**ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ**

**ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΤΟΥΡΙΣΜΟΥ**

**(πρώην Τμήμα Λογιστικής & Χρηματοοικονομικής – Μεσολόγγι)**

# ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# ΤΕΧΝΟΛΟΓΙΕΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΧΡΗΣΤΩΝ ΜΕ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ


**ΓΑΣΠΑΡΗΣ ΝΙΚΟΛΑΟΣ Α.Μ. : 11062**

**ΜΑΣΤΡΟΚΩΣΤΑΣ ΑΝΑΣΤΑΣΙΟΣ Α.Μ. : 18340**

**ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ : ΠΑΞΙΜΑΔΗΣ ΚΩΝ/ΝΟΣ**

**ΠΑΤΡΑ**

**ΙΟΥΛΙΟΣ 2020**

# *ΠΡΟΛΟΓΟΣ*

Το παρόν τεύχος αποτελεί την πτυχιακή εργασία που εκπονήθηκε στο τμήμα Λογιστικής & Χρηματοοικονομικής της Σχολής Διοίκησης & Οικονομίας. Αντικείμενο της εργασίας είναι οι τεχνολογίες ταυτοποίησης χρηστών με προστασία της ιδιωτικότητας, ένα θέμα πάντα επίκαιρο λόγω της ραγδαίας κυρίως τεχνολογικής εξέλιξης των διαδικτυακών εφαρμογών.

Η συνεχώς αυξανόμενη χρήση υπηρεσιών τόσο από κρατικούς όσο και από ιδιωτικούς φορείς με τις Τεχνολογίες Πληροφορίας και Επικοινωνίας (ΤΠΕ) αυξάνει πολύ σημαντικά τους κινδύνους των συστημάτων, το πλήθος και το εύρος των απειλών και των επιθέσεων, καθώς και τη σοβαρότητα των συνεπειών για τον πάροχο αλλά και τον τελικό χρήστη της εκάστοτε υπηρεσίας σε περίπτωση κάποιου περιστατικού ασφάλειας. Οι σημερινές επιθέσεις προς τις προσφερόμενες ηλεκτρονικές υπηρεσίες και τα πληροφοριακά συστήματα (ΠΣ) που τις υποστηρίζουν αποτελούν ένα νέο είδος ηλεκτρονικού πολέμου, ενώ μπορεί να έχουν ποινικό, οικονομικό ή τρομοκρατικό κίνητρο και να οδηγήσουν σε αποσταθεροποίηση της κοινωνίας. Διαρροές κρίσιμων πληροφοριών, τροποποίηση ευαίσθητων δεδομένων και μη διαθεσιμότητα βασικών λειτουργιών μπορεί να θέσουν σε κίνδυνο οικονομικά συμφέροντα εταιρειών αλλά και στρατηγικά συμφέροντα κρατών.

Δεδομένου ότι οι επιθέσεις εναντίον των ΤΠΕ εξελίσσονται συνεχώς και η ανίχνευσή τους γίνεται όλο και πιο δύσκολη, η εξασφάλιση ενός επαρκούς επιπέδου ασφάλειας και προστασίας της ιδιωτικότητας των χρηστών κρίνεται αναγκαία. Για τον λόγο αυτό, αποτελεί πλέον επιτακτική ανάγκη κατά τον σχεδιασμό και την ανάπτυξη ασφαλών πληροφοριακών συστημάτων να λαμβάνονται υπόψη: (α) η ποικιλία και ένταση των κινδύνων που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα, (β) οι Νομικές και Κανονιστικές απαιτήσεις για την προστασία ευαίσθητων δεδομένων και δεδομένων προσωπικού χαρακτήρα, καθώς και (γ) το σημαντικό κόστος από τυχόν σκόπιμες παραβιάσεις της ασφάλειας του συστήματος, όπως επίσης και των ακούσιων, τυχαίων και φυσικών γεγονότων που απειλούν ένα σύγχρονο πληροφοριακό σύστημα.

Για την αποτελεσματική αντιμετώπιση των ζητημάτων αυτών, καθοριστική συνεισφορά έχει η χάραξη στρατηγικών, ο ορισμός πολιτικών, η ανάπτυξη υπηρεσιών και μηχανισμών καθώς και η συνεχής αξιολόγηση του συνολικού εγχειρήματος για τη δημιουργία ενός ολοκληρωμένου περιβάλλοντος ασφάλειας και εμπιστοσύνης.

