τον πρώτο πυλώνα εξασφαλίζουμε ότι κάθε οντότητα στο πληροφοριακό-επικοινωνιακό σύστημα είναι αυτή που ισχυρίζεται και δεν υπάρχει κάποια πλαστοπροσωπία. Με το δεύτερο πυλώνα εξασφαλίζουμε την τοποθεσία, τη χρονική στιγμή και το είδος των μηνυμάτων που ανταλλάσσονται σε μία επικοινωνία. *Παράδειγμα αυθεντικότητας αποτελεί η κάθε είδους εισβολή και υποκλοπή προσωπικών στοιχείων της πιστωτικής μας κάρτας κατά τη διαδικασία μίας διαδικτυακής αγοράς. Τόσο ο οργανισμός θα πρέπει να κατανοεί ότι η αγορά γίνεται από πιστοποιημένη οντότητα όσο και ο αγοραστής να είναι σε θέση να επιβεβαιώσει ότι η αγορά έγινε από τον ίδιο, σε συγκεκριμένη χρονική στιγμή και σε συγκεκριμένη τοποθεσία.*
* **Μη αποποίηση (non-repudiation):** Κανένας χρήστης, είτε αυτός είναι αποστολέας είτε παραλήπτης, δεν μπορεί να αποποιηθεί τις πράξεις που έκανε στο παρελθόν. Ένας από τους πιο διαδεδομένους αλλά και ταυτόχρονα αποτελεσματικούς τρόπους εφαρμογής της μη αποποίησης είναι η χρήση των ψηφιακών υπογραφών και από τις δύο πλευρές.
* **Εγκυρότητα (validity):** Αφορά κυρίως εκείνους που χρησιμοποιούν συγκεκριμένες πληροφορίες του συστήματος. Οι εμπλεκόμενες πλευρές ενδιαφέρονται για την πληρότητα και την ακρίβειά αυτών των πληροφοριών, λόγω των αποφάσεων που πρέπει να λάβουν. Θα μπορούσαμε να εκλάβουμε την Εγκυρότητα ώς το άθροισμα της Ακεραιότητας και τη Αυθεντικότητας
* **Μοναδικότητα (Uniqueness):** Είναι η αδυναμία αντιγραφής και αναπαραγωγής της πληροφορίας χωρίς εξουσιοδότηση.

Πριν περάσουμε στο βασικό σκέλος της εργασίας μας και στην προστασία της ιδιωτικότητας αξίζει να αναφερθούμε σε ένα πολύ γνωστό επιστημονικό πεδίο, αυτό της Κρυπτογραφίας το οποίο διαδραματίζει αρκετά σημαντικό ρόλο στην επίτευξη της ασφάλειας των πληροφοριακών συστημάτων αλλά και των εμπλεκόμενων χρηστών.

* 1. Κρυπτογραφία

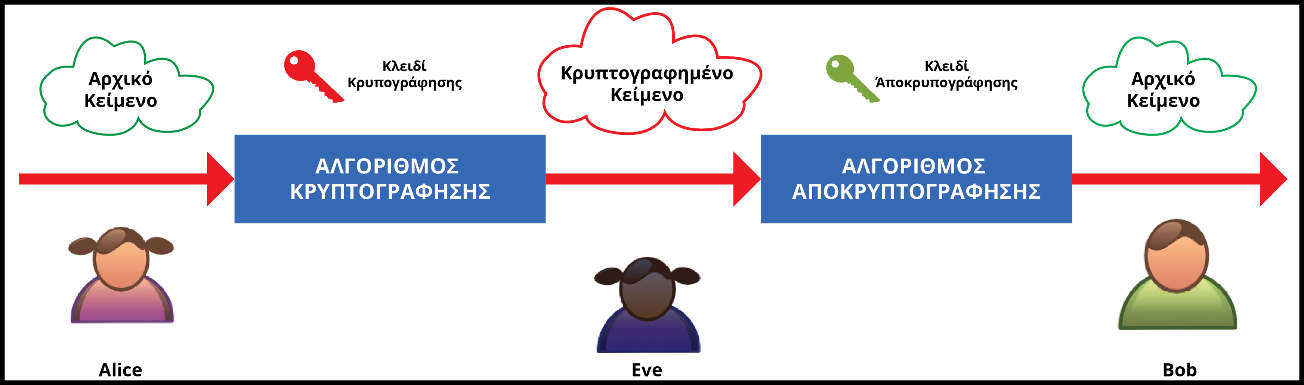
Ένας από τους πιο σημαντικούς κλάδους της επιστήμης των υπολογιστών είναι η κρυπτογραφία[[3]](#footnote-3). Με τη λέξη κρυπτογραφία εννοούμε την επιστήμη εκείνη που ασχολείται με τη σχεδίαση κρυπτογραφικών συστημάτων. Πρόκειται για συστήματα τα οποία μετατρέπουν χρήσιμη και εμπιστευτική πληροφορία σε τέτοια μορφή, η οποία να είναι κατανοητή μόνο από τον αποστολέα στον παραλήπτη, ενώ ταυτόχρονα να είναι άχρηστη και ασήμαντη σε οποιοδήποτε μη εξουσιοδοτημένο πρόσωπο. Η κρυπτογραφία, λοιπόν δημιουργήθηκε από την ανάγκη των ανθρώπων να μεταφέρουν μηνύματα ο ένας στον άλλο, χωρίς κάποιος τρίτος να μπορεί να τα αντιληφθεί. Έτσι, οι κύριοι χαρακτήρες που χρησιμοποιούνται διεθνώς στη βιβλιογραφία για την περιγραφή τέτοιων συστημάτων είναι η Alice και ο Bob που επιθυμούν να επικοινωνούν μεταξύ τους, χωρίς η Eve (το τρίτο πρόσωπο) να μπορεί να τους αντιληφθεί.

Η κρυπτογραφία εμφανίστηκε αρχικά, τουλάχιστον από όσα γνωρίζουμε μέχρι σήμερα, στην εποχή των αρχαίων Αιγυπτίων (2.000 π.Χ.), παίζοντας ένα πολύ σημαντικό ρόλο καθ’ όλη τη διάρκεια της ιστορίας. Ειδικότερα στον 2ο παγκόσμιο πόλεμο, τόσο οι Γερμανοί όσο και οι Ιάπωνες κατάφεραν να αναπτύξουν κρυπτογραφικές μηχανές όπως η Enigma και η Purple Machine αντίστοιχα. Αξίζει να σημειωθεί ότι αργότερα πολύπλοκες κρυπτογραφικές μέθοδοι επικοινωνίας αναπτύχθηκαν από λαθρεμπόρους, αλλά και στη συνέχεια ακόμη πιο πολύπλοκες αναπτύχθηκαν από μυστικές υπηρεσίες κυβερνήσεων. Τέλος, στις μέρες μας, η ανάγκη για κρυπτογραφημένα μηνύματα είναι πολύ μεγάλη, αρκεί μόνο να συλλογιστούμε πόσο απαραίτητο μας είναι πολλές φορές το γεγονός να ανταλλάσσουμε πληροφορίες μέσω διαδικτύου. Για παράδειγμα, η μεταφορά χρηματικών ποσών από ένα λογαριασμό σε έναν άλλο, που πλέον γίνεται εύκολα μέσω διαδικτύου, επιθυμούμε να γίνεται με τέτοιο τρόπο ώστε να είναι αδύνατο οι δύο αριθμοί λογαριασμών να γίνουν γνωστοί σε κάποιον τρίτο.

Κάθε κρυπτογραφικό σύστημα θα πρέπει να έχει τέτοιες ιδιότητες, ώστε να παρέχεται η επιθυμητή ασφάλεια στους χρήστες, όπως αυτές αναφέρονται στην ενότητα 1.1.2. Τη σημαντικότητα των συγκεκριμένων ιδιοτήτων θα προσπαθήσουμε να παρουσιάσουμε στο παρακάτω παράδειγμα.

Έστω ότι η Alice επιθυμεί να μεταφέρει χρήματα από έναν δικό της τραπεζικό λογαριασμό σε έναν τραπεζικό λογαριασμό του Bob μέσω διαδικτύου. Η Alice, φυσικά και επιθυμεί, η συγκεκριμένη επικοινωνία να είναι εμπιστευτική, μιας και κανένας τρίτος δεν πρέπει να λάβει γνώση τόσων των δύο αριθμών λογαριασμού όσο και του μεταφερόμενου χρηματικού ποσού. Από την άλλη πλευρά, ο Bob θα πρέπει να λάβει το μήνυμα πιστοποιημένο, ότι δηλαδή αυτό προέρχεται πράγματι από την Alice. Και οι δύο πλευρές (Alice και Bob) θα πρέπει να είναι βέβαιες ότι η ακεραιότητα του μηνύματος διατηρείται, όπως για παράδειγμα ότι το μεταφερόμενο χρηματικό ποσό δε δύναται να αλλαχθεί από κάποιον τρίτο κατά τη διαδικασία. Τέλος, ο Bob επιθυμεί την αποποίηση, δηλαδή η Alice αργότερα να μην μπορεί να ισχυριστεί ότι δεν έδωσε την εντολή μεταφοράς του χρηματικού ποσού.

Έτσι, κρυπτογράφηση ονομάζεται η διαδικασία εκείνη κατά την οποία ένα απλό κείμενο (plain text) μετατρέπεται σε ένα κρυπτογραφημένο κείμενο (cipher text). Ενώ αποκρυπτογράφηση είναι η ακριβώς αντίστροφη διαδικασία. Και οι δύο αυτές διαδικασίες πραγματοποιούνται με τη χρήση κλειδιών κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Η γενική μορφή ενός κρυπτογραφικού συστήματος μετάδοσης μηνύματος παρουσιάζεται στο παρακάτω σχήμα:



Σχήμα 1. Γενική μορφή ενός κρυπτογραφικού συστήματος μετάδοσης μηνύματος.

Όπως φαίνεται και στο πιο πάνω σχήμα, η Alice κρυπτογραφεί ένα μήνυμα χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης και το αντίστοιχο κλειδί κρυπτογράφησης και στη συνέχεια στέλνει το κρυπτογραφημένο πια μήνυμα στον Bob. Εκείνος με τη σειρά του το αποκρυπτογραφεί χρησιμοποιώντας έναν αλγόριθμο αποκρυπτογράφησης και το κλειδί αποκρυπτογράφησης. Η Eve είναι μια οποιαδήποτε οντότητα (τρίτο πρόσωπο) η οποία προσπαθεί να παρέμβει με κακόβουλο τρόπο στην επικοινωνία μεταξύ της Alice και του Bob. Αυτή η οντότητα (τρίτο πρόσωπο) στην κρυπτογραφία αποκαλείται υποκλοπέας (interceptor), ωτακουστής (eavesdropper) ή απλά επιτιθέμενος (attacker). Η διαδικασία που εκτελεί ο υποκλοπέας ονομάζεται κρυπτανάλυση. Συνεπώς, κρυπτανάλυση είναι η διαδικασία εκείνη κατά την οποία ο υποκλοπέας μελετά το κρυπτογραφημένο μήνυμα και προσπαθεί με διάφορες τεχνικές και μεθόδους και χωρίς φυσικά να διαθέτει το κλειδί αποκρυπτογράφησης, να εξάγει την αρχική πληροφορία (ή μέρος αυτής) του κρυπτογραφημένου μηνύματος. Η έννοια της κρυπτολογίας περιλαμβάνει μαζί την έννοια της κρυπτογραφίας και της κρυπτανάλυσης.

Πολύ συχνά στα κρυπτογραφημένα μηνύματα ορίζεται ένα Έμπιστο Τρίτο Μέλος (Trusted Third Party - TTP). Ο ρόλος του μέλους αυτού είναι η επίλυση διαφωνιών μεταξύ των υπολοίπων χρηστών του συστήματος ή ακόμα και η διευκόλυνση της μεταξύ τους επικοινωνίας. Το Έμπιστο Τρίτο Μέλος διακρίνεται σε λειτουργικά έμπιστο (fuctionally trusted) και σε άνευ όρων έμπιστο (unconditionally trusted). Λειτουργικά έμπιστο μέλος θεωρείται ένα ΤΤΡ το οποίο είναι έμπιστο για να λύσει διαφωνίες μεταξύ των χρηστών, αλλά δεν μπορεί να έχει πρόσβαση στα μυστικά κλειδιά τους. Ένα ΤΤΡ μέλος θεωρείται άνευ όρων έμπιστο μέλος μόνον εφόσον όλοι οι χρήστες του κρυπτογραφημένου συστήματος μπορούν να το εμπιστευθούν από κάθε άποψη, όπως για παράδειγμα να είναι γνώστης όλων των μυστικών κλειδιών των χρηστών.

Τέλος, αξίζει να σημειωθεί ότι η ασφάλεια του συστήματος εξαρτάται μόνο από την μυστικότητα των κλειδιών αποκρυπτογράφησης, μιας και οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης που χρησιμοποιούνται είναι γνωστοί σε όλους. Από αυτό και μόνο το γεγονός, είναι φανερό ότι η διανομή και διαχείριση των κλειδιών αποκρυπτογράφησης αποτελεί ένα από τα πιο βασικά και δύσκολα προβλήματα της επιστήμης της κρυπτογραφίας.

* + 1. Συμμετρικά και Μη Συμμετρικά Κρυπτογραφικά Συστήματα

Τα κρυπτογραφικά συστήματα διαχωρίζονται σε δύο είδη με βάση τα κλειδιά αποκρυπτογράφησης. Έτσι έχουμε:

* τα συμμετρικά (symmetric) ή συμβατικά (conventional) κρυπτογραφικά συστήματα και
* τα μη συμμετρικά (asymmetric) ή δημοσίου κλειδιού (public key) κρυπτογραφικά συστήματα.

Ένα κρυπτογραφικό σύστημα ονομάζεται συμβατικό όταν το κλειδί αποκρυπτογράφησής του μπορεί εύκολα να εξακριβωθεί από το αντίστοιχο κλειδί κρυπτογράφησης. Στην πληθώρα των περιπτώσεων των συμβατικών κρυπτογραφικών συστημάτων, τα δύο κλειδιά είναι ίδια. Αντίστοιχα, ένα κρυπτογραφικό σύστημα ονομάζεται δημοσίου κλειδιού όταν το κλειδί αποκρυπτογράφησής του εξακριβώνεται δύσκολα από το αντίστοιχο κλειδί κρυπτογράφησης.

Είναι πλέον σαφές ότι η ασφάλεια όλων των κρυπτογραφικών συστημάτων βασίζεται στην μυστικότητα του κλειδιού αποκρυπτογράφησης, το οποίο και δεν πρέπει να αποκαλυφθεί σε κανένα άλλον, πέραν των πιστοποιημένων χρηστών του κρυπτογραφικού συστήματος. Έτσι, για να θεωρείται ένα συμβατικό (συμμετρικό) κρυπτογραφικό σύστημα ασφαλές, να είναι δηλαδή ο δίαυλος επικοινωνίας των χρηστών του ασφαλής, θα πρέπει τόσο το κλειδί αποκρυπτογράφησης όσο και το κλειδί κρυπτογράφησης να είναι μυστικά. Αυτό το γεγονός από μόνο του αποτελεί ένα σημαντικό μειονέκτημα των συμβατικών κρυπτογραφικών συστημάτων. Αντίθετα, κάτι τέτοιο δεν απαιτείται για την ασφάλεια των κρυπτογραφικών συστημάτων δημοσίου κλειδιού. Μόνο και μόνο για το λόγο αυτό, η εισαγωγή τους στην [Dif76], αποτέλεσε μια νέα αρχή στο χώρο της κρυπτογραφίας.

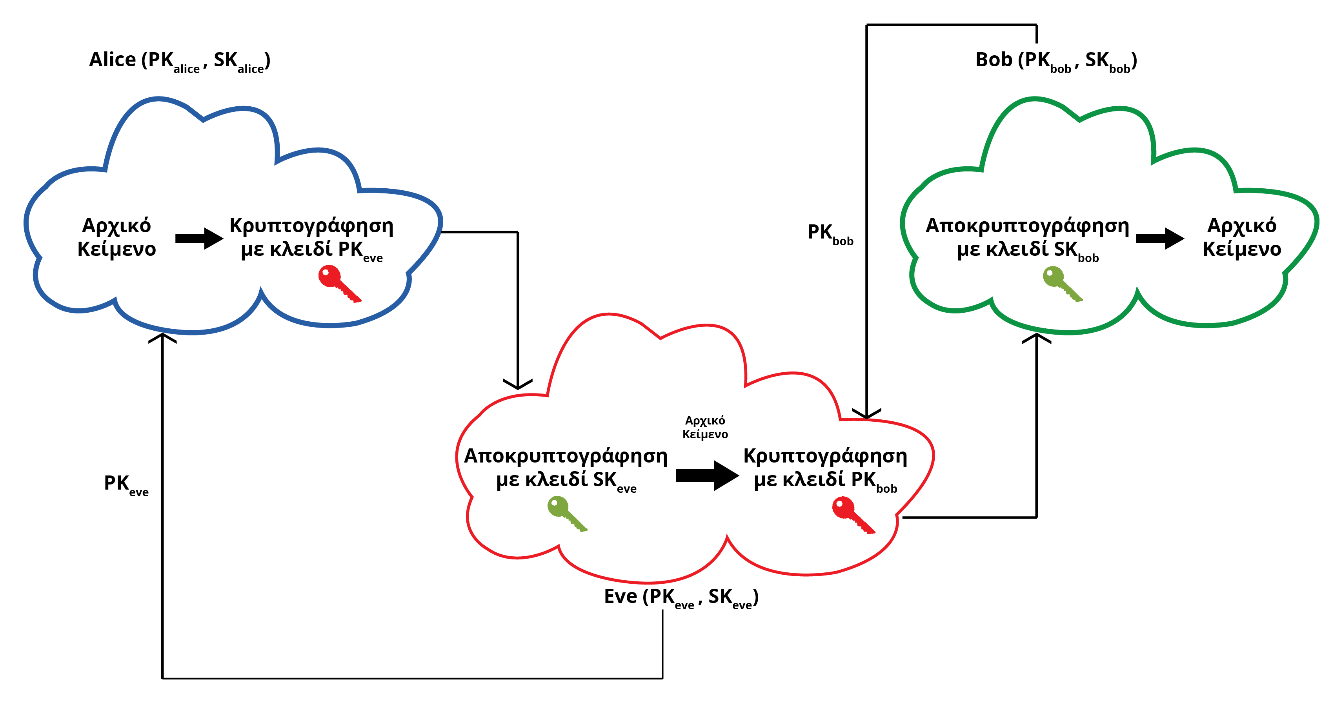
Στα κρυπτογραφικά συστήματα δημοσίου κλειδιού, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι με τέτοιο τρόπο σχεδιασμένοι ώστε τα αντίστοιχα κλειδιά, κρυπτογράφησης και αποκρυπτογράφησης, να είναι διαφορετικά μεταξύ τους. Η επιτυχία, και συνεπώς η ασφάλεια, αυτού του είδους των κρυπτογραφικών συστημάτων βασίζεται στο ότι παρά το γεγονός ότι το δημόσιο κλειδί κρυπτογράφησης είναι γνωστό σε όλους, ο υπολογισμός του κλειδιού αποκρυπτογράφησης είναι δύσκολος έως αδύνατος. Στα συστήματα αυτά, δημόσιο κλειδί καλείται το κλειδί κρυπτογράφηση, που είναι σε όλους γνωστό και ιδιωτικό κλειδί καλείται το άλλο κλειδί, το κλειδί αποκρυπτογράφησης.

Σύμφωνα με όλα τα παραπάνω, αυτό που προσδίδει ασφάλεια στα κρυπτογραφικά συστήματα δημοσίου κλειδιού είναι στην ουσία η δυσκολία που παρουσιάζεται στην επίλυση ενός μαθηματικού προβλήματος. Πιο συγκεκριμένα, η εξακρίβωση του ιδιωτικού κλειδιού με βάση το δημόσιο κλειδί, αλλά και κάποιες ακόμα παραμέτρους του συστήματος είναι ένα τρομερά δύσκολο υπολογιστικά πρόβλημα. Όσο πιο δυσεπίλυτο το πρόβλημα αυτό, τόσο πιο αποδοτικό και ασφαλές είναι το κρυπτογραφικό σύστημα.

Ας προσπαθήσουμε όμως μέσω ενός απλού παραδείγματος να κατανοήσουμε τη λειτουργία των κρυπτογραφικών συστημάτων δημοσίου κλειδιού. Έστω ότι η Alice θέλει να μεταφέρει ένα μήνυμα στον Bob. Η Alice και ο Bob έχουν από ένα δημόσιο και ένα ιδιωτικό κλειδί ο καθένας. Χρησιμοποιώντας η Alice το δημόσιο κλειδί του Bob μεταφέρει το μήνυμα στον Bob, ο οποίος με τη σειρά του, χρησιμοποιώντας το ιδιωτικό του κλειδί αποκρυπτογραφεί το μήνυμα που του έστειλε η Alice. Στη συνέχεια απαντάει με ένα ακόμα κρυπτογραφημένο μήνυμα στην Alice, χρησιμοποιώντας το δημόσιο κλειδί της Alice. Στο σημείο αυτό, πρέπει να αναφερθεί ότι όποιος γνωρίζει το δημόσιο κλειδί της Alice, μπορεί να της στείλει ένα κρυπτογραφημένο μήνυμα. Και αντίστοιχα ισχύουν και για τον Bob. Η Alice με τη σειρά της, μπορεί να αποκρυπτογραφήσει τα μηνύματα που λαμβάνει χρησιμοποιώντας το ιδιωτικό της κλειδί.

Διαβάζοντας τα παραπάνω, θα έλεγε κανείς ότι τα κρυπτογραφικά συστήματα δημόσιου κλειδιού είναι τα πλέον ιδανικά. Δυστυχώς όμως κάτι τέτοιο δεν ισχύει. Στο πιο κάτω σχήμα, Σχήμα 1.3, παρουσιάζεται ο τρόπος με τον οποίο ένας κακόβουλος χρήστης μπορεί να επιτεθεί σε ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού.

Επανερχόμενοι στο πιο πάνω παράδειγμα κρυπτογραφικού συστήματος δημοσίου κλειδιού, ας κάνουμε τώρα την υπόθεση ότι ο κακόβουλος χρήστης Eve θέλει να ανακτήσει το μήνυμα της Alice προς τον Bob. Έτσι, εισβάλει στην μεταξύ τους επικοινωνία παραπλανώντας τους, ενώ προσποιείται στην Alice ότι είναι ο Bob και στον Bob ότι είναι η Alice. Έτσι, η Eve κοινοποιεί στην Alice το δημόσιο κλειδί της, η οποία (Alice) θεωρεί ότι το δημόσιο κλειδί που της κοινοποιείται είναι του Bob και κρυπτογραφεί ένα μήνυμα. Το μήνυμα αυτό λαμβάνει η Eve, η οποία χρησιμοποιώντας το ιδιωτικό της κλειδί αποκρυπτογραφεί το μήνυμα της Alice κι έτσι το ανακτά. Στη συνέχεια, η Eve κρυπτογραφεί το μήνυμα της Alice, το οποίο έχει ανακτήσει, με το δημόσιο κλειδί του Bob. Αυτός με τη σειρά του λαμβάνει το μήνυμα της Alice, χωρίς όμως να γνωρίζει ότι δεν εστάλει από εκείνη, αλλά από την Eve. Στην προκειμένη δηλαδή περίπτωση, αποστολέας (Alice) και παραλήπτης (Bob) δεν μπορούν να γνωρίζουν τον υποκλοπέα (Eve) που παράκαμψε την επικοινωνία τους και έχει υποκλέψει το αρχικό μήνυμα. Σε άλλη περίπτωση, ο υποκλοπέας θα μπορούσε και να τροποποιήσει το αρχικό μήνυμα.



Σχήμα 1. Παρέμβαση τρίτου και υποκλοπή σε ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού.

Το παράδειγμα αυτό κάνει σαφές ότι η πιστοποίηση των οντοτήτων ενός κρυπτογραφικού συστήματος δημοσίου κλειδιού είναι ιδιαίτερα σημαντική.

Οι επιθέσεις που μπορεί να παρατηρηθούν σε ένα κρυπτογραφικό σύστημα, είτε συμβατικό (συμμετρικό) είτε δημοσίου κλειδιού (μη συμμετρικό) διακρίνονται σε:

* Ενεργές επιθέσεις (Active Attacks). Μία ενεργή επίθεση παρουσιάζεται στο Σχήμα 1.3. Πρόκειται για τις επιθέσεις εκείνες όπου ο υποκλοπέας έχει τη δυνατότητα να διαγράψει, προσθέσει ή να παρέμβει με οποιονδήποτε τρόπο στην επικοινωνία των δύο χρηστών.
* Παθητικές επιθέσεις (Passive Attacks). Τέτοιες επιθέσεις είναι οι ακόλουθες:

1. Επίθεση με γνωστό απλό κείμενο (Known – plain text attack). Κατά την επίθεση αυτή ο υποκλοπέας γνωρίζει κάποια από τα αρχικά κείμενα και τα αντίστοιχα κρυπτογραφημένα κείμενα και χρησιμοποιώντας τα προσπαθεί να ανακαλύψει το κλειδί αποκρυπτογράφησης.
2. Επίθεση με επιλεγμένο απλό κείμενο (Chosen – plain text attack). Σε αυτού του είδους την επίθεση ο υποκλοπέας επιλέγει ορισμένα αρχικά κείμενα και λαμβάνει τα κρυπτογραφημένα τους.
3. Προσαρμοζόμενη επίθεση με επιλεγμένο απλό κείμενο (Adaptive chosen – plain text attack). Είναι επίθεση παρόμοια με την προηγούμενη, με τη διαφορά ότι σε αυτή την περίπτωση ο υποκλοπέας μπορεί κατά τη διάρκεια της επίθεσης να αλλάξει τις επιλογές του για τα αρχικά κείμενα.
4. Επίθεση με επιλεγμένο κρυπτογραφημένο κείμενο (Chosen – cipher text attack). Στην προκειμένη περίπτωση συμβαίνει το αντίθετο από ότι προηγουμένως: ο υποκλοπέας επιλέγει ορισμένα κρυπτογραφημένα κείμενα και του παρέχονται με κάποιο τρόπο και τα αντίστοιχα αρχικά κείμενα.
5. Προσαρμοζόμενη επίθεση με επιλεγμένο κρυπτογραφημένο κείμενο (Adaptive chosen – cipher text attack). Πρόκειται για επίθεση παρόμοια με την προηγούμενη, με τη διαφορά όμως ότι ο υποκλοπέας μπορεί να αλλάξει τις επιλογές των κρυπτογραφημένων κειμένων κατά τη διάρκεια της επίθεσης.
6. Επίθεση στο κρυπτογραφημένο κείμενο (Cipher text – only attack). Σε αυτού του είδους την επίθεση ο υποκλοπέας προσπαθεί να ανακαλύψει το κλειδί αποκρυπτογράφησης ή το αρχικό κείμενο γνωρίζοντας μόνο το κρυπτογραφημένο κείμενο. Είναι προφανές ότι ένα τέτοιο κρυπτογραφικό σύστημα, ευάλωτο σε τέτοιες επιθέσεις, είναι τελείως ανασφαλές.

Ολοκληρώνοντας, αξίζει να αναφερθεί ότι τόσο τα συμβατικά (συμμετρικά) συστήματα όσο και τα συστήματα δημοσίου κλειδιού (μη συμμετρικά) παρουσιάζουν πλεονεκτήματα και μειονεκτήματα. Συνήθως, τα πλεονεκτήματα των συμμετρικών κρυπτογραφικών συστημάτων είναι μειονεκτήματα των μη συμμετρικών κρυπτογραφικών συστημάτων και αντίστοιχα ισχύουν για τα μειονεκτήματα των πρώτων συστημάτων σε σχέση με αυτά των δεύτερων.

Πιο αναλυτικά:

**Πλεονεκτήματα συμβατικών (συμμετρικών) κρυπτογραφικών συστημάτων**

* Τα συμμετρικά κρυπτογραφικά συστήματα είναι παλαιότερα των μη συμμετρικών και συνεπώς περισσότερο χρόνο δοκιμασμένα στην πράξη.
* Τα κλειδιά που χρησιμοποιούνται είναι σχετικά μικρά και συνεπώς βρίσκουν πολύ εύκολα εφαρμογή και σε ποιο οικονομικές περιπτώσεις, όπως για παράδειγμα τα κινητά τηλέφωνα.
* Πολύ γρήγορη κρυπτογράφηση (π.χ. εκατοντάδες Mbytes είναι δυνατό να κρυπτογραφηθούν σε δευτερόλεπτα).
* Είναι δυνατή η χρήση τους στις γεννήτριες τυχαίων αριθμών ή συναρτήσεων κατακερματισμού.
* Τέλος, υπάρχει η δυνατότητα να χρησιμοποιηθούν συνδυαστικά μεταξύ τους και να δώσουν ακόμη πιο ισχυρούς συμμετρικούς αλγόριθμους.

**Μειονεκτήματα συμβατικών (συμμετρικών) κρυπτογραφικών συστημάτων**

* Για την κατά το δυνατό μεγαλύτερη ασφάλεια των συστημάτων αυτών, απαιτείται ένας καλός και ασφαλής δίαυλος επικοινωνίας στην ανταλλαγή των κλειδιών.
* Κάθε κλειδί που χρησιμοποιείται μεταξύ δύο χρηστών θα πρέπει να αντικαθίσταται αρκετά συχνά.
* Ανάμεσα σε δύο χρήστες απαιτείται ένα κλειδί. Συνεπώς σε περίπτωση δικτύου n χρηστών απαιτούνται κλειδιά.
* Για να γίνει αποδοτικά η διαχείριση των μυστικών κλειδιών απαιτείται και η ύπαρξη ενός άνευ όρων Έμπιστου Τρίτου Μέλους - ΤΤΡ.
* Τέλος, σημειώνεται ότι οι ψηφιακές υπογραφές, με τις οποίες θα ασχοληθούμε στη συνέχεια και οι οποίες βασίζονται στα συμμετρικά κρυπτογραφικά συστήματα, απαιτούν είτε την ύπαρξη ενός Έμπιστου Τρίτου Μέλους – ΤΤΡ είτε την ύπαρξη μεγάλων κλειδιών.

Αντίστοιχα, τα πλεονεκτήματα και τα μειονεκτήματα των κρυπτογραφικών συστημάτων δημόσιου κλειδιού έχουν ως εξής:

**Πλεονεκτήματα κρυπτογραφικών συστημάτων δημοσίου κλειδιού (μη συμμετρικά συστήματα)**

* Δεν υπάρχει απαίτηση ασφαλούς δίαυλου επικοινωνίας.
* Δε θεωρείται απαραίτητη η αλλαγή των ζευγών των κλειδιών (δημόσιου και ιδιωτικού) ακόμα και για μεγάλο χρονικό διάστημα.
* Σε δίκτυα όπου ο αριθμός των χρηστών είναι n, τα κλειδιά που χρησιμοποιούνται είναι 2n. Έτσι σε σχέση με τα συμμετρικά κρυπτογραφικά συστήματα πολλών χρηστών, τα μη συμμετρικά απαιτούν πολύ μικρότερο αριθμό κλειδιών.
* Για να γίνει αποδοτική η διαχείριση των κλειδιών στα μη συμμετρικά κρυπτογραφικά συστήματα δεν απαιτείται η ύπαρξη ενός άνευ όρων Έμπιστου Τρίτου Μέλους, αλλά αρκεί η ύπαρξη ενός λειτουργικά Έμπιστου Τρίτου Μέλους.
* Τέλος, σημειώνεται ότι οι αλγόριθμοι δημιουργίας ψηφιακών υπογραφών που βασίζονται σε τεχνικές δημοσίου κλειδιού είναι πολύ πιο αποδοτικοί από τους αντίστοιχους των συμμετρικών αλγορίθμων.

**Μειονεκτήματα κρυπτογραφικών συστημάτων δημοσίου κλειδιού (μη συμμετρικά συστήματα)**

* Τα συστήματα αυτά είναι κατά πολύ νεότερα των συμμετρικών και δεν έχουν δοκιμαστεί τόσο πολύ.
* Τα κλειδιά που χρησιμοποιούνται (δημόσια και ιδιωτικά) είναι αρκετά μεγάλα.
* Η διαδικασία κρυπτογράφησης – αποκρυπτογράφησης είναι περισσότερο χρονοβόρα από ότι αυτή των συμμετρικών κρυπτογραφικών συστημάτων.
* Η ασφάλειά τους βασίζεται στη θεωρία αριθμών, των οποίων η επίλυση θεωρείται πολύ δύσκολη, πράγμα όμως που ακόμα δεν έχει αποδειχθεί τουλάχιστον θεωρητικά.

Στην πράξη τα συμμετρικά κρυπτογραφικά συστήματα βρίσκουν περισσότερες εφαρμογές, ενώ εκείνα του δημοσίου κλειδιού χρησιμοποιούνται κυρίως για την εγκατάσταση συμμετρικών κλειδιών και για τη δημιουργία ψηφιακών υπογραφών. Έτσι, συνδυάζονται τα πλεονεκτήματα και των δύο περιπτώσεων.

* + 1. Κρυπτογραφικά Πρωτόκολλα και Αλγόριθμοι

Στην συγκεκριμένη ενότητα θα ασχοληθούμε με τις πιο κυριότερες κρυπτογραφικές εφαρμογές.

* + - 1. Ψηφιακές Υπογραφές

Οι ψηφιακές υπογραφές (digital signatures), όπως και οι κοινές υπογραφές που χρησιμοποιούνται καθημερινά, αποτελούν ένα αξιόπιστο μέσο που συνδέει μία συγκεκριμένη οντότητα με μία συγκεκριμένη πληροφορία. Οι υπογραφές αυτές είναι στενά συνδεδεμένες με τις έννοιες της πιστοποίησης και της μη αποποίησης.

Κάθε πρωτόκολλο ψηφιακής υπογραφής αποτελείται στην ουσία από δύο αλγόριθμους, αυτόν της δημιουργίας της ψηφιακής υπογραφής και αυτόν της επαλήθευσής της. Ας το δούμε όμως αυτό μέσω ενός παραδείγματος. Έστω ότι η Alice θέλει να υπογράψει ένα μήνυμα m και να το στείλει στον Bob. Η υπογραφή της Alice είναι στην ουσία το αποτέλεσμα ενός αλγορίθμου, μίας συνάρτησης πιο απλά, έστω SA. Η είσοδος στη συνάρτηση είναι το μήνυμα της Alice, m, ενώ η έξοδος αυτής είναι η υπογραφή της Alice και η οποία εξαρτάται με κάποιο συγκεκριμένο τρόπο από μία πληροφορία που έχει στην κατοχή της μόνο η Alice. Η πληροφορία αυτή μπορεί να είναι το ιδιωτικό της κλειδί. Η έξοδος της συνάρτησης είναι: s = SA(m) και είναι η υπογραφή της Alice πάνω στο μήνυμα m προς τον Bob. Με τη σειρά του ο Bob λαμβάνει το ζευγάρι (s,m) και χρησιμοποιώντας μία δική του συνάρτηση –αλγόριθμο- (VA) λαμβάνει ένα αποτέλεσμα έστω u = VA (s,m). Το αποτέλεσμα αυτό μπορεί να πάρει τιμές 0 και 1, κάτι που εξαρτάται από μία δημόσια πληροφορία της Alice, όπως για παράδειγμα το δημόσιο κλειδί της. Εάν η τιμή της συνάρτησης του Bob ισοδυναμεί με τον αριθμό 1, τότε σημαίνει ότι αυτή είναι η ψηφιακή υπογραφή της Alice και γίνεται δεκτή από τον Bob. Σε αντίθετη περίπτωση αυτή απορρίπτεται.

Είναι πλέον φανερό ότι για να είναι κρυπτογραφικά ασφαλείς οι αλγόριθμοι δημιουργίας της ψηφιακής υπογραφής και επαλήθευσης αυτής, θα πρέπει να ικανοποιούνται οι πιο κάτω προϋποθέσεις:

* Μία ψηφιακή υπογραφή είναι έγκυρη μόνο εφόσον ο αλγόριθμος επαλήθευσης επιστρέφει την τιμή 1.
* Θα πρέπει να είναι υπολογιστικά αδύνατο για οποιονδήποτε χρήστη εκτός του υπογράφοντος, να δημιουργήσει μια ψηφιακή υπογραφή για την οποία το αποτέλεσμα της συνάρτησης VΑ του παραλήπτη να είναι εσφαλμένα ίσο με την τιμή 1.

Στα πρωτόκολλα ψηφιακών υπογραφών υπάρχει συνήθως ένα λειτουργικά έμπιστο τρίτο μέλος (ΤΤΡ). Το μέλος αυτό, στο παραπάνω παράδειγμα, θα επέλυε διαφωνίες του τύπου: η Alice αρνείται ότι υπέγραψε κάποιο μήνυμα ή ακόμα και τον ψευδή ισχυρισμό του Bob ότι έλαβε κάποιο μήνυμα από την Alice. Με τις ψηφιακές υπογραφές θα ασχοληθούμε στη συνέχεια.

* 1. Προσωπικά Δεδομένα και Ιδιωτικότητα

Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και το Νόμο 2472/1997 τα **Προσωπικά Δεδομένα** **ή Δεδομένα προσωπικού χαρακτήρα είναι**[[4]](#footnote-4)**:**

**“κ**άθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο εν ζωή, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες.”

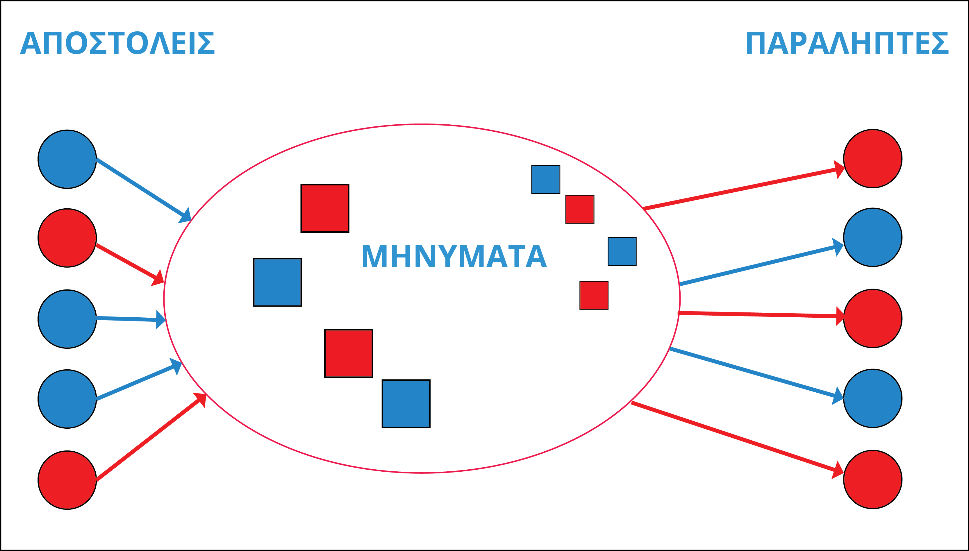
Επιπροσθέτως, εκτός από τα Δεδομένα προσωπικού χαρακτήρα υπάρχουν και τα **Ευαίσθητα προσωπικά δεδομένα** τα οποία προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα και ορίζονται ως[[5]](#footnote-5):

**“**τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.”

Από τη σκοπιά της πληροφορικής και της επικοινωνίας εντός δικτύου υπολογιστών η οντοτήτων αναφέρεται πολύ συχνά ο όρος **ιδιωτικότητα** και πιο συγκεκριμένα **προστασία της ιδιωτικότητας**. Στη συγκεκριμένη περίπτωση δεν αρκεί η Ελληνική ή αντίστοιχα η Ευρωπαϊκή νομοθεσία[[6]](#footnote-6) για να προστατέψει τα απλά και τα ευαίσθητα προσωπικά δεδομένα αλλά γίνεται λόγος κυρίως για τις τεχνολογίες που δημιουργήθηκαν για τον παραπάνω σκοπό. Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθούμε σε κάποιους περαιτέρω όρους που συνθέτουν την έννοια της ιδιωτικότητας. Οι όροι είναι βασισμένοι σε ένα **περιβάλλον**, όπου κάποιος χρήστης-αποστολέας στέλνει μηνύματα σε κάποιον ή κάποιους παραλήπτες μέσω ενός δικτύου επικοινωνίας. Εκτός από τις έννοιες του αποστολέα και παραλήπτη, **μια ενεργή οντότητα** μπορεί να είναι φυσικό πρόσωπο, νομικό πρόσωπο, υπολογιστής, ή διεργασία ενώ **ένα σύνολο ενεργών οντοτήτων** μπορεί να είναι ένας οργανισμός που δρα ως νομικό πρόσωπο δομημένο όμως από ενεργές οντότητες. Η έννοια του περιβάλλοντος μπορεί να γίνει ακόμη πιο σαφής με χρήση του συστήματος, το οποίο έχει τις εξής ιδιότητες:

* Το σύστημα έχει ένα εξωτερικό περιβάλλον, δηλ. τμήμα του κόσμου που βρίσκεται εκτός του συστήματος
* Η κατάσταση του συστήματος μπορεί να αλλάξει ανάλογα με τις ενέργειες εντός του συστήματος

Από την άλλη πλευρά ο επιτιθέμενος χρήστης ενδιαφέρεται για την παρακολούθηση όλων των επικοινωνιών εντός τους συστήματος, την καταγραφή των προτύπων επικοινωνίας που χρησιμοποιούνται με τελικό σκοπό τη χειραγώγηση της επικοινωνίας. Ακόμη υποθέτουμε ότι ο επιτιθέμενος χρήστης μπορεί να βρίσκεται εκτός του συστήματος και να παρακολουθεί τις γραμμές επικοινωνίας, ή να βρίσκεται εντός του συστήματος και να ελέγχει σταθμούς εργασίας. Η χειραγώγηση της επικοινωνίας αφορά την αξιοποίηση όλων των παραπάνω πληροφοριών ώστε να καταλήξει στα στοιχεία που ενδιαφέρουν γνωστά και ως *Items of Interest - IOIs*, π.χ.ποιος έστειλε, ποιος παρέλαβε, ποια μηνύματα[[7]](#footnote-7).