Το αντικείμενο όπως φαίνεται και από τα παραπάνω είναι πολύ σημαντικό και ενδιαφέρον και ευχαριστώ στο σημείο αυτό τον Καθηγητή μου Δρ. ___Ισίδωρο Πέρικο_____ για την επιλογή του συγκεκριμένου θέματος, την αμέριστη βοήθεια και συμπαράσταση κατά τη διάρκεια της εργασίας.

## *ΠΕΡΙΛΗΨΗ*

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

Ειδικότερα στο πρώτο κεφάλαιο της εργασίας γίνεται αναφορά στα πληροφοριακά συστήματα (ΠΣ), στα μέρη από τα οποία αποτελούνται καθώς και στην ασφάλεια και τους βασικούς άξονες αυτής ώστε να αποφεύγεται η χρήση πληροφοριών από μη εξουσιοδοτημένους χρήστες. Πολύ σημαντική εφαρμογή των ΠΣ γίνεται στις μέρες με όλο και εντονότερο ρυθμό σε εφαρμογές Ηλεκτρονικής Διακυβέρνησης (ΗΔ) με στόχο την καλύτερη εξυπηρέτηση των πολιτών σε παγκόσμια κλίμακα. Για το λόγο αυτό στο πλαίσιο του πρώτου κεφαλαίου αναλύεται η δομή των ΠΣ σε εφαρμογές ΗΔ και δίνονται τα κυριότερα χαρακτηριστικά δια λειτουργικότητας των ΠΣ στην ΗΔ. Μελετάται και αποτυπώνεται συνοπτικά η έννοια της ΗΔ, με την παράθεση των σημαντικότερων ορισμών. Στη συνέχεια παρουσιάζονται οι βασικές αρχές, οι τομείς, καθώς και τα διαφορετικά επίπεδα στα οποία μπορεί να ενταχθεί μία ηλεκτρονική υπηρεσία. Ακόμη παρουσιάζεται η εξέλιξη των ηλεκτρονικά παρεχόμενων υπηρεσιών σε παγκόσμιο επίπεδο, καθώς και η υπάρχουσα κατάσταση στην Ελλάδα τόσο σε επίπεδο ηλεκτρονικών υπηρεσιών όσο και σε επίπεδο νομικού και κανονιστικού πλαισίου.

Στο δεύτερο κεφάλαιο αναφέρονται μέθοδοι ταυτοποίησης με κάρτες και κωδικούς, μέθοδοι που γενικότερα σκοπό έχουν την μεγαλύτερη ασφάλεια των δεδομένων των χρηστών και την αποφυγή υποκλοπής ή αλλοίωσης κρίσιμων πληροφοριών – προσωπικών δεδομένων από τρίτα πρόσωπα.

Στο τρίτο κεφάλαιο γίνεται αναφορά στην ιδιωτικότητα, στον ορισμό των προσωπικών δεδομένων – στοιχείων, καθώς και στη σημασία της προστασίας. Επίσης γίνεται αναφορά και συζήτηση επί του GDPR



Λέξεις – Κλειδιά

Πληροφοριακά Συστήματα – ΠΣ

Ηλεκτρονική Διακυβέρνηση – ΗΔ

Τεχνολογία Πληροφοριών & Επικοινωνιών – ΤΠΕ

*Περιεχόμενα*

# Κατάλογος εικόνων

# *Εισαγωγή.*

Τα τελευταία χρόνια οι κοινωνίες χαρακτηρίζονται πολύ συχνά ως κοινωνίες της πληροφορίας, με την έννοια ότι η διάχυση της πληροφορίας με τη βοήθεια της τεχνολογίας και ειδικότερα της χρήσης του διαδικτύου είναι μια πολύ εύκολη διαδικασία. Πλέον το διαδίκτυο αποτελεί αναγκαίο εργαλείο για πλήθος καθημερινών αναγκών του ανθρώπου όπως επικοινωνία (πλατφόρμες κοινωνικής δικτύωσης – Facebook, Instagram), ψυχαγωγία (διαδικτυακά παιχνίδια, WebTV προγράμματα), εκπαίδευση (ιστοσελίδες πλήθους μαθημάτων προς βοήθεια μαθητών – φοιτητών ή και πιο συγκεκριμένων θεμάτων της επιστήμης), διεκπεραίωση συναλλαγών με τράπεζες και χρηματοπιστωτικά ιδρύματα.

Πέρα από τις παραπάνω διαδικασίες που μπορεί κανείς να ακολουθήσει με τη βοήθεια του προσωπικού του σταθερού ή φορητού υπολογιστή, πλέον η τεχνολογία προσφέρει και άλλες κινητές συσκευές όπως tablets, δίνοντας έτσι πρόσβαση στις διεργασίες από οποιοδήποτε σημείο και αν βρεθεί κανείς αρκεί να υπάρχει ένα ασύρματο δίκτυο εντός εμβέλειας, κάτι που στις μέρες μας γίνεται ολοένα και πιο εύκολα αφού η κάλυψη των δικτύων επεκτείνεται με γεωμετρική πρόοδο.

Στα πρώτα χρόνια της δημιουργίας του διαδικτύου οι χρήστες είχαν τη δυνατότητα ανάγνωσης και ενημέρωσης μόνο από το περιεχόμενο των ιστοσελίδων (Web 1.0), ενώ στις μέρες μας παρέχεται η δυνατότητα καταχώρησης διαχείρισης και δημοσίευσης απόψεων και άλλου πολυμέσου υλικού σε ποικίλα φόρουμ συζητήσεων κοινωνικής δικτύωσης (Web 2.0). Για να είναι εφικτή η πρόσβαση και η συμμετοχή των ενδιαφερομένων απαιτείται η δημιουργία λογαριασμών στους οποίους ο χρήστης καλείται να καταχωρήσει πλήθος προσωπικών δεδομένων πολλές φορές σε υπερβολικό βαθμό είτε εκούσια είτε ακούσια.

Κατά αυτό τον τρόπο και παρά την επιθυμία των χρηστών για ανωνυμία ώστε να προφυλάσσουν τα προσωπικά δεδομένα δηλ. την ιδιωτικότητα συχνά αυτά παραβιάζονται. Αυτή η παραβίαση αποτελεί το πρόβλημα των ημερών μας και οι αρχές προστασίας προσωπικών δεδομένων που δημιουργήθηκαν ως αντιστάθμισμα, συχνά καλούνται να επιβάλλουν ποινές σε εταιρίες – γίγαντες π.χ. κοινωνικής δικτύωσης (Facebook).

Απαιτείται συνεχής ενημέρωση των χρηστών για τα αποτελέσματα πιθανών υποκλοπών ή αλλοίωσης προσωπικών δεδομένων οι οποίοι ανύποπτοι καταχωρούν σε πλατφόρμες προσωπικές πληροφορίες (τηλέφωνα, διευθύνσεις κατοικίας, οικογενειακή κατάσταση) κατά τη συμμετοχή τους στα λεγόμενα κοινωνικά δίκτυα.

# *1. Πληροφοριακά Συστήματα.*

Ως Πληροφοριακό Σύστημα (ΠΣ) ορίζεται κάθε σύστημα που περιλαμβάνει τη συλλογή, οργάνωση, αποθήκευση και διαβίβαση πληροφοριών. Γενικότερα το ΠΣ πέρα από τις διαδικασίες για τις οποίες είναι επιφορτισμένο με τη βοήθεια λογισμικού υλικού που λειτουργεί επί του ηλεκτρονικού υπολογιστή, αποτελείται και από ανθρώπινους πόρους, (man power) δηλ. τις ώρες απασχόλησης των ανθρώπων που θα εργαστούν πάνω στην επεξεργασία - ερμηνεία των πληροφοριών και θα αποδώσουν κάποια συγκεκριμένα και ιδιαίτερα χαρακτηριστικά της συμπεριφοράς των πληροφοριών. Ο όρος ΠΣ χρησιμοποιείται πολλές φορές καταχρηστικά προκειμένου να περιγραφεί ένα συγκεκριμένα απαιτούμενο λογισμικό για την υλοποίηση μιας διαδικασίας με δείγμα που βρίσκεται πάνω σε μια βάση δεδομένων ή ακόμα και σε ένα προσωπικό ΗΥ (Φωτεινόπουλος 2016).

Ο συγκερασμός των παραπάνω χρήσεων του όρου ΠΣ οδήγησε την Jessup (2008) σε έναν ορισμό του ΠΣ ως ένα σύστημα που σχετίζεται τόσο με πληροφορίες όσο και με συμπληρωματικά δίκτυα (υλικό και λογισμικό) το οποίο χρησιμοποιείται από ανθρώπους και οργανισμούς 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. Στόχος κάθε ΠΣ είναι η αποτελεσματική υποστήριξη της διαχείρισης και λήψης αποφάσεων στο πλαίσιο ενός οργανισμού.

Κατά άλλους ερευνητές ένα ΠΣ αποτελεί μια ευρύτερη έννοια συμπεριλαμβανομένων τόσο των τεχνολογιών της πληροφορίας και των επικοινωνιών (ΤΠΕ), όσο και της αλληλεπίδρασης των ανθρώπων με την τεχνολογία, με ευρύτερο στόχο την υποστήριξη των όλων των διαδικασιών του οργανισμού στον οποίον μετέχουν (Bulgacs 2013, Kroenke 2008).