Σχήμα 1. Δίκτυο Επικοινωνίας ανταλλαγής μηνυμάτων με επιτιθέμενους

Όπως αναφέραμε η έννοια της ιδιωτικότητας συντίθεται από αρκετούς όρους και **απαιτήσεις** που εκτός των παραπάνω μερικές επιπρόσθετες αλλά εξίσου σημαντικές είναι οι εξής [Λαµ10]:

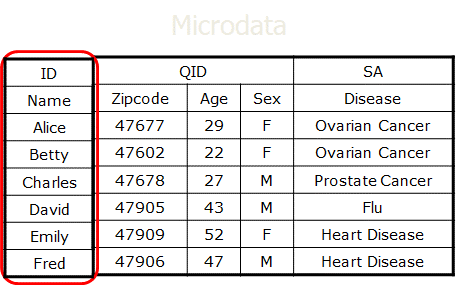
* Ανωνυμία
* Μη-Συνδεσιμότητα
* Ψευδωνυμία
* Διαχείριση Ταυτότητας
  + 1. Ανωνυμία

**Ανωνυμία** μιας οντότητας, σημαίνει ότι η οντότητα δεν είναι αναγνωρίσιμη δηλαδή δε διαφαίνονται τα μοναδικά της χαρακτηριστικά μέσα σε ένα σύνολο ανωνύμων οντοτήτων. Η ανωνυμία εξαρτάται από τη γνώση του εκάστοτε επιτιθέμενου και σε γενικές γραμμές εξασφαλίζει τη μη αποκάλυψη της ταυτότητας του χρήστη κατά την πρόσβαση σε δεδομένα ή υπηρεσίες. Βέβαια η ανωνυμία δεν αφορά την προστασία της ταυτότητας μιας οποιασδήποτε οντότητας-χρήστη αλλά προορίζεται για να επιβάλει στις οντότητες-χρήστες να μην μπορούν να ανακτήσουν την ταυτότητα του χρήστη-οντότητας μέσω της σύνδεσής του στο δίκτυο επικοινωνίας. Ο αποστολέας αλλά και ο παραλήπτης μπορεί να παραμένει ανώνυμος μόνον εντός ενός συνόλου αποστολέων και του συνόλου παραληπτών. Ακόμη, θεωρείται ως δεδομένο ότι ο επιτιθέμενος δεν ξεχνά καμία πληροφορία και η γνώση του συνεχώς αυξάνεται.

Ο επιτιθέμενος διατηρεί το δικό του σύνολο ανώνυμων οντοτήτων και στην περίπτωση όπου νέες οντότητες εισέρχονται στο σύστημα μετά από τον επιτιθέμενο, αυτές δε θα ανήκουν στο σύνολο ανωνύμων οντοτήτων του. Αν όμως δεν είναι γνωστός ο χρόνος εισαγωγής των οντοτήτων στο σύστημα, τότε το σύνολο των ανωνύμων οντοτήτων για τον επιτιθέμενο παραμένει σταθερό. Συμπερασματικά, ανωνυμία για μια οντότητα, σημαίνει ότι ο επιτιθέμενος δεν μπορεί να προσδιορίσει με ακρίβεια την οντότητα μέσα σε ένα σύνολο οντοτήτων. Τέλος μία συνολική ανωνυμία είναι ισχυρή όσο πιο ευρύ είναι το αντίστοιχο σύνολο ανωνύμων οντοτήτων και όσο πιο ισορροπημένη είναι η αποστολή και παραλαβή μηνυμάτων μεταξύ των οντοτήτων του συνόλου και συνεπώς ολόκληρου του συστήματος.

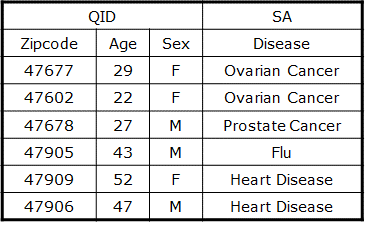
Microdata

Προσοχή όμως! Η ανωνυμία δεδομένων δεν διασφαλίζει, κατ’ ανάγκη, και την ιδιωτικότητα! Ας δούμε το εξής παράδειγμα μίας ιατρικής βάσης δεδομένων:

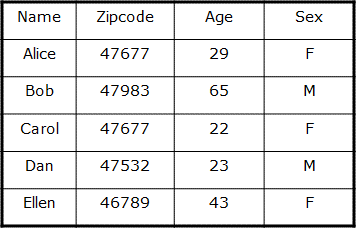


Η στήλη ID (Identity) περιέχει τα στοιχεία που *ταυτοποιούν* τον ασθενή πλήρως, π.χ. ονοματεπώνυμο και πατρώνυμο, ΑΜΚΑ, ΑΦΜ, αριθμός ταυτότητας κ.λπ. Οι στήλες QID (Quasi Identifier) περιέχουν στοιχεία που αποτελούν κάποια *μη ευαίσθητα* στοιχεία του ασθενούς που τον αφορούν αλλά δεν τον ταυτοποιούν. Τέλος τα στοιχεία στη στήλη SA (Sensitive Attributes). Προφανώς, δεν πρέπει, με κανέναν τρόπο, να διαρρεύσουν τα στοιχεία στη στήλη SA καθώς προδίδουν τις παθήσεις των ασθενών.

Δείτε, τώρα, τον εξής ανωνυμοποιημένο πίνακα:



Κάποιος που βλέπει τον πίνακα αυτό συμπεραίνει ότι δεν είναι εφικτή η ταυτοποίηση ασθενών και η αποκάλυψη της πάθησής τους. Υποθέστε, όμως, ότι έχει αναρτηθεί κάπου στο διαδίκτυο ο εξής κατάλογος συμμετεχόντων π.χ. σε μία διαδικασία ψηφοφορίας ή συμμετοχής σε μία διαβούλευση, ο οποίος δεν περιέχει ευαίσθητα προσωπικά δεδομένα:



Φαινομενικά, από τους δύο προηγούμενους πίνακες δεν διαρρέει κάποια ευαίσθητη πληροφορία, δηλαδή ασθένεια κάποιου ασθενούς: ο πρώτος περιέχει *ανωνυμοποιημένη* πληροφορία και ο δεύτερος περιέχει *μη ευαίσθητη* πληροφορία. Μία πιο προσεκτική εξέταση, όμως, των δύο πινάκων *συνδυασμένα*, αποκαλύπτει την ασθένεια της Αλίκης! Προσέξτε τις δύο πρώτες γραμμές των δύο πινάκων. Ο δεύτερος πίνακας βοηθά, με τα δεδομένα στις στήλες QID, να συνδεθεί (*identification through linking* ονομάζεται το αποτέλεσμα της σύνδεσης αυτής) το όνομα της Αλίκης με την εγγραφή του πρώτου πίνακα, αναιρώντας την ανωνυμία του πρώτου πίνακα όσον αφορά την Αλίκη. Το δίδαγμα είναι ότι τα ανώνυμα δεδομένα μπορεί να μην είναι και τόσο ανώνυμα τελικά!

* + 1. Μη–συνδεσιμότητα

Η **μη–συνδεσιμότητα** δύο ή περισσότερων οντοτήτων, μηνυμάτων ή συμβάντων σημαίνει ότι, ο επιτιθέμενος στο σύστημά μας, δε βρίσκεται σε θέση να κατανοήσει αν τα παραπάνω στοιχεία συνδέονται μεταξύ τους. Με λίγα λόγια η μη-συνδεσιμότητα εξασφαλίζει ότι οι οντότητες ενός συστήματος δεν είναι σε θέση να εξακριβώσουν αν ένας χρήστης έχει λάβει μέρος σε συγκεκριμένες διαδικασίες εντός του συστήματος.

Η μέτρηση της μη–συνδεσιμότητας δύο ή περισσοτέρων IOIs προσδιορίζεται από τη διαφορά ανάμεσα στις παρατηρήσεις του επιτιθέμενου, δηλαδή *Μη συνδεσιμότητα= Νέα Γνώση – Προγενέστερη Γνώση.* Η διατήρηση της μη-συνδεσιμότητας μιας οντότητας παραμένει σταθερή όταν η παραπάνω σχέση είναι μηδέν. Για να ισχύει η Μη συνδεσιμότητα, δε θα πρέπει σε καμία περίπτωση το αποτέλεσμα της παραπάνω σχέσης να είναι θετικό. Μία τέτοια περίπτωση θα σήμαινε ότι η ικανότητα του επιτιθέμενου να συσχετίσει τα στοιχεία εντός του συστήματος έχει αυξηθεί.

Η Ανωνυμία και η Μη-συνδεσιμότητα είναι δύο έννοιες άρρηκτα συνδεδεμένες. Για την περιγραφή αυτής της σύνδεσης συνήθως μας ενδιαφέρει να προσδιορίσουμε: «Ποιος έχει αποστείλει ή παραλάβει, ποια μηνύματα;». Πιο αναλυτικά, μας ενδιαφέρει ο αποστολέας έστω s να είναι ανώνυμος σε σχέση με την αποστολή ενός συγκεκριμένου μηνύματος m, καθώς και να είναι ανώνυμος εντός του συνόλου των ανώνυμων αποστολέων. Το ίδιο ισχύει προφανώς και για ένα σύνολο από μηνύματα M καθώς και για το σύνολο των παραληπτών R. Ανωνυμία Αποστολέα ορίζεται ότι κάθε μήνυμα σχετικό με τον εν δυνάμει αποστολέα είναι μη συνδέσιμο ενώ αντιστοίχως Ανωνυμία Παραλήπτη ορίζεται ότι κάθε μήνυμα σχετικό με τον εν δυνάμει παραλήπτη είναι μη συνδέσιμο. Ακόμη, Ανωνυμία Σχέσης ορίζεται η μη ανιχνεύσιμη επικοινωνία ανάμεσα σε αποστολέα και παραλήπτη, δηλαδή ο αποστολέας και ο παραλήπτης είναι μη-συνδέσιμοι. Τέλος ως Σύνολο Ανωνύμων Σχέσεων ορίζεται το καρτεσιανό γινόμενο δύο διαφορετικών συνόλων. Για παράδειγμα όταν μία οντότητα στέλνει ή λαμβάνει ένα μήνυμα, το σύνολο ανωνύμων σχέσεων είναι το σύνολο όλων των πιθανών παραληπτών ή αποστολέων του συγκεκριμένου μηνύματος.

* + 1. Ψευδωνυμία

H **Ψευδωνυμία** αφορά τη δημιουργία ενός προσδιοριστικού, δηλαδή ενός ψευδωνύμου, που απευθύνεται σε ένα αποστολέα ή παραλήπτη αντί για το πραγματικό του όνομα. Το συγκεκριμένο προσδιοριστικό μπορεί να είναι κάποιο τυχαίο όνομα ή μία ακολουθία από bits και είναι ανεξάρτητο από το πραγματικό όνομα της οντότητας ή των ιδιοτήτων της. Κάτοχος του ψευδωνύμου ονομάζεται η οντότητα στην οποία αναφέρεται και η οποία χρησιμοποιεί το ψευδώνυμο. Υπάρχουν δύο είδη ψευδωνύμων: *το Αποκλειστικό* και *το Μεταβιβάσιμο* ψευδώνυμο. Το αποκλειστικό αναφέρεται σε ένα μοναδικό κάτοχο, δε μεταβιβάζεται σε άλλες οντότητες και είναι αμετάβλητο ενώ το μεταβιβάσιμο μπορεί να μεταβιβαστεί από έναν κάτοχο σε άλλη οντότητα, η οποία θα είναι πλέον ο νέος κάτοχος.

Με την ψευδωνυμία εξασφαλίζεται ότι η οντότητα-χρήστης μπορεί να προσπελάσει δεδομένα ή υπηρεσίες χωρίς να πρέπει να αποκαλύψει την ταυτότητα του και χωρίς να μπορεί να προσδιοριστεί η ταυτότητά του από ένα σύνολο οντοτήτων. Παρόλα αυτά η οντότητα-χρήστης είναι υπόλογος για την ενέργειά του και μπορεί να του αποδοθεί ευθύνη. Όσον αφορά την ανωνυμία της οντότητας, σε αυτό το σημείο θα πρέπει να αποσαφηνιστεί πρώτα η διαφορά των όρων ανώνυμος και ψευδώνυμος. Ο όρος ανώνυμος αφορά την ιδιότητα μιας οντότητας συγκριτικά με την αναγνωρισιμότητα, ενώ ο όρος ψευδώνυμος αφορά τη χρήση κάποιου μηχανισμού, όπως χρήση προσδιοριστικών. Γενικά όσο πιο μικρή είναι η γνώση για τη σχέση ψευδωνύμου-κατόχου, τόσο πιο ισχυρή είναι η ανωνυμία. Από την άλλη πλευρά η ισχύς της ανωνυμίας θα μειώνεται όσο αυξάνει η γνώση για τη σχέση ψευδωνύμου-κατόχου.

Συμπερασματικά η ανωνυμία θα είναι πιο ισχυρή εάν έχουμε στην διάθεσή μας όσο το δυνατόν λιγότερες προσωπικές πληροφορίες του κατόχου του ψευδωνύμου που σχετίζονται με το ψευδώνυμο. Επιπλέον όσο λιγότερο χρησιμοποιούνται τα ψευδώνυμα και σε όσο το δυνατόν λιγότερες διαδικασίες τόσο πιο λίγες πληροφορίες για τον κάτοχο μπορούν να συσχετιστούν με αυτά. Το ίδιο προφανώς ισχύει ένα επιλέγονται αρκετά συχνά ψευδώνυμα με τυχαίο και ανεξάρτητο τρόπο για νέες χρήσεις.

* + 1. Διαχείριση Ταυτότητας

Η **Ταυτότητα** αφορά ένα υποσύνολο των ιδιοτήτων κάποιας οντότητα, είτε αυτή είναι φυσικό ή νομικό πρόσωπο, είτε υπολογιστής, είτε διεργασία και η οποία προσδιορίζει επακριβώς το πρόσωπο αυτό, σε ένα σύνολο προσώπων. Επειδή οι τιμές των ιδιοτήτων ή ακόμα και οι ιδιότητες μπορεί να αλλάζουν μέσα στο χρόνο δεν υφίσταται μία μοναδική ταυτότητα, αλλά πολλαπλές. Η Ψηφιακή ταυτότητα αφορά την απόδοση ιδιοτήτων σε μία συγκεκριμένη οντότητα και η οποία είναι άμεσα αξιοποιήσιμη (π.χ. το email σε μία λίστα).

Σε αντιστοιχία με το σύνολο των ανωνύμων οντοτήτων, μπορούμε να χρησιμοποιήσουμε και το σύνολο των αναγνωρίσιμων οντοτήτων προκειμένου να περιγράψουμε πιο αναλυτικά την ταυτότητα και την αναγνωρισιμότητα των οντοτήτων. Η αναγνωρισιμότητα μίας οντότητας αφορά στην ικανότητα του επιτιθέμενου να αναγνωρίσει την οντότητα ανάμεσα σε ένα σύνολο οντοτήτων.

Η **Διαχείριση Ταυτότητας** αφορά την προστασία της ιδιωτικότητας εφόσον διαφυλάττεται πλήρως η μη-συνδεσιμότητα μεταξύ των ταυτοτήτων. Η διαχείριση της ταυτότητας επιτυγχάνεται μέσω των συστημάτων διαχείρισης ταυτότητας (IMS), δηλαδή διάφορα εργαλεία, εφαρμογές και υποδομές που μπορούν να εγκατασταθούν και να λειτουργήσουν τόσο στην πλευρά του user όσο και του server και να λειτουργούν συνεργατικά. Τα συγκεκριμένα συστήματα ενισχύουν και προστατεύουν την ιδιωτικότητα όταν με βάση τους περιορισμούς από ένα σύνολο εφαρμογών λογισμικού, προστατεύουν τη μη-συνδεσιμότητα ανάμεσα σε ταυτότητες και τα αντίστοιχα ψευδώνυμα ενός φυσικού προσώπου.

Σε όλες τις παραπάνω απαιτήσεις θα μπορούσε να ενταχθεί και η **μη-παρατηρησιμότητα** η οποία και συναντάται στη βιβλιογραφία [Pfi10] ως τέταρτη απαίτηση έναντι της διαχείρισης ταυτότητας. Η μη-παρατηρησιμότητα στην ουσία χρησιμοποιεί ένα φάσμα ισχυρών μηχανισμών για να προστατεύσει την ιδιωτικότητα των χρηστών από επιτιθέμενους. Απαγορεύει δηλαδή στους επιτιθέμενους να παρατηρήσουν ή ανιχνεύσουν τους χρήστες τη στιγμή χρησιμοποιούν μια υπηρεσία πχ όταν περιηγούνται στο διαδίκτυο. Τέλος θα μπορούσαμε να θεωρήσουμε την μη-παρατηρησιμότητα ως υποκατηγορία της ανωνυμίας και της μη συνδεσιμότητας.

* 1. Απαιτήσεις Ταυτοποίησης

Πριν προχωρήσουμε στις τεχνολογίες προστασίας της ιδιωτικότητας (PETS) αρκεί να αναφερθούμε συνοπτικά σε δύο κλασσικές απαιτήσεις ταυτοποίησης χρηστών με προστασία της ιδιωτικότητας. Οι συγκεκριμένες απαιτήσεις ανήκουν και αυτές στο ευρύτερο φάσμα των απαιτήσεων της ιδιωτικότητας και θα μπορούσαν να αναφερθούν παραπάνω, όμως για διευκόλυνση εισαγωγής νέας ορολογίας και για λόγους παρουσίασης τις αναφέρουμε εδώ. **Ταυτοποίηση** μιας οντότητας καλείται η διαδικασία εκείνη, κατά την οποία η οντότητα παρέχει σε ένα Πληροφοριακό Σύστημα τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί µε μία οντότητα η οποία και δικαιούται προσπέλασης στους πόρους του.

* + 1. Αυθεντικοποίηση

**Αυθεντικοποίηση** μίας οντότητας, καλείται η διαδικασία εκείνη, κατά την οποία η ίδια η οντότητας παρέχει σε ένα Πληροφοριακό Σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης. Με λίγα λόγια είναι η διαδικασία επιβεβαίωσης της ταυτότητας μιας οντότητας. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης ενώ αποτελεί κυρίως απαίτηση ασφάλειας, παρά ιδιωτικότητας ενός συστήματος.

* + 1. Εξουσιοδότηση

**Εξουσιοδότηση** σε μία οντότητα ορίζεται η διαδικασία κατά την οποία η οντότητα αποκτά δικαιώματα σε μια μεμονωμένη υπηρεσία ή σε ένα σύνολο υπηρεσιών ενός Πληροφοριακού Συστήματος. Σε ένα Πληροφοριακό Σύστημα με πολλούς χρήστες, ο διαχειριστής έχει το δικαίωμα να εξουσιοδοτεί τον κάθε χρήστη με αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους μέσα στο σύστημα.

Εν κατακλείδι θα μπορούσαμε να ισχυριστούμε ότι μέσω της αυθεντικοποίηση ελέγχεται η ταυτότητα μίας οντότητας με τις κατάλληλες εξουσιοδοτήσεις (δικαιώματα) και ταυτοποιείται ως ενεργός χρήστης του συστήματος.

1. ο Κεφάλαιο – Τεχνολογίες Προστασίας Ιδιωτικότητας
   1. Εισαγωγή

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο η προστασία της ιδιωτικότητας επιτυγχάνεται κατά κύριος λόγο μέσα από τη Νομοθεσία για την προστασία των προσωπικών δεδομένων. Εκτός όμως από τη Νομοθεσία η ιδιωτικότητα προστατεύεται από διάφορους κώδικες δεοντολογίας που ακολουθούνται από επιχειρήσεις και από την υιοθέτηση διαφόρων τεχνολογιών προστασίας της ιδιωτικότητας από τους ίδιους τους χρήστες-καταναλωτές. Στο κεφάλαιο αυτό μελετώνται αυτές οι τεχνολογίες γνωστές και ως PETs (Privacy Enhancing Technologies) [Bla03]. Πρόκειται δηλαδή για ένα σύνολο εργαλείων και τεχνολογιών (λογισμικά) που βοηθούν τους χρήστες να προστατεύουν τα προσωπικά τους δεδομένα καθώς και να διατηρούν την ιδιωτικότητα και την ανωνυμία τους. Απώτεροι στόχοι είναι η ελαχιστοποίηση της αποκάλυψης και της συλλογής των προσωπικών δεδομένων των χρηστών σε τρίτους χρήστες (επιτιθέμενοι), η διεκπεραίωση συναλλαγών χωρίς την αποκάλυψη της ταυτότητας των χρηστών αλλά και η ελευθερία διαχείρισης των προσωπικών δεδομένων των χρηστών από τους ίδιους τους χρήστες. Στις επόμενες ενότητες θα αναφερόμαστε στο διαδίκτυο ως το σύστημα ή το περιβάλλον μέσα στο οποίο δρουν οι οντότητες-χρήστες.

* + 1. Συλλογή Δεδομένων

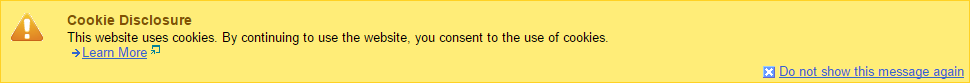
Όπως αναφέραμε και στην εισαγωγή η συλλογή δεδομένων είναι μία διαδικασία η οποία θα πρέπει να ελαχιστοποιείται ή να εξαλείφεται προκειμένου να διατηρείται η ιδιωτικότητα και η ανωνυμία των χρηστών. Η συλλογή δεδομένων στο διαδίκτυο μπορεί να γίνει με 2 τρόπους:

* Παθητική συλλογή προσωπικών δεδομένων και δεδομένων συναλλαγών
* Ενεργητική συλλογή προσωπικών δεδομένων και δεδομένων συναλλαγών

Στην παθητική συλλογή προσωπικών δεδομένων οι διαδικτυακοί εξυπηρετητές συλλέγουν προσωπικά δεδομένα του χρήστη, εν αγνοία του χρήστη. Με τέτοια περίπτωση είναι για παράδειγμα όταν ο φυλλομετρητής του χρήστη έχει ρυθμιστεί να αποθηκεύει το όνομα ή την διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη. Όσον αφορά τη συλλογή δεδομένων συναλλαγών, οι διαδικτυακοί εξυπηρετητές συλλέγουν δεδομένα πλοήγησης στο διαδίκτυο όπως τις ιστοσελίδες που επισκέφτηκε ο χρήστης, το url τους καθώς και το χρονικό διάστημα παραμονής του. Οι πληροφορίες αυτές δεν αποτελούν προσωπικά δεδομένα ή δεδομένα αναγνώρισης του χρήστη. Χρησιμοποιούνται όμως για σκοπούς marketing, ανάλυσης και βελτίωσης της λειτουργίας μίας ιστοσελίδας από την οπτική πάντα του κατόχου της ιστοσελιδας. Παρόλα αυτά η σύνδεση των χρηστών με προσωπικά δεδομένα (πρόσφατες επισκέψεις, IP διεύθυνση, ονοματεπώνυμο, email κλπ) μπορεί να επιτρέψει την κατασκευή προφίλ χρήστη ούτως ώστε να προβλέπονται οι επόμενες κινήσεις του στο διαδίκτυο.

Στην ενεργητική συλλογή προσωπικών δεδομένων και δεδομένων συναλλαγών διάφορες ιστοσελίδες συλλέγουν στοιχεία μέσω συγκεκριμένων διαδικασιών και τεχνολογιών με την συμμετοχή του χρήστη. Για παράδειγμα κατά τη δημιουργία email λογαριασμών ή λογαριασμών σε διάφορα ηλεκτρονικά καταστήματα ο χρήστης παρέχει πληροφορίες επικοινωνίας, προτιμήσεις καθώς και στοιχεία πιστωτικών καρτών. Ένα ακόμη παράδειγμα είναι η χρήση των διαδικτυακών φορμών για συμμετοχή σε on-line έρευνες, για δωρεάν λογισμικό, για περισσότερες πληροφορίες για προϊόντα και υπηρεσίες κλπ. Υπάρχουν όμως και περιπτώσεις όπου η συλλογή των δεδομένων δεν είναι προφανής στον χρήστη. Παραδείγματα τέτοια αποτελούν τα Web bugs (διαφορετικά Web beacon) τα οποία είναι αρχεία ή μικρές εικόνες που τοποθετούνται σε ιστοσελίδες για να συλλέγουν πληροφορίες για τη χρήση της ίδιας της ιστοσελίδας, την IP διεύθυνση του χρήστη και ανακτούν πληροφορίες που αποθηκεύονται στα cookies του ίδιου του χρήστη. Τα Cookies από της άλλη πλευρά είναι διάφορα αρχεία κειμένου τα οποία εγκαθίστανται στον υπολογιστή του χρήστη από τον διαδικτυακό εξυπηρετητή στον οποίο συνδέεται μέσω του φυλλομετρητή. Με αυτόν τον τρόπο επιτρέπουν στο διαδικτυακό εξυπηρετητή να αποθηκεύσει και να ανακτήσει πληροφορίες για τις σελίδες που επισκέφτηκε ο χρήστης καθώς και για όλες τις επιλογές του χρήστη κατά τη διάρκεια πλοήγησης στο διαδίκτυο. Στο παρελθόν εγκαθίστανται εν αγνοία του χρήστη και χωρίς να δώσει τη συγκατάθεσή του για τη συλλογή των πληροφοριών που τον αφορούν. Το τελευταίο διάστημα όμως ο χρήστης λαμβάνει προειδοποιητικά μηνύματα ως προς της εγκατάσταση των cookies.





Σχήμα 1. Μήνυμα προειδοποίησης αποδοχής cookies στο φυλλομετρητή του χρήστη.

Τέλος τα cookies διακρίνονται σε δύο ευρείες κατηγορίες: Αυτά που παραμένουν στον υπολογιστή του χρήστη μέχρι την ημερομηνία λήξης τους (Persistent cookies) και αυτά που διαγράφονται τον υπολογιστή (Temporary cookies) μετά την διακοπή της σύνδεσης του χρήστη στον διαδικτυακό εξυπηρετητή.

* + 1. Προβλήματα και απειλές κατά της ιδιωτικότητας

Στην προηγούμενη ενότητα αναφέρθηκαν διαδικασίες σχετικά με τη συλλογή των προσωπικών δεδομένων των χρηστών από τρίτους. Οι διαδικασίες αυτές δεν μπορούν πάρα να εμφανίζονται ως απειλές κατά της ιδιωτικότητας και να κατηγοριοποιούνται σε τέσσερις μεγάλες κατηγορίες [Lee12]:

* Απώλεια της εμπιστευτικότητας (loss of confidentiality)
* Κλοπή ταυτότητας (identity theft)
* Αυτόκλητα Μηνύματα – Μη επιθυμητή Επικοινωνία (unsolicited messages – spam)
* Δημιουργία προφίλ χρηστών (user – consumer profiling)

Στην **πρώτη** κατηγορία και στην *απώλεια της εμπιστευτικότητας* γίνεται ανεπιθύμητη εισβολή σε ηλεκτρονικούς φακέλους χρηστών με παράλληλη δημοσίευση προσωπικών δεδομένων σε άγνωστα πρόσωπα.

Στη **δεύτερη** κατηγορία και στην *κλοπή ταυτότητας* γίνεται ανάκτηση πιστοποιητικών και χρήση τους στην εκτέλεση διαφόρων ηλεκτρονικών συναλλαγών αγνοία των χρηστών. Η κλοπή ταυτότητας έχει δυσχερείς οικονομικές συνέπειες οι οποίες και προκαλούνται από ανεξέλεγκτες συναλλαγές με παράλληλη αποκάλυψη πληροφοριών σε τρίτες πηγές. Επιπλέον τα κλεμμένα πιστοποιητικά χρησιμοποιούνται για την έκδοση άλλων πιστοποιητικών κυρίως φυσικών όπως διαβατήρια, άδειες οδήγησης, πιστωτικών καρτών κλπ. Τέλος για την *κλοπή ταυτότητας* ακολουθούνται κάποιες τεχνικές γνωστές ώς phishing ή social engineering οι οποίες προτρέπουν (εξαπατούν) τους χρήστες των ηλεκτρονικών υπηρεσιών προκειμένου να αποκαλύψουν προσωπικές πληροφορίες πρόσβασης στους λογαριασμούς τους. Ένα τέτοιο παράδειγμα αποτελούν διάφορες ιστοσελίδες τραπεζικών ιδρυμάτων με domain names παρόμοια με αυτά των πραγματικών τραπεζικών ιδρυμάτων που έχω ως σκοπό να εξαπατήσουν τους χρήστες τους ώστε να καταχωρίσουν εμπιστευτικές πληροφορίες διαχείρισης των λογαριασμών τους.

Στην **τρίτη** κατηγορία και στη *μη επιθυμητή επικοινωνία* γίνεται αρχικά μαζική αποστολή και προώθηση διαφημιστικών μηνυμάτων προϊόντων και υπηρεσιών μέσω ηλεκτρονικού ταχυδρομείου, sms, newsletters καθότι είναι τα κατάλληλα μέσα μεταφοράς επιβλαβούς λογισμικού. Με αυτόν τον τρόπο και με την ενεργητική συμμετοχή του χρήστη επιτυγχάνεται η παραβίαση της ιδιωτικότητάς του και κατά συνέπεια το επιβλαβές λογισμικό μεταφέρεται σε όλο το δίκτυο επικοινωνίας του.

Στην **τέταρτη** κατηγορία και στη *δημιουργία προφίλ χρηστών* γίνεται συλλογή και καταγραφή όλων των πληροφοριών των χρηστών κατά τη διάρκεια της περιήγησής τους στο διαδίκτυο. Έπειτα επεξεργάζονται, αναλύονται και συσχετίζονται προκειμένου να προσδιοριστεί και να καταγραφεί η συνήθεια των χρηστών καθώς και η καταναλωτική τους συμπεριφοράς.

* + 1. Κατηγορίες και Εργαλεία PETs (Privacy Enhancing Technologies)

Για την προστασία ενός δικτύου επικοινωνίας-συστήματος έχουν δημιουργηθεί διάφορα εργαλεία και τεχνολογίες με σκοπό τη *διαχείριση* και *ενίσχυση* της ιδιωτικότητας των χρηστών. Με λίγα λόγια υποστηρίζουν την διαχείριση των κανόνων της ιδιωτικότητας ενώ παράλληλα αποκρύπτουν πληροφορίες οι οποίες θα μπορούσαν να οδηγήσουν σε άμεση προσωποποίηση των χρηστών.

Για την ενίσχυση της ιδιωτικότητας έχουν αναπτυχθεί τεχνολογίες και εργαλεία όπως: *εργαλεία ψευδωνυμοποίησης* *(pseudonymizer tools), εργαλεία ανωνυμοποίησης (anonymizer products and services), εργαλεία κρυπτογράφησης (encryption tools), φίλτρα και λογισμικό παρεμπόδισης (Filters and blockers)* καθώς και *λογισμικά διαγραφής πειστηρίων και ιχνών (Track and evidence erasers)* ενώ για τη διαχείριση της ιδιωτικότητας έχουν προταθεί δύο υποκατηγορίες εργαλείων, αυτά της *πληροφόρησης (information tools)* και της *διαχείρισης (administrative tools)* [Σιο06] .

Πιο αναλυτικά τα *εργαλεία ψευδωνυμοποίησης* χρησιμοποιούνται για τη δημιουργία ψηφιακών ψευδωνύμων πλοήγησης ούτως ώστε να ικανοποιούνται οι απαιτήσεις των χρηστών για ανώνυμες αγορές και ανώνυμο profiling.

Τα *εργαλεία ανωνυμοποίησης* χρησιμοποιούνται για τη δημιουργία ανώνυμης ηλεκτρονικής αλληλογραφίας μεταξύ των χρηστών με τις πιο γνωστές τεχνολογίες remailers-nymservers / Anonymous / Pseudonymous servers. Στην κατηγορία αυτών των εργαλείων-υπηρεσιών ανήκουν οι Έμπιστες Τρίτες Οντότητες (Trusted Third Parties -TTPs) και τα ψηφιακά πιστοποιητικά (Digital certificates) τα οποία εκδίδουν για την πραγμάτωση μίας επικοινωνίας μεταξύ δύο χρηστών. Επίσης, δε θα πρέπει να παραλείψουμε και τις εικονικές ψηφιακές υπογραφές (Blind digital signatures) οι οποίες εγγυόνται την αυθεντικότητα ενός μηνύματος, αποτελούν ένα είδος ψηφιακών υπογραφών, με τη μόνη διαφορά ότι το περιεχόμενο ενός μηνύματος μεταμφιέζεται (blinded) πριν ακόμη υπογραφεί. Τέλος στα εργαλεία ανωνυμοποίησης ανήκει και το ανώνυμο ψηφιακό χρήμα (Anonymous digital cash) σύμφωνα με το οποίο από την στιγμή που θα γίνει η ανάληψή του από έναν τραπεζικό λογαριασμό, μπορεί να χρησιμοποιηθεί χωρίς να καθίσταται δυνατή η παρακολούθηση της πορείας του από κάποιον τρίτο. Το ανώνυμο χρήμα λειτουργεί με την χρήση αριθμημένων αλλά ανώνυμων τραπεζικών λογαριασμών κάνοντας χρήση εικονικών υπογραφών (blind signatures).

Στα *εργαλεία κρυπτογράφησης* ανήκουν διάφορες υπηρεσίες κρυπτογράφησης ηλεκτρονικών μηνυμάτων, κρυπτογράφησης συναλλαγών και κρυπτογράφησης ηλεκτρονικών εγγράφων και αρχείων. Αξίζει να αναφέρουμε την ψηφιακή στενογραφία και υδατογράφηση ως επιπρόσθετες υπηρεσίες κρυπτογράφησης. Η στεγανογραφία έχει ως σκοπό να αποκρύψει την πληροφορία που πρέπει να αποσταλεί σε κάποιον παραλήπτη μέσα σε ένα μέσο, πχ ένα αρχείο κειμένου μέσα σε μία εικόνα. Η ψηφιακή υδατογράφηση είναι η διαδικασία κατά την οποία δημιουργείται ένα ψηφιακό σήμα (υδατόσημο) με σκοπό να ενσωματωθεί μέσα σε ένα αρχείο ήχου, βίντεο ή εικόνας και αποτελεί μια από τις πιο γνωστές μεθόδους προστασίας για το δημιουργό του αρχείου/προγράμματος

Στα *φίλτρα και στο λογισμικό παρεμπόδισης* ανήκουν διάφορες τεχνολογίες που κατά κύριο λόγο προφυλάσσουν το χρήστη κατά την περιήγησή του στο διαδίκτυο και συναντώνται στην καθημερινότητα σχεδόν όλων των χρηστών του διαδικτύου. Μερικές από αυτές είναι: το φιλτράρισμα των spam emails, το φιλτράρισμα διαδικτυακού περιεχομένου, παρεμπόδιση εμφάνισης αναδυόμενων παραθύρων (adblocks) και από τις πιο σημαντικές τα τείχη προστασίας (firewalls) τα οποία ελέγχουν την κίνηση των δεδομένων στην περίμετρο ενός δικτύου.

Ειδικότερα, το firewall έχει τα εξής πλεονεκτήματα:

* Το firewall απλοποιεί τη διαχείριση ασφάλειας, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο.
* Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το δίκτυο, υλοποιώντας την πολιτική ασφάλειας του οργανισμού.
* Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο.
* Το firewall προστατεύει τα διαφορετικά δίκτυα εντός του ίδιου οργανισμού.
* Το firewall έχει τη δυνατότητα απόκρυψης των πραγματικών διευθύνσεων της επιχείρησης.

Όμως, έχει και τα εξής μειονεκτήματα:

* Το firewall δεν μπορεί να προστατεύσει από προγράμματα-ιούς.
* Το firewall δεν μπορεί να προστατεύσει απέναντι στις επιθέσεις κακόβουλων χρηστών από το εσωτερικό του οργανισμού.
* Το firewall δε μπορεί να προστατέψει τον οργανισμό απέναντι σε επιθέσεις σχετιζόμενες με δεδομένα.
* Το firewall δεν μπορεί να προστατέψει τον οργανισμό από απειλές άγνωστου τύπου.
* Το firewall δεν μπορεί να προστατέψει από συνδέσεις οι οποίες δε διέρχονται από αυτό.
* Η αυστηρή ρύθμιση της ασφάλειας διαμέσου του firewall.

Τώρα, στη *διαγραφή πειστηρίων και ιχνών* ανήκουν διάφορα εργαλεία τα οποία συναντώνται και αυτά στην καθημερινότητα σχεδόν όλων των χρηστών Η/Υ και αφορούν τη προστασία των λειτουργικών συστημάτων από λογισμικά άγνωστης προέλευσης. Έτσι σε αυτή την κατηγορία συγκαταλέγονται: ο εντοπισμός και η διαγραφή επιβλαβούς λογισμικού (antispyware/antivirus), εργαλεία διαχείρισης των Cookies, εργαλεία καθαρισμού του φυλλομετρητή, διαγραφή ιχνών της δραστηριότητας του χρήστη (tracks erasers) και των δεδομένων των σκληρών δίσκων.

Ειδικότερα για τα Cookies, ας δούμε λίγο πιο αναλυτικά τα είδη τους και την λειτουργία τους στις διαδικτυακές υπηρεσίες. Το Cookie είναι ένα ψηφιακό κείμενο (συνήθως μικρού μεγέθους) που αποστέλλεται από έναν web server σε έναν browser ή αποθηκεύεται στο αποθηκευτικό μέσο του web client (π.χ. στο σκληρό δίσκο). Ο κύριος σκοπός ενός cookie είναι να ταυτοποιεί ένα χρήστη και να θυμάται πληροφορίες που σχετίζονται με τις συνεδρίες και τις συναλλαγές του με web servers και διαδικτυακές υπηρεσίες (π.χ. τα προϊόντα που έχουν εισαχθεί στο καλάθι ηλεκτρονικών αγορών σε ένα ηλεκτρονικό κατάστημα). Επίσης, αποθηκεύει πληροφορίες από τη διαδικασία ταυτοποίησης του χρήστη (user login information) έτσι ώστε να μην ζητηθούν πάλι αν γίνει επανασύνδεση.

Κάποια από τα πιο σημαντικά είδη Cookies είναι τα εξής:

1. Session Cookies (cookies συνεδριών). Αποθηκεύονται στην μνήμηκαι έχουν ισχύ για την *τρέχουσα*, μόνο, συνεδρία (είναι *εφήμερα* δηλαδή). Με άλλα λόγια, ισχύουν από τη στιγμή που επισκεπτόμαστε ένα site μέχρι που το αφήνουμε. Παράδειγμα: shopping cart (καλάθι αγορών).
2. Persistent Cookies (μόνιμα cookies): αποθηκεύονται στο αποθηκευτικό μέσο της συσκευής του χρήστη. Αποθηκεύονται για *περισσότερες από μία* συνεδρίες του browser (συνεπώς, αποθηκεύονται στο αποθηκευτικό μέσο, π.χ. σκληρό δίσκο). Τα μόνιμα cookies *παραμένουν* στον browser ακόμα και αφού τον έχετε τερματίσει οπότε την επόμενη φορά που θα ανοίξετε τον browser και προσπελάσετε το site που τοποθέτησε το cookie στο browser σας, θα εντοπίσει το cookie που είχε τοποθετήσει. Παράδειγμα: είδη προϊόντων που είχαμε δει ή γλώσσα που προτιμήσαμε. Τα μόνιμα cookies είναι πολύ χρήσιμα (κρύβουν, όμως, κινδύνους για την ιδιωτικότητά μας).
3. Secure – HTTPS Cookies (ασφαλή cookies). Είναι χρήσιμα μόνο όταν μεταφέρονται δεδομένα μέσω του πρωτοκόλλου https (ασφαλές πρωτόκολλο μεταφοράς δεδομένων). Χρησιμοποιείται για *ασφαλή μετάδοση πληροφοριών* σε κρίσιμες συναλλαγές όπως είναι οι τραπεζικές. Υπάρχει διασφάλιση ότι το cookie είναι πάντα *κρυπτογραφημένο* κατά την μεταφορά μεταξύ server/client. Αυτό καθιστά ένα secure cookie λιγότερο πιθανό να εκτεθεί  
   σε υποκλοπή.
4. HTTPS only cookies. Μπορούν να χρησιμοποιηθούν μόνο από το HTTP πρωτόκολλο. Ένα τέτποιο cookie αυτό περιορίζει την προσπέλασή του πό άλλα μη-HTTP πρωτόκολλα όπως είναι το java script και θεωρείται πιο ασφαλές από τα κοινά cookies.
5. Third party cookies. Τα *πρωτογενή cookie* (first party cookies) αποθηκεύονται από το domain (site) που επισκέπτεστε. Επιτρέπουν στους κατόχους ιστότοπων να συλλέγουν data analytics, να θυμούνται ρυθμίσεις γλώσσας και να εκτελούν άλλες χρήσιμες λειτουργίες που βοηθούν στην προσφορά μιας καλής εμπειρίας χρήσης των υπηρεσιών τους.

Τα *τριτογενή cookie* (third party cookies) τρίτων παρόχων υπηρεσιών, δημιουργούνται από domains διαφορετικά από αυτό που επισκέπτεστε απευθείας, και γι' αυτό ονομάζονται «τρίτων παρόχων». Χρησιμοποιούνται για παρακολούθηση περιηγήσεων μεταξύ *ιστότοπων*, *επαναστόχευση* (retargeting) και *προβολή διαφημίσεων*.

Η ορολογία *δευτερογενή cookie* (second party cookies) δεν είναι ακόμη γενικά παραδεκτή. Τα cookie αυτά μεταφέρονται από μία εταιρία (αυτή που σας έστειλε ένα πρωτογενές cookie) σε άλλη εταιρεία μέσω κάποιου είδους *εταιρικής σχέσης διαμοίρασης δεδομένων*. Για παράδειγμα, μια αεροπορική εταιρεία θα μπορούσε να πουλήσει τα πρωτογενή cookie που έχει στείλει σε πελάτες (αλλά και άλλα πρωτογενή δεδομένα πελατών, όπως είναι όπως ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου κ.λπ.) σε μια αξιόπιστη αλυσίδα ξενοδοχείων για *στοχευμένη* διαφήμιση. Άρα τα cookie αυτά μπορούν να ονομαστούν δευτερογενή.

Από την άλλη πλευρά για τη διαχείριση της ιδιωτικότητας, όπως αναφέρθηκε παραπάνω, συναντούμε δύο μεγάλες κατηγορίες: *τα εργαλεία πληροφόρησης* και τα *εργαλεία διαχείρισης*.

Στην πρώτη κατηγορία και στα *εργαλεία πληροφόρησης* ανήκουν κάποιες υπηρεσίες, όπως *η παραγωγή πολιτικών προστασίας ιδιωτικότητας*. Πιο συγκεκριμένα υπάρχουν εταιρείες οι οποίες αναλαμβάνουν με αυτόματο τρόπο και δημιουργούν πολιτικές προστασίας ιδιωτικότητας, χωρίς τη μεσολάβηση δικηγόρου και προκειμένου να προστεθούν στον εκάστοτε διαδικτυακό τόπο. Στη συνέχεια ο κάθε επισκέπτης, κατά την περιήγησή του στο διαδικτυακό τόπο, μπορεί να τις αναγνώσει, να τις αποδεχθεί (ή και να τις απορρίψει) και να γίνει με αυτό τον τρόπο ενεργός (να συμμορφωθεί) στη διαχείριση των προσωπικών του στοιχείων από το διαδικτυακό τόπο.

Στη δεύτερη κατηγορία και στα *εργαλεία διαχείρισης* ανήκουν υπηρεσίες όπως *η διαχείριση της ταυτότητας (Identity management), οι Βιομετρικές μέθοδοι (Biometrics), οι Έξυπνες κάρτες (Smart cards), η Διαχείριση των δικαιωμάτων πρόσβασης (Permission management), τα Εργαλεία συλλογής και ανάλυσης ψηφιακών πειστηρίων (Forensic tools)* κλπ. Πιο συγκεκριμένα η *διαχείριση ταυτότητας* αφορά τεχνολογικές λύσεις που επιτρέπουν αφενός την μοναδική και αδιαμφισβήτητη ταυτοποίηση του χρήστη και αφετέρου την αδιάβλητη διαχείριση και χρηστή χρήση των δεδομένων που συλλέγουν τα συστήματα δεδομένου ότι είναι ευαίσθητου χαρακτήρα.

Στις *βιομετρικές μεθόδους* εννοούμε όλες εκείνες τις τεχνικές πιστοποίησης της ταυτότητας των χρηστών μέσω της ανάλυσης κάποιων χαρακτηριστικών τους (όπως δακτυλικών αποτυπωμάτων, ανάλυσης της κόρης του ματιού, του DNA, στην ανάλυση συμπεριφοράς, φωνής, υπογραφής κλπ). Στην Ελληνική πραγματικότητα η χρήση των βιομετρικών μεθόδων και όσον αφορά την πρόσβαση ατόμων σε χώρους εργασίας δεν είναι πάντοτε επιτρεπτή καθώς θίγονται διάφορες αρχές όπως αυτή της ανθρώπινης αξιοπρέπειας και της προσωπικότητας. Σε αρκετές περιπτώσεις όμως η χρήση είναι επιτρεπτή και καθόλα υποχρεωτική όπως για παράδειγμα η πρόσβαση σε χώρους αυξημένης επικινδυνότητας ή στρατιωτικές εγκαταστάσεις[[8]](#footnote-8).

Οι *Έξυπνες κάρτες (smart cards)* είναι κάρτες, οι οποίες μοιάζουν εξωτερικά με τις πιστωτικές κάρτες. Ενώ η πιστωτική κάρτα είναι ένα απλό κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία (magnetic stripe), στην οποία είναι εγγεγραμμένα κάποια στοιχεία του χρήστη. Η έξυπνη κάρτα, σε σχέση με την πιστωτική κάρτα, η οποία αποτελείται από κομμάτι πλαστικού, στο οποίο έχει ενσωματωθεί μια μαγνητική ταινία, ενσωματώνει ένα μικροεπεξεργαστή, ο οποίος βρίσκεται κάτω από μια επαφή από χρυσό, προσαρμοσμένο στη μια πλευρά της. Είναι μία πολύ σημαντική διαφορά, καθότι στην έξυπνη κάρτα δεν επιτρέπεται καμία παραχάραξη δεδομένων πριν από τη σύνδεση του μικροεπεξεργαστή με τον υπολογιστή. Μερικές από τις εφαρμογές των έξυπνων καρτών είναι οι κάρτες που χρησιμοποιούμε σε τραπεζικές συναλλαγές (συσκευές ΑΤΜ), σε συναλλαγές με υπηρεσίες κοινής ωφέλειας (ηλεκτρονικό βιβλιάριο υγείας), σε αυτόματα μηχανήματα πώλησης αγαθών κ.α.

Τα *E-token* είναι συσκευές νέας τεχνολογίας, που παρέχουν αυξημένη προστασία κατά τον έλεγχο της ταυτότητας ενός χρήστη. Για να μπορέσει κάποιος να μιμηθεί το χρήστη και να αποκτήσει πρόσβαση στις υπηρεσίες του θα πρέπει να έχει τόσο τη συσκευή όσο και τους κωδικούς πρόσβασης του χρήστη. Στην ουσία πρόκειται για ένα μηχανισμό υλικού, φορητό και μικρού μεγέθους. Ο μηχανισμός παράγει με κρυπτογραφημένο αλγόριθμο ένα συνήθως οκταψήφιο αριθμό μίας χρήσεως ο οποίος έχει διάρκεια ζωής μερικά δευτερόλεπτα και ο οποίος σε συνδυασμό με τον κωδικό χρήστης (User ID), πιστοποιεί ότι η πρόσβαση/συναλλαγή προέρχεται από το συγκεκριμένο χρήστη. Μπορεί να χρησιμοποιηθεί ευρύτατα στις συναλλαγές μέσω διαδικτύου όπως το e-banking και το e-commerce, καθώς και στις χρηματιστηριακές συναλλαγές παρέχοντας ασφαλή λύση απομακρυσμένης πρόσβασης

Ακόμη μία υπηρεσία είναι η *Διαχείριση των δικαιωμάτων πρόσβασης (Permission management)* με την οποία εννοούμε τεχνικές και διαδικασίες παροχής δικαιωμάτων πρόσβασης χρηστών σε υπηρεσίες ή σε Πληροφοριακά συστήματα μέσω του διαχειριστή (βλ. Εξουσιοδότηση 1.4.2) και τέλος τα *Εργαλεία συλλογής και ανάλυσης ψηφιακών πειστηρίων (Forensic tools)*. Θα μπορούσαν να χαρακτηριστούν και εργαλεία ψηφιακής εγκληματολογίας καθότι επεξεργάζονται αποδεικτικά στοιχεία που βρίσκονται από τις αρμόδιες αρχές σε υπολογιστές και σε ψηφιακά μέσα αποθήκευσης. Στόχος τους είναι να εξετάσουν τα ψηφιακά μέσα ώστε να εντοπίσουν, να ανακτήσουν, να αναλύσουν και να παρουσιάσουν γεγονότα και απόψεις που προέκυψαν μέσα από την ψηφιακή πληροφορία.

Πριν κλείσουμε αυτή την ενότητα αξίζει να αναφέρουμε ότι τα εργαλεία που παρουσιάστηκαν παραπάνω, είτε αυτά αφορά την ενίσχυση είτε τη διαχείριση της ιδιωτικότητας χρησιμοποιούνται και συνδυαστικά σε πολλές περιπτώσεις όπως: στην ασφάλεια του δημοσίου τομέα, σε χρηματοπιστωτικές συναλλαγές, σε ανώνυμες αγορές στο διαδίκτυο, στον τομέα της υγείας, σε τηλεπικοινωνιακούς τομείς, στην ηλεκτρονική διακυβέρνηση, στον εντοπισμό χρηστών ανάλογα με τη γεωγραφική τους θέση κλπ. Αρκετά από τα παραπάνω θα αναλυθούν σε μεγαλύτερο βαθμό και στη συνέχεια καθώς θα προχωράμε σε πιο τεχνικά ζητήματα. Στο σημείο όμως αυτό παραθέτουμε τους δύο πίνακες συνοψίζουν όλα όσα περιγράψαμε.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Κατηγορία | Υποκατηγορία | Τυπικά χαρακτηριστικά | Ι | 1 | 2 | 3 | 4 | S |
| Διαχείριση της ιδιωτικότητας  1: Μη παρατηρησιμότητα - Unobservability  2: Μη συνδεσιμότητα - Unlinkability  3: Ανωνυμία -Anonymity  4: Ψευδωνυμία – Pseudonymity  S: Δευτερεύοντα - Secondary  I: Πληροφοριακά -Informational | Εργαλεία πληροφόρησης | Παραγωγή πολιτικών | Ι |  |  |  |  |  |
| Ανάγνωση-επικύρωση | Ι |  |  |  |  |  |
| Έλεγχος συμμόρφωσης | Ι |  |  |  |  |  |
| Εργαλεία διαχείρισης | Διαχείριση ταυτότητας |  |  |  | Χ | Χ |  |
| Βιομετρικά |  |  |  | Χ | Χ |  |
| Έξυπνες κάρτες |  | X |  | Χ | Χ |  |
| Ε-token |  | X |  | Χ | Χ |  |
| Δικαιώματα πρόσβασης |  | X |  | Χ | Χ |  |
| Εργαλεία ελέγχου |  | X |  |  |  | S |
| Εργαλεία πειστηρίων |  |  |  |  |  | S |

Πίνακας Εργαλεία Διαχείρισης Ιδιωτικότητας

Πηγή Πίνακα: [Σιο06]

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Κατηγορία | Υποκατηγορία | Τυπικά χαρακτηριστικά | Ι | 1 | 2 | 3 | 4 | S |
| Προστασία της Ιδιωτικότητας  1: Μη παρατηρησιμότητα - Unobservability  2: Μη συνδεσιμότητα - Unlinkability  3: Ανωνυμία -Anonymity  4: Ψευδωνυμία – Pseudonymity  S: Δευτερεύοντα - Secondary  I: Πληροφοριακά –Informational | Εργαλεία Ψευδωνυμοποίησης | Διαχείριση εφαρμογών |  |  | X |  | X |  |
| Ψευδώνυμα πλοήγησης |  |  |  |  | X |  |
| Προϊόντα και υπηρεσίες ανωνυμοποίησης | Ανώνυμο ταχυδρομείο |  |  |  | X |  |  |
| Εξυπηρετητές αν/μιας – ψευδ/μίας |  |  |  | X | X |  |
| Έμπιστες Τρίτες Οντότητες |  |  | X | X | X |  |
| Μοναδικά πρωτεύοντα κλειδιά |  |  | X |  |  |  |
| Τυφλές ψηφιακές Υπογραφές |  |  | X | X | X |  |
| Ανώνυμο ψηφιακό χρήμα |  |  | X | X | X |  |
| Εργαλεία Κρυπτογράφησης | Κρυπτογράφηση μηνυμάτων |  | X |  |  |  |  |
| Κρυπτογράφηση συναλλαγών |  | X |  |  |  |  |
| Κρυπτογράφηση αρχείων |  | X |  |  |  |  |
| Ψηφιακή στεγανογραφία |  |  | Χ |  |  |  |
| Ψηφιακό υδατογράφημα |  | Χ | Χ |  |  |  |
| Φίλτρα και λογισμικό εμπόδισης | Φίλτρο αζήτητης επικοινωνίας |  |  |  |  |  | S |
| Φιλτράρισμα περιεχομένου |  |  |  |  |  | S |
| Εμπόδιση εμφάνισης παραθύρων |  |  |  |  |  | S |
| Firewalls |  |  |  |  |  | S |
| Διαγραφή πειστηρίων και ιχνών | Διαγραφή επιβλαβούς λογισμικού |  | Χ | Χ | Χ |  |  |
| Διαχείριση cookies |  | Χ | Χ |  |  |  |
| Εργαλεία καθαρισμού browser |  | Χ | Χ |  |  |  |
| Διαγραφή ιχνών |  | Χ | Χ |  |  |  |
| Διαγραφή σκληρών δίσκων |  | Χ | Χ | Χ |  |  |

Πίνακας Εργαλεία Ενίσχυσης της Ιδιωτικότητας

Πηγή Πίνακα: [Σιο06]

* 1. Διαπιστευτήρια (Credentials)

Μεγάλο μέρος της εργασίας μας αφορά τα credentials ή αλλιώς διαπιστευτήρια[[9]](#footnote-9). Ως credential θα μπορούσαμε να ορίσουμε οποιοδήποτε μέσο που χρησιμοποιείται για να πιστοποιήσει σε μία τρίτη οντότητα την εγκυρότητα των στοιχείων ενός κατόχου. Η πιστοποίηση αυτή μπορεί να αφορά από ένα και μόνο χαρακτηριστικό μέχρι και το σύνολο των χαρακτηριστικών ενός κατόχου.

Για παράδειγμα η αστυνομική ταυτότητα μπορεί να πιστοποιήσει την υπηκοότητα ενός κατόχου, όμως με το ίδιο μέσο μπορεί να πιστοποιηθεί και άλλο χαρακτηριστικό όπως η ημερομηνία γέννησης, ή το ύψος του κατόχου. Τα credentials εκδίδονται από μία αρμόδια οντότητα (και μάλιστα έμπιστη-trusted) που ονομάζεται Εκδούσα Αρχή ή Αρχή Πιστοποίησης (Certificate Authority) ή απλώς Αρχή. Άλλα παραδείγματα διαπιστευτηρίων περιλαμβάνουν ακαδημαϊκά πτυχία, διάφορες βεβαιώσεις, άδειες οδήγησης, φορολογικές ενημερότητες, διαβατήρια, πληρεξούσια και ούτω καθεξής.

Στις ακόλουθες ενότητες θα μελετήσουμε τα ψηφιακά διαπιστευτήρια και πιο συγκεκριμένα τα διαπιστευτήρια χαρακτηριστικών (Attribute Based Credentials).

* + 1. Ψηφιακά Credentials (Digital Credentials)

Την τελευταία δεκαετία οι συναλλαγές στην καθημερινότητα των χρηστών γίνονται όλο και περισσότερο ηλεκτρονικά. Η ανησυχία για την προστασία και την ενίσχυση της ιδιωτικότητας ολοένα και αυξάνεται ενώ παράλληλα αποτελεί ζήτημα μείζονος σημασίας για τους παρόχους ηλεκτρονικών υπηρεσιών. Θα πρέπει να μεριμνούν τόσο στην έγκριση και πιστοποίηση των εγγεγραμμένων χρηστών όσο και στην προστασία των πληροφοριακών τους υποδομών.

Για τον παραπάνω λόγο γίνεται χρήση ψηφιακών διαπιστευτηρίων (digital certificates) τα οποία θα μπορούσαν να θεωρηθούν ως ηλεκτρονικό-ψηφιακό ισοδύναμο των κλασσικών διαπιστευτηρίων που περιγράψαμε παραπάνω. Η έκδοσή τους γίνεται και αυτή μετά από αίτηση του χρήστη σε μία Αρχή Πιστοποίησης (CA), η οποία με τη σειρά της επιβεβαιώνει την ταυτότητα του ενδιαφερόμενου και εκδίδει το διαπιστευτήριο. Συνήθως τα ηλεκτρονικά διαπιστευτήρια περιλαμβάνουν: ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του διαπιστευτηρίου, το δημόσιο κλειδί του κατόχου του διαπιστευτηρίου, την ημερομηνία λήξης του διαπιστευτηρίου και το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε[[10]](#footnote-10). Συνεπώς η διαδικασία αφορά αρχικά την αίτηση του χρήστη και αργότερα την αποδοχή του παρόχου (issuer)[[11]](#footnote-11) ότι ο ενδιαφερόμενος κατέχει έγκυρο σύνολο ιδιοτήτων ή χαρακτηριστικών.

Παράδειγμα ψηφιακών διαπιστευτηρίων είναι η υιοθέτηση του μοντέλου των ηλεκτρονικών ταυτοτήτων eIDs από κάποιες χώρες, για χρήση σε συναλλαγές.

1. ο Κεφάλαιο – Πρωτόκολλο SSL (Secure Socket Layer)
   1. Γενικά

Το SSL πρωτόκολλο αναπτύχθηκε και εξελίχθηκε από την Netscape Communications, και σκοπός της ήταν να υπάρξει κατά πρώτον όσο γίνεται πιο ασφαλής επικοινωνία στο Internet και δεύτερον να προφυλαχθούν σηµαντικές πληροφορίες και δεδοµένα όπως είναι τα προσωπικά δεδοµένα και οι πιστωτικές κάρτες. Για το πρωτόκολλο αυτό έχει αποδειχθεί ότι είναι από τα καλύτερα standard για να χρησιµοποιηθεί κωδικοποιηµένη επικοινωνία και για ένα όσο γίνεται πιο σωστό authentication µεταξύ των clients και των servers.

Το συγκεκριµένο πρωτόκολλο SSL είναι γενικού σκοπού και χρησιµοποιείται, εκτός των άλλων χρήσεων και για κρυπτογραφηµένες πληροφορίες ή δεδοµένα µέσω του Internet. Αυτό που κάνει είναι να κρυπτογραφήσει τις πληροφορίες που αποστέλλονται από τον client, µέσω του Internet, προς τον server. Στον server γίνεται η διαδικασία της αποκρυπτογράφησης όλων των δεδοµένων που εστάλησαν. Το SSL είναι σχεδιασµένο µε τέτοιον τρόπο ώστε να εξασφαλίζεται το απόρρητο της επικοινωνίας ανάµεσα σε δύο χρήστες που ο ένας λειτουργεί σαν client και ο άλλος σαν server, πράγµα που σηµαίνει ότι προσφέρεται µια point to point υπηρεσία η οποία είναι αξιόπιστη και ασφαλής. Πιο συγκεκριµένα το πρωτόκολλο SSL, όταν το χρησιµοποιεί κάποιος χρήστης µπορεί να κάνει κάποιες ενέργειες, όπως να εισάγει τον αριθµό της πιστωτικής του κάρτας, σε κάποια φόρµα η οποία είναι ασφαλής, µέσω ενός web browser, τον οποίο (αριθµό της κάρτας του) µπορεί να µεταδώσει µέσα από το Internet προς έναν server που είναι ασφαλής, χωρίς δηλαδή να υπάρχει κίνδυνος να αποκαλυφθεί η µεταδιδόµενη πληροφορία ή τα δεδοµένα.

Το πρωτόκολλο SSL τρέχει πάνω από το TCP/IP Protocol και κάτω από τα πρωτόκολλα HTTP, IMAP, TELNET. Το πρωτόκολλο αυτό έχει την δυνατότητα να επεκταθεί ή ακόµη και να προσαρµοστεί. Τώρα αν κάποιος από τους επικοινωνούντες δεν χρησιµοποιεί τους ίδιους αλγο- ρίθµους, τότε δεν συνεργάζονται και δεν δουλεύουν τα πρωτόκολλα κρυπτογράφησης. ΄Ετσι στην περίπτωση που κάποιο πρόγραµµα, που δουλεύει το SSL, κάνει την προσπάθεια να επικοινωνήσει µε κάποιο άλλο πρόγραµµα, τότε αυτά τα δύο προγράµµατα κάνουν σύγκριση ηλεκτρονικά των στοι- χείων τα οποία καθορίζουν το ποιος είναι ο πιο δυνατός κρυπταλγόριθµος, τον οποίο διαθέτουν από κοινού.

* 1. Υπηρεσίες που προσφέρει το SSL

Οι κυριότερες υπηρεσίες που προσφέρει το SSL είναι:

* παρέχει εµπιστευτικότητα με χρήση κρυπτογράφησης δεδοµένων
* παρέχει ακεραιότητα στα δεδοµένα, με χρήση της τεχνικής MACs (Message Authenti- cation Codes)
* παρέχει επικύρωση της ταυτότητας του client και του server αν αυτοί το επιθυµούν, µε υπογεγραµµένα ψηφιακά πιστοποιητικά, που εκδίδονται από έµπιστες τρίτες οντότητες οι οποίες είναι πιστοποιηµένες

Η χρήση του SSL συναντάται σε πολλές εφαρµογές όπως είναι οι περιπτώσεις του Web-banking και Web-shopping στα οποία ο κάθε χρήστης θα πρέπει να αποστείλει κάποια προσωπικά του δεδοµένα όπως είναι στοιχεία από πιστωτικές κάρτες. Σε περιπτώσεις πιθανών υποκλοπών σε πληροφορίες ή δεδοµένα, το οποίο είναι ότι χειρότερο θα µπορούσε να συµβεί, εµφανίζεται ο SSL, ο οποίος κάνει κρυπτογράφηση των δεδοµένων, ώστε κανένας να µην µπορεί να τα υποκλέψει.

* 1. Χαρακτηριστικά του SSL

Η τρίτη έκδοση 3.0 του SSL προσφέρει πολλά θεωρητικά καθώς και πρακτικά χαρακτηριστικά, τα οποία παρουσιάζουν εξαιρετικό ενδιαφέρον. Τέτοια χαρακτηριστικά θα αναφερθούν στην συνέχεια:

* Διαχωρισµός καθηκόντων: το πρωτόκολλο SSL χρησιµοποιεί ξεχωριστούς αλγορίθ- µους για την κρυπτογράφηση, την απόδειξη για την γνησιότητα καθώς και για την εξα- σφάλιση της ακεραιότητας των δεδοµένων. Ακόµη χρησιµοποιεί και διαφορετικά κλειδιά για την κάθε λειτουργία του πρωτοκόλλου. Από αυτά, τα µεν µεγάλα κλειδιά χρησιµεύουν για να αποδειχθεί η γνησιότητα και η ακεραιότητα των δεδοµένων, τα δε µικρά κλειδιά χρησι- µεύουν για την μυστικότητα. Για το µήκος των κλειδιών, µετά από ρυθµίσεις, µπαίνουν κάποιοι περιορισµοί, µόνο όµως για την εµπιστευτικότητα και όχι για την ακεραιότητα και την γνησιότητα των δεδοµένων.
* Αποτελεσµατικότητα: είναι το χαρακτηριστικό µε το οποίο το SSL µε τις εφαρµογές του µπορεί να αποθηκεύει κρυφά ένα µυστικό (master secret) το οποίο παραµένει αναλλοίωτο, στις διάφορες συνδέσεις του SSL. Η διαδικασία αυτή χρειάζεται γιατί η κρυπτογράφηση και η αποκρυπτογράφηση είναι διαδικασίες οι οποίες είναι χρονοβόρες.
* Πιστοποιητικό βασισµένο στην απόδειξη γνησιότητας: παρέχεται από το πρω- τόκολλο SSL για να αποδεικνύεται η γνησιότητα και του client αλλά και του server. Αυτό επιτυγχάνεται µε την χρήση των ψηφιακών πιστοποιητικών καθώς και µε τις *ψηφιακά υπογεγραµµένες προκλήσεις αναγνώρισης*. Η τρίτη έκδοση του SSL χρησιμοποιεί τα X.509 version 3 πιστοποιητικά.
* Αναγνωστικό πρωτόκολλο: αν και το SSL πρωτόκολλο σχεδιάστηκε για να τρέχει πάνω από το TCP/IP Protocol, στην ουσία µπορεί να τρέξει στην κορυφή του κάθε αξιόπιστου connection-oriented protocol και ένα τέτοιο είναι το Χ.25, ενώ το IP User Datagram Protocol δεν είναι αξιόπιστο.
* Υποστήριξη για συµπίεση: επειδή τα κρυπτογραφηµένα δεδοµένα δεν είναι δυνατόν να συµπιεστούν, τη διαδικασία αναλαµβάνει το SSL πρωτόκολλο που στο µέλλον θα έχει αυτήν την ικανότητα, αφού σήµερα δεν υπάρχει εφαρµογή του SSL που να ενσωµατώνει την διαδικασία της συµπίεσης.
  1. SSL Ψηφιακά Πιστοποιητικά

Το πρωτόκολλο SSL κάνει σε µεγάλο βαθµό χρήση των πιστοποιητικών δηµόσιου κλειδιού, ώστε να υπάρχει η δυνατότητα να αποδειχθεί η γνησιότητα των επικοινωνούντων οντοτήτων στις SSL ανταλλαγές. Ακόµη κάνει χρήση των Χ.509 version 3 πιστοποιητικών, ώστε να γίνει έλεγχος στα RSA ζεύγους κλειδιών. Κάνει επιπλέον έλεγχο µε ένα Χ.509, το οποίο είναι τροποποιηµένο, στα δηµόσια κλειδιά.

Το πρωτόκολλο SSL υποστηρίζει κάποια είδη πιστοποιητικών τα οποία είναι:

* Τα RSA πιστοποιητικά δηµόσιου κλειδιού, µε δηµόσια κλειδιά αυθαιρέτου µήκους
* Τα RSA πιστοποιητικά δηµόσιου κλειδιού που περιορίζονται στα 512 bits για χρήση τα κρυπτογραφικά λογισµικά που πρόκειται να εξαχθούν
* Τα RSA πιστοποιητικά που είναι µόνο για υπογραφή, τα οποία περιέχουν RSA δηµόσια κλειδιά και χρησιµοποιούνται µόνο για την υπογραφή δεδοµένων και όχι για κρυπτογράφηση
* Τα DSS πιστοποιητικά
* Τα Diffie-Helman πιστοποιητικά

Η χρήση όλων αυτών των πιστοποιητικών δεν είναι υποχρεωτική. Το πρωτόκολλο SSL έχει απαίτηση για πιστοποιητικά server, εκτός από τη περίπτωση που οι SSL εφαρµογές και του client και του server χρησιµοποιούν το πρωτόκολλο για ανταλλαγή κλειδιών Diffie-Helman. Τα προϊόντα όµως Netscape δεν εφαρµόζουν τους αλγορίθµους Diffie-Helman.

* 1. Αντοχή του SSL σε γνωστές επιθέσεις

**Dictionary Attack**

Αυτή η επίθεση µπορεί να λειτουργήσει στην περίπτωση που ένα µέρος µόνο ενός µη κρυπτογρα- φηµένου κειµένου περιέλθει στην κατοχή µη εξουσιοδοτηµένων ατόµων, οπότε το κοµµάτι αυτό κρυπτογραφείται κάνοντας χρήση κάθε πιθανού κλειδιού. Κατόπιν ελέγχεται όλο το κρυπτοκείµε- νο, έως ότου βρεθεί κάποιο τµήµα του το οποίο να ταιριάζει µε κάποιο από τα προϋπολογισµένα. Αν τύχει και η έρευνα πετύχει, τότε το κλειδί που κρυπτογραφήθηκε το µήνυµα έχει βρεθεί. Ε- πειδή τα κλειδιά των αλγορίθµων του πρωτοκόλλου είναι αρκετά µεγάλα, µε µέγεθος 128 bits, τότε το πρωτόκολλο δεν κινδυνεύει από αυτό το είδος της επίθεσης. Ακόµα και οι αλγόριθµοι σε εξαγόµενα προϊόντα, υποστηρίζουν κλειδιά µε µέγεθος 128 bits, παρά το ότι τα 88 bits από αυτά µεταδίδονται χωρίς ασφάλεια. Ο υπολογισµός 240 διαφορετικών ακολουθιών, ο οποίος θα πρέπει να γίνει, κάνει αδύνατη την επιτυχία αυτής της επίθεσης.

**Replay Attack**

Η επίθεση αυτή γίνεται στην περίπτωση που κάποιο τρίτο άτοµο καταγράφει την ανταλλαγή µηνυµάτων µεταξύ δύο οντοτήτων οι οποίες επικοινωνούν. Τότε λοιπόν το τρίτο αυτό άτοµο προσπαθεί να κάνει χρήση των µηνυµάτων του client για να µπορέσει να αποκτήσει πρόσβαση στον server. Όμως το πρωτόκολλο SSL κάνει χρήση του connection-id το οποίο παράγεται από τον server µε κάποιον τυχαίο τρόπο και το οποίο διαφέρει για την κάθε σύνδεση. ΄Ετσι λοιπόν δεν υπάρχει περίπτωση να υπάρξουν δύο ίδια connection-id και όλα τα µηνύµατα που χρησιµοποιήθηκαν δεν είναι δυνατόν να γίνουν δεκτά από τον server. Το connection-id έχει µέγεθος 128 bits, ώστε να υπάρχει επιπλέον ασφάλεια.

**Brute Force Attack (επίθεση «ωμής βίας»)**

Με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση, µπορεί να πετύχει αυτή η επίθεση. ΄Οσο όµως µεγαλύτερα είναι σε µέγεθος τα κλειδιά τα οποία χρησιµοποιούνται, τόσο πιο πολλά είναι τα πιθανά κλειδιά. ΄Ετσι λοιπόν η επίθεση αυτή σε αλγορίθµους οι οποίοι χρησιµοποιούν κλειδιά των οποίων το µέγεθος είναι στα 128 bits είναι χωρίς ουσία. Μόνο ο αλγόριθµος DES µε µέγεθος 56 bits cipher έχει ευαισθησία σε αυτές τις επιθέσεις και για αυτόν τον λόγο δεν συνιστάται η χρήση του.

**Man-In-Middle- Attack**

Αυτή η επίθεση γίνεται όταν κάποιος τρίτος µπορεί να παρεµβαίνει στην επικοινωνία µεταξύ δύο οντοτήτων που επικοινωνούν µεταξύ τους. Πρώτα αυτός κάνει επεξεργασία στα µηνύµατα του client, αµέσως µετά τα τροποποιεί όπως επιθυµεί αυτός και τελικά τα προωθεί στον server. Το ίδιο ακριβώς κάνει και στα µηνύµατα τα οποία στέλνονται από τον server. Το πρωτόκολλο SSL υποχρεώνει τον server να φανερώνει την ταυτότητά του, χρησιµοποιώντας ένα έγκυρο πιστοποιη- τικό, στο οποίο δεν µπορεί να γίνει τροποποίηση. ΄Οπως όµως είναι γνωστό, υπάρχει η ευχέρεια επικοινωνίας των κλειδιών υπογεγραµµένα.

Υπάρχουν, όμως, και κάποιες γενικές αδυναμίες του SSL. Το πρωτόκολλο SSL δεν εξασφαλίζει τον κάθε χρήστη από διάφορους κακόβουλους, µε τους οποίους πιθανώς να θέλει κάποιου είδους συνεργασία, χωρίς βέβαια ο χρήστης να γνωρίζει τις προθέσεις τους. Για να µπορέσει το SSL να εξασφαλίζει την εµπιστευτικότητα στην σύνδεση µεταξύ δύο οντοτήτων οι οποίες επικοινωνούν µεταξύ τους, χρησιµοποιεί µία µέθοδο η οποία είναι γνωστή σαν public key authentication. ΄Οµως υπάρχει ένα πρόβληµα το οποίο αφορά το ποιοι συνδέονται µεταξύ τους µε την µέθοδο αυτή.

Αν ο server και ο client έχουν πρόβληµα, τα πράγµατα θα δυσκολέψουν και αυτό γίνεται γιατί ο SSL server δεν µπορεί να εκτελέσει κάποιον έλεγχο στο εάν ο client είναι πράγµατι ο νόµιµος ή κάποιος επιτιθέµενος που υπέκλεψε τα στοιχεία του. ΄Ενα άλλο πρόβληµα είναι η παραδοχή ότι όλοι οι clients είναι οι νόµιµοι, πράγµα το οποίο θα οδηγήσει σίγουρα σε καταστάσεις εκτός ελέγχου δυσάρεστες για τους χρήστες. ΄Οταν κάποιος χρήστης εκτελεί κάποια συναλλαγή και αµέσως µετά την ακυρώνει, αυτό σηµαίνει ότι ο χρήστης που έκανε την παραγγελία, ίσως να µην είναι εξουσιοδοτηµένος. Αυτό γίνεται επειδή το SSL αφήνει το χρήστη εκτός αφού κάνει αυτοµατοποίηση στις διαδικασίες.

Αφού όπως φαίνεται το SSL πρωτόκολλο έχει κάποια κενά ασφάλειας, για να µπορεί ο κάθε χρήστης να προφυλαχθεί, θα πρέπει να καταφύγει στις εξής λύσεις:

* Να επισκέπτεται sites που ξέρει ότι έχουν καλό επίπεδο ασφάλειας και αξιοπιστίας.
* Πριν χρησιµοποιήσει ο χρήστης την πιστωτική του κάρτα να βεβαιωθεί για την αξιοπιστία του server που παρέχει τη διαδικτυακή υπηρεσία προς την οποία απευθύνει την πληρωμή.
* Ο χρήστης πρέπει ακόµη να ελέγχει, στο μέτρο του δυνατού, το site που επισκέπτεται ως προς το αν παρέχει ασφάλεια και σε πιο επίπεδο.

1. ο Bitcoin
   1. Γενικά

Η τεχνολογία πίσω από το Bitcoin είναι ιδιαίτερα περίπλοκή. Για να λειτουργήσει όλο το σύστημα του Bitcoin χρειάζεται η συμβολή υπολογιστών από όλο τον κόσμο που ανταγωνίζονται ο ένας τον άλλον, λύνοντας κρυπτογραφημένες συναρτήσεις για να επιβεβαιώσουν τις συναλλαγές.

Πρoτού πραγματοποιηθεί μια συναλλαγή ελέγχεται η ορθότητα και η εγκυρότητα της όπως θα δούμε αναλυτικότερα και παρακάτω. Οι συναλλαγές ελέγχονται και επαληθεύονται από τους κόμβους του δικτύου μέσω της μεθόδου κρυπτογράφησης και αποκρυπτογράφησης και καταγράφονται σε ένα αποκεντρωμένο «λογιστικό βιβλίο» κοινής χρήσης το οποίο ονομάζεται Blockchain.

Επειδή όπως αναφέρθηκε το Bitcoin είναι ένα σύστημα «peer to peer» ή αλλιώς «P2P» δεν υπάρχει κάποιος κεντρικός διακομιστής που να αναλαμβάνει τους μαθηματικούς υπολογισμούς που είναι αναγκαίοι για την επιβεβαίωση των συναλλαγών, όλοι οι χρήστες του δικτύου είναι το ίδιο υπεύθυνοι για την λειτουργία του και ανταγωνίζονται ο ένας τον άλλον για την επίλυση των μαθηματικών προβλημάτων.

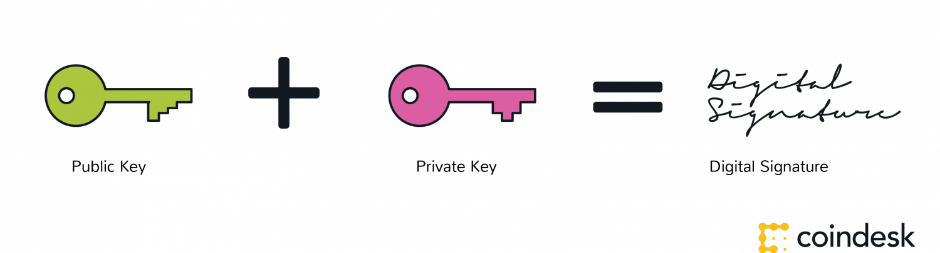
Ουσιαστικά, η διαδικασία επιβεβαίωσης των συναλλαγών περιλαμβάνει την λύση του αλγορίθμου απόδειξης εργασίας (Proof of Work – PoW), ο οποίος στην ουσία αποδεικνύει την μεγάλη επεξεργαστική ισχύ που έχει ξοδέψει ο miner για να βρει την λύση του προβλήματος για την επιβεβαίωση της συναλλαγής. H διαδικασία αυτή ονομάζεται εξόρυξη «mining» (mine= ορυχείο) και τα άτομα που αναλαμβάνουν την εξόρυξη ονομάζονται εξορύκτες «miners».

Οι miners ανταμείβονται τόσο με τα νέα bitcoins που παράγονται όσο και με τις προμήθειες που προκύπτουν από τις συναλλαγές «transaction fees». Όπως θα αναλυθεί στη συνέχεια ο μέγιστος αριθμός των μονάδων bitcoin που μπορεί να παραχθεί δεν θα ξεπεράσει ποτέ τα 21 εκατομμύρια. Για τον λόγο αυτό κάθε τέσσερα χρόνια αυξάνεται και η δυσκολία της εξόρυξης, έτσι ώστε να μειωθεί ο ρυθμός των παραγόμενων bitcoin.

* 1. Βασικές έννοιες του bitcoin
     1. Ψηφιακά κλειδιά και ψηφιακές υπογραφές:

Η ψηφιακή υπογραφή και τα ψηφιακά κλειδιά είναι απαραίτητα για την επαλήθευση του χρήστη όπως είναι αναγκαία η προσκόμιση της ταυτότητας μας όταν πηγαίνουμε στην τράπεζα για την διεκπεραίωση μιας συναλλαγής.

Τα ψηφιακά κλειδιά (δείτε Ενότητα 1.2.2.1) δημιουργούνται από το πορτοφόλι του χρήστη και αποθηκεύονται σε αυτό. Δημιουργούν την ψηφιακή υπογραφή η οποία είναι αναγκαία για την εκτέλεση οποιασδήποτε συναλλαγής, αφού εξασφαλίζει αρχικά ότι το μήνυμα έχει αποσταλεί από τον καθορισμένο αποστολέα και ότι το μήνυμα αυτό δεν έχει παραβιαστεί. Για να δημιουργηθεί η ψηφιακή υπογραφή είναι αναγκαίο να κατακερματιστεί το μήνυμα που μεταδίδεται στο δίκτυο και στην συνέχεια ο κατακερματισμός να κρυπτογραφηθεί.



Ένα ψηφιακό κλειδί αποτελείται από ένα ζευγάρι δημόσιου κλειδιού (public key) και ενός ιδιωτικού κλειδιού (private key) τα οποία είναι συνδεδεμένα μεταξύ τους μέσω μίας μαθηματικής σχέσης και είναι απαραίτητα για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων. Όταν η κρυπτογράφηση γίνει με το δημόσιο κλειδί η αποκρυπτογράφηση πραγματοποιείται με το ιδιωτικό κλειδί και αντιστρόφως όταν η κρυπτογράφηση γίνει με το ιδιωτικό κλειδί για την αποκρυπτογράφηση απαιτείται το δημόσιο κλειδί. Tο ιδιωτικό κλειδί δημιουργεί το δημόσιο κλειδί και αυτό με την σειρά του δημιουργεί την διεύθυνση (bitcoin address):

**PRIVATE KEY PUBLIC KEY BITCOIN ADRESS**

* + 1. Ιδιωτικό κλειδί (Private key) – Δημόσιο κλειδί (Public key)

Το ιδιωτικό κλειδί είναι μια κρυπτογραφικά κωδικοποιημένη σειρά τυχαίων χαρακτήρων και αριθμών που γνωρίζει μόνο ο ιδιοκτήτης. Το ιδιωτικό κλειδί είναι αυτό που δημιουργεί το δημόσιο κλειδί, τις ψηφιακές υπογραφές και είναι ο μόνος τρόπος για έναν χρήστη να έχει πρόσβαση στα χρήματα του, τα οποία συνδέονται με μια διεύθυνση (bitcoin address). Είναι σημαντικό ο χρήστης να το κρατάει μυστικό όπως ακριβώς το PIN των καρτών του, αφού σε αντίθετη περίπτωση τα χρήματα του θα τεθούν σε κίνδυνο. Σημαντικό είναι επίσης ο χρήστης να κατέχει ένα αντίγραφο ασφαλείας του ιδιωτικού κλειδιού αφού η απώλεια του σημαίνει αυτομάτως και απώλεια του ψηφιακού του πορτοφολιού και άρα απώλεια των χρημάτων. Όπως είπαμε το ιδιωτικό κλειδί δημιουργεί το δημόσιο κλειδί το οποίο είναι και αυτό μια πολύ μεγάλη σειρά αριθμών όπως παρατηρείται στην παρακάτω εικόνα. Το δημόσιο κλειδί είναι φανερό στο διαδίκτυο, χρησιμοποιείται για τη λήψη bitcoin, και δημιουργεί την διεύθυνση (bitcoin address) που είναι όπως φαίνεται της ίδιας μορφής, δηλαδή συνδυασμός ψηφίων και γραμμάτων και μπορεί να χρησιμοποιηθεί από τον καθένα για να στείλει μονάδες bitcoin.

<https://coinsource.net/private-keys-public-keys-addresses-and-wallets/>

* + 1. Κρυπογραφικές λειτουργίες κατακερματισμού (Hashing)

To Hashing που παρουσιάζεται στην παραπάνω εικόνα είναι ένας αλγόριθμος κατακερματισμού που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει μια έξοδο καθορισμένου αλλά μικρότερου σε σχέση με την είσοδο μεγέθους. Το μέγεθος τους κυμαίνεται από 32 bit μέχρι 256 bit. Οι τιμές που επιστρέφει η συνάρτηση κατακερματισμού ονομάζονται hashes. Οι τιμές αυτές είναι διαφορετικές για κάθε είσοδο, αφού η ταυτοποίηση των δεδομένων είναι η βασική λειτουργία τους. Στην ουσία είναι μια μαθηματική συνάρτηση η οποία μετατρέπει μια τιμή εισόδου γρήγορα σε μια τιμή εξόδου χωρίς όμως η αντίστροφη διαδικασία να είναι δυνατή, αφού μέσω μιας τιμής εξόδου είναι αδύνατο να υπολογιστεί η αρχική τιμή εισόδου.

* + 1. Αλυσίδα των μπλοκ – Blockchain

To Blockchain είναι στην ουσία είναι ένα αποκεντρωμένο αρχείο καταγραφής κοινής χρήσης, ένα δημόσιο λογιστικό βιβλίο ή αλλιώς μια βάση δεδομένων στην οποία καταγράφονται όλες οι επιβεβαιωμένες χρηματοοικονομικές συναλλαγές. Το Blockchain χαρακτηρίζεται από κατανεμημένη συναίνεση, αυτό σημαίνει ότι για να επιβεβαιωθεί και να πραγματοποιηθεί μια συναλλαγή πρέπει πρώτα να εγκριθεί από τους κόμβους του δικτύου, δηλαδή τους υπολογιστές που συμμετέχουν στην εξόρυξη των bitcoins, ο καθένας από τους οποίους ελέγχει την ορθότητα και εγκυρότητά της συναλλαγής. Εάν η πλειονότητα των κόμβων εγκρίνει την συναλλαγή τότε αυτή θα ενσωματωθεί σε ένα μπλοκ και το μπλοκ αυτό στην αλυσίδα του Blockchain.

Τα μπλοκ (blocks) θα μπορούσαμε να πούμε ότι μοιάζουν με φακέλους που μέσα έχουν μια λίστα από επιβεβαιωμένες συναλλαγές. Κάθε μπλοκ μπορεί να συμπεριλάβει έναν ορισμένο αριθμό καταχωρημένων συναλλαγών και όταν αυτό δεν χωράει άλλες συναλλαγές τότε δημιουργείται ένα νέο μπλοκ το οποίο αναφέρεται στο ακριβώς προηγούμενο μπλοκ του. Κάθε κόμβος έχει ένα αντίγραφο του δημόσιου αρχείου Blockchain και σε κάθε υπολογιστή που κάνει mining είναι αποθηκευμένο το αντίγραφο αυτό, ξεκινώντας από το «genesis block» , δηλαδή το πρώτο μπλοκ που δημιουργήθηκε καταλήγοντας στο τελευταίο μπλόκ που έχει προστεθεί στην αλυσίδα Blockchain. Το Blockchain ενημερώνεται κάθε δέκα λεπτά αυτομάτως, με αποτέλεσμα να καθίσταται αδύνατη οποιαδήποτε άλλη αλλαγή πέραν της προσθήκης νέων καταχωρήσεων.[[12]](#footnote-12),[[13]](#footnote-13)

* + 1. Τι είναι η εξόρυξη (mining)

Όπως αναφέρθηκε η εξόρυξη (mining) είναι η διαδικασία δαπάνης υπολογιστικής δύναμης, απαραίτητη για την δημιουργία νέων bitcoins, την επαλήθευση των συναλλαγών και την ασφάλεια και διατήρηση του συγχρονισμένου δικτύου. Ο συγχρονισμός αποτελεί την διαδικασία μεταφόρτωσης και επαναεπιβεβαίωσης όλων των προηγούμενων ολοκληρωμένων συναλλαγών. Oι έγκυρες και επιβεβαιωμένες συναλλαγές ομαδοποιούνται στα μπλοκ. [[14]](#footnote-14)Τα μπλοκ, δηλαδή οι ομάδες συναλλαγών ασφαλίζονται από τους εξορύκτες του Bitcoin και χτίζονται το ένα πάνω στο άλλο σχηματίζοντας μια αλυσίδα. Με λίγα λόγια, επειδή η φύση του Bitcoin είναι αποκεντρωμένη απαιτείται η συμβολή τυχαίων υπολογιστών από όλον τον κόσμο για την επιβεβαίωση της εγκυρότητας των συναλλαγών. Την εργασία αυτή την αναλαμβάνουν οι miners οι οποίοι χρησιμοποιούν ένα λογισμικό το οποίο είναι αναγκαίο όπως θα δούμε παρακάτω για την εξόρυξη, και ως αντάλλαγμα εκδίδεται ένας αριθμός bitcoin. Με τον τρόπο αυτό εκδίδεται το νόμισμα και δημιουργείται συνεχώς κίνητρο για mining.

Ο αλγόριθμος κρυπτογράφησης είναι έτσι φτιαγμένος ώστε να μεταβάλλει τον βαθμό δυσκολίας των μαθηματικών προβλημάτων που πρέπει να λυθούν για να παραχθεί ακόμη ένα bitcoin ανάλογα με την ταχύτητα επίλυσης τους. Αυτό σημαίνει ότι όσο περισσότερα άτομα συμμετέχουν στην διαδικασία της εξόρυξης bitcoin τόσο πιο δύσκολα πραγματοποιείται η εξόρυξη, ώστε η δημιουργία των bitcoin να μην υπερβαίνει τα 50 bitcoins ανά 10 λεπτά. Έτσι, όσο περισσότεροι οι ανθρακωρύχοι τόσο ο ρυθμός δημιουργίας των μπλόκ θα μειώνεται. Για τον λόγο αυτό οι miners ανακάλυψαν και ανέπτυξαν έναν τρόπο να δουλεύουν μαζί σε ομάδες εξόρυξης (mining pools) όπως θα επεξηγηθεί στην συνέχεια.

Στην πραγματικότητα, ο πρωταρχικός σκοπός της εξόρυξης είναι να επιτρέψει στα μπλοκ να φθάσουν σε μια ασφαλή, αμετάβλητη και ισχυρή απέναντι στις παραβιάσεις θέση στο δίκτυο. Τα μπλοκ είναι άρρηκτα συνδεδεμένοι μεταξύ τους και η σχέση κάθε νέου μπλοκ από τα προηγούμενα βασίζεται σε έναν μαθηματικό αλγόριθμο ο οποίος δύσκολα μπορεί να παραβιαστεί. Σημαντικό είναι επίσης να τονιστεί ότι οποιοδήποτε μπλοκ εξορύσσετε από κακόβουλους ανθρακωρύχους θα απορρίπτεται από όλους στο δίκτυο και άρα θα είναι άχρηστο.

Mε λίγα λόγια η εξόρυξη εξυπηρετεί δύο σκοπούς, την εισαγωγή bitcoin στο σύστημα, που περιλαμβάνει επίσης την προσθήκη των δεδομένων των συναλλαγών στο παγκόσμιο κοινόχρηστο αρχείο συναλλαγών του Bitcoin και την εξασφάλιση της ασφάλειας του δικτύου από τις δόλιες συναλλαγές.

Η εξόρυξη θα μπορούσαμε να πούμε ότι μοιάζει με την εξόρυξη χρυσού, με την διαφορά ότι η εξόρυξη bitcoin προσφέρει στους εξορύκτες μια ανταμοιβή για την εργασία τους που προκύπτει από τα νέα bitcoins καθώς και από τις προμήθειες που προκύπτουν από τις συναλλαγές. Επίσης η άλλη διαφορά είναι ότι το mining θα είναι αναγκαίο ακόμα και μετά την δημιουργία του τελευταίου bitcoin. Με άλλα λόγια κάθε χρήστης που θέλει να παράγει bitcoins συνδέεται στο δίκτυο χρησιμοποιώντας ένα ειδικό λογισμικό το οποίο παράγει εκατομμύρια μαθηματικές λύσεις ανά δευτερόλεπτο. Οι υπολογισμοί αυτοί είναι αναγκαίοι για να αποκρυπτογραφηθούν οι αλγόριθμοι κρυπτογράφησης που φυλάσσουν το σύστημα. Κάθε λύση που δημιουργείται από τους μαθηματικούς υπολογισμούς ονομάζεται hush και είναι στην ουσία ένα κλειδί ή μια σειρά από bitcoins τα οποία προσπαθούν να λύσουν τον αλγόριθμο κρυπτογράφησης μιας νέας συναλλαγής. Μόλις ολοκληρωθούν οι μαθηματικοί υπολογισμοί, κάθε έγκυρη συναλλαγή καταγράφεται. Προστίθεται αρχικά στο τελευταίο μπλόκ (block) και αυτό με την σειρά του προστίθεται στο λογιστικό αρχείο (log) που ονομάζεται Blockchain.[[15]](#footnote-15)

* + 1. Τρόποι εξόρυξης bitcoin

Στην αρχή η εξόρυξη ήταν εύκολή και σχεδόν καθόλου απαιτητική ή χρονοβόρα και οποιοσδήποτε χρήστης μπορούσε να συμβάλει στην διαδικασία της εξόρυξης χρησιμοποιώντας απλώς την κεντρική μονάδα επεξεργασίας (CPU) του υπολογιστή του, στην συνέχεια όμως η εξόρυξη νέων μπλοκ έγινε δυσκολότερη αφού όλο και περισσότεροι άνθρωποι άρχισαν να ασχολούνται με την διαδικασία αυτή. Πλέον η εξόρυξη απαιτεί συγκεκριμένο εξοπλισμό.[[16]](#footnote-16)

*Κάρτες FPGA MINING*

Η κάρτα FPGA δημιουργήθηκε για να έχει μικρό μέγεθος κι εξαιρετικά μικρή κατανάλωση ενέργειας παράγοντας εκατομμύρια hashes/δευτερόλεπτο, πράγμα που αποτελεί ένα μεγάλο πλεονέκτημα για τους ανθρακωρύχους με υψηλούς λογαριασμούς ηλεκτρικού ρεύματος. Η κάρτα FPGA είναι έτσι σχεδιασμένη ώστε να μπορεί να διαμορφωθεί εύκολα από έναν πελάτη ή έναν προγραμματιστή ακόμη και μετά την κατασκευή της. Δεδομένου ότι αυτή η τεχνολογία είναι ειδικά προσαρμοσμένη στην εξόρυξη bitcoin, συνήθως εκτελείται πολύ καλύτερα από CPUs (κεντρικός επεξεργαστής) και GPUs (επεξεργαστής γραφικών).

*ASIC Mining*

Πρόκειται για ολοκληρωμένα κυκλώματα εξειδικευμένης χρήσης αποκλειστικά για bitcoin Mining. Είναι νεότερης τεχνολογίας και αγγίζουν τα δισεκατομμύρια hashes /δευτερόλεπτο με χαμηλή κατανάλωση ρεύματος. H συγκεκριμένη επιλογή δεν αποτελεί μια οικονομική λύση, ωστόσο, πολλοί ανθρακωρύχοι θεωρούν ότι η επένδυση αυτή αξίζει λόγω της γρήγορης ταχύτητας τους. Το Asic Mining έχει πολύ καλύτερη απόδοση από τις FPGA κάρτες και συνήθως είναι αυτό που προτιμάται από τους εξορύκτες, υστερεί όμως στην προσαρμοστικότητα και έτσι όσοι προτιμούν πιο ευέλικτες επιλογές καταλήγουν στις κάρτες FPGA MINING.

* + 1. Άλλοι τρόποι απόκτησης bitcoin

Εξόρυξη εξ αποστάσεως: Αυτός ο τρόπος εξόρυξης δημιουργήθηκε λόγω της αυξανόμενης δυσκολίας και των μεγάλων απαιτήσεων σε λογισμικό, που έχει καταστήσει την εξόρυξη ιδιαίτερα δύσκολη, δαπανηρή και συχνά ζημιογόνα, αφού τα έξοδα του ηλεκτρικού ρεύματος συχνά είναι μεγαλύτερα ακόμη και από τα έσοδα που προκύπτουν τελικά από την εξόρυξη. Για τον λόγο αυτό μεγάλες εταιρείες έχουν ανοίξει κάποια κέντρα τα οποία είναι εξοπλισμένα με μηχανήματα εξόρυξης κυρίως σε χώρες με οικονομικό ηλεκτρικό ρεύμα και χαμηλή θερμοκρασία για να μην υπερθερμαίνονται τα μηχανήματα. Η εξόρυξη εξ αποστάσεως μπορεί να λάβει δύο μορφές:

*Remote Hosted Mining*: Η συγκεκριμένη μορφή εξόρυξης απευθύνεται σε άτομα με υψηλή τεχνογνωσία και εμπειρία στην εξόρυξη. Στην συγκεκριμένη μορφή η εξόρυξη γίνεται με λογισμικό το οποίο φιλοξενείται σε ένα κέντρο δεδομένων. Τον έλεγχο της εγκατάστασης του λογισμικού την έχει ο χρήστης ο οποίος πληρώνει κάποια τέλη στην εταιρεία για τα έξοδα της φιλοξενίας, της συντήρησης και της ηλεκτρικής ενέργειας.

*Cloud Mining:* Ο δεύτερος και προτιμότερος τρόπος εξόρυξης είναι αυτός της εξόρυξης εξ αποστάσεως, γιατί δεν απαιτείται καμία γνώση ή αντίστοιχη εμπειρία στην διαδικασία εξόρυξης. Με την συγκεκριμένη μέθοδο ο χρήστης αγοράζει ένα συμβόλαιο το οποίο είναι συνήθως ετήσιο από κάποια εταιρεία η οποία θα αναλάβει στην ουσία όλη την διαδικασία της εξόρυξης αποδίδοντας στους πελάτες τα bitcoins που εξορύχθηκαν.

*Πισίνες εξόρυξης- Mining Pools:* Το επίπεδο δυσκολίας της εξόρυξης και οι πόροι που απαιτούνται για την εξόρυξη όπως αναφέρθηκε έχουν αυξηθεί σε βαθμό που είναι πρακτικά αδύνατον κάποιος χρήστης να παράγει μόνος του bitcoins ακόμη και αν διαθέτει έναν καλό εξοπλισμό. Λόγω της μεγάλης αυτής δυσκολίας, οι miners βρήκαν έναν τρόπο να δουλεύουν όλοι μαζί συντονισμένοι σε ομάδες εξόρυξης που ονομάζονται πισίνες εξόρυξης «mining pools» και ο καθένας ανταμείβεται βάσει της συνεισφοράς του. Έτσι ακόμη και ένας αρχάριος χρήστης μπορεί να ενταχθεί σε μια ομάδα εξόρυξης, αρκεί να βρει εκείνη που του ταιριάζει. Υπάρχουν πολλές πισίνες εξόρυξης, διαφορετικές ως προς το μέγεθος και την πολιτική ανταμοιβών που προσφέρουν. Συνήθως οι μεγαλύτερες σε μέγεθος πισίνες προσφέρουν συχνές πληρωμές, ενώ οι μικρότερες πισίνες προσφέρουν υψηλότερα οφέλη αφού η ανταμοιβή μοιράζεται σε λιγότερους miners. Επιπλέον, κάποιες πισίνες εξόρυξης χρεώνουν τέλη τα οποία μπορεί να φτάσουν μέχρι και το 4% της ανταμοιβής.

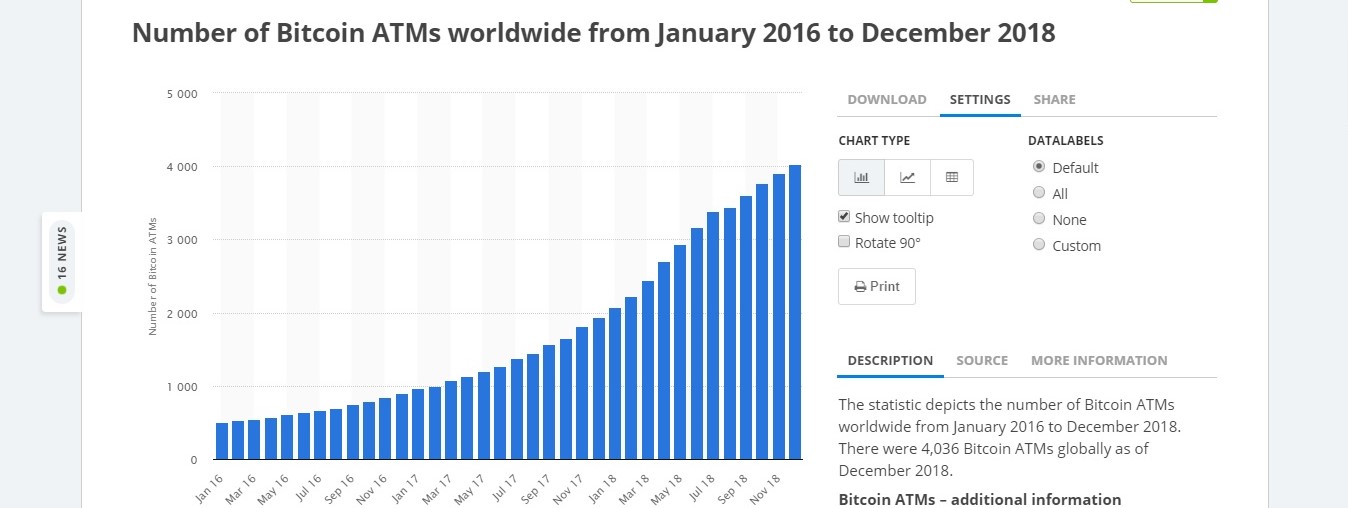
*Τα Ανταλλακτήρια – Exchanges*: Εκτός από την εξόρυξη υπάρχουν και άλλοι τρόποι να αποκτήσει κάποιος bitcoins. Tα ανταλλακτήρια μοιάζουν με τα χρηματιστήρια αξιών και επιτρέπουν σε οποιονδήποτε χρήστη να αγοράσει και να πουλήσει bitcoins. H τιμή αγοράς και πώλησης των bitcoins αλλάζει συνεχώς και καθορίζεται μέσω του νόμου της προσφοράς και της ζήτησης. Τα ανταλλακτήρια αυτά μπορεί να προσφέρουν και υπηρεσίες ασφαλούς φύλαξης των bitcoins. Υπάρχει πληθώρα επιλογών, ενδεικτικά κάποια από τα γνωστότερα ανταλλακτήρια είναι τα (Kraken , CoinBase και Bitcoin.de). Ο χρήστης θα πρέπει να είναι ιδιαιτέρα προσεκτικός κατά την επιλογή του ανταλλακτήριού, ιδιαίτερα μετά την πτώχευση της εταιρείας Mt. Gox, η οποία ήταν ένα από τα μεγαλύτερα ανταλλακτήρια Bitcoin στον κόσμο και διαχειριζόταν πάνω από το 70% των συναλλαγών παγκοσμίως. Η πτώχευση της έκανε πολλούς χρήστες να αμφισβητήσουν την ασφάλεια των ανταλλακτηρίων αλλά και του ίδιου του νομίσματος.

*Bitcoin ATM (ΒΑΤΜ)*: Άλλος ένας τρόπος απόκτησης bitcoin είναι τα Bitcoin ATMs (συντομογραφία BATM), πρόκειται για ένα μηχάνημα που επιτρέπει σε ένα άτομο να αγοράσει bitcoins χρησιμοποιώντας μια αυτόματη μηχανή. Ορισμένα BATM προσφέρουν αμφίδρομη λειτουργικότητα που επιτρέπει τόσο την αγορά bitcoin, όσο και την πώληση των bitcoins με μετρητά, αλλά τα περισσότερα, σε ποσοστό 64% είναι one way δηλαδή μόνο αγοράς bitcoin. Τα μηχανήματα αυτά αν και δεν είναι ακριβώς ίδια με τα παραδοσιακά ΑΤΜ, ο τρόπος λειτουργίας τους είναι πανομοιότυπος. Ουσιαστικά είναι μηχανήματα που είναι συνδεδεμένα στο Internet, επιτρέποντας την εισαγωγή μετρητών ή πιστωτικών καρτών ως αντάλλαγμα με bitcoins. Δεν συνδέονται με κάποιον τραπεζικό λογαριασμό. Συνδέουν τον πελάτη απευθείας με μια ανταλλαγή Βitcoin. Η τιμή του Bitcoin σε αυτά τα μηχανήματα είναι κατά κανόνα 5-10% υψηλότερη από τις τρέ,,χουσες συναλλαγματικές ισοτιμίες, λόγω πρόσθετων εξόδων όπως είναι η συντήρηση μηχανημάτων και το Internet.

Πώς ακριβώς, όμως, λειτουργούν τα BATM; Όπως συμβαίνει και με τα παραδοσιακά μηχανήματα ATM στην αρχή απαιτείται η επαλήθευση της ταυτότητας του χρήστη, αυτό μπορεί να γίνει για παράδειγμα, με τον αριθμό του κινητού τηλεφώνου. Στην συνέχεια, αφού έχει γίνει η επαλήθευση, το ΑΤΜ θα ζητήσει να πληκτρολογήσουμε το ποσό των χρημάτων που επιθυμούμε να ανταλλάξουμε. Μόλις κατατεθούν τα χρήματα στο ATM, το μηχάνημα θα δημιουργήσει ένα χαρτοφυλάκιο με έναν κωδικό QR και θα εκτυπώσει επίσης μια απόδειξη για τη συναλλαγή. Έπειτα θα πρέπει να σαρωθεί ο κωδικός QR με την εφαρμογή του ψηφιακού πορτοφολιού και αυτομάτως τα bitcoins θα μεταφερθούν.



Όπως φαίνεται στο παρακάτω διάγραμμα ο αριθμός των εγκατεστημένων Bitcoin ΑΤΜ τον Ιανουάριο του 2016 έφτανε μόλις τα 501 μηχανήματα. Δύο χρόνια αργότερα, τον Ιανουάριο του 2018 παρατηρείται ότι ο αριθμός αυτός να τετραπλασιάζεται και να αγγίζει τα 2073 εγκατεστημένα μηχανήματα. Σήμερα ο αριθμός των BATM έχει συνολικά φτάσει τα 4063 σε πάνω από 75 χώρες. Τα μισά σχεδόν είναι εγκατεστημένα στις Ηνωμένες Πολιτείες της Αμερικής και ακολουθούν ο Καναδάς, η Αυστρία και το Ηνωμένο Βασίλειο.

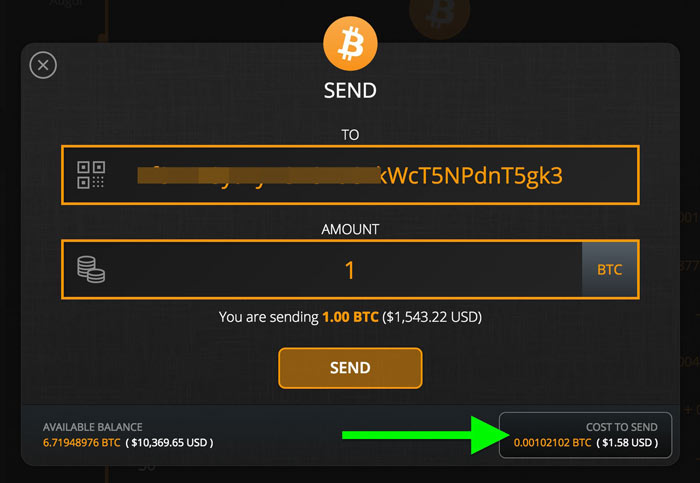
Εικόνα: <https://www.statista.com/statistics/343127/number-bitcoin-atms/>

Στην Ελλάδα τα εγκατεστημένα BATM φτάνουν τα δέκα, εκ των οποίων τα πέντε είναι τοποθετημένα στην Αθήνα και τα υπόλοιπα πέντε στην Θεσσαλονίκη, την Λάρισα, τα Ιωάννινα, την Καστοριά αλλά και την Μύκονο. Αξιοσημείωτο είναι ότι σε διάρκεια ενός έτος έχουν εξυπηρετηθεί πάνω από 1500 πελάτες (<https://weacceptbitcoin.gr/>).

* 1. Συναλλαγές με bitcoin και ψηφιακά πορτοφόλια

Οι συναλλαγές πραγματοποιούνται με τη χρήση μιας γλώσσας Scripting που μοιάζει με Forth και αποτελούνται από μία ή περισσότερες εισόδους και μία ή περισσότερες εξόδους.

Όταν ένας χρήστης θέλει να στείλει bitcoins, ορίζει την διεύθυνση αποστολής και τον αριθμό των bitcoins που επιθυμεί να αποστείλει στην συγκεκριμένη διεύθυνση σε μια έξοδο.



Για να αποφευχθεί η διπλή δαπάνη, κάθε είσοδος πρέπει να αναφέρεται σε μια προηγούμενη αχρησιμοποίητη έξοδο του Blockchain. Επίσης, πριν πραγματοποιηθεί μια συναλλαγή, ελέγχεται η εγκυρότητα της. Ελέγχονται δηλαδή για παράδειγμα οι διευθύνσεις των δύο διαφορετικών πορτοφολιών, του αγοραστή και του πωλητή, αν ο αποστολέας έχει δώσει τη σωστή ψηφιακή υπογραφή (Private Key) για να ξεκλειδώσει τη μεταφορά του ποσού από τη διεύθυνση του όπως και το αν υπάρχουν στο πορτοφόλι αρκετά bitcoins για την πραγματοποίηση της συναλλαγής.

Το επόμενο βήμα περιλαμβάνει την μετάδοση του μηνύματος της συναλλαγής, στο οποίο συμπεριλαμβάνονται οι διευθύνσεις του αποστολέα και του παραλήπτη, το απαιτούμενο ποσό της συναλλαγής και η ψηφιακή υπογραφή που δημιουργήθηκε από τον αποστολέα. Έπειτα η συναλλαγή εκχωρείται σε μια ομάδα που ονομάζεται mempool (συντομογραφία του memory pool) το οποίο στην ουσία είναι ένα σημείο αναμονής των εκκρεμών συναλλαγών, δηλαδή των συναλλαγών εκείνων που αναμένουν να επιβεβαιωθούν.

Στη συνέχεια, η συναλλαγή αναλαμβάνεται από τους miners οι οποίοι είναι οι μεσολαβητές που επικυρώνουν τις συναλλαγές. Συνήθως οι συναλλαγές ξεκινάνε να επιβεβαιώνονται μέσα σε 10 λεπτά. Όταν ο miner βρει την λύση του προβλήματος, δηλαδή την κρυπτογραφημένη συνάρτηση κατακερματισμού (hash), τότε τοποθετεί την ολοκληρωμένη συναλλαγή στο τελευταίο μπλοκ των επιβεβαιωμένων συναλλαγών του Blockchain.

Η αποθήκευση των bitcoins όμως είναι η απαραίτητη προϋπόθεση για την πραγματοποίηση των αγορών, για τον λόγο αυτό καθίσταται αναγκαία η κατοχή ενός ψηφιακού πορτοφολιού (Bitcoin wallet). Το πορτοφόλι αυτό μπορεί να βρίσκεται είτε απλά σαν μια εφαρμογή στο κινητό ή τον υπολογιστή, σε μια ιστοσελίδα ή ακόμη και σε μια συσκευή που διαχειρίζεται τα ιδιωτικά κλειδιά Bitcoin. Κάθε Bitcoin πορτοφόλι έχει μια συγκεκριμένη διεύθυνση, η οποία είναι αναγκαία για την πραγματοποίηση των ανώνυμων μεταφορών. Στην ουσία, το σύνολο των bitcoin είναι αποθηκευμένο στα Bitcoin πορτοφόλια των ατόμων.

* + 1. Ψηφιακά πορτοφόλια – Bitcoin wallets

Το Bitcoin όπως προαναφέρθηκε σε αντίθεση με τα περισσότερα συμβατικά νομίσματα, είναι ένα ψηφιακό νόμισμα. Αυτό σημαίνει ότι ο τρόπος που λειτουργεί το συγκεκριμένο νόμισμα διαφέρει από τον τρόπο που λειτουργεί το κοινό χρήμα, κυρίως όσον αφορά την απόκτηση και την αποθήκευσή του. Καθώς τα bitcoins δεν υπάρχουν σε κάποια φυσική μορφή δεν μπορούν τεχνικά να αποθηκευτούν οπουδήποτε. Για τον λόγο αυτόν απαιτούνται τα ψηφιακά πορτοφόλια.

Το ψηφιακό πορτοφόλι είναι το πρώτο βήμα που απαιτείται για την είσοδο του χρήστη στον χώρο του Bitcoin. Είναι ένα εργαλείο το οποίο είναι αναγκαίο για να μπορέσουν οι χρήστες να λαμβάνουν, να ξοδεύουν και να αποθηκεύουν τα bitcoins τους.

Ένα πορτοφόλι κρυπτογράφησης εκτός από τα bitcoins αποθηκεύει και τα δημόσια και ιδιωτικά κλειδιά που απαιτούνται για την εκτέλεση οποιασδήποτε συναλλαγής και μπορεί να περιέχει ένα σύνολο από πολλά ζεύγη δημόσιων και ιδιωτικών κλειδιών. Το κύριο καθήκον των ψηφιακών πορτοφολιών δηλαδή είναι να αποθηκεύουν το μυστικό κλειδί που απαιτείται για την πρόσβαση στη διεύθυνση Bitcoin και κατά συνέπεια τα χρήματα των κατόχων.[[17]](#footnote-17)

* + 1. Τύποι ψηφιακών πορτοφολιών

Υπάρχουν διάφοροι τύποι πορτοφολιών που μπορούν να χρησιμοποιηθούν για την αποθήκευση των κρυπτονομισμάτων. Υπάρχουν σε διάφορες μορφές και είναι σχεδιασμένες για διαφορετικούς τύπους συσκευών. Η επιλογή πρέπει πάντα να γίνεται με βάση τις προσωπικές ανάγκες και δυνατότητες του χρήστη.

*Software (λογισμικού)*: Τα πορτοφόλια λογισμικού διατίθενται σε τρεις μορφές:

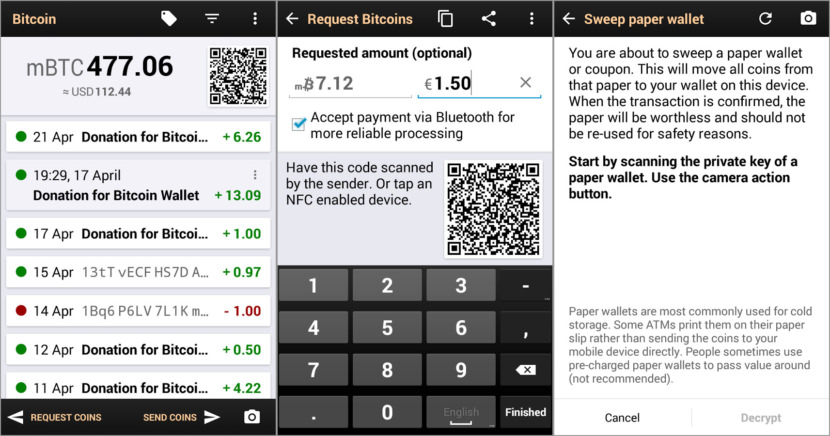
* Desktop
* Mobile
* Online.

*Dekstop wallets (Επιτραπέζια πορτοφόλια)*: Τα πορτοφόλια για επιτραπέζιους υπολογιστές είναι προγράμματα υπολογιστών που αποθηκεύουν τα χρήματα στον σταθερό ή στον φορητό υπολογιστή. Ένα από τα βασικά πλεονεκτήματα του επιτραπέζιου πορτοφολιού είναι ότι προσφέρει πλήρη έλεγχο του νομίσματος στους χρήστες, χωρίς να βασίζεται σε οποιαδήποτε διεπαφή τρίτου μέρους.

Tα μειονεκτήματα των επιτραπέζιων πορτοφολιών είναι ότι ολόκληρος ο έλεγχος και η ασφάλεια εξαρτάται από τους χρήστες, έτσι άν χακαριστεί ο υπολογιστής ή ο σκληρός δίσκος καταρρεύσει τα χρήματα μπορεί να χαθούν για πάντα. Κάποιοι για να προστατευτούν από την πειρατεία προτιμούν να χρησιμοποιούν αχρησιμοποίητους ή εφεδρικούς υπολογιστές που δεν έχουν ποτέ πρόσβαση στο διαδίκτυο για να αποθηκεύσουν τα νομίσματα τους.

*Mobile wallets (Κινητά πορτοφόλια):* Για όσους χρησιμοποιούν τα bitcoins ενεργά σε καθημερινή βάση ένα κινητό πορτοφόλι είναι βασικό εργαλείο. Εκτελείται ως εφαρμογή στο smartphone, αποθηκεύοντας τα ιδιωτικά κλειδιά και επιτρέποντας τις πληρωμές απευθείας από το τηλέφωνο.

Οποιοσδήποτε χρήστης bitcoin κρατά ένα αντίγραφο του Blockchain, το οποίο αυξάνεται συνεχώς, αυτό σημαίνει ότι απαιτείται αποθήκευση πολλών gigabytes. Τα κινητά πορτοφόλια λειτουργούν μόνο με πολύ μικρά υποσύνολα του Blockchain, βασιζόμενα σε αξιόπιστους κόμβους του δικτύου για να εξασφαλίσουν ότι έχουν τις σωστές πληροφορίες, με αυτό τον τρόπο τα κινητά πορτοφόλια επωφελούνται από την απλοποιημένη τεχνολογία επαλήθευσης πληρωμών.



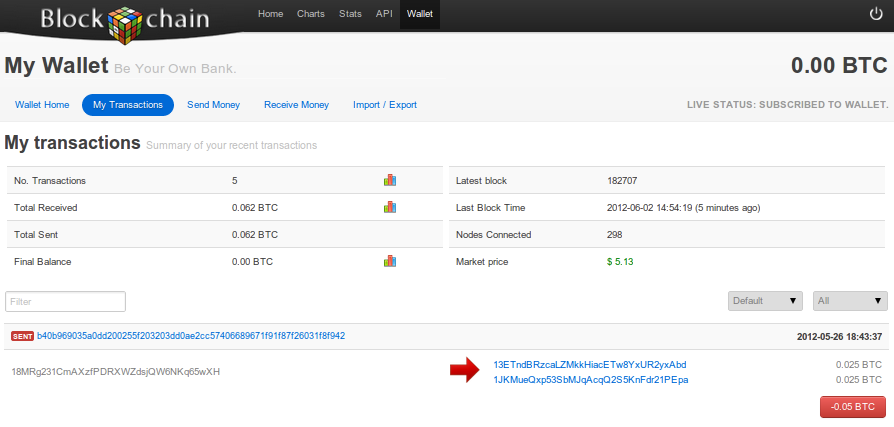
Το κύριο πλεονέκτημα των φορητών πορτοφολιών είναι ότι επιτρέπουν στους χρήστες να έχουν γρήγορη πρόσβαση και να χρησιμοποιούν εύκολα τα κέρματά τους σε ένα φυσικό κατάστημα.

Τα κινητά πορτοφόλια έρχονται σε δύο μορφές, ο ένας τύπος εφαρμογής αποθηκεύει τα νομίσματά τοπικά στην κινητή συσκευή και έχει τα ίδια ακριβώς πλεονεκτήματα και μειονεκτήματα με τα πορτοφόλια για επιτραπέζιους υπολογιστές, ενώ ο άλλος τρόπος που είναι αυτός του φορητού πορτοφολιού, παρέχει πρόσβαση σε διακομιστές αποθήκευσης και έχει τα ίδια πλεονεκτήματα και μειονεκτήματα με τα online πορτοφόλια τα οποία θα παρουσιαστούν στη συνέχεια.

Ουσιαστικά παρά το γεγονός ότι τα κινητά πορτοφόλια είναι μια βολική λύση για την αποθήκευση των bitcoins, τα κινητά πορτοφόλια είναι πολύ επιρρεπή σε επιθέσεις χάκερ. Επιπλέον, ο έλεγχος του πορτοφολιού μπορεί να χαθεί αν κάποιος άλλος αποκτήσει πρόσβαση στην κινητή συσκευή.

Υπάρχει μια μεγάλη ποικιλία εφαρμογών Bitcoin wallet για συσκευές που εκτελούνται σε Android. Η Apple απαγόρευσε τα Bitcoin wallets από το AppStore τον Φεβρουάριο του 2014, αλλά ανέτρεψε την απόφασή της κάποιους μήνες αργότερα.

*Online wallets (Διαδικτυακά πορτοφόλια)*: Είναι πορτοφόλια που βασίζονται στο διαδίκτυο, είναι προσβάσιμα από οποιαδήποτε συσκευή, και είναι επομένως πολύ βολικά.



Ωστόσο, το κύριο μειονέκτημα τους είναι ότι τα ιδιωτικά κλειδιά αποθηκεύονται στο διαδίκτυο από τους ιδιοκτήτες των ιστοτόπων και όχι τοπικά στη συσκευή, συνεπώς αυτός ο τύπος πορτοφολιού απαιτεί μεγάλη εμπιστοσύνη στους κατόχους των ηλεκτρονικών πορτοφολιών και στα επίπεδα ασφαλείας τους.

*Paper wallets (χαρτοφυλάκιο χαρτιού)*: Ένα χαρτοφυλάκιο χαρτιού είναι ουσιαστικά ένα έγγραφο που περιέχει μια δημόσια διεύθυνση που μπορεί να χρησιμοποιηθεί για τη λήψη bitcoins και ένα ιδιωτικό κλειδί το οποίο όπως είπαμε επιτρέπει στον χρήστη να ξοδεύει ή να μεταφέρει τα bitcoins που είναι αποθηκευμένα στη διεύθυνση αυτή. Αυτά συχνά εκτυπώνονται με τη μορφή QR κωδικών, έτσι ώστε να μπορούν να σαρωθούν γρήγορα και να προστεθούν τα κλειδιά σε ένα πορτοφόλι λογισμικού για την πραγματοποίηση της συναλλαγής.



Ένα Paper wallet μπορεί να δημιουργηθεί χρησιμοποιώντας υπηρεσίες όπως το BitAddress ή το Bitcoinpaperwallet. Το παραγόμενο έγγραφο μπορεί στη συνέχεια να εκτυπωθεί, με ορισμένες υπηρεσίες που προσφέρουν ανθεκτικότητα στην παραβίαση. Το κύριο πλεονέκτημα ενός χάρτινου πορτοφολιού είναι ότι τα κλειδιά δεν αποθηκεύονται ψηφιακά, γεγονός που το καθιστά εντελώς άνοσο σε επιθέσεις χάκερ, κακόβουλων λογισμικών που μπορεί να καταγράψουν τις πληκτρολογήσεις του χρήστη και γενικά οποιαδήποτε μορφή ψηφιακής κλοπής.

Ωστόσο, πρέπει να ληφθούν ορισμένες προφυλάξεις κατά τη δημιουργία και διατήρηση ενός χάρτινου πορτοφολιού, όπως το να χρησιμοποιείται εκτυπωτής που δεν είναι συνδεδεμένος στο διαδίκτυο και τη προστασία του χαρτιού από την γενική φθορά, την υγρασία κτλ.

*Hardware wallets (Πορτοφόλι υλικού ή υλισμικού)*: Το πορτοφόλι υλικού ή υλισμικού (hardware) είναι μια φυσική ηλεκτρονική συσκευή, που έχει κατασκευαστεί αποκλειστικά για την ασφαλή φύλαξη των bitcoins. Αποθηκεύει τα ιδιωτικά κλειδιά του χρήστη σε μια ασφαλή συσκευή υλικού. Είναι ο πιο ασφαλής τρόπος αποθήκευσης των bitcoins αφού δεν έχουν υπάρξει επαληθεύσιμα κρούσματα υποκλοπής χρημάτων από αυτόν τον τύπο πορτοφολιού. Επιπλέον, τα πορτοφόλια υλικού είναι πλήρως προστατευμένα ακόμη κι αν η συσκευή συνδεθεί με υπολογιστή που έχει μολυνθεί με κακόβουλο λογισμικό αφού είναι ανοσοποιημένα από ιούς.

Η δημιουργία και η διαφύλαξη ιδιωτικών κλειδιών εκτός διαδικτύου με τη χρήση πορτοφολιού υλικού εξασφαλίζει ότι οι χάκερ δεν μπορούν να αποκτήσουν πρόσβαση στα bitcoins. Ακόμη και αν το πορτοφόλι χαθεί η καταστραφεί εφόσον ο χρήστης δημιουργήσει έναν μυστικό κωδικό ασφαλείας τα bitcoins γίνεται να ανακτηθούν. Το μεγαλύτερο μειονέκτημα είναι ότι οι συσκευές αυτές είναι ακριβές.[[18]](#footnote-18)

Τα τρία πιο δημοφιλή πορτοφόλια υλικού είναι τα εξής:

|  |  |  |
| --- | --- | --- |
| tilt5b7jk7801  Ledger Nano S 58€ | αρχείο λήψης  KeepKey 99€ | 1_Wd8j7VCF1wyIrChOoADhLg  Trezor 99€ |

* + 1. Πως ακριβώς γίνεται η δημιουργία ενός ψηφιακού πορτοφολιού:

Στο συγκεκριμένο παράδειγμα θα δημιουργήσουμε ένα ψηφιακό πορτοφόλι μέσω της ιστοσελίδας <https://www.bitgo.com>

1. Όπως φαίνεται στην εικόνα, για την δημιουργία ενός ψηφιακού πορτοφολιού είναι αναγκαία αρχικά η δημιουργία ενός λογαριασμού χρήστη. Η εγγραφή αυτή χρειάζεται τη διεύθυνση email και έναν κωδικό χρήστη.



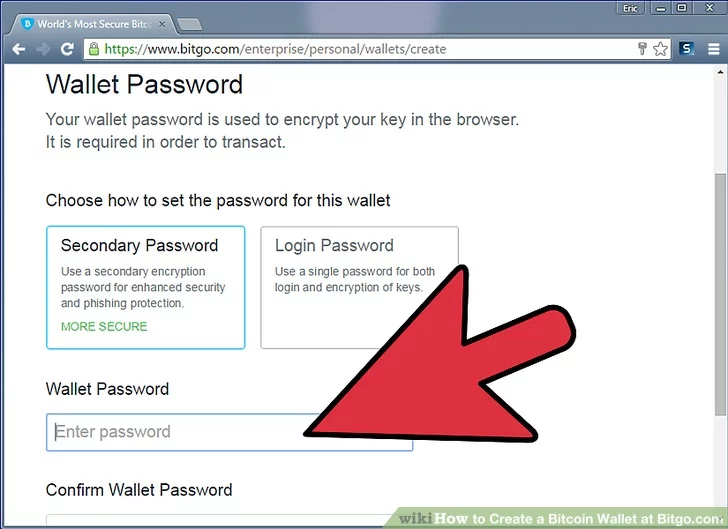
1. Στο δεύτερο βήμα: click στο Create a wallet.



1. Στο τρίτο βήμα ο χρήστης επιλέγει ένα όνομα για το ηλεκτρονικό πορτοφόλι.



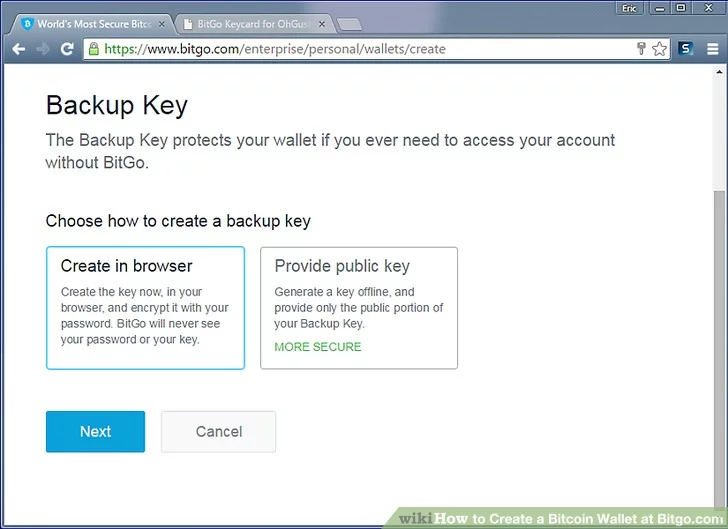
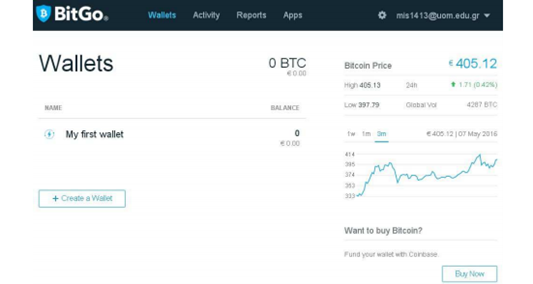
1. Στην συνέχεια θα ζητηθεί η δημιουργία ενός κωδικού που θα ανήκει στο ηλεκτρονικό πορτοφόλι.



1. Στο πέμπτο βήμα γίνεται ο έλεγχος ταυτότητας δύο παραγόντων μέσω ενός κωδικού που αποστέλλεται στο κινητό τηλέφωνο για μεγαλύτερη ασφάλεια.



1. Στη συνέχεια επιλέγεται ο τρόπος, με τον οποίο δημιουργείται το «Backup key» το οποίο είναι αναγκαίο για την πρόσβαση στον λογαριασμό μας χωρίς την πλατφόρμα του BitGo.



1. Έπειτα ο χρήστης είναι έτοιμος να προσθέσει bitcoins στον λογαριασμό πατώντας το κουμπί Buy Now.[[19]](#footnote-19)
   1. Πλεονεκτήματα & Μειονεκτήματα του Bitcoin
      1. Πλεονεκτήματα του Bitcoin

Τα σημαντικότερα πλεονεκτήματα είναι τα εξής:

1. Αποκέντρωση: H αποκέντρωση είναι το σημαντικότερο χαρακτηριστικό του Βitcoin αφού όπως προαναφέρθηκε δεν εποπτεύεται από κάποια χώρα, αρχή ή πρόσωπο. Ο χρήστης είναι αυτός που έχει τον πλήρη έλεγχο της εκτέλεσης των συναλλαγών εφόσον το ιδιωτικό του κλειδί δεν έχει παραβιαστεί. Δεν υπάρχει άλλο ηλεκτρονικό σύστημα μετρητών στο οποίο ο λογαριασμός να μην διαχειρίζεται από κάποιον τρίτο. Ο κώδικας του λογισμικού δηλαδή του Blockchain είναι ανοιχτός και συντηρείται από διάφορους χρήστες σε όλο τον κόσμο.
2. Ιδιωτικότητα συναλλαγών: Στο δίκτυο του Bitcoin δεν απαιτείται η ταυτότητα του χρήστη ή προσωπικές πληροφορίες. Τον ρόλο αυτόν τον εξυπηρετούν η διεύθυνση ή οι διευθύνσεις των bitcoin που κατέχει ο χρήστης. Οι διευθύνσεις αυτές είναι ψευδώνυμες και δεν έχουν καμία σχέση με τα προσωπικά στοιχεία του χρήστη ή την τοποθεσία του, αν και έχουν αναγνωρίσιμα χαρακτηριστικά για να εντοπίζονται από το διαδίκτυο. H ικανότητα της πραγματοποίησης των συναλλαγών καθορίζεται καθαρά και μόνο από την κατοχή των απαραίτητων πόρων για την επιθυμητή συναλλαγή.
3. «Ασπίδα» απέναντι στον πληθωρισμό: Όπως ήδη γνωρίζουμε στα συμβατικά νομίσματα fiat (ευρώ, δολάρια, γιέν κτλ) η προσφορά δεν είναι προκαθορισμένη και οι κεντρικές τράπεζες μπορούν να εκδώσουν όσα χρήματα επιθυμούν. Μπορούν ακόμη και να επιχειρήσουν να χειραγωγήσουν την αξία κάποιου νομίσματος σε σχέση με τα υπόλοιπα. Αντίθετα, στην περίπτωση του Bitcoin γνωρίζουμε ότι ο αριθμός των bitcoin που μπορεί να παραχθεί φτάνει τα 21 εκατομμύρια. Αυτό εμποδίζει την ύπαρξη πληθωρισμού αφού όσο και αν αυξηθεί η ζήτηση για τα bitcoins η προσφορά θα παραμείνει ίδια. Αυτό είναι ιδιαίτερα αισιόδοξο αν σκεφτούμε ότι η ιστορία είναι γεμάτη από νομίσματα που κάποια στιγμή απλά έπαψαν να χρησιμοποιούνται λόγω του υπερπληθωρισμού.
4. Μεγαλύτερη ασφάλεια για τους εμπόρους: Οι συναλλαγές με bitcoin χαρακτηρίζονται από μεγάλη ασφάλεια και μη αναστρεψιμότητα. Αυτό σημαίνει ότι ο έμπορος δεν εκτίθεται σε κινδύνους όπως δόλιες επιστροφές χρημάτων (chargebacks) που συμβαίνoυν συχνά σε συναλλαγές που πραγματοποιούνται μέσω πιστωτικών καρτών ή τραπεζικών συναλλαγών όπου ο αποστολέας έχει τη δυνατότητα να αντιστρέψει ή να "χρεώσει" την πληρωμή. Μέσω της χρήσης του Bitcoin, υπάρχει η δυνατότητα επέκτασης σε καινούργιες αγορές ακόμη και σε αυτές όπου οι πιστωτικές και χρεωστικές κάρτες δεν μπορούν να χρησιμοποιηθούν ή ακόμη και σε αυτές που τα ποσοστά απάτης είναι εξαιρετικά μεγάλα.
5. Χαμηλό κόστος μεταφοράς και μεγάλη ταχύτητα συναλλαγών: Κατά τη μεταφορά bitcoin τα τέλη είναι εξαιρετικά χαμηλά και σταθερά σε σxέση με τις συμβατικές μεθόδους μεταφοράς χρημάτων και δεν επηρεάζονται από την αξία που μεταφέρει κανείς. Ένα κανονικό τέλος bitcoin είναι 0,0005 BTC ανά μεταφορά, το οποίο χρεώνεται για την πληρωμή των miner που είδαμε παραπάνω. Αντίθετα σε μια τυπική διεθνή μεταφορά χρημάτων μπορεί τα τέλη να φτάσουν από 18ε έως και 34ε.
6. Ταχύτητα συναλλαγών: η μεγάλη ταχύτητα των συναλλαγών που χαρακτηρίζει τo bitcoin είναι ένα από τα σπουδαιότερα πλεονεκτήματα του, αφού οι συναλλαγές που πραγματοποιούνται με αυτό επιβεβαιώνονται συνήθως σε λιγότερο από μια ώρα χωρίς κάποια άδεια πληρωμής. Αντίθετα, οι διεθνείς τραπεζικές μεταφορές μπορούν να διαρκέσουν από λίγες ημέρες έως περισσότερο από μία εβδομάδες ή ακόμη και να μην γίνουν ποτέ αποδεκτές αν η δικαιοδοσία δεν τις θεωρήσει έγκυρες.
7. Δεν υπάρχει γραφειοκρατία: καθένας, από οποιαδήποτε χώρα, οποιασδήποτε ηλικίας, μπορεί να δεχτεί και να στείλει bitcoins μέσα σε λίγα λεπτά. Δεν απαιτείται ταυτότητα, διαβατήριο ή απόδειξη διεύθυνσης σε αντίθεση με τις συμβατικές τράπεζες που ζητούν όλα αυτά σε όποιον θέλει να ανοίξει έναν λογαριασμό. Το μόνο που χρειάζεται όπως είδαμε είναι η εγκατάσταση ενός προγράμματος bitcoin wallet και να δημιουργηθεί μια διεύθυνση bitcoin.
8. Οι πληροφορίες είναι διαφανείς: με την αλυσίδα μπλοκ, όλες οι οριστικοποιημένες συναλλαγές είναι διαθέσιμες για όλους, αλλά οι προσωπικές πληροφορίες είναι ανώνυμες. Όπως είπαμε μόνο το δημόσιο κλειδί είναι ορατό και αυτό δεν συνδέεται με τα προσωπικά στοιχεία του χρήστη.
9. Άμυνα απέναντι στην κρίση: η οικονομική κρίση έχει δημιουργήσει τεράστια κρίση εμπιστοσύνης στο χρηματοπιστωτικό σύστημα κατά συνέπεια, όλο και περισσότερος κόσμος ψάχνει για εναλλακτικές λύσεις. Σημαντικό είναι το γεγονός ότι το Bitcoin είναι ένα νόμισμα το οποίο δεν έχει χρέη, για αυτό το λόγο συχνά λέμε ότι μοιάζει περισσότερο στον χρυσό παρά στο συμβατικό χρήμα.
   * 1. Μειονεκτήματα του Bitcoin

Τα κυριότερα μειονεκτήματα είναι τα εξής:

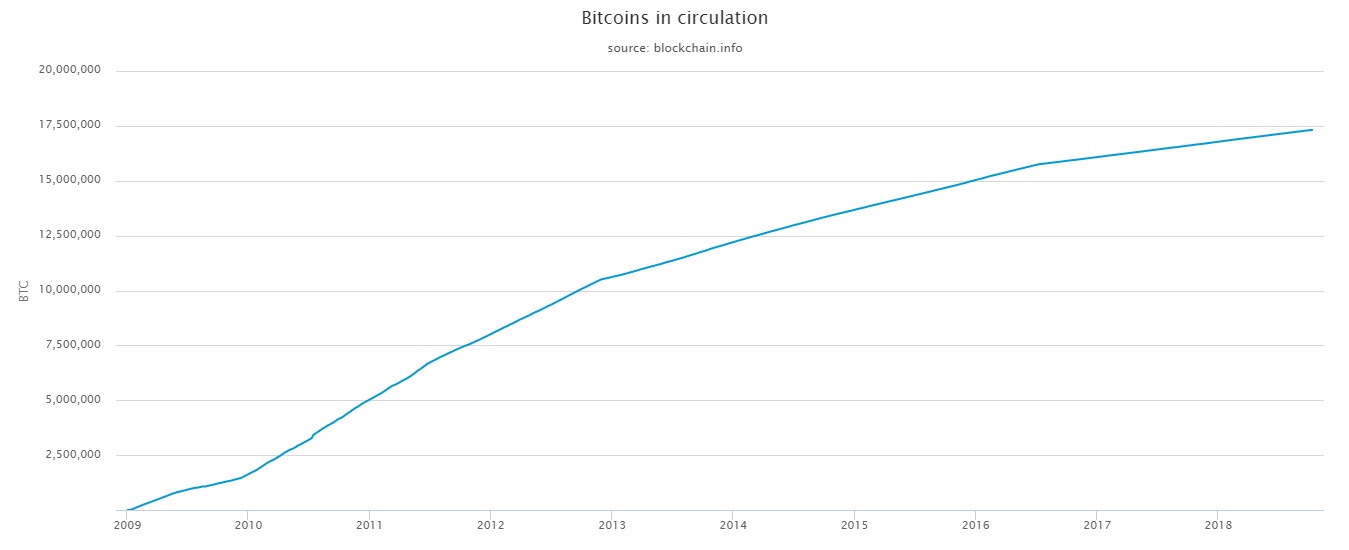
1. Χαμηλός βαθμός αποδοχής: Ο βαθμός αποδοχής παραμένει χαμηλός αφού πολλοί άνθρωποι δεν είναι ενήμεροι σχετικά με το Bitcoin ή δεν το εμπιστεύονται. Αν και καθημερινά όλο και περισσότερες επιχειρήσεις αρχίζουν να δέχονται τα bitcoins ως ένα μέσo πληρωμής ο αριθμός παραμένει περιορισμένος.
2. Τα ψηφιακά πορτοφόλια μπορεί να χαθούν ή να καταστραφούν: Εάν ένας σκληρός δίσκος χαλάσει ή ένας ιός καταστρέψει δεδομένα ή το ψηφιακό πορτοφόλι χαθεί, τότε και τα bitcoins με την σειρά τους χάνονται. Σρη περίπτωση αυτή δεν υπάρχει περιθώριο ανάκτησης. Αυτά τα χρήματα θα είναι ‘’ορφανά’’ για πάντα στο σύστημα. Αυτό μπορεί να χρεοκοπήσει έναν πλούσιο επενδυτή bitcoin μέσα σε λίγα δευτερόλεπτα χωρίς καμία μορφή ανάκαμψης. Τα νομίσματα που κατέχει ο επενδυτής θα παραμείνουν αναξιοποίητα στο σύστημα.
3. Αστάθεια τιμών: Η αξία των bitcoins διαρκώς κυμαίνεται ανάλογα με τη ζήτηση. Όπως φαίνεται και στο παρακάτω διάγραμμα, σε μόλις έναν χρόνο το Βitcoin έχασε την αξία του σε ποσοστό 63,50%. Στα μέσα του Δεκέμβρη του 2017 η αξία του Bitcoin άγγιζε τα 19,539.22 $ ενώ στις αρχές του Δεκεμβρίου του 2018 η αξία του φτάνει μόλις τα 4,105.34$ (<https://www.coinbase.com/price/bitcoin>).



1. Ακόμη μεγαλύτερη αίσθηση προκαλεί το γεγονός ότι η πρώτη συναλλαγή που πραγματοποιήθηκε με bitcoins το 2010 όπως είδαμε και παραπάνω ήταν για την αγορά δυο κουτιών με πίτσα έναντι 10,000 bitcoins που τότε άξιζαν περίπου 23$, ενώ σήμερα η αξία τους αγγίζει τα 40 εκατομμύρια. Φαίνεται λοιπόν πόση αστάθεια παρουσιάζει το συγκεκριμένο νόμισμα και τι υπεραξία δημιουργεί. Αυτό σημαίνει ότι είναι δύσκολο να εξυπηρετεί τις καθημερινές μας αγορές αφού η αποτίμηση των αγαθών και των υπηρεσιών λόγω της αστάθειας της τιμής του Bitcoin καθίσταται αδύνατη.
2. Δεν υπάρχει προστασία αγοραστών: Όπως είδαμε ένα από τα θετικά χαρακτηριστικά του Bitcoin είναι η μη αναστρεψημότητα. Το συγκεκριμένο χαρακτηριστικό όμως ωφελεί μόνο τους εμπόρους τους οποίους και προστατεύει από πολλούς κινδύνους, δυστυχώς όμως για τους αγοραστές μπορεί να αποβεί ζημιογόνο, αφού στην περίπτωση που ο πωλητής δεν στείλει το υποσχόμενο αντικείμενο δεν μπορεί να γίνει τίποτα για να αντιστραφεί η συναλλαγή. Αξίζει να τονιστεί ότι αυτός ο κίνδυνος μπορεί να αποφευχθεί χρησιμοποιώντας μια υπηρεσία μεσεγγύησης τρίτου μέρους όπως είναι το ClearCoin. Η υπηρεσία αυτή στην ουσία αναλαμβάνει τον ρόλο των τραπεζών, αυτό όμως σημαίνει ότι το Bitcoin χάνει το σπουδαιότερο χαρακτηριστικό του, αυτό της αποκέντρωσης.
3. Δεν υπάρχει εγγύηση αποτίμησης: Δεδομένου ότι το Bitcoin δεν εποπτεύεται από κάποια κεντρική αρχή κανείς δεν μπορεί να εγγυηθεί την ελάχιστη αποτίμησή του. Έτσι αν για κάποιο λόγο η αποτίμηση των bitcoins μειωθεί σημαντικά αυτό μπορεί να προκαλέσει μεγάλη ζημιά, ιδιαίτερα σε εκείνους που έχουν μετατρέψει ή επενδύσει μεγάλο μέρος των χρημάτων τους σε bitcoins.
4. Μεγάλες απαιτήσεις σε ενέργεια: Όλο το σύστημα του Bitcoin όπως είδαμε βασίζεται στην αλυσίδα Βlockchain και την επιβεβαίωση των συναλλαγών που πραγματοποιούνται από υπολογιστές σε όλο τον κόσμο. Οι υπολογιστές αυτοί πραγματοποιούν συνεχείς υπολογισμούς και ανταγωνίζονται ο ένας τον άλλον για να δημιουργήσουν το επόμενο μπλοκ συναλλαγών στην αλυσίδα. Ακόμη και οι χρήστες που τελικά δεν κερδίζουν, δαπανούν υπολογιστική ισχύ. Όσο η δυσκολία αυξάνεται τόσο περισσότερο αυξάνεται και η δαπανωμένη ηλεκτρική ενέργεια. Οι αυξανόμενες απαιτήσεις ηλεκτρικής ενέργειας του Bitcoin έχουν αρχίσει να προβληματίζουν το ευρύ κοινό και τα ερωτήματα και οι προβληματισμοί για τις περιβαλλοντικές επιπτώσεις της εξόρυξης και χρήσης του κρυπτονομίσματος είναι πολλά.[[20]](#footnote-20) Σύμφωνα με μια έρευνα, η ελάχιστη τρέχουσα χρήση του δικτύου Bitcoin είναι 2,55 gigawatts, δηλαδή σχεδόν όσο η ηλεκτρική ενέργεια που καταναλώνει ετησίως η Ιρλανδία. Μάλιστα προβλέπεται ότι σύντομα το δίκτυο μπορεί να αγγίξει τα 7,7 gigawatts, ενέργεια που εξισώνεται με την ενέργεια που δαπανά ολόκληρη η Αυστρία, και το 0,5% της παγκόσμιας κατανάλωσης.
   1. Στατιστικά στοιχεία
      1. Πλήθος Βitcoin σε κυκλοφορία

Από τον πρώτο χρόνο κυκλοφορίας του νομίσματος μέχρι και τις αρχές του 2010 παρατηρείται μια σχετικά ομαλή αύξηση των παραγόμενων μονάδων του εικονικού νομίσματος που αγγίζει τα 1,7 εκατομμύρια bitcoins.

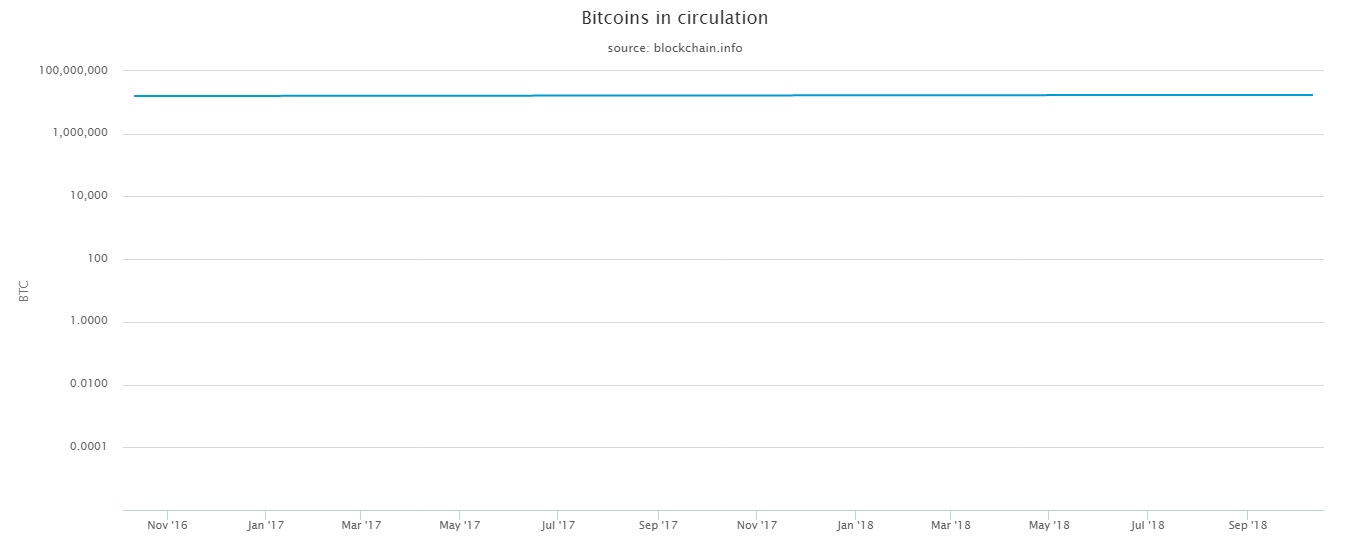
Από το 2010 ο ρυθμός παραγωγής γίνεται όλο και μεγαλύτερος. Στις αρχές του 2011 τα bitcoins φτάνουν τα 5,5 περίπου εκατομμύρια, το 2013 καταφέρνουν να διπλασιαστούν και να αγγίξουν τα 11 εκατομμύρια.



[https://www.blockchain.com/el/charts/total-bitcoins?timespan=all#](https://www.blockchain.com/el/charts/total-bitcoins?timespan=all)

Στις αρχές του 2014 παρατηρείται ότι τα bitcoins φτάνουν τα 12 εκατομμύρια και μέχρι τα τέλη του 2016 καταφέρνουν να αγγίξουν τα 16 εκατομμύρια. Φαίνεται επίσης ότι μέχρι το τέλος του 2017 και τις αρχές του 2018 δεν υπήρξε κάποια αξιοσημείωτη αύξηση αφού τα bitcoins παρέμειναν στα 16 εκατομμύρια.

Παρατηρώντας εκτενέστερα τα δυο τελευταία έτη από το παρακάτω διάγραμμα, φαίνεται ότι όντως υπάρχει μια μεγάλη στασιμότητα ως προς τον ρυθμό μεταβολής. Το γεγονός αυτό όμως δεν προκαλεί εντύπωση, αφού όπως προαναφέρθηκε ο ρυθμός παραγωγής των bitcoins μειώνεται κάθε τέσσερα χρόνια και θα σταματήσει όταν το πλήθος των bitcoin αγγίξει τα 21 εκατομμύρια, έτσι η εξόρυξή γίνεται όλο και δυσκολότερη. Σήμερα ο ακριβής αριθμός των bitcoins είναι 17,3 εκατομμύρια, αυτό σημαίνει ότι έχει ήδη παραχθεί πάνω από το 80% των bitcoins.



<https://www.blockchain.com/el/charts/total-bitcoins?timespan=2years&scale=1>)

* + 1. Tιμή αγοράς Bitcoin

Η τιμή του Bitcoin καθορίζεται από την αλληλεπίδραση μεταξύ της προσφοράς και τη ζήτησης του νομίσματος. Ορισμένοι ερευνητές έδειξαν ότι δείκτες όπως ο Dow Jones και η τιμή του πετρελαίου μπορούν μακροπρόθεσμα να επηρεάσουν την ζήτηση και άρα την τιμή του Bitcoin. Θετική σχέση επίσης έχει διαπιστωθεί μεταξύ της τιμής του Bitcoin και του Google search, Wiki views,Google Trends κτλ.



<https://www.blockchain.com/el/charts/market-price?timespan=all>

Καθοριστικό ρόλο επίσης στην τιμή του Bitcoin παίζει το ρυθμιστικό πλαίσιο λειτουργίας του Bitcoin, αφού κρατικές παρεμβάσεις όπως οι απαγορεύσεις της Κίνας για συναλλαγές με ψηφιακά νομίσματα ή οι περιοριστικοί κανόνες που επέβαλε η Νέα Υόρκη ως προς τα ανταλλακτήρια κρυπτονομισμάτων συνέβαλλαν στην μείωση της τιμής. Σημαντικό ρόλο έπαιξε επίσης η κλοπή και η πτώχευση ορισμένων ανταλλακτηρίων Bitcoin.

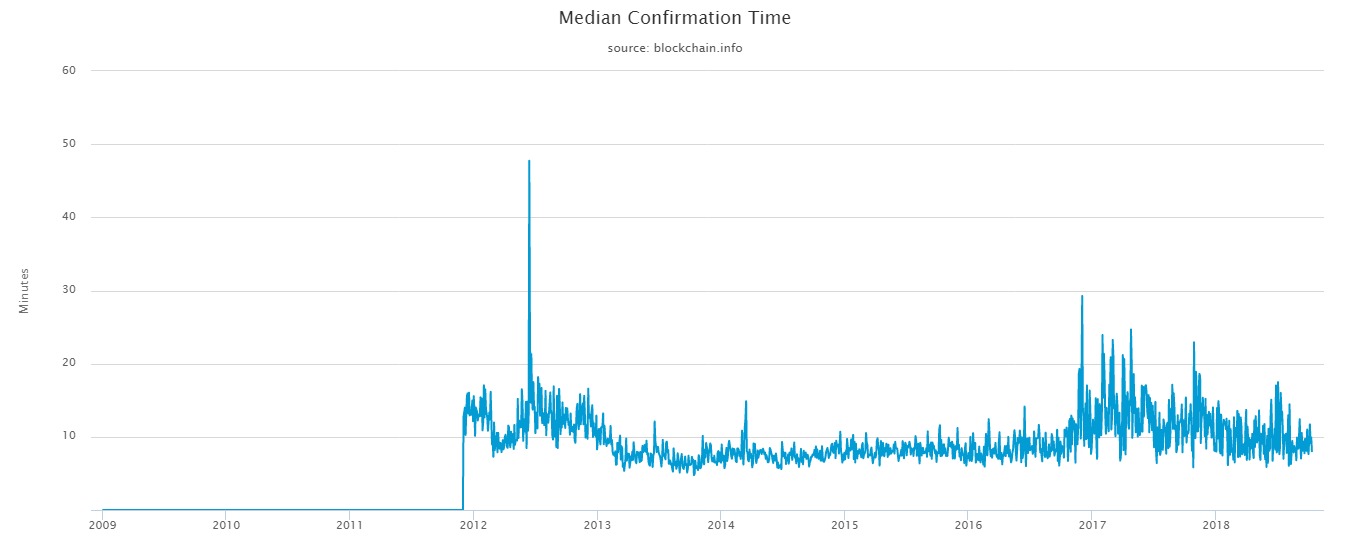
Όπως φαίνεται από το παραπάνω διάγραμμα από το 2009 μέχρι τα μέσα του 2013 η τιμή αγοράς του Bitcoin δεν ξεπέρασε τα 200 δολάρια. Τον Νοέμβριο του 2013 ήρθε η πρώτη μεγάλη αύξηση της τιμής, παρατηρείται ότι η τιμή τετραπλασιάστηκε και έφτασε τα 1150 δολάρια, σταδιακά όμως άρχισε να μειώνεται. Η μείωση της τιμής επήλθε πιθανώς ύστερα από το κλείσιμο της ιστοσελίδας Silk road που θα αναλυθεί στην συνέχεια. Από το 2015 έως τις αρχές του 2016 η τιμή δεν ξεπέρασε τα 450 δολάρια. Έπειτα βλέπουμε μια συνεχώς αυξανόμενη πορεία ώσπου τον Δεκέμβριο του 2017 η τιμή του Bitcoin άγγιξε τα 19.200 δολάρια στην πλατφόρμα συναλλαγών Bitfinex. Στο παρακάτω διάγραμμα στο οποίο φαίνονται μόνο οι τιμές για το 2017 και το 2018 παρατηρείται ότι δύο μήνες μετά την κορύφωση της τιμής η αξία της μειώθηκε στο ήμισυ και έφτασε τα 7000 δολάρια. Τον Δεκέμβριο του 2018 δεν ξεπερνά τα 3400 δολάρια. Το ξεπούλημα του Bitcoin αλλά και άλλων κρυπτονομισμάτων από τον Ιάνουάριο του 2018, έπειτα από την άνθηση των τιμών τον Δεκέμβριο του 2017 ονομάστηκε Bitcoin crash. Μερικοί οικονομολόγοι, διάσημοι επενδυτές και επαγγελματίες του χρηματοπιστωτικού τομέα προειδοποίησαν ότι οι ταχέως αυξανόμενες τιμές θα μπορούσαν να προκαλέσουν έκρηξη της «φούσκας».



<https://www.blockchain.com/el/charts/market-price?timespan=2years>)

* + 1. Χρόνος επιβεβαίωσης συναλλαγών

Ένα από τα μειονεκτήματα των συναλλαγών με bitcoins είναι η καθυστέρηση που υπάρχει πριν το δίκτυο ξεκινήσει να επιβεβαιώνει τη συναλλαγή συμπεριλαμβάνοντάς την σε ένα μπλοκ και πριν να μπορέσουν τα bitcoins να χρησιμοποιηθούν.

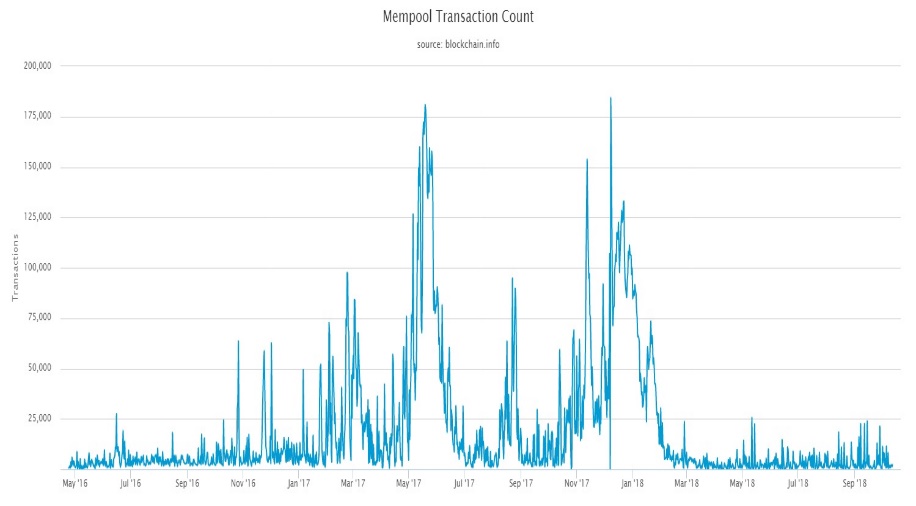


<https://www.blockchain.com/el/charts/median-confirmation-time?timespan=all>

Φαίνεται ότι μέχρι τον Νοέμβριο του 2011 ο χρόνος που απαιτούνταν για την επιβεβαίωση μιας συναλλαγής ήταν μηδενικός. Από το 2012 και έπειτα όσο η εξόρυξη των bitcoins αυξανόταν με ραγδαίο ρυθμό όπως είδαμε από το πρώτο διάγραμμα αυξήθηκε και ο απαιτούμενος χρόνος επιβεβαίωσης, φτάνοντας στα μέσα του 2012 τα 48 λεπτά. Το 2013 ο χρόνος μειώθηκε φτάνοντας μέχρι και τα 5 λεπτά. Στα ίδια περίπου επίπεδα κινήθηκε και τα επόμενα δυο χρόνια, στα τέλη του 2016 βλέπουμε πάλι τον χρόνο να αυξάνεται και να φτάνει τα 29 λεπτά το μέγιστο. Σήμερα ο απαιτούμενος χρόνος αγγίζει τα 8 λεπτά.

* + 1. Αριθμός των συναλλαγών που αναμένεται να επιβεβαιωθεί.

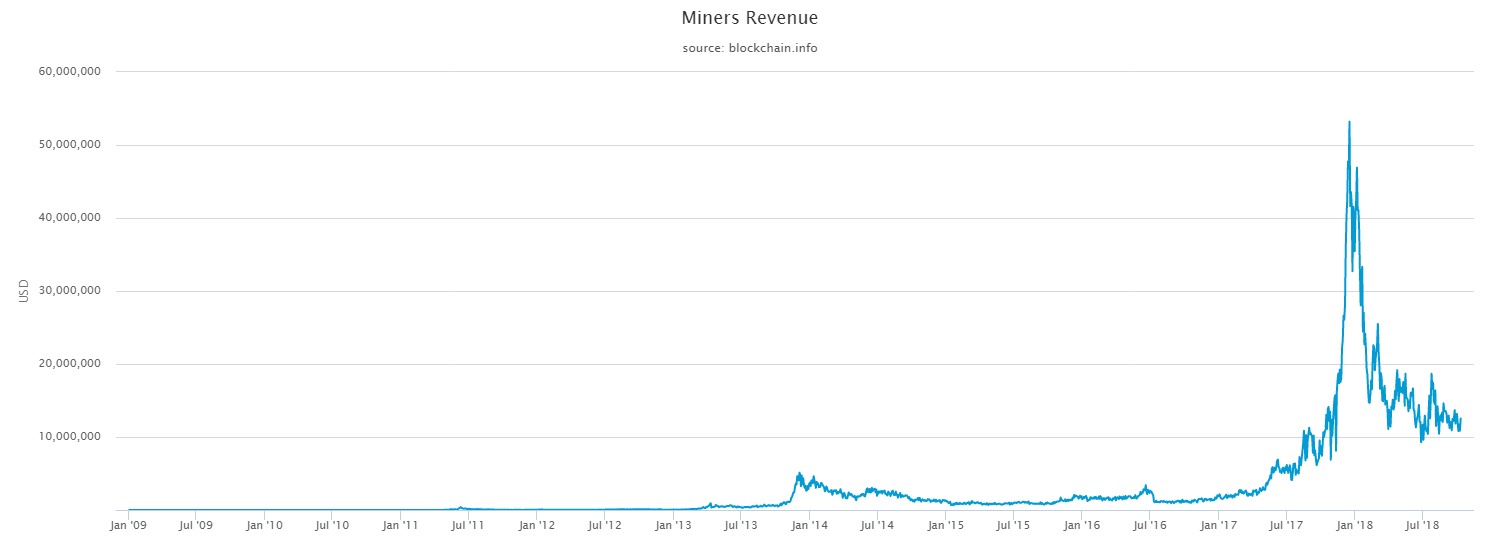
Όπως παρουσιάστηκε στο προηγούμενο διάγραμμα το 2016 ο αριθμός των bitcoin που εξορύχθηκε άγγιζε τα 15 εκατομμύρια και ο αριθμός των συναλλαγών που αναμένονταν να επιβεβαιωθεί έφτανε τις 58 χιλιάδες. Στα μέσα του 2017 φτάνουν τα 180 χιλιάδες bitcoins που αναμένονταν να επιβεβαιωθούν. Από τις αρχές του 2018 παρατηρείται ο αριθμός αυτός να μειώνεται σημαντικά και να φτάνει ακόμη και τις 545 συναλλαγές, γεγονός που ίσως προκύπτει από την μείωση του χρόνου επιβεβαίωσης των συναλλαγών που παρουσιάζεται στο πιο κάτω διάγραμμα.



<https://www.blockchain.com/btc/unconfirmed-transactions>

* + 1. Συνολική αξία των ανταμοιβών που καταβάλλονται στους miners

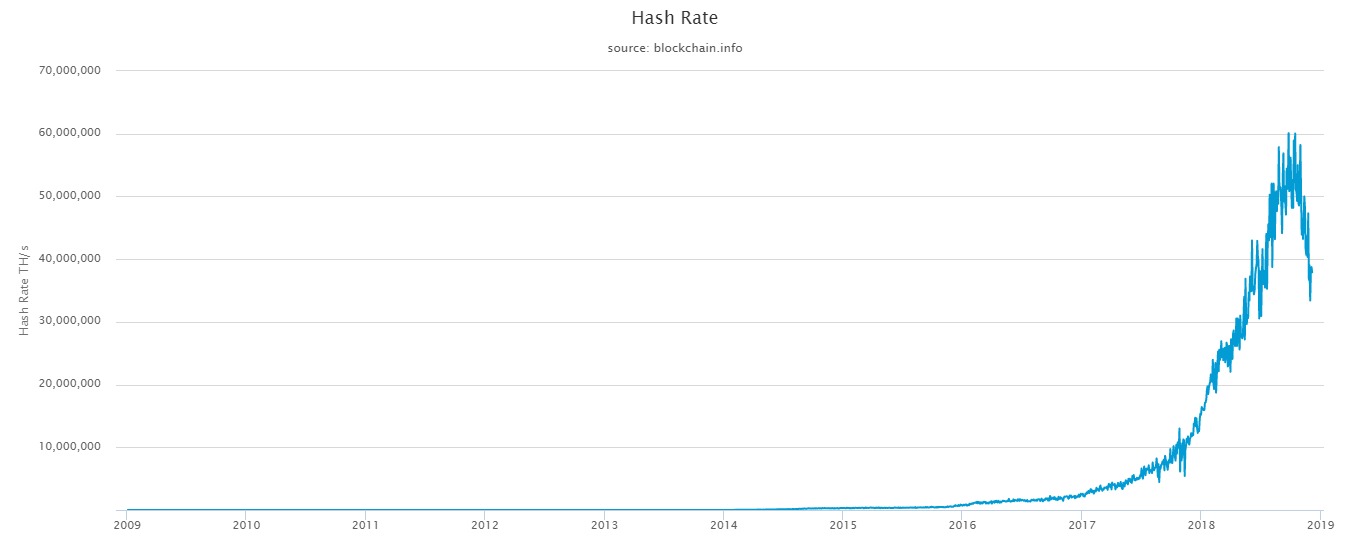
Από το πιο κάτω διάγραμμα φαίνεται ότι μέχρι τα τέλη του 2010 οι ανθρακωρύχοι δεν έπαιρναν κάποια αμοιβή, στα μέσα του 2011 η αμοιβή έφτασε τα 390 χιλιάδες δολάρια και στις αρχές του 2014 ξεπέρασε τα 3 εκατομμύρια. Στις αρχές του 2018 οι αμοιβές άγγιξαν τα 52 εκατομμύρια. Σήμερα δεν ξεπερνάνε τα 12 εκατομμύρια δολάρια.



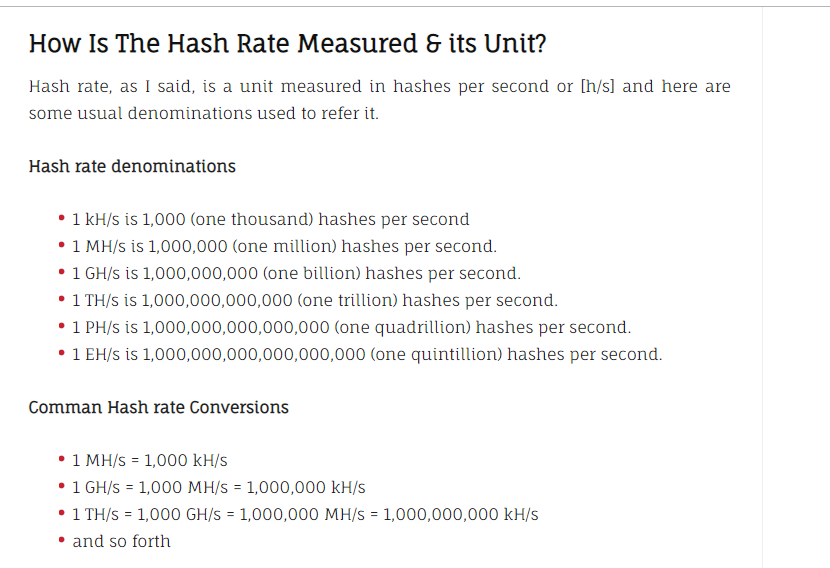
<https://www.blockchain.com/el/charts/miners-revenue?timespan=all>

* + 1. Hast rate και κατανάλωση ηλεκτρικής ενέργειας (για trillions of hashes/sec)

To Ηash rate είναι μονάδα μέτρησης που υπολογίζει πόση ενέργεια καταναλώνει το δίκτυο Bitcoin για να είναι σε λειτουργία. Όπως φαίνεται στο πιο κάτω διάγραμμα μέχρι τα μέσα του 2013 τα hashes που καταναλωνόντουσαν ήταν σχεδόν μηδενικά. Έπειτα άρχισαν σταδιακά να αυξάνονται. Στις αρχές του 2016 έφτασε τα 1,242,261 ΤΗ/sec. Ένα χρόνο μετά διπλασιάστηκε. Τον Ιανουάριο του 2018 έφτασε τα 16,415,541 ΤΗ/sec ενώ τον Σεπτέμβριο του 2018 άγγιξε την κορυφή των 55,000,000 περίπου. Τον Δεκέμβριο του 2018 διακρίνεται μια σημαντική μείωση που φτάνει τα 33,404,487 TH/ δευτερόλεπτο. Ο πιο κάτω πίνακας θα βοηθήσει στην κατανόηση της σημαντικότητας αυτών των μεγεθών. Όπως, φαίνεται 1TH είναι 1,000,000,000,000 hashes.



<https://www.blockchain.com/el/charts/hash-rate>



<https://coinsutra.com/hash-rate-or-hash-power/>

1. ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)
   1. Γενικά

Η Προστασία Προσωπικών Δεδομένων και η επεξεργασία αυτών δεν αποτελεί νέο εγχείρημα τόσο στον Ευρωπαϊκό όσο και στον διεθνή χώρο. Από τα τέλη του 1960, όπου έκαναν την εμφάνισή τους οι Ηλεκτρονικοί υπολογιστές, μεταβλήθηκε και η βασική έννοια της επεξεργασίας αλλά και των νομοθετημάτων. Έννοιες όπως προσωπική ελευθερία, άσυλο κατοικίας και ιδιωτική ζωή παύουν πλέον να ισχύουν με την υπάρχουσα μορφή λόγω της τεχνολογικής ανάπτυξης. Το ηλεκτρονικό εμπόριο ήταν το σημείο στο οποίο η αθέμιτη επεξεργασία προσωπικών δεδομένων έλαβε τις μεγαλύτερες διαστάσεις και συγκεκριμένα κατά τη σύναψη ηλεκτρονικών συμβάσεων με ηλεκτρονικά καταστήματα. Προκειμένου ο μέσος καταναλωτής να προβεί σε αγορά μέσω ενός e-shop, αναγκάζεται να κοινοποιήσει σε αυτό προσωπικά δεδομένα, όπως για παράδειγμα, ονοματεπώνυμο, διεύθυνση, email κ.ο.κ. Γι αυτό λοιπόν, στη διάρκεια αυτής της διαδικασίας, θα πρέπει το ηλεκτρονικό κατάστημα να είναι σε θέση να εγγυηθεί στον εκάστοτε πελάτη, πως τα προσωπικά του δεδομένα μπορούν να παραμείνουν ασφαλή στη διάρκεια της ηλεκτρονικής σύμβασης. Το ηλεκτρονικό κατάστημα, θα πρέπει να φροντίσει να κάνει γνωστή στον καταναλωτή την πολιτική απορρήτου που ακολουθεί, όπως επίσης και τα δικαιώματα του πελάτη του κατά την επεξεργασία των προσωπικών δεδομένων. Πολύ σημαντικό εγχείρημα όσον αφορά την άρση του άδικου χαρακτήρα της επεξεργασίας των προσωπικών δεδομένων, είναι η λήψη συγκατάθεσης από το υποκείμενο των δεδομένων.

Ο *Γενικός Κανονισμός Προστασίας Δεδομένων* (ΓΚΠΔ) (GDPR – General Data Protection Regulation) τέθηκε σε ισχύ στις 25 Μαΐου 2018 προς εφαρμογή από κάθε κράτος μέλος της ΕΕ. Ο ΓΚΠΔ Επηρεάζει κάθε οργανισμό και εταιρεία στην Ευρώπη, που διαχειρίζονται με οποιονδήποτε τρόπο προσωπικά δεδομένα πολιτών της ΕΕ κάθε μορφής καθώς και κάθε εταιρεία που συναλλάσσεται στην επικράτεια της Ευρωπαϊκής Ένωσης

O ΓΚΠΔ, ουσιαστικά, διευρύνει το φάσμα της διαφάνειας και καθορίζει τις υποχρεώσεις που αφορούν τη δημοσιοποίηση των παραβάσεων από την πλευρά των εταιριών. Τα ηλεκτρονικά καταστήματα, θα πρέπει να προβούν σε υιοθέτηση, τεχνικά αλλά και οργανωτικά, μέτρων ασφαλείας προκειμένου να μη βρεθούν στη δυσάρεστη θέση της επιβολής σε αυτά, σε περίπτωση παραβίασης προσωπικών δεδομένων καταναλωτών τους, πρόστιμα ύψους 20 εκατομμυρίων ευρώ ή 4% του συνολικού ετήσιου παγκόσμιου τζίρου τους.

* 1. Πεδίο εφαρμογής και στόχοι της οδηγίας

Η οδηγία εφαρμόζεται σε κάθε υπηρεσία, η οποία παρέχεται έναντι αμοιβής, είτε εξ αποστάσεως με ηλεκτρονικά μέσα και έπειτα από προσωπική αίτηση ενός αποδέκτη υπηρεσιών. Ο ΓΚΠΔ Εφαρμόζεται σε κάθε πληροφορία η οποία αφορά *ταυτοποιημένο ή ταυτοποιήσιμο*φυσικό πρόσωπο. Ειδικότερα, ο ΓΚΠΔ επικεντρώνεται στην προστασία των *ευαίσθητων προσωπικών δεδομένων*, τα οποία συμπεριλαμβάνουν και τα εξής: *δεδομένα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένα που αφορούν σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό*.

Όμως, ο Κανονισμός *δεν εφαρμόζεται* στις εξής περιπτώσεις:

* στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν νομικά πρόσωπα,
* Σε ζητήματα προστασίας θεμελιωδών δικαιωμάτων και ελευθεριών
* Σε ζητήματα εθνικής ασφάλειας ή πολιτικής ασφάλειας της Ένωσης
* Στην επεξεργασία προσωπικών δεδομένων από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας
* Στα δεδομένα προσωπικού χαρακτήρα θανούντων.

Πρέπει να αναφερθεί, όμως, ότι ο Κανονισμός αναφέρει πως το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν είναι απόλυτο δικαίωμα αλλά θα πρέπει να εκτιμάται σύμφωνα με την *αρχή της αναλογικότητας*. Για παράδειγμα, είναι δυνατόν το πιο κάτω μέτρο για τον περιορισμό και την καταπολέμηση της πανδημίας μπορούν να θεωρηθεί νόμιμο, φυσικά ύστερα από εξέταση των συνθηκών από ανώτατες δικαστικές αρχές: *η συλλογή και επεξεργασία προσωπικών δεδομένων (συμπεριλαμβανομένων των δεδομένων υγείας) των εργαζομένων από τον εργοδότη προκειμένου να προληφθεί ή να περιοριστεί η διάδοση του ιού στους εργαζομένους όσο το δυνατόν καλύτερα. Αυτό περιλαμβάνει ιδίως πληροφορίες σχετικά με τις περιπτώσεις στις οποίες έχει εντοπιστεί μία λοίμωξη ή ο εργαζόμενος έχει έρθει σε επαφή με ένα αποδεδειγμένα μολυσμένο άτομο και κατά τις οποίες πραγματοποιήθηκε κατά την σχετική περίοδο διαμονή σε περιοχή χαρακτηρισμένη ως περιοχή κινδύνου*.

Έτσι, με βάση τις πιο πάνω εξαιρέσεις, ο κανονισμός δεν εφαρμόζεται στον φορολογικό τομέα, σε ζητήματα προστασίας προσωπικών δεδομένων, σε θέματα ή πρακτικές που διέπονται από τη νομοθεσία σχετικά με τα καρτέλ, σε συμβολαιογραφικές δραστηριότητες και άλλες αντίστοιχες όπως η εκπροσώπηση πελάτη ενώπιον δικαστηρίου και τη συμμετοχή σε τυχερά παιχνίδια. Όσο αφορά τα τυχερά παιχνίδια, η εξαίρεση από το πεδίο εφαρμογής αφορά μόνο τα λαχεία, τα στοιχήματα και τα παιχνίδια τύχης, στα οποία ο παίκτης στοιχηματίζει νομισματική αξία και όχι στους διαφημιστικούς διαγωνισμούς ή περιπτώσεις στις οποίες αποσκοπούν σε πώληση αγαθών και υπηρεσιών, στα οποία οι πληρωμές χρησιμεύουν αποκλειστικά στην απόκτηση διαφημιζόμενων αγαθών ή υπηρεσιών.

Για τη διασφάλιση της ασφάλειας δικαίου και της εμπιστοσύνης του καταναλωτή, η οδηγία προσπάθησε να καθορίσει ένα ευρύ πλαίσιο ώστε να καλύπτει κάποιες από τις νομικές πτυχές του ηλεκτρονικού εμπορίου όσο αφορά στην εσωτερική αγορά. Βασικός στόχος ήταν το να εξασφαλιστεί η ελεύθερη κυκλοφορία των υπηρεσιών, μεταξύ των κρατών- μελών, αλλά και η ομαλή λειτουργία στην εσωτερική αγορά. Ουσιαστικά, αυτό που προσπάθησαν οι επινοητές του ΓΚΠΔ να επιτύχουν, ήταν η δημιουργία ενός «χώρου» χωρίς εθνικά σύνορα.

Η οδηγία αυτή δεν συμπεριλαμβάνεται στον κύκλο οδηγιών που έχουν εκδοθεί για σκοπούς προστασίας καταναλωτή. Στο άρθρο 3 παράγραφο 1, αναφέρεται πως αυτή «δεν θίγει το επίπεδο προστασίας, ειδικά της δημόσιας υγείας και των συμφερόντων του καταναλωτή, όπως θεσπίζεται στις κοινοτικές και εθνικές νομοθετικές πράξεις στο μέτρο που δεν υφίσταται περιορισμός της ελευθερίας παροχής υπηρεσιών της κοινωνίας της πληροφορίας». Πρόκειται δηλαδή, για την εξασφάλιση της θεμελιώδους αρχής του κοινοτικού κεκτημένου (acquis Communautaire), το οποίο στην προκειμένη περίπτωση εξειδικεύεται ως κεκτημένο προστασίας του καταναλωτή (acquis consommateur). Ερμηνεύεται, λοιπόν, ως υποχρέωση όλων των κρατών μελών για την τήρηση του παράγωγου κοινοτικού και εναρμονισμένου εθνικού δικαίου, το οποίο και ρυθμίζει όλα τα επιμέρους ζητήματα της προστασίας του καταναλωτή.

Όσον αφορά τον κανόνα αυτό, θα πρέπει να εφαρμόζεται με επιφύλαξη του μη περιορισμού της ελευθερίας κυκλοφορίας των υπηρεσιών κοινωνίας πληροφορίας. Οι συντάκτες της οδηγίας, δεν εστίασαν τόσο στην επίτευξη των στόχων κοινωνικής πολιτικής, αλλά βασικά στην εγκαθίδρυση μιας αγοράς χωρίς σύνορα, όσο αφορά τις υπηρεσίες της κοινωνίας πληροφορίας, η οποία κατά συνέπεια θα μπορούσε να οδηγήσει σε επίτευξη ενός υψηλού επιπέδου κοινοτικής ολοκλήρωσης. Η οδηγία αυτή, καθαυτή έχει κυρίως συμπληρωματικό χαρακτήρα προς το ισχύον ενωτικό δίκαιο, χωρίς όμως να θίγει το κοινοτικό κεκτημένο σε ζητήματα δημόσιας υγείας και προστασίας καταναλωτών και χωρίς τη θέσπιση πρόσθετων κανόνων ως προς τον τομέα του Ιδιωτικού Διεθνούς Δικαίου.

* 1. Οι βασικές αρχές της οδηγίας

Βασική αρχή της οδηγίας, είναι το να εξασφαλιστεί η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας , ανάμεσα στα κράτη- μέλη και διέπεται από τρείς βασικές αρχές:

* Αρχή της χώρας προέλευσης (country of origin principle). Σύμφωνα με αυτή, το κράτος, όπου ο φορέας μιας υπηρεσίας κοινωνίας πληροφοριών είναι εγκατεστημένος, είναι υπεύθυνο για την νομιμότητα της δραστηριότητας της. Συνεπώς, η εκάστοτε δραστηριότητα των ηλεκτρονικών καταστημάτων, στα πλαίσια των on-line υπηρεσιών τους, θα ορίζονται από το δίκαιο του κράτους όπου είναι εγκατεστημένα. Υποχρέωση του κάθε κράτους -μέλους είναι να μην επιβάλλει περιορισμούς στις υπηρεσίες κοινωνίας της πληροφορίας οι οποίες προέρχονται από διαφορετικό κράτος- μέλος, αντιθέτως θα πρέπει να εμπιστεύονται τις εθνικές νομοθεσίες των υπόλοιπων κρατών και να εφαρμόζουν την αρχή της αμοιβαίας αναγνώρισης. Σε ειδικές περιπτώσεις, δίνεται η δυνατότητα παρέκκλισης, για λόγους δημοσίας τάξεως, προστασίας της δημόσιας υγείας και ασφάλειας, αλλά και προστασίας του καταναλωτή/ επενδυτή. Τα λαμβανόμενα μέτρα ως παρέκκλιση, θα πρέπει όμως πάντοτε να είναι, σύμφωνα με την αρχή της αναλογικότητας και να περιορίζονται στα απολύτως αναγκαία.
* Αρχή της μη αναγκαίας προηγούμενης άδειας. Το κεφάλαιο ΙΙ της οδηγίας που τιτλοφορείται «Αρχές» συμπεριλαμβάνει αναφορά στην αρχή της μη αναγκαίας προηγούμενης άδειας στο άρθρο 4, εξαιρώντας τις περιπτώσεις καθεστώτων έγκρισης που δεν αφορούν ειδικά και αποκλειστικά τις υπηρεσίες κοινωνίας της πληροφορίας.
* Υποχρεώσεις πληροφόρησης και διαφάνειας. Στο ίδιο κεφάλαιο τονίζονται ως αρχές της Οδηγίας οι υποχρεώσεις πληροφόρησης και διαφάνειας. Πιο συγκεκριμένα, για να καταστεί εφικτή η διαφάνεια και η προστασία των καταναλωτών, προβλέπεται, η παροχή ορισμένων πληροφοριών, στις οποίες ο φορέας υπηρεσιών, και επί του πλαισίου το ηλεκτρονικό κατάστημα, οφείλει να παρέχει στους αποδέκτες των υπηρεσιών του, άλλως καταναλωτές. Αξίζει να αναφέρουμε στο σημείο αυτό, πως ο κοινοτικός νομοθέτης, προσδίδει στη διαφάνεια και την παροχή ουσιώδους πληροφόρησης , ιδιαίτερη βαρύτητα, κυρίως όταν πρόκειται για καταναλωτικές συμβάσεις, θεωρώντας , ότι με αυτόν τον τρόπο επιτυγχάνεται μετριασμός του γνωσιολογικού ελλείμματος του ως είθισται ανίδεου αποδέκτη και του δίνεται παράλληλα η δυνατότητα να λάβει συνειδητή και υπεύθυνη απόφαση.

Συνεπώς, σύμφωνα και με το άρθρο 5 του ΓΚΠΔ, για να είναι νόμιμη η επεξεργασία προσωπικών δεδομένων (απλών και ειδικών κατηγοριών «ευαίσθητων»), θα πρέπει η επεξεργασία να διέπεται από συγκεκριμένες αρχές. Αυτές είναι οι εξής 7 βασικές αρχές (δείτε και την ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων[[21]](#footnote-21)):

1. Η *αρχή της νομιμότητας*, αντικειμενικότητας και διαφάνειας. Σύμφωνα με τη συγκεκριμένη αυτή αρχή, τα δεδομένα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.
2. Η *αρχή του περιορισμού του σκοπού*, σύμφωνα με την οποία, τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.
3. Η *αρχή της αναλογικότητας* ή «ελαχιστοποίησης των δεδομένων», σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας.
4. Η *αρχή της ακρίβειας των δεδομένων*, σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων.
5. Η *αρχή της «ακεραιότητας και εμπιστευτικότητας»*, σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους.
6. Η *αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας* ή «περιορισμός της περιόδου αποθήκευσης», σύμφωνα με την οποία τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας.
7. Η *αρχή της λογοδοσίας του υπευθύνου επεξεργασίας,* σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή με τον Κανονισμό ενώπιον των εποπτικών αρχών και των δικαστηρίων.
   1. Το περιεχόμενο του κανονισμού

Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης αποφάσισαν στις 27 Απριλίου 2016 την υιοθέτηση ενός νέου νομικού πλαισίου στην Ε.Ε. για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Το συγκεκριμένο νομικό πλαίσιο αποτελείται από μια Οδηγία (2016/680) και έναν Κανονισμό. Τα δυο νομοθετήματα αυτά, αποτελούν πραγματικές τομές, στην προστασία των προσωπικών δεδομένων σε Ενωσιακό επίπεδο, αλλά ο Κανονισμός 2016/679 ή Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) απαριθμεί 99 άρθρα έναντι 34 της Οδηγίας και προβάλλει ως το πλέον βασικό ευρωπαϊκό κείμενο για την προστασία των προσωπικών δεδομένων στην Ε.Ε. Ο Γενικός Κανονισμός Προστασίας Δεδομένων, τέθηκε σε ισχύ στις 25 Μαΐου 2018.

Η Επιτροπή ωστόσο, πρότεινε ως νομοθετικό εργαλείο έναν Κανονισμό, εγκαταλείποντας την μέθοδο της προσαρμογής μέσω των Οδηγιών, διότι απέβλεπε στην συνεκτικότητα της ρύθμισης. Ο Κανονισμός σίγουρα οδηγεί σε μεγαλύτερο βαθμό εναρμόνισης, καθώς καθίσταται μέρος του εθνικού κανονιστικού συστήματος, χωρίς την ανάγκη υιοθέτησης εθνικών κανόνων, έχει άμεσο αποτέλεσμα, ανεξάρτητο από το εθνικό δίκαιο και υπερισχύει αντίθετων εθνικών κανόνων. Η υιοθέτηση του μοντέλου του Κανονισμού, αποσκοπούσε στην απλούστευση των διαδικασιών αλλά και στη μείωση του «κόστους συμμόρφωσης», ιδίως για τις εταιρίες που δραστηριοποιούνται σε περισσότερες χώρες της Ε.Ε. Η επιλογή αυτή συνάντησε τόσο αποδοχή όσο και επιφυλάξεις. Η επιλογή του Κανονισμού κρίθηκε από πολλούς, καθώς η δεσμευτική ισχύς του, ερχόταν σε αντίθεση με τις εθνικές αντιλήψεις και προτιμήσεις σχετικά με το επίπεδο προστασίας των προσωπικών δεδομένων. Οι επιφυλάξεις, αφορούσαν κυρίως στον κίνδυνο του πλήρους αποκλεισμού των εθνικών ρυθμίσεων, η οποία οδήγησε και σε μια αντίληψη «συγκεντρωτικής και μονοπωλιακής νομοθέτησης», καταργώντας μια βασική πτυχή του ενωσιακού δικαίου, την αρχή της επικουρικότητας. Οι αντιδράσεις, οφείλονταν σε μεγάλο βαθμό και στο γεγονός, ότι η πρόταση του Κανονισμού, έδινε στην Ευρωπαϊκή Επιτροπή ευρύτατη κανονιστική αρμοδιότητα, ώστε να προσδιορίζει το περιεχόμενο των ρυθμίσεων και των υποχρεώσεων. Συγκεκριμένα, οι αντιδράσεις είχαν προκύψει λόγω του ότι «αναγνωρίζονταν» στην Επιτροπή να υιοθετεί πράξεις κατ’ εξουσιοδότηση και εκτελεστικές πράξεις, μία αρμοδιότητα που ήταν ιδιαίτερα κρίσιμη. Το διακυβευόμενο αγαθό άλλωστε αποτελούσε και αποτελεί ένα θεμελιώδες δικαίωμα, επομένως θεωρήθηκε, ότι ενέπιπτε στην αρμοδιότητα του νομοθέτη (Συμβούλιο και Κοινοβούλιο). Παρά τις επιφυλάξεις για την ενίσχυση της κανονιστικής εξουσίας της Επιτροπής, μια ουσιαστική επιφύλαξη, αφορούσε στη δυνατότητα της Επιτροπής, να επεμβαίνει ακόμη και σε μεμονωμένες περιπτώσεις, καταστρατηγώντας τον ρόλο των εθνικών ανεξάρτητων αρχών. Η επιλογή του Κανονισμού, ως ρυθμιστικού εργαλείου, ώστε να εξασφαλίζεται «συνεκτικό και υψηλό επίπεδο προστασίας», «ισοδύναμο σε όλα τα κράτη μέλη» μέσω της «συνεκτικής και ομοιόμορφης εφαρμογής» επικράτησε τελικά, επιβεβαιώνοντας την κεντρική θέση που λαμβάνει το πεδίο της προστασίας προσωπικών δεδομένων μεταξύ των πολιτικών της Ε.Ε. και την μετάβαση από την εθνική στην ενωσιακή ρυθμιστική σφαίρα. Ωστόσο, παρά τον συμβιβασμό αυτό και τη φύση του Κανονισμού, ο Γενικός Κανονισμός Προστασίας Δεδομένων, περιέχει αρκετές «ρήτρες ευελιξίας», παραχωρώντας στα κράτη μέλη, την ευχέρεια να εξειδικεύσουν τους κανόνες του, συμπεριλαμβανομένων αυτών, που αφορούν την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, και να προσδιορίζουν τις περιστάσεις ειδικών καταστάσεων επεξεργασίας, μεταξύ άλλων τον ακριβέστερο καθορισμό των προϋποθέσεων, υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων επιβάλλει ένα ευρύ φάσμα απαιτήσεων σε εταιρείες που συλλέγουν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένης της απαίτησης συμμόρφωσης, με έξι βασικές αρχές:

1. Διαφάνεια, δικαιοσύνη και νομιμότητα στο χειρισμό και τη χρήση των προσωπικών δεδομένων. Θα πρέπει να καθίσταται απόλυτα σαφές στα άτομα, το πώς χρησιμοποιούνται τα προσωπικά τους δεδομένα και θα χρειαστεί επίσης μια "νόμιμη βάση" για την επεξεργασία αυτών των δεδομένων.
2. Περιορισμός της επεξεργασίας των προσωπικών δεδομένων σε καθορισμένους, σαφείς και νόμιμους σκοπούς. Δεν θα επιτρέπεται να επαναχρησιμοποιούνται ή να αποκαλύπτονται προσωπικά δεδομένα για σκοπούς που δεν είναι "συμβατοί" με το σκοπό για τον οποίο συλλέχθηκαν αρχικά.
3. Μείωση της συλλογής και αποθήκευσης δεδομένων προσωπικού χαρακτήρα σε εκείνα που είναι επαρκή και σχετικά για τον επιδιωκόμενο σκοπό.
4. Εξασφάλιση της ακρίβειας των προσωπικών δεδομένων και της δυνατότητας διαγραφής ή διόρθωσης. Θα χρειαστεί η λήψη μέτρων για να βεβαιωθεί το άτομο, ότι τα προσωπικά του δεδομένα είναι ακριβή και μπορούν να διορθωθούν αν προκύψουν σφάλματα.
5. Περιορισμός της αποθήκευσης προσωπικών δεδομένων. Θα χρειαστεί η διασφάλιση, ότι διατηρούνται προσωπικά δεδομένα, μόνο για όσο διάστημα είναι απαραίτητο για την επίτευξη των σκοπών για τους οποίους συλλέχθηκαν τα δεδομένα.
6. Επισφράγιση της ασφάλειας, της ακεραιότητας και της εμπιστευτικότητας των προσωπικών δεδομένων. Η εταιρεία πρέπει να λάβει μέτρα για την ασφαλή φύλαξη των προσωπικών δεδομένων μέσω τεχνικών και οργανωτικών μέτρων ασφαλείας.
   1. Τα δικαιώματα του υποκείμενου των δεδομένων

Τα δικαιώματα του υποκειμένου των δεδομένων, σύμφωνα με τον ΓΚΠΔ, είναι τα εξής[[22]](#footnote-22):

ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΕΝΗΜΕΡΩΣΗ

Ο υπεύθυνος επεξεργασίας δεδομένων λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σχετικά με την επεξεργασία των δεδομένων του σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, μεταξύ άλλων, εφόσον ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα.

Συνεπώς, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της, αλλά και να πληροφορείται κατά την διαδικασία της συλλογής, του δίνει τη δυνατότητα να εκτιμήσει την κατάσταση, να προσδιορίσει την πληροφοριακή συμπεριφορά του αλλά και να ασκήσει τα δικαιώματα τα οποία κατοχυρώνει ο νόμος. Η ενημέρωση που είχε εισαχθεί με την Οδηγία 95/46/ΕΚ ως δικαίωμα «δεύτερης γενιάς» είναι διατυπωμένη ταυτόχρονα ως δικαίωμα του υποκειμένου των δεδομένων και υποχρέωση του υπευθύνου επεξεργασίας. Η υποχρέωση ενημέρωσης υπάρχει, είτε οι σχετικές πληροφορίες προς επεξεργασία συλλέγονται από το ίδιο το υποκείμενο (άρθρο 13), είτε από άλλες πηγές (άρθρο 14).

Ο Κανονισμός περιλαμβάνει αρκετά λεπτομερείς ρυθμίσεις για το εύρος της πληροφορίας που πρέπει να παρέχεται σε κάθε περίπτωση, κοινώς, την πληροφόρηση για την ταυτότητα του υπεύθυνου επεξεργασίας, τους σκοπούς και τη νομική βάση της επεξεργασίας, το χρονικό διάστημα τήρησης, τους αποδέκτες, την πρόθεση διασυνοριακής διαβίβασης καθώς και τα δικαιώματα του προσώπου.

Άξιο αναφοράς είναι, ότι έχει ρητά εισαχθεί υποχρέωση ενημέρωσης και στην περίπτωση που τα δεδομένα, θα χρησιμοποιηθούν για άλλο σκοπό από εκείνον για τον οποίο αρχικά συλλέχθηκαν. Ο Κανονισμός αναφέρεται με λεπτομέρειες στο χρονικό σημείο και διάστημα εντός του οποίου, πρέπει να λαμβάνει χώρα η ενημέρωση αυτή.

Υφίστανται εξαιρέσεις ως προς το δικαίωμα ενημέρωσης, οι οποίες είναι:

1. Όταν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή συνεπάγεται δυσανάλογη προσπάθεια,
2. Όταν η επεξεργασία αφορά σκοπούς αρχειοθέτησης ή επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς,
3. Όταν η απόκτηση ή κοινοποίηση της πληροφορίας έχει ως έρεισμα διάταξη νόμου ή θα διακύβευε την εμπιστευτικότητα που επιβάλλεται από υποχρεώσεις τήρησης επαγγελματικού απορρήτου.

Το εύρος των ανωτέρω εξαιρέσεων έχει ως φυσικό επακόλουθο τον κίνδυνο αποδυνάμωσης του δικαιώματος ενημέρωσης

ΔΙΚΑΙΩΜΑ ΠΡΟΣΒΑΣΗΣ ΔΙΟΡΘΩΣΗΣ ΚΑΙ ΑΝΤΙΤΑΞΗΣ

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει αυτό, να γνωρίζει επακριβώς τους σκοπούς και λεπτομέρειες της επεξεργασίας, μεταξύ άλλων.

Κατά συνέπεια, η έγκαιρη, έγκυρη και κατανοητή πληροφόρηση αποτελεί βασική προϋπόθεση για την άσκηση του δικαιώματος πρόσβασης. Το δικαίωμα πρόσβασης κατέχει μια από τις σημαντικότερες θέσεις στο σύνολο των δικαιωμάτων, αφού διασφαλίζει τη δυνατότητα ενός προσώπου να ζητά επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα, που το αφορούν, υφίστανται επεξεργασία και εάν συμβαίνει αυτό, την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και σε πληροφορίες που αφορούν τους σκοπούς της επεξεργασίας, τις κατηγορίες των δεδομένων, τους αποδέκτες και σε λοιπά στοιχεία (άρθρο 15 ΓΚΠΔ) . Το δικαίωμα πρόσβασης, θα ήταν ατελέσφορο, αν δεν συνοδευόταν από τα δικαιώματα διόρθωσης και διαγραφής των προσωπικών δεδομένων. Το δικαίωμα διόρθωσης, συνυφασμένο πια με την αρχή της ακρίβειας των προσωπικών δεδομένων (άρθρο 5 παρ. 1 δ), συνίσταται στο δικαίωμα διόρθωσης ανακριβών ή και συμπλήρωσης ελλιπών προσωπικών δεδομένων (άρθρο 16). Το σύνολο των δικαιωμάτων, μέσω των οποίων ένα πρόσωπο, μπορεί να ασκήσει έλεγχο στην επεξεργασία των δεδομένων του, συμπληρώνεται με το δικαίωμα διαγραφής (άρθρο 17), του περιορισμού της επεξεργασίας (άρθρο 18), της φορητότητας (άρθρο 20), της εναντίωσης (άρθρο 21) και της μη αυτοματοποιημένης λήψης απόφασης (άρθρο 22). Ένα πρόσωπο δικαιούται να τίθεται ενάντια στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν ανά πάσα στιγμή, η οποία επεξεργασία όμως, επιβάλλεται για λόγους είτε εκπλήρωσης δημοσίου συμφέροντος (άρθρο 6 παρ. 1 ε) είτε ικανοποίησης εννόμου συμφέροντος (άρθρο 6 παρ. 1 στ.). Ο υπεύθυνος επεξεργασίας φέρει το βάρος να αποδείξει την συνδρομή επιτακτικών και νόμιμων λόγων για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων.

Το δικαίωμα του περιορισμού της επεξεργασίας αντιστοιχεί σε ένα δικαίωμα «μερικής ή προσωρινής εναντίωσης», έχει ουσιαστικά τον χαρακτήρα των ασφαλιστικών μέτρων. Το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν ισχύει ένας από έναν αριθμό λόγων που αναφέρονται στον κανονισμό για το δικαίωμα περιορισμού της επεξεργασίας. Ένα παράδειγμα τέτοιου λόγου είναι όταν η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για το χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα. Κατά συνέπεια, το υποκείμενο μπορεί, τελικά, να παρεμβαίνει αναστέλλοντας την επεξεργασία των δεδομένων του, εάν εκκρεμεί η επαλήθευση της ακρίβειας αυτών ή και της ίδιας της νομιμότητας της επεξεργασίας. Ως προς το δικαίωμα αυτό συμβαίνει το εξής παράδοξο, το υποκείμενο των δεδομένων να έχει την δυνατότητα να ζητήσει την διατήρηση των δεδομένων, προκειμένου να τα χρησιμοποιήσει στην θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

ΤΟ ΔΙΚΑΙΩΜΑ ΣΤΗ ΔΙΑΓΡΑΦΗ (ΔΙΚΑΙΩΜΑ ΣΤΗ «ΛΗΘΗ»)

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει κάποιος από έναν αριθμό λόγων που αναφέρονται στον κανονισμό για το δικαίωμα διαγραφής. Ένα παράδειγμα τέτοιου λόγου είναι όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Το δικαίωμα στη λήθη αποτελεί ένα νέο ψηφιακό δικαίωμα, το οποίο περιλαμβάνεται στο άρθρο 17 του ΓΚΠΔ. Η Viviane Reding, ωστόσο, πρώην Επίτροπος Δικαιοσύνης της Ε.Ε. και πρώην Αντιπρόεδρος της Επιτροπής έχει υπογραμμίσει, πως το δικαίωμα στη λήθη βασίζεται σε ήδη υπάρχοντες κανόνες και δεν αποτελεί δικαίωμα ex novo .

Το δικαίωμα στη λήθη αναγνωρίστηκε σε Ενωσιακό επίπεδο μετά την απόφαση της 13ης Μαΐου 2014 του Δικαστηρίου της Ε.Ε.. Η υπόθεση αυτή αφορούσε στις μηχανές αναζήτησης και την υποχρέωσή τους να αφαιρούν συνδέσμους προς ιστοσελίδες από τις λίστες των αποτελεσμάτων τους, έπειτα από αιτήματα των υποκειμένων των δεδομένων, με το επιχείρημα, ότι οι πληροφορίες αυτές δε θα πρέπει πλέον να συνδέονται με το όνομά τους μέσω ενός τέτοιου καταλόγου.

Πιο συγκεκριμένα, στις 5 Μαρτίου 2010 ο M. Costeja González, κάτοικος Ισπανίας, υπέβαλε στην Ισπανική Αρχή Προστασίας Δεδομένων (εφεξής AEPD) καταγγελία κατά της La Vanguardia Ediciones SL, η οποία εκδίδει καθημερινή εφημερίδα μεγάλης κυκλοφορίας, καθώς και κατά της Google Spain και της Google Inc. Η καταγγελία αυτή υποβλήθηκε, επειδή όταν ένας χρήστης του διαδικτύου εισήγε το ονοματεπώνυμο του M. Costeja González στη μηχανή αναζήτησης της Google, εμφανίζονταν σύνδεσμοι προς δύο σελίδες, η μια της εφημερίδας La Vanguardia, στις οποίες περιλαμβανόταν ανακοίνωση, με το ονοματεπώνυμο του M. Costeja González, για πλειστηριασμούς ακινήτων κατόπιν κατάσχεσης που του επιβλήθηκε λόγω κοινωνικοασφαλιστικών οφειλών .

Η AEPD απέρριψε την εν λόγω καταγγελία, κατά το μέρος που αφορούσε την La Vanguardia, εκτιμώντας ότι η εν λόγω δημοσίευση από πλευράς της των επίμαχων πληροφοριών ήταν από νομικής άποψης δικαιολογημένη, έγινε όμως δεκτή κατά το μέρος που αφορούσε την Google Spain και την Google Inc. Η AEPD έκρινε, ότι οι φορείς εκμετάλλευσης μηχανών αναζήτησης, υπόκεινται στη νομοθεσία περί προστασίας των δεδομένων, δεδομένου ότι, προβαίνουν σε επεξεργασία δεδομένων για την οποία φέρουν ευθύνη και ότι ασκούν δραστηριότητες μέσω της κοινωνίας της πληροφορίας.

Η Google Spain και η Google Inc. προσβάλαν, η καθεμία από πλευράς της, την εν λόγω απόφαση ενώπιον του Audiencia Nacional, το οποίο ανέστειλε την ενώπιον του διαδικασία και υπέβαλε στο Δικαστήριο σειρά προδικαστικών ερωτημάτων, ως προς το κατά πόσον οι σχετικές διατάξεις της Οδηγίας, θα μπορούσαν να χρησιμεύσουν ως νομική βάση για τις αξιώσεις του M. Costeja González περί αφαίρεσης των προσωπικών του δεδομένων από τη λίστα αποτελεσμάτων αναζήτησης που πραγματοποιείται στο διαδίκτυο. Η επιρροή του Δικαστηρίου, τόσο από την ήδη δημοσιευμένη τότε πρόταση της Επιτροπής και τη σκοπούμενη κατοχύρωση του δικαιώματος στη λήθη όσο και από την επακόλουθη δέσμευσή του στη διαδικασία μεταρρύθμισης του νομικού πλαισίου για την προστασία δεδομένων είναι εμφανής και από το επιχείρημά του, ότι ακόμη και η αρχικώς νόμιμη επεξεργασία, μπορεί να καταστεί ασυμβίβαστη με την Οδηγία, σε περίπτωση που τα εν λόγω δεδομένα δεν είναι πλέον απαραίτητα σύμφωνα με τους σκοπούς για τους οποίους συλλέχθηκαν ή υπέστησαν επεξεργασία.

Εν συνεχεία, προσφεύγοντας δε και σε ρυθμίσεις του πρωτογενούς Ενωσιακού δικαίου, τονίστηκε πως το δικαίωμα του υποκειμένου των δεδομένων να ζητά αφαίρεση των πληροφοριών που το αφορούν από τα αποτελέσματα των μηχανών αναζήτησης βασίζεται στα άρθρα 7 και 8 του Χάρτη και τα ότι τα δικαιώματα αυτά παρακάμπτουν, όχι μόνο το οικονομικό συμφέρον του χειριστή της μηχανής αναζήτησης, αλλά και το ενδιαφέρον του ευρύτερου κοινού για την εύρεση πληροφοριών σχετικά με το υποκείμενο των δεδομένων. Εξαίρεση, αποτελούν τα δημόσια πρόσωπα, καθώς η παρέμβαση στα θεμελιώδη δικαιώματά τους δικαιολογούνται από το επικρατέστερο ενδιαφέρον του ευρύτερου κοινού να έχει πρόσβαση στις εν λόγω πληροφορίες. Τελικά, υπάγοντας στα πραγματικά περιστατικά της κύριας δίκης στα αποτελέσματα της ερμηνευτικής του προσέγγισης, το Δικαστήριο έκρινε πως πράγματι θεμελιώνεται το δικαίωμα του υποκειμένου των δεδομένων να μη συνδέονται πλέον οι πληροφορίες αυτές με το όνομά του μέσω των αποτελεσμάτων αναζήτησης.

Οι μηχανές αναζήτησης, λοιπόν, έχουν συμμορφωθεί πλέον με την απόφαση του Δικαστηρίου και ανταποκρίνονται , στα αιτήματα διαγραφής. Μετά την Google, τόσο η Bing όσο και η Yahoo έχουν δημοσιεύσει ηλεκτρονική αίτηση για διαγραφή. Ωστόσο, το ψηφιακό δικαίωμα στη λήθη δεν αφορά μόνο στην υποχρέωση των μηχανών αναζήτησης να αφαιρούν συνδέσμους που αφορούν προσωπικά δεδομένα. Αυτό συμβαίνει, καθότι ενσαρκώνει στην ουσία, το αίτημα των ατόμων, να έχουν τη δυνατότητα να επιτυγχάνουν την αφαίρεση των προσωπικών τους δεδομένων, ιδίως εκείνων που έχουν δημοσιευθεί σε μέσα κοινωνικής δικτύωσης, εκτός εάν υπάρχει επιτακτικός λόγος για τη διατήρησή τους.

Επί της ουσίας, το δικαίωμα στη λήθη αφορά τη δυνατότητα αποτελεσματικής αντιμετώπισης των συνεπειών του Διαδικτύου που «δεν ξεχνά ποτέ», διασφαλίζοντας την προσωπική αυτονομία του ατόμου και την προστασία της ιδιωτικής ζωής. Στον ψηφιακό κόσμο, το δικαίωμα αυτό παίρνει μια πιο ρεαλιστική μορφή: γίνεται αντιληπτό ως το αίτημα ενός ατόμου σε διαγραφή των δεδομένων που τον αφορούν και μπορεί κάλλιστα να αναδιατυπωθεί ως «δικαίωμα στη λήθη του κυβερνοχώρου» .

Παρά τη φιλοδοξία της Επιτροπής και τις προσδοκίες που καλλιεργήθηκαν η τελική αποτύπωση του δικαιώματος δεν συνιστά προφανώς μια «αλλαγή παραδείγματος» ως προς την προστασία των προσώπων. Το «δικαίωμα στη λήθη» αντιμετωπίζεται από αρκετούς περισσότερο ως μια επέκταση, μια επεξήγηση του δικαιώματος διαγραφής των δεδομένων. Πράγματι στον Κανονισμό εντάσσεται στο δικαίωμα διαγραφής (άρθρο 17) που ωστόσο φέρει ως –κατά τι αληθή εντός παρενθέσεως και εισαγωγικών – παράτιτλο «δικαίωμα στη λήθη».

Σύμφωνα με τη ρύθμιση, ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράφει τα δεδομένα, εφόσον: α) στερούνται νόμιμης βάσης (ανάκληση συγκατάθεσης, παράνομη επεξεργασία, υπέρβαση αναγκαίου για τον σκοπό χρόνου τήρησης), β) η διαγραφή επιβάλλεται από τον νόμο, γ) ασκείται λυσιτελώς το δικαίωμα εναντίωσης στην επεξεργασία, δ) πρόκειται για δεδομένα που είχαν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε ανήλικο,

Ειδικότερα, όσον αφορά το δικαίωμα εναντίωσης, το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν. Κατά συνέπεια, ο υπεύθυνος επεξεργασίας δεν υποβάλλει πλέον τα δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Το δικαίωμα διαγραφής δεν είναι απεριόριστο αλλά οροθετείται από την ύπαρξη νομικής υποχρέωσης προς επεξεργασία, το δημόσιο συμφέρον ή τα δικαιώματα ή τα έννομα συμφέροντα άλλων προσώπων (ελευθερία έκφρασης, δικαίωμα ενημέρωσης, δικαίωμα στην έννομη προστασία) καθώς και για σκοπούς που αφορούν την επιστημονική ή ιστορική έρευνα που επιβάλλουν την διατήρηση των δεδομένων και την απόρριψη του αιτήματος διαγραφής.

Μία βασική διαφορά του δικαιώματος έναντι των άλλων δικαιωμάτων (εναντίωση, περιορισμός) υπογραμμίζεται στην αναδρομικότητά του. Η διαγραφή αλλάζει εν τέλει την έκταση της επεξεργασίας, ακόμη κι αν αυτή είχε πραγματοποιηθεί σύννομα στο παρελθόν.

ΔΙΚΑΙΩΜΑ ΣΤΗ ΦΟΡΗΤΟΤΗΤΑ

Τσ υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα τύπο αρχείου, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα όταν συντρέχουν κάποιο λόγοι που αναφέρονται στο σχετικό άρθρο του κανονισμού.

Το δικαίωμα στη φορητότητα αποτελεί μία καινοτομία του Κανονισμού και συνίσταται σε δύο βασικές πτυχές: το δικαίωμα του προσώπου να λαμβάνει δεδομένα που έχει παράσχει σε υπεύθυνο επεξεργασίας και το δικαίωμα να διαβιβάζει τα δεδομένα του σε άλλο υπεύθυνο επεξεργασίας, χωρίς να εμποδίζεται σε αυτό από τον υπεύθυνο επεξεργασίας, στον οποίο αρχικά παρασχέθηκαν (άρθρο 20). Η Επιτροπή ευελπιστούσε στη δυνατότητα της ευχέρειας της «μετακίνησης» δεδομένων από πάροχο σε πάροχο, κυρίως με γνώμονα τα ψηφιακά κοινωνικά δίκτυα. Χαρακτηριστικό παράδειγμα, είναι η παροχή δικαιώματος στον χρήστη υπηρεσιών κοινωνικής δικτύωσης, όπως το Facebook αλλά και της δυνατότητας, αφενός να ελέγχει όλες τις πληροφορίες που έχει αναρτήσει στη συγκεκριμένη πλατφόρμα και αφετέρου να ζητήσει τη μεταφορά τους σε άλλη πλατφόρμα.

Η Επιτροπή επιδίωκε να αντιμετωπίσει το λεγόμενο lock – in των χρηστών και ως αποτέλεσμα να αυξήσει τον ανταγωνισμό μεταξύ των παρόχων κοινωνικών δικτύων. Η εισαγωγή του δικαιώματος αυτού αντιμετωπίστηκε με επιφύλαξη, διότι προσιδίαζε περισσότερο στο δίκαιο του ανταγωνισμού και στο δίκαιο του καταναλωτή.

Το δικαίωμα αυτό, λοιπόν, εφαρμόζεται σε κάθε υπεύθυνο επεξεργασίας που επεξεργάζεται προσωπικά δεδομένα με ηλεκτρονικά μέσα, αποκλείοντας από το πεδίο εφαρμογής του δικαιώματος τα έντυπα και αρχεία τυπωμένα σε χαρτί. Γίνεται μάλιστα δεκτό, ότι εφαρμόζεται και στην περίπτωση των παρόχων υπηρεσιών υπολογιστικού νέφους.

Παρόλο, που το δικαίωμα φορητότητας προβλέφθηκε προκειμένου να ενισχύσει την θέση του υποκειμένου, το πεδίο εφαρμογής του είναι ιδιαίτερα περιορισμένο και αρκείται στις περιπτώσεις που η επεξεργασία θεμελιώνεται στη συγκατάθεση του προσώπου ή σε μια συμβατική σχέση με αυτό. Ως εκ τούτου, το δικαίωμα αυτό, περιορίζεται στα δεδομένα που έχει παράσχει το ίδιο το πρόσωπο και δεν επεκτείνεται σε αυτά που παράγονται από τον πάροχο για το πρόσωπο. Η άσκηση του δικαιώματος φορητότητας δεν θα πρέπει να επηρεάζει τα δικαιώματα και τις ελευθερίες τρίτων .

Όσον αφορά, την απευθείας διαβίβαση μεταξύ παρόχων, η εφαρμογή της εξαρτάται εν τέλει από το εάν είναι τεχνικά εφικτή (άρθρο 20 παρ. 2).

* 1. Ζητήματα προστασίας προσωπικών δεδομένων στο ηλεκτρονικό εμπόριο
     1. Συγκατάθεση πελάτη

Ο όρος «συγκατάθεση» εμφανίζεται σε πολλούς κλάδους του δικαίου, ως νομιμοποιητικό γεγονός, ως όρος, δηλαδή, που άρει την απαγόρευση μιας, πρωτίστως, μη επιτρεπόμενης ενέργειας. Στο δίκαιο των προσωπικών δεδομένων, δεν εισάγεται για πρώτη φορά με τον Γενικό Κανονισμό Προστασίας Δεδομένων. Υπό το καθεστώς της Οδηγίας 95/46/ΕΚ η συγκατάθεση του υποκειμένου, έχει την έννοια δήλωσης βουλήσεως του υποκειμένου των δεδομένων, η οποία είναι ελεύθερη, ρητή και δίδεται υπό καθεστώς πλήρους επίγνωσης για τα έννομα αποτελέσματά της και με την οποία το υποκείμενο των δεδομένων δηλώνει ότι δέχεται, πως τα δεδομένα του, δύνανται να αποτελέσουν αντικείμενο επεξεργασίας.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, στο στοιχείο 11’ του άρθρου 4 δίνει τον ορισμό της συγκατάθεσης, ο οποίος φαίνεται, να αποτελεί αντιγραφή της προηγούμενης ρύθμισης. Έτσι λοιπόν, ως συγκατάθεση του υποκειμένου των δεδομένων ορίζεται κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρη επίγνωση με την οποία το υποκείμενο των δεδομένων εκδηλώνει, ότι συμφωνεί, με δήλωση ή σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα, που το αφορούν. Η πρώτη μεγάλη διαφορά είναι, πως η συγκατάθεση του, πρέπει να έχει τη μορφή δήλωσης ή σαφούς θετικής ενέργειας.

Ακολουθώντας μια μακρά ερμηνευτική προσέγγιση των εποπτικών αρχών επί του ζητήματος, ο Ενωσιακός νομοθέτης προχωρά στην περαιτέρω διευκρίνηση της συγκατάθεσης, στο άρθρο 7 του Γενικού Κανονισμού Προστασίας Δεδομένων, για την περίπτωση που αυτή (η συγκατάθεση) αποτελεί τη νομιμοποιητική βάση της επεξεργασίας. Πλέον, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει, ότι το υποκείμενο των δεδομένων, έχει δώσει τη συγκατάθεσή του για την επεξεργασία. Το υποκείμενο, διατηρεί το δικαίωμα να ανακαλέσει τη συγκατάθεσή του, ανά πάσα στιγμή, χωρίς η ανάκληση αυτή να θίγει τη νομιμότητα της επεξεργασίας. Χρήζει δε, να ενημερώνεται σχετικά για την ύπαρξη του δικαιώματος ανάκλησης και για τον τρόπο που αυτή θα ανακαλείται, ο οποίος μάλιστα θα πρέπει να είναι ο ίδιος με αυτόν της αρχικής χορήγησης της συγκατάθεσης.

Άξιο αναφοράς είναι και το γεγονός πως για να θεωρηθεί μια συγκατάθεση ότι έχει ληφθεί σύννομα, σε περίπτωση που παρέχεται στο πλαίσιο γραπτής δήλωσης που αφορά και άλλα θέματα. Το αίτημα για συγκατάθεση πρέπει να υποβάλλεται κατά διακριτό τρόπο από τα υπόλοιπα θέματα και σε κατανοητή και εύκολα αντιληπτή μορφή. Χαρακτηριστική καινοτομία είναι και η ειδική ρύθμιση. ‘Όσον αφορά περιπτώσεις συγκατάθεσης που ελήφθησαν μέχρι και την ημέρα εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων και αφορούν επεξεργασία που συνεχίζεται και μετά από την ημέρα αυτή, σωστότερο κρίνεται να δεχθούμε πως δεν απαιτείται συγκατάθεση εάν καλύπτονται οι αυστηρότερες προϋποθέσεις που θέτει ο Κανονισμός.

Επίσης, η εγκυρότητα της συναίνεσης εκτιμάται κατ’ αναλογία με τις ρυθμίσεις του δικαίου των δικαιοπραξιών. Δηλαδή, η συναίνεση πρέπει να είναι ελεύθερη, γεγονός, το οποίο αναλύεται όχι μόνο στο πλαίσιο του θεσμού του εξαναγκασμού ή της ψυχικής πίεσης, αλλά το άρθρο 7 ευρύτερα ορίζει, πως ουσιώδες στοιχείο για την εκτίμηση της ελευθερίας της συναίνεσης του υποκειμένου των δεδομένων είναι το γεγονός, ότι η εφαρμογή όλης της σύμβασης, εξαρτάται από την αποδοχή της επεξεργασίας, ενώ η ίδια η επεξεργασία, δεν είναι στην ουσία απαραίτητη για την εκτέλεση της σύμβασης. Για παράδειγμα, αμφισβητείται η νομιμότητα της πρακτικής ενός ιστοτόπου, ο οποίος απαγορεύει σε ένα χρήστη γενική πρόσβαση στις ιστοσελίδες του, εάν αυτός δεν δεχθεί πρώτα τα “cookies” του, ενώ ο ιστοτόπος δεν προορίζεται, ειδικά, σε παροχή υπηρεσιών επεξεργασίας προσωπικών δεδομένων. Σε αυτή την περίπτωση, η συναίνεση του επισκέπτη είναι δυνατό να κριθεί ως πλασματική.

Συνεπάγεται, ότι απαιτείται μια θετική ενέργεια, η οποία πρέπει να καταγράφεται και η οποία μπορεί να λάβει τη μορφή μιας γραπτής δήλωσης αλλά και ενός κλικ, ενός πατήματος στην οθόνη, μιας κίνησης, κ.λπ. Αντιθέτως, δεν είναι συμβατός με τον θεσμό προστασίας ο μηχανισμός ο οποίος εξ αρχής (by default, «πλην ρητής αρνήσεως») προϋποθέτει, την συναίνεση του υποκειμένου των δεδομένων. Αντίθετα ,προωθείται από τον Κανονισμό, η έννοια της ενσωματωμένης πρόβλεψης της προστασίας («privacy by design»), παρόλο που αυτή η μορφή «κωδικοποίησης» του θεσμού προστασίας σε τεχνικά μέτρα προκαλεί ήδη κάποιες αντιδράσεις σε θεωρητικό επίπεδο.

* + 1. Γενικοί Όροι Συναλλαγών (ΓΟΣ)

Οι Γενικοί Όροι Συναλλαγών, συνιστούν τυποποιημένους όρους που προορίζονται να αποτελέσουν περιεχόμενο μεγάλου αριθμού ομοιόμορφων συμβάσεων έχοντας διαμορφωθεί πριν από τη σύναψή τους από τον κατά τεκμήριο οικονομικά και οργανωτικά ισχυρότερο συμβαλλόμενο. Η έννοιά τους νομοθετικά ορίζεται στο άρθ. 2 παρ. 1 του ν.2251/1994, όπου χαρακτηρίζονται ως ΓΟΣ, οι «όροι που έχουν διατυπωθεί εκ των προτέρων για μελλοντικές συμβάσεις» ανάμεσα στους προμηθευτές και τους καταναλωτές.

Στην παρ. 10 του ίδιου άρθρου μάλιστα, ο νόμος ερευνά το πεδίο εφαρμογής του, ορίζοντας ότι οι διατάξεις του «εφαρμόζονται και για κάθε όρο σύμβασης που δεν αποτέλεσε αντικείμενο ατομικής διαπραγμάτευσης», δηλαδή όταν ο καταναλωτής δεν μπόρεσε να επηρεάσει το περιεχόμενό του. Παρά τα πλεονεκτήματα που προσφέρει η χρήση των ΓΟΣ (όπως π.χ. η επιτάχυνση των διαδικασιών διαπραγμάτευσης και της κατάρτισης των συμβάσεων, η απλοποίηση των συναλλαγών, η ασφάλεια δικαίου κλπ.), υπάρχουν ουκ ολίγοι, κίνδυνοι για τους καταναλωτές, ακριβώς επειδή οι ΓΟΣ διαστρεβλώνονται μονομερώς από τους προμηθευτές, οι οποίοι περιορίζουν τις δικές τους υποχρεώσεις ή θέτουν στους καταναλωτές συμβατικά βάρη που, σύμφωνα με το ενδοτικό δίκαιο του Αστικού Κώδικα, οι ίδιοι έπρεπε να φέρουν. Για παράδειγμα, είναι σύνηθες να επιβάλλουν απαλλακτικές ρήτρες για την ευθύνη τους λόγω εσφαλμένης διαβίβασης των μηνυμάτων ή λόγω αλλοίωσης, διαρροής ή υποκλοπής των δεδομένων που αποστέλλονται μέσω του Διαδικτύου, εξαιτίας δικής τους αμέλειας ή δόλιας ενέργειας τρίτων. Έτσι, δημιουργείται μια ανισορροπία μεταξύ των εκατέρωθεν δικαιωμάτων και υποχρεώσεων των μερών εις βάρος των ασθενέστερων μερών, δηλαδή των καταναλωτών. Εξάλλου, οι καταναλωτές δεν μπορούν να διαπραγματευθούν τους ΓΟΣ, απλώς έχουν την ελευθερία είτε να προσχωρήσουν σε αυτούς και να καταρτίσουν τη σύμβαση δεχόμενοι τους επιβαλλόμενους όρους, ως έχουν, χωρίς αλλαγές, είτε να απέχουν από την ολοκλήρωση της συμφωνίας.

* + 1. Οι γενικοί όροι συναλλαγών στο ηλεκτρονικό εμπόριο

Στον χώρο του Διαδικτύου οι συμβάσεις καταρτίζονται κατά κανόνα βάσει προσυντεταγμένων ΓΟΣ, οι οποίοι περιλαμβάνονται συνήθως είτε στην ιστοσελίδα του προμηθευτή ή στη φόρμα παραγγελίας είτε στα e-mail, που αυτός αποστέλλει στους χρήστες - πελάτες. Μάλιστα, εξαιτίας της έλλειψης προσωπικής επαφής και της παρεμβολής του τηλεπικοινωνιακού μέσου στην επικοινωνία των συμβαλλομένων, οι καταναλωτές επέρχονται σε ακόμη δυσμενέστερη θέση, καθώς εκμηδενίζεται κάθε δυνατότητα διαπραγμάτευσης των όρων της σύμβασης και η επιχείρηση απολαμβάνει την απεριόριστη σχεδόν δυνατότητα, να διαμορφώσει το συμβατικό περιεχόμενό της, όπως εκείνη επιθυμεί. Κατά κύριο λόγο, οι ΓΟΣ που χρησιμοποιούνται στο Διαδίκτυο έχουν το ακόλουθο περιεχόμενο:

* Ενημέρωση του καταναλωτή για την ύπαρξη ΓΟΣ στη συγκεκριμένη ιστοσελίδα και ανάλυση του τρόπου με τον οποίο αυτός μπορεί να λάβει γνώση του περιεχομένου τους.
* Διασφάλιση από τον επιχειρηματία της δυνατότητάς του για μονομερή τροποποίηση ή ανανέωση των ΓΟΣ.
* Έμφαση στο δικαίωμα υπαναχώρησης του αγοραστή από τη σύμβαση.
* Εξαίρεση από τη δυνατότητα επιστροφής ορισμένων προσωποποιημένων αγαθών που έχουν παραγγελθεί για την κάλυψη συγκεκριμένων αναγκών και κατά παρέκκλιση από τα κοινώς πωλούμενα.
* Αποκλεισμός ή περιορισμός της ευθύνης του πωλητή για ζημίες από τη μη εκτέλεση ή την καθυστέρηση εκτέλεσης της σύμβασης.
* Καθορισμός τρόπων πληρωμής και κατοχύρωση της ασφάλειάς τους.
* Υπενθύμιση των νομοθετικών διατάξεων για την προστασία της προσωπικής ασφάλειας από τη χρήση ηλεκτρονικών δεδομένων προσωπικού χαρακτήρα.
* Εγγυήσεις για την ακαταλληλότητα των προϊόντων και την ανταπόκρισή τους σε διεθνείς και ευρωπαϊκούς κανόνες ασφαλείας (π.χ. πρότυπα ISO).
* Μονομερής καθορισμός εκ μέρους του πωλητή της διεθνούς δικαιοδοσίας και του εφαρμοστέου δικαίου για την επίλυση μελλοντικών διαφορών.
  1. Μέτρα συμμόρφωσης με τον κανονισμό
     1. Καταγραφή δεδομένων – ροές δεδομένων (DATA INVENTORY- FLOWS)

O Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) φέρνει το ζήτημα της Προστασίας των προσωπικών δεδομένων στο επίκεντρο, όπως ήδη έχει διατυπωθεί. Ο GDPR απαιτεί από τις εταιρείες που δρουν είτε ως υπεύθυνοι επεξεργασίας είτε ως εκτελούντες την επεξεργασία, να διασφαλίζουν την ασφάλεια των προσωπικών δεδομένων, που έχουν συλλέξει ή τους έχουν παραχωρηθεί προς επεξεργασία. Απαιτείται από τον κανονισμό, οι εταιρείες που επεξεργάζονται προσωπικά δεδομένα να τεκμηριώνουν και να υποδεικνύουν, από που προέρχονται τα δεδομένα καθώς και το πως διαφυλάσσονται κατά την επεξεργασία και την μεταφορά τους καθ’ όλη τη διάρκεια του κύκλου ζωής τους. Στο πλαίσιο του κανονισμού, δίνεται έμφαση στο γεγονός, ότι όλα τα προσωπικά δεδομένα, πρέπει να καταγράφονται και κάθε εταιρεία, πρέπει να διαθέτει ένα σύστημα, που να παρακολουθεί σε μόνιμη βάση τις διάφορες ενέργειες, που διεξάγονται στα δεδομένα προσωπικού χαρακτήρα. Για να γίνει αυτό, απαιτείται από τις εταιρείες να διατηρούν ένα μητρώο δεδομένων (Data Inventory) το οποίο θα περιγράφει την δραστηριότητα των δεδομένων, έτσι ώστε να γίνεται η διακυβέρνηση αυτών καθώς επίσης να μπορούν να εφαρμόζονται οι σωστές διαδικασίες για την ορθή διαφύλαξη τους. Ο GDPR απαιτεί όχι μόνο να είναι σε θέση μια εταιρεία, να προσδιορίσει και να προστατεύσει τα δεδομένα, όπου και αν βρίσκονται αλλά και να είναι υπεύθυνη, για την ακρίβεια των δεδομένων που κατέχει.

Για την εφαρμογή των κανονιστικών απαιτήσεων πρέπει πρώτα να εντοπιστούν αυτά τα δεδομένα στα συστήματά που φιλοξενούνται, εφόσον πρόκειται για ηλεκτρονικά δεδομένα και να περιγράφει σε ποια επεξεργασία υπόκεινται. Αυτή η διαδικασία ονομάζεται χαρτογράφηση δεδομένων (data mapping) ή καταγραφή δεδομένων (data inventorying) και είναι απαραίτητη, ώστε να τεκμηριώνονται, αυτές οι πληροφορίες. Το άρθρο 30 του GDPR (καταγραφή των δραστηριοτήτων επεξεργασίας) είναι η χαρτογράφηση δεδομένων. Δίχως χαρτογράφηση δεδομένων και ακριβή απογραφή των δεδομένων, την επεξεργασία τους, τις ροές τους, τα μέσα με τα οποία μεταδίδονται, τα άτομα που επεξεργάζονται τα δεδομένα, είναι αδύνατο για μια εταιρεία ή οργανισμό να εκπληρώσει τις απαιτήσεις της σύμφωνα με το GDPR.

* + 1. Αρχεία καταγραφής δραστηριοτήτων επεξεργασίας και μεθοδολογία καταγραφής

Κάθε υπεύθυνος επεξεργασίας θα πρέπει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας στο πλαίσιο της ευθύνης του για τα δεδομένα που επεξεργάζεται, συμπεριλαμβανομένων:

* Όνομα και στοιχεία επικοινωνίας του controller και, κατά περίπτωση, του joint controller, τον εκπρόσωπο του controller και τον υπεύθυνο προστασίας δεδομένων (DPO).
* Τους σκοπούς της επεξεργασίας.
* Περιγραφή των κατηγοριών των υποκειμένων των δεδομένων.
* Περιγραφή των κατηγοριών προσωπικών δεδομένων.
* Κατηγορίες αποδεκτών στους οποίους έχουν διαβιβαστεί ή πρόκειται να αποκαλυφθούν τα προσωπικά δεδομένα συμπεριλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς.
* Κατά περίπτωση, διαβιβάσεις δεδομένων προσωπικού χαρακτήρα προς Τρίτη χώρα, συμπεριλαμβανομένης την γνωστοποίηση της εν λόγω τρίτης χώρας και τον μηχανισμό μεταβίβασης που επικαλείται.
* Όπου είναι δυνατόν, τις προβλεπόμενες προθεσμίες για τη διαγραφή των διαφόρων κατηγοριών δεδομένων.
* Όπου είναι δυνατόν, γενική περιγραφή της τεχνικής και οργανωτικής ασφάλειας μέτρα.

Η μεθοδολογία καταγραφής δεδομένων (data inventorying) είναι ακρογωνιαίος λίθος της συμμόρφωσης με το GDPR και θα πρέπει να εκτελείται σε συγκεκριμένα βήματα, καθώς και να διατηρεί ακριβές το αποτέλεσμα ώστε να αποτυπώνεται ορθά. Για αυτό τον λόγο, θα πρέπει ο εκτελών την μεθοδολογία να καταρτίζει ένα ακριβές πλάνο εκτέλεσης, το οποίο θα συλλέγει από όλες τις πήγες ενός οργανισμού ή μιας εταιρείας τις κατάλληλες πληροφορίες που θα κάνουν την καταγραφή των δεδομένων ακριβή.

Οι βασικές μέθοδοι που χρησιμοποιούνται για την εκτέλεση της μεθοδολογίας καταγραφής δεδομένων είναι κυρίως οι εξής:

Α. Διαδικασία συνεντεύξεων,

Β. Αυτόματος εντοπισμός των δεδομένων με χρήση λογισμικού,

Γ. Ανατροφοδότηση από άλλα συστήματα.

Φυσικά μπορεί να χρησιμοποιηθεί και συνδυασμός, ώστε να γίνει διασταύρωση ή εμπλουτισμός του data inventory από διαφορετικές πηγές. Η διαδικασία των συνεντεύξεων θα πρέπει να είναι οργανωμένη με ερωτήσεις, που να απευθύνονται σε μέρη που επεξεργάζονται ή παίρνουν μέρος στην επεξεργασία και να απαντούν κατά βάση στα Γιατί - Ποιος - Πότε – Που (Why-Who-When-Where). Με βάση την μεθοδολογία των 5W’s όπως την ονομάζουμε δημιουργούμε σετ ερωτήσεων οι οποίες θα μας δώσουν απαντήσεις ώστε να συμπληρώσουμε το data inventory μας.

* + 1. Εκτίμηση επιπτώσεων στην προστασία δεδομένων (DPIA)

Με σκοπό να εφαρμοστεί η DPIA (Data Protection Impact Assessment) σε ένα νέο πληροφοριακό σύστημα επεξεργασίας δεδομένων, διατυπώνεται στη συνέχεια μια γενική προσέγγιση μεθοδολογίας, η οποία θα αποτελείται από τις κατάλληλες δραστηριότητες, ώστε η εκτίμηση των επιπτώσεων, σχετικά με τη προστασία των δεδομένων, να εκτελείται με όσον το δυνατόν περισσότερη σαφήνεια και μεθοδικότητα. Η διαδικασία αυτή αποτελείται από τα εξής βήματα: καθορισμός της ανάγκης για την διενέργεια της DPIA (Τι είδους προσωπικά δεδομένα επεξεργάζονται; Ποιος ο υπεύθυνος επεξεργασίας; Ενδέχεται να υπάρξουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα; Έχουν ληφθεί μέτρα προστασίας;), προσδιορισμός της ομάδας εκτέλεσης της DPIA, αναγνώριση και περιγραφή της εφαρμογής / διαδικασίας (Περιγραφή του σχεδιασμού της εφαρμογής και των διεπαφών της με άλλα συστήματα και της διαδικασίας, της ροής των δεδομένων, των εμπλεκόμενων χρηστών και των επιμέρους υποσυστημάτων της εφαρμογής), σύσκεψη με τους εμπλεκόμενους (Άτομα από το εσωτερικό και εξωτερικό του οργανισμού επισημαίνουν τους κινδύνους που αφορούν το δικό τους πεδίο εξειδίκευσης), αναγνώριση των σχετικών κινδύνων (Αναγνώριση των συνθηκών και των πιθανών κινδύνων που μπορεί να απειλήσουν τα προσωπικά δεδομένα των ατόμων και να επηρεάσουν την ιδιωτικότητά τους), διαχείριση των κινδύνων (Αξιολόγηση των ενδεχόμενων απειλών και των δυσμενών γεγονότων που έχουν αρνητικές επιπτώσεις για τα φυσικά πρόσωπα, λήψη μέτρων αντιμετώπισης και ασφάλειας), έλεγχος νομοθετικής συμμόρφωσης, τεκμηρίωση και ολοκλήρωση της σχετικής έκθεσης, εξωτερικός έλεγχος και ανασκόπηση.

Κάθε επεξεργασία δεδομένων εντός της εταιρείας πρέπει να συμμορφώνεται με τις απαιτήσεις προστασίας δεδομένων και κάθε εταιρεία πρέπει να είναι σε θέση να αποδείξει την συμμόρφωση της. Το θέμα της εκτίμησης των επιπτώσεων στην αξιολόγηση κινδύνου / προστασία δεδομένων ("DPIA"), αποτελεί στοιχείο της γενικής έννοιας του GDPR για την προστασία δεδομένων. Το άρθρο 32 του GDPR διευκρινίζει την "ασφάλεια στην επεξεργασία" και στο άρθρο 35 του GDPR, την αξιολόγηση των επιπτώσεων στην προστασία δεδομένων.

Και τα δύο άρθρα περιγράφουν τις ευθύνες του υπεύθυνου επεξεργασίας, σύμφωνα με το οποίο το άρθρο 32 του GDPR ισχύει και για τους εκτελούντες της επεξεργασία. Σύμφωνα με το άρθρο 32 του GDPR, η αξιολόγηση βασίζεται στην πιθανότητα εμφάνισης και τη σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σε πολλές εταιρείες, τα μέτρα που πρέπει να εφαρμοστούν έχουν ήδη αξιολογηθεί όσον αφορά τις πτυχές, που σχετίζονται με τον κίνδυνο - συχνά σε συμφωνία με την ασφάλεια των πληροφοριών σύστημα διαχείρισης ("ISMS").

Όσον αφορά το άρθρο 32 του GDPR, η μεθοδολογία που χρησιμοποιείται σήμερα, είναι αυτή, που ήδη εφαρμόζεται και είναι διαδεδομένη από την κλασσική ανάλυση και εκτίμηση κινδύνου. Όπως έχει ήδη καθιερωθεί σε πολλές εταιρείες, μπορεί να γίνει διάκριση μεταξύ βασικής ασφάλειας πληροφοριών, η οποία βασικά ισχύει για όλες τις διαδικασίες και εισαγωγή ειδικών μέτρων για την διαδικασία επεξεργασίας πληροφοριών. Η αξιολόγηση αντίκτυπου για την προστασία των δεδομένων (άρθρο 35 του GDPR) είναι το αντίστοιχο του προηγούμενου (άρθρο 20 της οδηγίας 95/46/ ΕΚ).

Μια σημαντική καινοτομία που επιφέρει ο ΓΚΠΔ, συνίσταται στην καταρχήν κατάργηση της γενικής υποχρέωσης γνωστοποίησης προς την αρχή ελέγχου (εκάστοτε αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) της επεξεργασίας, που προέβλεπε η Οδηγία 95/46/ΕΚ και η οποία βάρυνε τους υπευθύνους επεξεργασίας, και στην αντικατάστασή της:

* Αφενός, από την υποχρέωση για τους υπευθύνους επεξεργασίας να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας, για τις οποίες είναι υπεύθυνοι, καθώς και την υποχρέωση για τους εκτελούντες την επεξεργασία να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας, που διεξάγονται για λογαριασμό υπευθύνου επεξεργασίας,
* Αφετέρου, από την υποχρέωση για τους υπευθύνους επεξεργασίας να διενεργούν εκτίμηση αντικτύπου (Data protection impact assessment - DPIA) σχετικά με την προστασία δεδομένων σε συγκεκριμένες κατηγορίες επεξεργασιών.

Η κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προς τις Αρχές Προστασίας Δεδομένων Προσωπικού Χαρακτήρα δικαιολογήθηκε, από τη διαπίστωση, ότι η υποχρέωση αυτή, παρά το ότι επιφέρει στις αρχές ελέγχου και, ιδίως, στους υπευθύνους επεξεργασίας διοικητικό και οικονομικό φόρτο, δεν συνέβαλε σε όλες τις περιπτώσεις, στη βελτίωση της προστασίας των δεδομένων προσωπικού χαρακτήρα. Προκρίθηκε, συνεπώς, η αντικατάσταση αυτής της γενικής υποχρέωσης γνωστοποίησης από «αποτελεσματικές διαδικασίες και μηχανισμούς που επικεντρώνονται σε εκείνους τους τύπους πράξεων επεξεργασίας που ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους».

Ως «τύποι πράξεων» επεξεργασίας, από τους οποίους ενδέχεται να προκύψουν κίνδυνοι για τα υποκείμενα των δεδομένων, χαρακτηρίζονται, ιδίως, εκείνοι που περιλαμβάνουν τη χρήση νέων τεχνολογιών ή είναι νέου τύπου και δεν έχει διενεργηθεί προηγούμενη εκτίμηση αντικτύπου ως προς την προστασία των δεδομένων από τον υπεύθυνο επεξεργασίας ή παρίσταται αναγκαία η αξιολόγησή τους, λόγω του χρόνου που έχει παρέλθει από την αρχική επεξεργασία.

Στο πλαίσιο αυτό, η ρητή θέσπιση υποχρέωσης διενέργειας DPIA παρίσταται, καταρχάς, ως ένα αντιστάθμισμα στην κατάργηση της γενικής υποχρέωσης γνωστοποίησης της επεξεργασίας, με σκοπό την αντιμετώπιση των υψηλών κινδύνων, που ενδέχεται να προκύψουν, για τα υποκείμενα των δεδομένων από συγκεκριμένες κατηγορίες επεξεργασιών, λόγω της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών τους.

Υπό την έννοια αυτή, η υποχρέωση διενέργειας DPIA σημαίνει, ότι ο υπεύθυνος επεξεργασίας, έχει την υποχρέωση να αξιολογήσει όλες τις παραμέτρους των κρίσιμων πράξεων επεξεργασίας πριν από την έναρξή τους, προκειμένου να διασφαλίσει την αποτελεσματική προστασία των υποκειμένων. Επιπλέον, εάν απαιτείται από τις περιστάσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να πραγματοποιεί σχετικά διαβούλευση με την αρμόδια Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, πριν από την έναρξη της επεξεργασίας. Συνακόλουθα, η υποχρέωση διενέργειας DPIA σημαίνει, επίσης, ότι πρόκειται για ένα μέτρο, το οποίο είναι πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξορισμού (Privacy by design /Privacy by default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του Γενικού Κανονισμού Προστασίας Δεδομένων.

* + 1. Κρυπτογράφηση δεδομένων και χρήση ψευδωνύμων

Στον Γενικό Κανονισμό Προστασίας Δεδομένων δεν περιλαμβάνεται ένας ακριβής ορισμός της κρυπτογράφησης. Ωστόσο, ο όρος αυτός θα μπορούσε να περιγραφεί ως η εφαρμογή μιας διαδικασίας μετασχηματισμού μέσω κάποιου αλγορίθμου με τη χρήση «κλειδιών κρυπτογράφησης» (encryption keys), ενός συνόλου προσωπικών δεδομένων σε μία ακατανόητη (ακατάληπτη) μορφή ώστε να μην μπορούν να αναγνωσθούν από κανέναν εκτός του(ων) νόμιμου(ων) ιδιοκτήτη(τών) των κλειδιών κρυπτογράφησης.

Αντιθέτως, ο ΓΚΠΔ ορίζει επαρκώς την τεχνική της ψευδωνυμοποίησης. Σύμφωνα με το άρθρο 4 παρ. 5: «ψευδωνυμοποίηση» είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τέτοιο τρόπο, ώστε τα δεδομένα να μην μπορούν πλέον, να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο». Ωστόσο, ένας όρος που συχνά συγχέεται με την ψευδωνυποποίηση στο πεδίο της ασφάλειας και της προστασίας των προσωπικών δεδομένων είναι η ανωνυμοποίηση. Ουσιαστικά πρόκειται για δύο διαφορετικές τεχνικές που θα πρέπει να διαχωρίζονται μεταξύ τους, πολύ περισσότερο μάλιστα στο πλαίσιο του ΓΚΠΔ, δεδομένου ότι τα «ανωνυμοποιημένα δεδομένα» και τα «ψευδωνυποιημένα δεδομένα» αντιμετωπίζονται ως δύο εντελώς διαφορετικές κατηγορίες.

Ως ανωνυμοποίηση ορίζεται η διαδικασία διαγραφής των αναγνωριστικών προσωπικού χαρακτήρα σε εγγραφές δεδομένων, έτσι ώστε να μην είναι πλέον εφικτό τα ανωνυμοποιημένα δεδομένα να συσχετιστούν με το υποκείμενο των δεδομένων. Κατά συνέπεια από τους δύο αυτούς ορισμούς (δηλαδή αυτούς της ψευδωνυμοποίησης και της ανωνυμοποίησης) προκύπτει ότι, η χρήση της ανωνυμοποίησης έχει ως αποτέλεσμα την αδυναμία προσδιορισμού του υποκειμένου των δεδομένων, ενώ η ψευδωνυμοποίηση αντικαθιστά την ταυτότητα του υποκειμένου των δεδομένων με τέτοιο τρόπο, ώστε να απαιτούνται πρόσθετες πληροφορίες για την εκ νέου αναγνώριση του υποκειμένου των δεδομένων.

Βάσει του κανονισμού [Αιτ. Σκέψη υπ’ αριθμ. (26)], οι βασικές αρχές της προστασίας δεδομένων δεν θα πρέπει να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή σε πληροφορίες που δεν μπορούν να συσχετιστούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί.

Ως εκ τούτου, ο ΓΚΠΔ δεν αφορά την επεξεργασία τέτοιων ανώνυμων πληροφοριών. Αντιθέτως, τα δεδομένα προσωπικού χαρακτήρα, που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζουν να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και κατά συνέπεια συνεχίζουν να εμπίπτουν στις διατάξεις και στους περιορισμούς του ΓΚΠΔ.

* + 1. Κρυπτογράφηση και ανωνυμοποίηση από την πλευρά των εταιριών

Η κρυπτογράφηση και η ψευδωνυμοποίηση μπορούν να μειώσουν σημαντικά τους κινδύνους που σχετίζονται με την επεξεργασία δεδομένων. Για τον λόγο αυτόν, ο ΓΚΠΔ παροτρύνει και δημιουργεί κίνητρα για τους υπεύθυνους επεξεργασίας να εφαρμόζουν τις τεχνικές αυτές στα προσωπικά δεδομένα που συλλέγουν, μέσω μάλιστα και της ελαστικοποίησης ορισμένων απαιτήσεων που τους αφορούν σε ορισμένα σημαντικά άρθρα του κανονισμού.

Ήδη από το άρθρο 6 («Νομιμότητα της επεξεργασίας»), όταν «η επεξεργασία για σκοπό άλλον από αυτόν για τον οποίο έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα, δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση».

Η «Προστασία των Δεδομένων ήδη από τον Σχεδιασμό και εξ’ Ορισμού» (data protection by design and by default), που περιγράφεται στο άρθρο 25, προβλέπει, ότι ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση.

Το άρθρο 32 («Ασφάλεια Επεξεργασίας»), θεωρεί ότι η κρυπτογράφηση και η ψευδωνυμοποίηση δύνανται να διασφαλίσουν το κατάλληλο επίπεδο ασφάλειας στα δεδομένα προσωπικού χαρακτήρα έναντι των κινδύνων. Παράλληλα, στο άρθρο 34 («Ανακοίνωση Παραβίασης Δεδομένων Προσωπικού Χαρακτήρα στο Υποκείμενο των Δεδομένων») καθορίζεται ότι, δεν απαιτείται ενημέρωση του υποκειμένου των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που το αφορούν, εφόσον τα δεδομένα αυτά (μεταξύ και άλλων προϋποθέσεων) είναι κρυπτογραφημένα. Βάσει του άρθρου 40 («Κώδικες Δεοντολογίας»), ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας παροτρύνονται να εκπονούν κώδικες δεοντολογίας, προκειμένου να προσδιορίσουν την εφαρμογή του κανονισμού ΓΚΠΔ όσον αφορά μεταξύ άλλων και την ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα.

Τέλος, στο άρθρο 89 («Διασφαλίσεις και παρεκκλίσεις σχετικά με την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς») η ψευδωνυμοποίηση περιλαμβάνεται μεταξύ των εγγυήσεων ότι έχουν θεσπιστεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε (περαιτέρω) επεξεργασία για λόγους αρχειοθέτησης για λόγους γενικού συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

* 1. Παραβίαση των προσωπικών δεδομένων

Ακριβώς επειδή σε μια ηλεκτρονική σύμβαση τα δύο αντισυμβαλλόμενα μέρη δεν βρίσκονται στον ίδιο φυσικό χώρο, αλλά δρουν δικαιοπρακτικά μέσω ενός Η/Υ, δημιουργείται γόνιμο έδαφος για την ολοκλήρωση συμφωνιών σε διασυνοριακό επίπεδο. Αποτελεί σύνηθες φαινόμενο στις μέρες μας, για παράδειγμα, ένας πολίτης /καταναλωτής κράτους μέλους της ΕΕ να προβαίνει συστηματικά σε αγορές προϊόντων τα οποία πωλεί μια επιχείρηση, η οποία έχει την έδρα της σε ένα άλλο κράτος μέλος της ΕΕ ή ακόμη και εκτός αυτής. Καθώς όμως μια ηλεκτρονική σύμβαση μπορεί να συνδέεται με περισσότερες από μία έννομες τάξεις, είναι σαφές ότι οι εθνικοί κανόνες δικαίου του εκάστοτε κράτους περιέχουν διαφορετικές μεταξύ τους ρυθμίσεις. Εγείρονται, λοιπόν, ερωτήματα σχετικά με τις διαφορές που μπορεί να προκύψουν από αυτή τη διασυνοριακή δραστηριότητα. Εξάλλου, ο διεθνής χαρακτήρας του ηλεκτρονικού εμπορίου έχει δώσει έναυσμα για επαναπροσδιορισμό των παραδοσιακών κανόνων του Ιδιωτικού Διεθνούς Δικαίου.

Σαφώς, σε μια ηλεκτρονική σύμβαση τα μέρη μπορούν ελεύθερα να συμφωνήσουν ποιας πολιτείας τα δικαστήρια θα είναι αρμόδια να επιλύσουν τις διαφορές που ενδέχεται να προκύψουν. Μάλιστα, στην ιστοσελίδα του προμηθευτή συχνά υπάρχει ένας ρητός όρος παρέκτασης της διεθνούς δικαιοδοσίας, ο οποίος για να έχει ισχύ (όπως και η σύμβαση) θα πρέπει φυσικά να γίνει αποδεκτός από το χρήστη με μια ηλεκτρονικά διαβιβαζόμενη δήλωση βούλησής του.

Στην περίπτωση, που τίθενται όροι στη σύμβαση, οι οποίοι αποκλείουν την υπαγωγή των διαφορών στο φυσικό τους δικαστή, προβλέποντας αποκλειστική αλλοδαπή δικαιοδοσία ή δωσιδικία, είναι καταχρηστικοί, σύμφωνα με το άρθ. 2 § 7 στ. λα’ του ν. 2251/1994, αφού αποστερούν τον καταναλωτή από τη δυνατότητα να ζητήσει δικαστική προστασία αποφεύγοντας τα έξοδα, τις δυσκολίες και το ρίσκο εναγωγής του προμηθευτή σε αλλοδαπή χώρα. Η διάταξη αυτή του ν. 2251/1994 αποκτά ιδιαίτερη σημασία όταν ο προμηθευτής έχει την έδρα του εκτός της ΕΕ και η ρήτρα προβλέπει δικαιοδοσία του κράτους, όπου ο ίδιος βρίσκεται, οπότε δεν εφαρμόζεται η προστατευτική νομοθεσία του Κανονισμού «Βρυξέλλες Ι».

Σύμφωνα, λοιπόν, με το άρθ. 4 § 1 του νέου Κανονισμού Βρυξελλών 1215/2012, τα πρόσωπα που έχουν την κατοικία τους σε έδαφος κράτους μέλους της ΕΕ ενάγονται ενώπιον των δικαστηρίων αυτού του κράτους μέλους, ανεξάρτητα από την ιθαγένειά τους. Έτσι, οι αστικές ή εμπορικές διαφορές που προκύπτουν από μια διαδικτυακή συναλλαγή, πρέπει κατ’ αρχήν να εισάγονται στο καθ’ ύλην αρμόδιο δικαστήριο, στην περιφέρεια του οποίου βρίσκονται η κατοικία (εφόσον πρόκειται για φυσικό πρόσωπο) ή η έδρα (εφόσον πρόκειται για νομικό πρόσωπο) του εναγόμενου.

Ωστόσο, η γενική δωσιδικία της κατοικίας παρουσιάζει προβλήματα, διότι πολλοί από τους χρήστες δεν εμφανίζονται με την πραγματική τους ταυτότητα στον εικονικό χώρο του ηλεκτρονικού εμπορίου, αλλά χρησιμοποιούν κωδικούς ή ψευδώνυμα, με αποτέλεσμα ο αντισυμβαλλόμενος να μην γνωρίζει κύρια στοιχεία τους, όπως τον τόπο κατοικίας ή συνήθους διαμονής τους και, συνεπώς, ο προσδιορισμός του κατά τόπον αρμόδιου δικαστηρίου να είναι δυσχερής.

Για να αντιμετωπιστεί αυτό το πρόβλημα ο κοινοτικός νομοθέτης, μέσω του άρθ. 5 § 1 στ. β’ της Οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο, υποχρέωσε τους φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας να παρέχουν, μεταξύ άλλων, πληροφορίες για τη γεωγραφική διεύθυνση, όπου είναι εγκατεστημένοι.

Επίσης, στις διαφορές που προκύπτουν από τις ηλεκτρονικές συμβάσεις, όπως και σε κάθε εκ συμβάσεως διαφορά, καθιερώνεται συντρέχουσα δικαιοδοσία υπέρ των δικαστηρίων, στην περιφέρεια των οποίων εκπληρώθηκε ή οφείλεται να εκπληρωθεί η παροχή, σύμφωνα με το άρθ. 7 § 1 στ. α’ του Κανονισμού. Έτσι, ο ενάγων μπορεί να προτιμήσει να ενάγει τον αντισυμβαλλόμενό του σε αυτά τα δικαστήρια αντί εκείνου, στην περιφέρεια του οποίου ο τελευταίος έχει την κατοικία ή έδρα του.

Σύμφωνα με το άρθ. 6 § 1, εάν ο εναγόμενος δεν έχει την κατοικία του σε κράτος μέλος της ΕΕ, η διεθνής δικαιοδοσία ρυθμίζεται από το εσωτερικό δίκαιο του δικάζοντος δικαστή. Στην Ελλάδα, η διεθνής δικαιοδοσία των ελληνικών δικαστηρίων σε διαφορές από συμβάσεις ρυθμίζεται από τα άρθ. 3, 22 και 33 του Κώδικα Πολιτικής Δικονομίας και εξαρτάται από τη θεμελίωση τοπικής αρμοδιότητας.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα από κατάστημα ηλεκτρονικού εμπορίου, το υποκείμενο των δεδομένων κινείται ενώπιον των δικαστηρίων του κράτους μέλους, στο οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν την εγκατάσταση. Εναλλακτικά, η εν λόγω διαδικασία μπορεί να κινηθεί ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο το υποκείμενο των δεδομένων έχει τη συνήθη διαμονή του.

Συμπερασματικά, παρότι η συμμόρφωση φαίνεται να συνεπάγεται υψηλά κόστη και βαριές διαδικασίες, οι ειδικοί του χώρου επιμένουν: Εκείνος που θα μετατρέψει την κουλτούρα σεβασμού και προστασίας των προσωπικών δεδομένων σε πυρήνα της καθημερινής του λειτουργίας, θα αποκτήσει αυτόματα ένα «ανταγωνιστικό πλεονέκτημα». Γιατί θα είναι εκείνος που θα είναι διαρκώς σε θέση να αποδείξει στον καταναλωτή, τον πελάτη, τον εργαζόμενο, όχι μόνο ότι έχει λάβει τα απαραίτητα μέτρα προστασίας των προσωπικών δεδομένων τους, αλλά και ότι είναι διαρκώς σε θέση να τα διατηρεί προστατευμένα. Στην παρούσα Μελέτη επικεντρωθήκαμε σε δύο κυρίως ζητήματα: α) στην παρουσίαση των βασικών σημείων του Κανονισμού με τρόπο απλό και κατανοητό και β) στην καθοδήγηση των επιχειρήσεων σχετικά με τον τρόπο επίτευξης της «έξυπνης» συμμόρφωσης, δηλαδή της αξιοποίησης των ευκαιριών που παρουσιάζονται από τον Κανονισμό.

Συνοψίζοντας, θα θέλαμε να σημειώσουμε ότι τα κύρια σημεία του Κανονισμού που διαφαίνεται να δυσκολεύουν τις επιχειρήσεις στην πορεία συμμόρφωσης, στη δεδομένη χρονική στιγμή (δηλαδή τους πρώτους μήνες συμμόρφωσης) είναι:

* Οι υποχρεώσεις γύρω από τον Υπεύθυνο Προστασίας Δεδομένων (κυρίως ποιο είναι το σωστό πρόσωπο και πώς θα ασκήσει τα καθήκοντά του στην πράξη),
* Τα ζητήματα σχετικά με την εκπόνηση Εκτίμησης Αντικτύπου,
* Η ετοιμότητα για τη διαχείριση των περιπτώσεων παραβίασης των δεδομένων,
* Ο χειρισμός του δικαιώματος στη λήθη,
* Ο τρόπος εξασφάλισης της συγκατάθεσης,
* Π χειρισμός των αιτημάτων περί φορητότητας δεδομένων και
* Οι όροι των συμβάσεων με τρίτα μέρη.

Είναι κατανοητό ότι όσο οι επιχειρήσεις, αλλά και τα υποκείμενα προσωπικών δεδομένων, εξοικειώνονται με τις υποχρεώσεις και τις απαιτήσεις του Κανονισμού, τόσο τα πεδία που σήμερα φαίνονται να προβληματίζουν θα εξαλείφονται ή θα αντικαθίστανται από άλλα.

Όσον αφορά στη διαδικασία συμμόρφωσης, παρουσιάσαμε πώς, με την τεχνολογία πολύτιμο συμπαραστάτη, και ακολουθώντας τα 10 + 1 βήματα για έξυπνη συμμόρφωση που ο ΣΕΒ (Σύνδεσμος Επιχειρήσεων και Βιομηχανιών) προτείνει, είναι εφικτή η υιοθέτηση λύσεων προσαρμοσμένων στις ανάγκες και τις ιδιαιτερότητες κάθε οργανισμού. Το «νοικοκύρεμα» των προσωπικών δεδομένων, η μετατροπή της υποχρέωσης συμμόρφωσης σε ανταγωνιστικό πλεονέκτημα και η επένδυση σε λύσεις που προσφέρει η τεχνολογία και, μέσω αυτής της διαδικασίας, η είσοδος στην εποχή της ψηφιακής οικονομίας, αποτελούν τις βασικές αρχές που θα πρέπει να διέπουν κάθε οργανισμό.

Συμπερασματικά, είναι σημαντικό οι επιχειρήσεις να κατανοήσουν ότι η διαδικασία συμμόρφωσης με τον Κανονισμό αφενός επιφέρει οφέλη στη λειτουργία τους, σε επίπεδο φήμης και αναδιοργάνωσης και αφετέρου ότι πρόκειται για ένα ταξίδι που δεν τελείωσε με την παρέλευση της 25ης Μαΐου, ούτε με την ολοκλήρωση των ενεργειών συμμόρφωσης. Αντιθέτως, είναι ένα συνεχές ταξίδι συμμόρφωσης που μπορεί να αναδειχθεί σε ταξίδι επιχειρηματικής επιτυχίας.

1. ο Επίλογος – οι θεμέλιοι λίθοι της σύγχρονης κρυπτογραφίας
   1. Προβλήματα, αλγόριθμοι και τα όρια της υπολογισιμότητας

Στις αρχές του αιώνα μας, ένας από τους μεγαλύτερους μαθηματικούς, ο David Hilbert, στα πλαίσια της περίφημης διάλεξής του στο Διεθνές Συνέδριο Μαθηματικών στο Παρίσι το 1900 αναφέρθηκε σε 23 ανοικτά προβλήματα τα οποία θεωρούσε ως τα πιο σημαντικά για εκείνη την εποχή. Το δέκατο από αυτά ρωτούσε εάν μπορούσε να βρεθεί μια διαδικασία που να απαντά στο εάν μία δοσμένη διοφαντική εξίσωση έχει λύση ή όχι. Αρκετά χρόνια μετά, το 1928, στο Διεθνές Συνέδριο Μαθηματικών στη Μπολόνια και ως συνέχεια της προηγούμενης διαλεξής του, έθετε το πρόβλημα του να βρεθεί διαδικασία που θα μπορούσε να ελέγχει εάν ένα μαθηματικό (λογικό) σύστημα, όπως είναι για παράδειγμα η Ευκλείδειος Γεωμετρία, είναι συνεπές, δηλαδή δεν εμπεριέχει αντιφάσεις. Είναι προφανές το πόσο χρήσιμη θα ήταν μια τέτοια διαδικασία, καθώς ένας μαθηματικός που προτείνει ένα πολύπλοκο μαθηματικό σύστημα, το οποίο λόγω του όγκου των αξιωμάτων ή της πληθώρας των αποδεικτικών μεθόδων που περιέχει ξεφεύγει από την δυνατότητα ελέγχου από τον άνθρωπο, απλά θα τροφοδοτούσε (με μια κατάλληλη αναπαράσταση) το μαθηματικό του σύστημα στη μηχανική διαδικασία και η διαδικασία θα απαντούσε στο ερώτημα του αν το σύστημα αυτό περικλείει αντιφάσεις. Ένα άλλο προβλημα που έθεσε ο Hilbert στη διαλεξή του το 1928 και που ήταν κατά κάποιον τρόπο γενίκευση του δέκατου προβλήματος της διάλεξης του 1900, ήταν δοθέντος ενός μαθηματικού συστήματος να διαπιστωθεί εάν μια δοσμένη μαθηματική πρόταση αποτελεί θεώρημα του συστήματος ή όχι, το περίφημο Entscheidungsproblem. Ο Hilbert ήλπιζε ότι για τα παραπάνω προβλήματα θα έπρεπε να υπήρχε κάποια διαδικασία που να τα απαντά μέσα σε πεπερασμένο αριθμό βημάτων (περατοκρατική διαδικασία ή αλγόριθμος, όπως θα δούμε πιο κάτω).

Το 1931, ο μαθητής του Hilbert και εξίσου μεγάλος μαθηματικός Kurt Gödel, απέδειξε στην περίφημη εργασία του [Go31] ότι, δυστυχώς δύο από τις πεποιθήσεις του Hilbert ήταν λανθασμένες. Πιο συγκεκριμένα, ο Gödel παρουσίασε μια μαθηματική πρόταση στα πλαίσια του αξιωματικού συστήματος των φυσικών αριθμών (η πρώτη προσπάθεια αξιωματοποίησης του συστήματος των φυσικών αριθμών έγινε το 1910 από τους Whitehead και Russell, στο τρίτομο έργο τους Principia Mathematica [WhRu10]) για την οποία δεν ήταν δυνατό να αποδειχθεί με χρήση των αποδεικτικών μεθόδων του συστήματος αυτού ούτε ότι είναι θεώρημα ούτε ότι δεν είναι. Αυτή η μεγάλη ανακάλυψη, είναι το περίφημο θεώρημα μη πληρότητας του Gödel. Επιπλέον, ο Gödel απέδειξε ότι η συνέπεια ενός μαθηματικού συστήματος δεν είναι δυνατόν να αποδειχθεί με κανόνες και μεθόδους του ίδιου του συστήματος.

Το 1936 ο Alan Turing γινόταν ο θεμελιωτής της επιστήμης των υπολογιστών, με την ιστορική εργασία του “On computable numbers, with an application to the Entscheidungsproblem” ([Tu36]). Στην εργασία αυτή ο Turing όρισε ένα υπολογιστικό μοντέλο, που ονομάστηκε μετά προς τιμή του Μηχανή Turing (Turing Machine) το οποίο δεν είναι τίποτε άλλο παρά μια αφαιρετική περιγραφή, ένα μοντέλο, της έννοιας της αλγοριθμικής υπολογισιμότητας και του ηλεκτρονικού υπολογιστή όπως τον ξέρουμε σήμερα (δείτε Ενότητα 2). Επιπλέον, απαντώντας αρνητικά και στο τρίτο πρόβλημα του Hilbert, Entscheidungsproblem, απέδειξε ότι το πρόβλημα του εάν μια Μηχανή Turing τερματίζει για μια δοσμενη είσοδο, είναι μη αλγοριθμικά αποφασίσιμο. Με άλλα λόγια, δεν υπάρχει αλγόριθμος (Μηχανή Turing δηλαδή) που να δέχεται ως είσοδο την περιγραφή της μηχανής και της εισόδου της και να αποφασίζει αν κάποτε θα σταματήσει η μηχανή. (Δύο πολύ καλές αναφορές για όλα τα παραπάνω, είναι τα βιβλία των Davis [Da58] και van Heijenoort [vanHe67].)

Η συνεισφορά του Turing ήταν διπλή. Κατ' αρχήν συμπλήρωσε το αποτέλεσμα του Gödel. Παρεκκλίνοντας λίγο, στην πραγματικότητα, η απόδειξη του Turing ήταν μια απλούστερη έκδοση της απόδειξης μη πληρότητας του Gödel. Όμως, ο Turing είχε το πλεονέκτημα ότι εργαζόταν σε ένα μαθηματικό σύστημα που διευκόλυνε το έργο της επίδειξης μιας πρότασης για την οποία δεν υπάρχει αλγόριθμος που να αποφασίζει εάν είναι θεώρημα ή όχι. Η πρόταση, όπως είπαμε, είναι η εξής: Η μηχανή Turing M τερματίζει κάποτε με είσοδο τη συμβολοσειρά x; Ο Gödel, από την άλλη μεριά, είχε το μειονέκτημα ότι εργαζόταν σε ένα κάπως δύσκαμπτο φορμαλισμό, αυτόν των αναδρομικών συναρτήσεων, και έπρεπε να εφεύρει, κατά κάποιον τρόπο, μία μέθοδο γραφής μαθηματικών προτάσεων με χρήση απλά και μόνο αναδρομικών συναρτήσεων σε φυσικούς αριθμούς. Εάν προσέξει κανείς την απόδειξή του, θα διαπιστώσει ότι, πριν επιδείξει την περίφημη αυτοαναφερόμενη πρόταση που δεν μπορεί να αποδειχθεί εάν είναι θεώρημα ή όχι, χτίζει βήμα-βήμα μια μηχανή, που προσομοιάζει το μηχανισμό υπολογισμού της γνωστής συναρτησιακής γλώσσας προγραμματισμού Lisp. Αυτή είναι και η ομορφιά της απόδειξης του. Επανερχόμενοι όμως στην επόμενη συνεισφορά του Turing, η οποία είχε μεγάλη επίδραση στη μετέπειτα πορεία της επιστήμης των υπολογιστών, μέσα από τη χρησιμοποίηση της μηχανής που πρότεινε για την περιγραφή αλγόριθμων για διάφορα προβλήματα, υπήρξε η συνειδητοποίηση ότι πέρα από τη διαπίστωση ότι ένα πρόβλημα είναι επιλύσιμο (με το να επιδείξουμε έναν αλγόριθμο, ή μηχανή Turing, που να το επιλύει) μας ενδιαφέρει η επίλυση να γίνεται όσο το δυνατόν γρηγορότερα.

Ο πρώτος που διερεύνησε ζητήματα σχετικά με την πολυπλοκότητα της αλγοριθμικής επίλυσης προβλημάτων, ήταν ο ίδιος ο Gödel το 1956, πάλι σε σχέση με απόδειξη θεωρημάτων στα πλαίσια αξιωματικών συστημάτων. Με ένα γράμμα του προς τον John von Neumann, ο Gödel αναρωτιέται σχετικά με την πολυπλοκότητα εύρεσης αποδείξεων σε θεωρήματα που είναι διατυπωμένα με βάση τους κανόνες ενός τυπικού συστήματος (για μια αναφορά σε αυτό το γεγονός, δείτε την εργασία του Juris Hartmanis [Har89] καθώς και την τεχνική αναφορά [ChHa94]). Πιο συγκεκριμένα, αναφέρεται στη μηχανή Turing ως υπολογιστικό μοντέλο, και μετά ρωτά ποια είναι η συνάρτηση που φράσσει τον αριθμό των βημάτων που χρειάζονται για να βρεθούν αποδείξεις μήκους . Στην πραγματικότητα ο Gödel ρωτούσε τον von Neumann, σύμφωνα με τη σημερινή τεχνική ορολογία, για την ντετερμινιστική (deterministic) υπολογιστική πολυπλοκότητα του προβλήματος της απόδειξης θεωρημάτων (theorem proving). Στο ίδιο γράμμα, ο Gödel επίσης ρωτάει σχετικά με την υπολογιστική πολυπλοκότητα του ελέγχου εάν ένας φυσικός αριθμός είναι πρώτος (primality testing), και μας εκπλήσσει κάπως το γεγονός ότι εκφράζει την πεποίθηση ότι η απόδειξη θεωρημάτων δεν πρέπει να είναι και τόσο δύσκολο πρόβλημα υπολογιστικά. Δυστυχώς, ο von Neumann ήδη έπασχε από καρκίνο και πέθανε ένα χρόνο αργότερα. Ποτέ δεν υπήρξε απάντηση στο γράμμα, και φαίνεται ότι ο Gödel δεν προσπάθησε να διερευνήσει περισσότερο το πολύ σημαντικό ερώτημα που έθεσε.

* 1. Γρήγορα Επιλύσιμα Προβλήματα: η κλάση P και η πρακτική υπολογισιμότητα

Πριν ορίσουμε τις βασικές έννοιες υπολογιστικής πολυπλοκότητας θα δώσουμε μία σύντομη περιγραφή της μηχανής Turing (δείτε Σχήμα 1). Μια μηχανή Turing αποτελείται από ένα πεπερασμένο μηχανισμό ο οποίος βρίσκεται πάντα σε κάποια κατάσταση ανάλογα με την πορεία των υπολογισμών, μια απεριόριστου μήκους ταινία διαιρεμένη σε κελιά, και μια κεφαλή ανάγνωσης των κελιών η οποία μπορεί να διαβάζει τα περιεχόμενα ενός κελιού κάθε φορά. Η ταινία έχει όριο προς τα αριστερά, ενώ εκτείνεται στο άπειρο προς τα δεξιά. Σε κάθε ένα από τα κελιά μπορεί να βρίσκεται ένα σύμβολο μέσα από ένα πεπερασμένο αριθμό συμβόλων που αποτελούν το αλφάβητο της ταινίας της μηχανής. Για να ξεκινήσει ο υπολογισμός, ένας αριθμός από τα πρώτα συνεχόμενα κελιά περιέχει στην αρχή την είσοδο της μηχανής η οποία αποτελείται από σύμβολα μέσα από το αλφάβητο εισόδου της μηχανής.

0

0

1

0

1

*q*0

*q*1

*qn*

(*q*1,0)

⇓

(*q*2,1,→)

Σχήμα 1: Μία μηχανή Turing *n* καταστάσεων που ετοιμάζεται να μεταβεί στην κατάσταση *q*2, γράφοντας στη θέση του 0 το 1 και μεταφέροντας την κεφαλή μία θέση δεξιά

Σε κάθε βήμα, μια μηχανή Turing μπορεί να κάνει κάτι από τα ακόλουθα: (α) να αλλάξει εσωτερική κατάσταση (β) να αλλάξει το σύμβολο το οποίο βρίσκεται στο κελί που διαβάζει η κεφαλή ή (γ) να μετακινήσει την κεφαλή δεξιά ή αριστερά κατά ένα κελί. Όπως έχουμε ήδη πει, αυτό το τόσο απλό μοντέλο είναι γενικά αποδεκτό ότι μπορεί να υπολογίσει κάθε τι που μπορεί να υπολογιστεί αλγοριθμικά (η περίφημη υπόθεση του Church) και είναι ισοδύναμο ως προς το τι μπορεί να υπολογιστεί με τον ηλεκτρονικό υπολογιστή μας.

Ας επανέλθουμε όμως στο ζήτημα του πόσο χρόνο μπορεί να χρειαστεί μια μηχανή Turing για να επιλύσει ένα πρόβλημα. Όπως είδαμε, πρώτος Gödel έθεσε αυτό το ερώτημα, χωρίς όμως να το διερευνήσει περισσότερο. Μέσα στο διάστημα 1965-1967, ο J. Edmonds σε δύο εργασίες του, χρησιμοποίησε για πρώτη φορά την έννοια καλός (αποδοτικός) αλγόριθμος για εκείνους τους αλγόριθμους (μηχανές Turing) που για να επιλύσουν ένα στιγμιότυπο μεγέθους χρειάζονται το πολύ βήματα, για κάποιους σταθερούς (δηλαδή ανεξάρτητους του ) θετικούς αριθμούς .

Γρήγορα έγινε αποδεκτό, με βάση διάφορα πειστικά επιχειρήματα που μπορεί κανείς να βρει αναλυτικά στα βιβλία [Papa94] και [HoUl79], ότι τα προβλήματα που θα πρέπει να θεωρούνται γρήγορα επιλύσιμα είναι η κλάση όλων των προβλημάτων για τα οποία υπάρχει αλγόριθμος (μηχανή Turing) που τα επιλύει χρησιμοποιώντας πολυωνυμικό αριθμό βημάτων στο μέγεθος του στιγμιότυπου. Ένα από τα ισχυρότερα επιχειρήματα είναι το ότι για κάθε ρεαλιστικό μοντέλο υπολογισμού M, εάν ένας αλγόριθμος είναι πολυωνυμικού χρόνου για μια μηχανή Turing, τότε ο αλγόριθμος θα είναι πολυωνυμικού χρόνου ακόμα και αν περιγραφτεί στα πλαίσια των κανόνων του μοντέλου M και αντίστροφα. Με άλλα λόγια, η ιδιότητα της επιλυσιμότητας ενός προβλήματος γρήγορα (δηλαδή σε πολυωνυμικό αριθμό στοιχειωδών βημάτων) είναι μία αμετάβλητη ιδιότητα μέσα στην κλάση όλων των ρεαλιστικών μοντέλων της έννοιας της μηχανικής υπολογισιμότητας.

Ο Edmonds είχε σωστή διαίσθηση όσον αφορά το τι πρέπει να είναι καλός αλγόριθμος, και είχε εντοπίσει προβλήματα που επιδέχονται τέτοιους αλγορίθμους, Όμως για ένα συγκεκριμένο πρόβλημα, το Πρόβλημα του Περιπλανώμενου Πωλητή (Traveling Salesman Problem ή TSP) δεν είχε καταφέρει να βρει έναν καλό (δηλαδή *γρήγορο*) αλγόριθμο. Πριν όμως ορίσουμε το πρόβλημα αυτό θα εξετάσουμε κάποιο άλλο. Έστω ότι δίνεται ένας χάρτης μιας χώρας με συνδέσεις μεταξύ των πόλεων με δρόμους και δύο συγκεκριμένες πόλεις A και B (Σχήμα 2).

Το Σχήμα 2: Ένα οδικό δίκτυο πόλεων και μία σύνδεση μεταξύ των πόλεων Α και Β

**Α**

**Β**

πρόβλημα που τίθεται είναι εάν το δίκτυο επιτρέπει τη σύνδεσή τους, έστω και μέσα από άλλες πόλεις (ας καλέσουμε το πρόβλημα αυτό PATH). Αυτό είναι σημαντικό πρόβλημα καθώς εάν το προτεινόμενο δίκτυο δεν επιτρέπει τη σύνδεση κάποιων πόλεων τότε είναι λανθασμένο και θα πρέπει να επανασχεδιαστεί. Το πρόβλημα αυτό έχει μια απλή και γρήγορη μηχανική λύση που φαίνεται στο Σχήμα 3. Μια πρόχειρη ανάλυση μας δείχνει ότι ο αλγόριθμος τερματίζει μετά από το πολύ n2 βήματα για κάθε χάρτη με n πόλεις.

(Έχοντας ξεκινήσει από την πόλη Α)

**Μέχρι** να φτάσεις στην πόλη Β κάνε *ένα* από τα εξής τρία βήματα:

* Εάν βρίσκεσαι στην πόλη Α και **δεν υπάρχει** δρόμος που να μην έχεις ακολουθήσει ξανά, **τερμάτισε** και **δήλωσε** ότι οι πόλεις Α και Β δεν συνδέονται μεταξύ τους.
* Από την πόλη που βρίσκεσαι, κοίταξε όλους του δρόμους που φεύγουν από αυτήν και **ακολούθησε** κάποιο δρόμο που δεν έχεις ακολουθήσει παλαιότερα.
* Εάν όμως έχεις ακολουθήσει κάποτε **όλους** τους δρόμους που φεύγουν από την τρέχουσα πόλη **γύρισε πίσω** σε μία πόλη που είχες επισκεφτεί πιο πριν ακολουθώντας προς τα πίσω το δρόμο από τον οποίο **πρωτοεπισκεύτηκες** την τρέχουσα πόλη.

**Δήλωσε** ότι οι πόλεις Α και Β συνδέονται μεταξύ τους.``

Σχήμα 3: Ένας αλγόριθμος ελέγχου σύνδεσης μεταξύ των πόλεων Α και Β (πρόβλημα PATH)

Επίσης, βλέπουμε ότι η παραπάνω λύση αποτελείται από στοιχειώδη και εύκολα υλοποιήσιμα βήματα, μπορεί να εκτελεστεί εντελώς μηχανικά δοσμένου του χάρτη της χώρας με το οδικό δίκτυο, και πάντοτε τερματίζει δίνοντας τη σωστή απάντηση, δηλαδή είναι ένας αλγόριθμος. Στο Σχήμα 3 βλέπουμε μία πιθανή εύρεση διασύνδεσης μεταξύ των Α και Β.

Ας αλλάξουμε όμως λίγο το πρόβλημα έτσι ώστε να μην μας ενδιαφέρει απλά και μόνο η σύνδεση των δύο πόλεων μέσα από το οδικό δίκτυο αλλά να μας ενδιαφέρει επιπρόσθετα να συνδέονται με κάποια διαδρομή η οποία να περνά ακριβώς μία φορά από όλες τις υπόλοιπες πόλεις. Αυτό είναι και το πρόβλημα του Πρόβλημα του Περιπλανώμενου Πωλητή (Traveling Salesman Problem – TSP). Κάποιος αμέσως θα σκεφτόταν να εφαρμόσει μια παραλλαγή του αλγόριθμου στο Σχήμα 2 και σε αυτό το πρόβλημα. Επίσης, θα περίμενε κανείς και το καινούριο πρόβλημα να είναι επιλύσιμο σε περίπου τον ίδιο αριθμό βημάτων. Μοιάζουν τόσο, εξάλλου, τα δύο προβλήματα. Τα πράγματα είναι όμως πολύ διαφορετικά! Πραγματικά, μπορούμε να εφαρμόσουμε έναν αλγόριθμο όπως ο παραπάνω που απλά θα ξεκινά από την A και θα ακολουθεί τους δρόμους μέχρι να βρει την B, κρατώντας κάθε φορά μία σημείωση των πόλεων που έχει επισκεφτεί. Εάν από μία πόλη μπορεί να επισκεφτεί μόνο πόλεις που έχει ήδη επισκεφτεί, τότε ο αλγόριθμος μπορεί π.χ. να επιστρέψει σε μία προηγούμενη πόλη και να ακολουθήσει κάποιον άλλο δρόμο ελπίζοντας αυτή τη φορά να βρει τη ζητούμενη διαδρομή. Εάν μελετήσουμε τον αριθμό των βημάτων αυτού του αλγόριθμου, θα δούμε ότι μάλλον δεν είναι και τόσο μικρός! Ο αλγόριθμος αυτός μπορεί να εξερευνά διαδρομές που ξαφνικά διαπιστώνεται ότι δεν μπορεί να αποτελούν μέρος μίας καθολικής διαδρομής που περνά από όλες τις πόλεις. Και τότε ο αλγόριθμος θα πρέπει να ψάξει για άλλη διαδρομή. Μία προσεκτική ανάλυση του αλγόριθμου που προτείναμε, αποκαλύπτει ότι για έναν χάρτη με n πόλεις, ο αριθμός των βημάτων στη χειρότερη περίπτωση μπορεί να φθάσει, χονδρικά, μέχρι nn.Ακόμη και με τους ταχύτερους υπολογιστές στον κόσμο σήμερα, για έναν χάρτη 1000 πόλεων, θα χρειαστούν πάρα πολλά χρόνια υπολογισμού για να βρεθεί το πολυπόθητο μονοπάτι! Στο Σχήμα 4 βλέπουμε ποια αποτελέσματα έχει η τεχνολογία όσον αφορά το πόσο μεγάλα στιγμιότυπα μπορούν να επιλυθούν σε μία ώρα (δείτε [GaJo79]).

|  |  |  |  |
| --- | --- | --- | --- |
| Χρόνος τρεξίματος αλγόριθμου | Μέγιστο μέγεθος στιγμιότυπου με σημερινή τεχνολογία | 100 φορές πιο γρήγορη τεχνολογία | 1000 φορές πιο γρήγορη τεχνολογία |
| N | N1 | 100N1 | 1000N1 |
| *n*2 | N2 | 10N2 | 31.6N2 |
| n3 | N3 | 4.64N3 | 10N3 |
| *n*5 | N4 | 2.5N4 | 3.98N4 |
| 2*n* | N5 | 6.64+N5 | 9.97+N5 |
| 3*n* | N6 | 4.19+N6 | 6.29+N6 |

Σχήμα 4: Το μεγαλύτερο στιγμιότυπο που επιλύεται μέσα σε μία ώρα

Ίσως όμως, να σκεφτεί κανείς, να υπάρχει κάποιος καλύτερος αλγόριθμος. Αρκεί κανείς να σκεφτεί πιο προσεκτικά. Όμως ο Edmonds, όπως και πολλοί άλλοι μετέπειτα, δεν είχε κατορθώσει να βρει ένα γρήγορο αλγόριθμο γι’ αυτό το πρόβλημα και αμέσως διατύπωσε την εικασία ότι μάλλον δεν πρέπει να υπάρχει πολυωνυμικός αλγόριθμος γι' αυτό το πρόβλημα. Όμως, μια άλλη σημαντική παρατήρηση, με δεδομένο ότι το πρόβλημα δεν φαινόταν να επιλύεται από πολυωνυμικό αλγόριθμο, ήταν ότι εάν μας δοθεί μια διαδρομή που κάποιος ισχυρίζεται ότι είναι λύση ενός στιγμιότυπου του TSP, τότε είναι εύκολο υπολογιστικά να ελέγξουμε γρήγορα (δηλαδή σε πολυωνυμικό αριθμό βημάτων) ότι πράγματι αυτή η διαδρομή είναι η επιθυμητή. Η κλάση, λοιπόν, των προβλημάτων που έχουν αυτή την ιδιότητα ονομάστηκε NP (συνήθως ο ορισμός δίνεται με βάση τις μη ντετερμινιστικές μηχανές Turing αλλά, για απλούστευση, αποφύγαμε να χρησιμοποιήσουμε το φορμαλισμό αυτών των μηχανών). Προσέξτε, επίσης, ότι η κλάση P είναι υποσύνολο της κλάσης NP, δηλαδή P ⊆ NP, χωρίς μέχρι σήμερα να έχει αποδειχθεί (αποτελεί σημαντικό ανοικτό πρόβλημα της θεωρίας της πολυπλοκότητας) εάν η σχέση υποσυνόλου είναι γνήσια (δηλαδή εάν P ⊂ NP).

Οι ερευνητές, λοιπόν, είχαν στα χέρια τους προβλήματα για τα οποία είχαν ήδη βρει πολυωνυμικούς αλγορίθμους επίλυσης, και προβλήματα που αν και δεν διαφαινόταν εάν μπορούσαν να επιλυθούν από πολυωνυμικό αλγόριθμο ή όχι, παρόλα αυτά, εάν παρεχόταν μια υποψήφια λύση, υπήρχε πολυωνυμικός αλγόριθμος που να ελέγχει εάν πράγματι αυτή είναι λύση ή όχι. Η επόμενη σκέψη ήταν να βρεθούν εκείνα τα προβλήματα αυτής της κλάσης που πρέπει να είναι τα πιο δύσκολα να επιλυθούν δηλαδή αυτά που αντιπροσωπεύουν τη δυσκολία όλης της κλάσης με την έννοια ότι εάν μπορούσαμε να λύναμε πολυωνυμικά ένα από αυτά, θα λύναμε πάλι πολυωνυμικά όλα τα προβλήματα του NP. Έτσι γεννήθηκε η έννοια της αναγωγής πολυωνυμικού χρόνου από ένα πρόβλημα σε ένα άλλο. Σύμφωνα με αυτή την έννοια, για να δείξουμε ότι ένα πρόβλημα είναι τουλάχιστον τόσο δύσκολο όσο ένα άλλο όσον αφορά την επίλυση με πολυωνυμικό αλγόριθμο, αρκεί να βρούμε μια απεικόνιση στιγμιότυπων του πρώτου σε στιγμιότυπα του δευτέρου που γρήγορα, έτσι ώστε μια λύση στο δεύτερο πρόβλημα να αντιστοιχεί σε μία λύση του πρώτου. Έτσι, δείχνουμε ότι το δεύτερο πρόβλημα δεν μπορεί να είναι πιο εύκολο να λυθεί από το πρώτο. Τα προβλήματα που ανήκουν στο NP και έχουν αυτή την ιδιότητα καλούνται πλήρη ως προς την κλάση NP (NP-complete).

Το πρώτο πρόβλημα που βρέθηκε να έχει αυτή την ιδιότητα, είναι το πρόβλημα της ικανοποιησιμότητας λογικών προτάσεων (SATISFIABILITY ή SAT) και η σημαντική αυτή ανακάλυψη, γνωστή ως Θεώρημα του Cook, έγινε από τον Stephen Cook το 1971. Την ανακάλυψη αυτή, ακολούθησαν πλήθος δημοσιεύσεων όπου μια πληθώρα άλλων προβλημάτων βρέθηκαν να είναι πλήρη ως προς την κλάση NP ([GaJo79]). Το θεμελιώδες ερώτημα,, που παραμένει βασανιστικά αναπάντητο, είναι το εάν ισχύει P=NP, με την επιστημονική κοινότητα να συγκλίνει στο ότι κάτι τέτοιο δεν ισχύει. Στο Σχήμα 5 βλέπουμε την πρωταρχική κατάταξη των προβλημάτων ανάλογα με την ευκολία επίλυσής τους.

NP: περιέχει δύσκολα προβλήματα;

P⊆NP: γρήγορα επιλύσιμα προβλήματα

Σχήμα 5: Η εικόνα των προβλημάτων σε σχέση με την πολυπλοκότητα επίλυσής τους

* 1. Συμπεράσματα και προοίμιο στην κρυπτογραφία

Μέσα από τις προσπάθειες που περιγράψαμε προηγουμένως γεννήθηκε, και σήμερα έχει πια ωριμάσει, η Θεωρία Πολυπλοκότητας. Η θεωρία αυτή εξετάζει τα διάφορα προβλήματα ως προς το πόσο γρήγορα μπορούν να επιλυθούν και μία από τις μεγαλύτερες επιτυχίες της είναι η κατάταξή τους σε δύο μεγάλες κατηγορίες. Στην πρώτη ανήκουν τα προβλήματα για τα οποία έχει ήδη βρεθεί κάποιος γρήγορος αλγόριθμος που για στιγμιότυπα (π.χ. όπως ο χάρτης) μεγέθους n (ο αριθμός των πόλεων του χάρτη) απαιτούνται το πολύ , , ή, γενικά, βήματα, για κάποιο σταθερό θετικό ακέραιο . Τα προβλήματα αυτά καλούνται προβλήματα επιλύσιμα σε πολυωνυμικό χρόνο (λόγω της μορφής, πολυώνυμο, που έχει η έκφραση για τον αριθμό βημάτων) και αποτελούν την περίφημη κλάση P. H δεύτερη κατηγορία συμπεριλαμβάνει προβλήματα όπως το TSP που είναι από τα δυσκολότερα προβλήματα του NP και για τα οποία μέχρι τώρα δεν έχει βρεθεί γρήγορος αλγόριθμος, ενώ οι ταχύτεροι αλγόριθμοι που έχουν προταθεί απαιτούν αριθμό βημάτων της μορφής 2n, 3n ή ακόμα και nn, δηλαδή εκθετικά πολλά βήματα. Τα προβλήματα αυτά αποτελούν την περίφημη κλάση των NP πλήρων προβλημάτων, των πιο δύσκολων στο NP. Αυτό που πρέπει να έχουμε κατά νου είναι ότι αν και μέχρι σήμερα κανείς δεν έχει αποδείξει ότι γι’ αυτά τα προβλήματα πραγματικά δεν υπάρχουν γρήγοροι αλγόριθμοι, η Θεωρία της Πολυπλοκότητας, μέσα από μια μαθηματικά θεμελιωμένη μεθοδολογία και επιχειρηματολογία, δίνει πειστήρια για το ότι δεν μπορεί να υπάρχουν τέτοιοι αλγόριθμοι.

Μα ο αναγνώστης (εύλογα) θα διαμαρτυρηθεί ότι μέχρι τώρα πουθενά δεν έχουμε αναφερθεί στην κρυπτογραφία και ίσως το θέμα που πραγματευτήκαμε να φαίνεται απόμακρο και πολύ θεωρητικό για να αποτελεί το θεμέλιο μιας τόσο εφαρμοσμένης και μεγάλης πρακτικής σημασίας περιοχής. Όμως η αλήθεια είναι εντελώς διαφορετική. Όλο το οικοδόμημα των σύγχρονων κρυπτογραφικών εφαρμογών στην ασφαλή επικοινωνία και στις ασφαλείς οικονομικές συναλλαγές παίρνει ζωή και υπάρχει μέσα από την ύπαρξη δύσκολων προβλημάτων όπως αυτά που εξετάσαμε πιο πάνω και κυρίως προβλημάτων της Θεωρίας Αριθμών, όπως είναι η *παραγοντοποίηση ακεραίων* και ο *διακριτός λογάριθμος*, τα οποία φαίνεται ότι είναι δύσκολα να επιλυθούν όχι απλά στη χειρότερη περίπτωση (πράγμα που δεν μας αρκεί στην κρυπτογραφία) αλλά σχεδόν για όλα τα δυνατά στιγμιότυπά τους! Ο αναγνώστης που θα επιθυμούσε μία εμπεριστατωμένη (και μαθηματικά θεμελιωμένη) συζήτηση σε αυτό το «φλέγον» ζήτημα μπορεί να συμβουλευτεί τις πολύ καλές εργασίες [Aj96,AjDw97,GoGo98].

* 1. Βιβλιογραφία Kεφαλαίου 5

[Aj96] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th Symposium on Theory of Computing (STOC)*, pp. 99-108, 1996.

[AjDw97] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th Symposium on Theory of Computing (STOC)*, pp. 284-293, 1997.

[ChHa94] S. Chari and J. Hartmanis. On the Intellectual Terrain around NP. *Technical Report*, MPI-I-94-103, Max Planck Institut für Informatik, 1994.

[Da58] M. Davis. *Computability and unsolvability*. McGraw-Hill, 1958.

[GaJo79] M.R. Garey and D.S. Johnson. *Computers and Intractability*. Freeman, San Francisco, CA, 1979.

[Go31] K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I (On formally undecidable theorems in Principia Mathematica and related systems). *Monatshefte für Math. und Physik*, 38:173-198, 1931. Για μία μετάφραση στα Αγγλικά. δείτε την αναφορά [vanHe67] πιο κάτω.

[GoGo98] O. Goldreich and S. Goldwasser. On the possibility of basing cryptography on the assumption P NP. *Manuscript*. 1998.

[Har89] J. Hartmanis. Gödel, von Neumann and the P=?NP problem. *Bulletin of the EATCS*, 38:101-107, 1989.

[vanHe67] J. van Heijenoort. *From Frege to Gödel: A Source Book in Mathematical Logic*. MA: Harvard University Press, 1967.

[HoUl79] J.E. Hopcroft and J.D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison-Wesley, 1979.

[Papa94] C.H. Papadimitriou. *Computational Complexity*. Addison - Wesley, 1994.

[Tu36] A.M. Turing. On computable numbers, with an application to the *Entsceidungsproblem*. Proc. London Math. Society 2(43):230-265, 1936. Μία διόρθωση στην αρχική εργασία: 2(43): 544-546, 1937.

[WhRu10] A.N. Whitehead and B. Russell. *Principia Mathematica*. Τρεις τόμοι, Cambridge University Press, London, 1910, 1912, 1913.

Βιβλιογραφικές Αναφορές

|  |  |
| --- | --- |
| [Acm05] | ACM (2005): *The Joint Task Force for Computing Curricula 2005*. |
| [Alc85] | Alchourron C.E.; Gärdenfors P. and Makinson D. (1985): On The logic of theory change: Partial meet functions for contraction and revision. *Journal of Symbolic Logic*, 50. S. 510-530. |
| [Bch12] | Bcheri S.; Götze N.; Liagkou V. et al. (2012): *D5.1 Scenario Definition for both Pilots*. (Deliverable) ABC4trust. |
| [Bic10] | Bichsel P. and Camenisch J. (2010): Mixing identities with ease. In: Leeuw D.; Fischer-Hübner S. and Fritsch L. (Hg.): *IFIP Working Conference on Policies & Research in Identity Management (IDMAN ’10)*. Springer. S. 1-17. |
| [Bic14] | Bichsel P.; Camenisch ; Dubovitskaya M. et al. (2014): *D2.2 - Architecture for Attribute-based Credential Technologies - Final Version (Dilevarable)*. ABC4trust. |
| [Bjo14] | Bjones R.; Krontiris I.; Paillier P. et al. (2014): Integrating Anonymous Credentials with eIDs for Privacy-Respecting Online Authentication. In *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg. S. 111-124. |
| [Bla03] | Blarkom v.; Borking and Olk J.G.E. (2003): *Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents)*. Netherlands: College bescherming persoonsgegevens. |
| [Bra00] | Brands S. (2000): *Rethinking Public Key Infrastructures and Digital Certificates Building in Privacy*. MIT Press. |
| [Bul13] | Bulgacs S. (2013): The first phase of creating a standardised international innovative technological implementation framework/software application. *International Journal of Business and Systems Research (IJBSR) Vol. 7 No. 3*. |
| [Cam01] | Camenisch J. and Lysyanskaya A. (May 6-10, 2001): An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann B. (Hg.): *Advances in Cryptology --- EUROCRYPT 2001: International Conference on the Theory and Application of Cryptographic Techniques Innsbruck*. Berlin, Heidelberg: Springer Berlin Heidelberg. S. 93-118. |
| [Cam02] | Camenisch J. and Herreweghen V. (2002): Design and implementation of the idemix anonymous credential. In: ACM (Hg.): *In CCS ’02: Proceedings of the 9th ACM conference on Computer and*. New York, NY, USA. S. 21–30. |
| [Cam03] | Camenisch J. and Lysyanskaya A. (2003): A Signature Scheme with Efficient Protocols. In: Springer-Verlag (Hg.): *Proceedings of the 3rd International Conference on Security in Communication Networks*. Amalfi, Italy. S. 268-289. |
| [Cam04] | Camenisch J. and Lysyanskaya A. (2004): Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Heidelberg S.B. (Hg.): *Advances in Cryptology -- CRYPTO 2004: 24th Annual International Cryptology Conference*. Santa Barbara, California, USA. S. 56-72. |
| [Cam05] | Cameron K. (2005): *Kim Cameron’s Identity Weblog The laws of identity*. http://www.identityblog.com/?p=354, |
| [Cha85] | Chaum D. (1985): Security without identification: transaction systems. Communications of the ACM, 28.. S. 1030–1044. |
| [Dif76] | Diffie and Hellman M.E. (1976): New directions in cryptography. *IEEE Transactions on Information Theory, 22*. S. 644–654. |
| [Heu10] | Heupel M. (2010): *Porting and evaluating the performance of IDEMIX and TOR anonymity on modern smartphones (Master Thesis)*. Deutschland: University of Siegen. |
| [Hun07] | Hunter Α. and Delgrande J. (2007): Belief Change and Cryptographic Protocol Verification. In: *AAAI*.. S. 427-433. |
| [Jes08] | Jessup; Leonard Μ. and Joseph S. (2008): *Information Systems Today (3rd ed.)*. Valacich : Pearson Publishing. |
| [Kom08] | Komar Β. (2008): *PKI and Cerrtificate Security*. Redmond, Washington: Microsoft Press. |
| [Kra98] | Krause M. and Tipton H.F. (1998): *Handbook of Information Security Management*. Auerbach Publications, CRC Press LLC. |
| [Kro08] | Kroenke D.M. ( (2008)): *Experiencing MIS*. Upper Saddle River, NJ: Prentice-Hall. |
| [Lau88] | Laudon K.C. and Laudon J.P. (1988): *Management Information Systems*. 2nd edition. Aufl. Macmillan. |
| [Lee12] | Lee (2012): *Electronic Commerce Management For Business Activities And Global Enterprises: Competitive Advantages*. Hershey, PA: Business Science Reference. |
| [Nau09] | Naumann and Hogben G. (2009): *Privacy Features of European eID Card Specifications*. (Position Paper) ENISA. |
| [Nau091] | Naumann Ι. (November 2009): Privacy and Security Risks when Authenticating on the Internet. In *Risk Assessment Report*. ENISA. |
| [Nev08] | Neven G. (2008): *A Quick Introduction to Anonymous Credentials*. IBM Zürich Research Laboratory. https://idemix.files.wordpress.com/2009/08/neven2008-quick\_introduction\_to\_anonymous\_credentials.pdf, |
| [Pat09] | Bichsel P.; Binding C.; Camenisch J. et al. (2009): *Cryptographic Protocols of the Identity Mixer Library*. (Research Report) Zurich Research Laboratory: IBM Research GmbH. |
| [Pfi10] | Pfitzmann A. and Hansen M. (2010): *terminology for talking about privacy by data minimization: Anonymity, unlinkability,undetectability, unobservability, pseudonymity, and identity management.* Dresden: TU Dresden. |
| [Ran15] | Rannenberg K.; Camenisch J. and Sabouri A.e. (2015): *Attribute-based Credentials for Trust: Identity in the Information Society*. Switzerland: Springer International Publishing. |
| [Sil95] | Silver M.S.; Lynne M. and Beath C.M. (Sep 1995): The Information Technology Interactive Model: A Foundation for the MBA Core Course. MIS Quarterly. S. 361–390. |
| [War70] | Ware W. (1970): *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*. Washington: Rand Corporation for the office of the director of defense research and engineering. |
| [Zhe09] | Zheng J. (2009): *Environment Information PeopleTechnology Input Output Boundary Purpose Processes and Interactions*. |
| [Zwi11] | Zwingelberg Η. (2011): Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card. In: Fischer-Hübner S. et al. (Hg.): *Privacy and Identity Management for Life: 6th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, August 2-6, 2010, Revised Selected Papers*. Helsingborg, Sweden, : Springer Berlin Heidelberg. S. 151-163. |
| [Γκρ03] | Γκρίτζαλης Δ.Α.; Γκρίτζαλης Σ. and Κάτσικας Σ. (2003): *Ασφάλεια δικτύων υπολογιστών*. Παπασωτηρίου. |
| [Κων09] | Κωνσταντίνου Ε. (2009): *Σημειώσεις Μαθήματος Κρυπτογραφίας*. Πανεπιστήμιο Αιγαίου - Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Σάμος. |
| [Λαµ10] | Λαµπρινουδάκης Κ.; Μήτρου Ε.; Γκρίτζαλης Σ. et al. (2010): *Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών*. Παπασωτηρίου. |
| [Μάλ01] | Μάλλιαρης Π. (2001): *Εισαγωγή στο Μάρκετινγκ*. Αθήνα: Σταμούλης ΑΕ. |
| [Σιο06] | Σιουγλέ Ε. (2006): *Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies - PETs)*. Εθνική Σχολή Δημόσιας Διοίκησης. http://84.205.229.18/securityc/d/greek/Privacy%20Enhancing%20Technologies.ppt, |
| [Σιώ08] | Σιώμκος Γ. and Μαύρος Δ. (2008): *Έρευνα Αγοράς*. Αθήνα: Αθ. Σταμούλης. |

1. Οι αρχικές ερμηνείες και πληροφορίες σχετικά με τα πληροφορικά συστήματα αντλήθηκαν (5/5/2015) από τους παρακάτω ηλεκτρονικούς συνδέσμους:

   http://www.businessdictionary.com/definition/information-system.html

   http://pespmc1.vub.ac.be/ASC/INFORM\_SYSTE.html

   http://global.britannica.com/EBchecked/topic/287895/information-system [Jes08] [↑](#footnote-ref-1)
2. Το Unix είναι λειτουργικό σύστημα Ηλεκτρονικών Υπολογιστών, το οποίο αναπτύχθηκε κατά τις δεκαετίες του 1960 και του 1970 από τους Ken Thompson, Dennis Ritchie και Douglas McIlroy. [↑](#footnote-ref-2)
3. Η ενότητα της κρυπτογραφίας βασίστηκε στις πανεπιστημιακές σημειώσεις του μαθήματος Κρυπτογραφίας [Κων09] που διεξάγεται στο Πανεπιστήμιου Αιγαίου καθώς και στις παραδόσεις του ιδίου μαθήματος που διεξήχθη το έτος 2012 στο Πανεπιστήμιου Πατρών και στο Δ.Π.Μ.Σ Μαθηματικά των Υπολογιστών και των Αποφάσεων με διδάσκων τον Δρ. Μελετίου Γεράσιμο. [↑](#footnote-ref-3)
4. Ο ορισμός αυτός αποτελεί αυτούσιο και αναπόσπαστο μέρος από τον ιστότοπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα <http://www.dpa.gr/> με ημερομηνία ανάκτησης 6/5/2015 [↑](#footnote-ref-4)
5. Ομοίως με παραπάνω [↑](#footnote-ref-5)
6. Οδηγίες 95/46/ΕΚ, 2002/58/ΕΚ, 2006/24/ΕΚ, 2009/136/ΕΚ [↑](#footnote-ref-6)
7. Οι έννοιες και οι ερμηνείες σχετικά με την ιδιωτικότητα αντλήθηκαν (5/6/2015) από τους παρακάτω ηλεκτρονικούς συνδέσμους:

   http://www.ct.aegean.gr/people/kalloniatis/Privacy\_Intellectual\_Property/PRIVACY\_Terminology.pdf

   http://dud.inf.tu-dresden.de/Anon\_Terminology.shtml [↑](#footnote-ref-7)
8. <http://www.dpa.gr/portal/page?_pageid=33,37057&_dad=portal&_schema=PORTAL>

   Βλ. Αποφάσεις Αρχής: 245/9/2000, 115/2001, 9/2003, 52/2003, 39/2004, 59/2005, 50/2007, 62/2007 [↑](#footnote-ref-8)
9. Ο όρος αυτός συναντάται περισσότερο ως credential παρά στην επίσημη μετάφρασή του. Στο υπόλοιπο της εργασίας μας θα χρησιμοποιούμε άλλοτε τον όρο credential και άλλοτε τον όρο διαπιστευτήριο. Πολλές φορές θα το συναντήσουμε και ως πιστοποιητικό. [↑](#footnote-ref-9)
10. https://simple.wikipedia.org/wiki/Digital\_certificates (ημερομηνά ανάκτησης 5/3/2016) [↑](#footnote-ref-10)
11. Σε πολλές περιπτώσεις θα συναντάμε την Αρχή Πιστοποίησης και με τον όρο πάροχος ή issuer [↑](#footnote-ref-11)
12. Πώς λειτουργεί η τεχνολογία Blockchain. Οδηγός για αρχάριους.  
    Διαθέσιμο:<https://iguru.gr/2018/12/11/what-the-blockchain-guide-for-beginners/> [↑](#footnote-ref-12)
13. Technology: Beyond Bitcoin  
    Διαθέσιμο: <https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>  
      
     [↑](#footnote-ref-13)
14. Bitcoin Documentary 2017 - Bitcoin Documentary on Netflix.   
    Διαθέσιμο:<https://www.youtube.com/watch?v=TRYCVEGQ1PY> [↑](#footnote-ref-14)
15. What is Bitcoin? Banking On Bitcoin (Netfilix Original).  
    Διαθέσιμο: <https://www.netflix.com/gr/title/80154500>  
     [↑](#footnote-ref-15)
16. Ada Ivanova. What Is FPGA and Is It the Future of Crypto Mining.  
    Διαθέσιμο: <https://www.maketecheasier.com/what-is-fpga/> [↑](#footnote-ref-16)
17. Ποιο είναι το καλύτερο πορτοφόλι Bitcoin? Ο απόλυτος οδηγός.  
    Διαθέσιμο: <https://www.buybitcoinworldwide.com/el/portofolia-bitcoin/> [↑](#footnote-ref-17)
18. Copay Wallet Review.  
    Διαθέσιμο:<https://www.bitdegree.org/tutorials/copay-wallet> [↑](#footnote-ref-18)
19. How to Create a Bitcoin Wallet at Bitgo.com.  
    Διαθέσιμο: <https://www.wikihow.com/Create-a-Bitcoin-Wallet-at-Bitgo.com> [↑](#footnote-ref-19)
20. Bitcoin’s Growing Energy Problem.  
    Διαθέσιμο: <https://digiconomist.net/bitcoins-growing-energy-problem>  
     [↑](#footnote-ref-20)
21. https://www.dpa.gr/portal/page?\_pageid=33,211315&\_dad=portal&\_schema=PORTAL [↑](#footnote-ref-21)
22. https://www.hba.gr/UplDocs/GDPR/%CE%86%CF%81%CE%B8%CF%81%CE%B112\_21\_GDPR.pdf [↑](#footnote-ref-22)