Θα πρέπει να αναγνωρίζεται πάντως η ύπαρξη σαφούς διάκρισης μεταξύ των ΠΣ, των συστημάτων πληροφορικής και των επιχειρηματικών διαδικασιών. Τα ΠΣ μπορεί να περιλαμβάνουν κάποια στοιχεία 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 (Φωτεινόπουλος 2016).

Παλαιότερες εκδοχές των ΠΣ (Silver 1995) περιλαμβάνουν το λογισμικό, το υλικό, τα δεδομένα, τους ανθρώπους, και τις διαδικασίες. Ενισχύοντας της παραπάνω προσέγγιση στην έννοια του ΠΣ μπορούν να προστεθούν άλλα στοιχεία όπως το περιβάλλον, ο σκοπός, τα όρια και οι αλληλεπιδράσεις μεταξύ των χρηστών (Zheng 2009).

## *1.1 Τμήματα Πληροφοριακών Συστημάτων*

Ανάμεσα στους τύπους των ΠΣ, μπορούν να αναφερθούν για παράδειγμα

- συστήματα επεξεργασίας συναλλαγών,
- συστήματα υποστήριξης αποφάσεων,
- συστήματα διαχείρισης γνώσης,
- συστήματα διαχείρισης μάθησης,
- συστήματα διαχείρισης βάσεων δεδομένων,
- συστήματα αυτοματισμού κλπ.

Υψηλής σημασίας για τα ΠΣ είναι η χρήση τεχνολογιών που σχεδιάζονται για την υλοποίηση λειτουργιών που ο ανθρώπινος εγκέφαλος δυσκολεύεται ή αδυνατεί να εκτελέσει, όπως η διαχείριση μεγάλου όγκου πληροφοριών, η εκτέλεση πολύπλοκων υπολογισμών, και ο έλεγχος πολλών και ταυτόχρονων διεργασιών. Ο άνθρωπος τότε στέκεται σε ένα

υψηλότερο επίπεδο ελέγχοντας το ΠΣ και αυτό φαίνεται από το ότι στις μέρες μας πολλές εταιρείες και οργανισμοί έχουν δημιουργήσει επιτελικές θέσεις Πληροφοριακών Συστημάτων και Πληροφορικής (Chief Information Office r - (CIO)) ανάλογες με αυτές του Διευθύνοντα Σύμβουλου (CEO), Οικονομικού Διευθυντή (CFO), Τεχνικού Διευθυντή. Επιπλέον κατά περίπτωση υπάρχει και η θέση του Διευθυντή Ασφάλειας Πληροφοριών (CISO) η οποία επικεντρώνεται στη διαχείριση της ασφάλειας των πληροφοριών (Φωτεινόπουλος 2016).

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

- Υλικό (Hardware),
- Λογισμικό (Software),
- Δεδομένα (Data)
- Διαδικασίες (Procedures)
- Άνθρωποι (People)
- Ανατροφοδότηση (Feedback)

Συνοπτικά ο όρος *υλικό* αναφέρεται στα μηχανήματα, στην κεντρική μονάδα επεξεργασίας (CPU), καθώς και το σύνολο του εξοπλισμού υποστήριξης. Σε αυτό τον εξοπλισμό συμπεριλαμβάνονται οι συσκευές εισόδου και εξόδου, οι συσκευές αποθήκευσης και οι 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 ΠΣ, 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 συστημάτων, για παράδειγμα αυτούς που συλλέγουν τα δεδομένα για να εισαχθούν αργότερα στο ΠΣ. Τέλος η *ανατροφοδότηση* είναι ένα συστατικό 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 (Γκρίτζαλης 2003).

Κατά την κλασική άποψη της δεκαετία του 1980, ένα ΠΣ συνιστάται από μια πυραμίδα επιμέρους συστημάτων, που αντανακλούν 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 (Laudon 1988).

Το κλασικό μοντέλο πυραμίδας από τη δεκαετία του 1980 έχει υποστεί μεταβολές και τροποποιήσεις, ωστόσο παραμένει χρήσιμο, κυρίως για εκπαιδευτικούς σκοπούς αλλά και για να εξάρει τη σημασία της ιεράρχησης των τεχνολογιών, των διαδικασιών καθώς και το ρόλο των ανθρώπων μέσα σε ένα οργανισμό. Στις μέρες μας έχουν αναπτυχθεί νέες τεχνολογίες και κατηγορίες ΠΣ, μερικά από τα οποία δεν μπορούν να ενσωματωθούν με ευκολία στο αρχικό μοντέλο πυραμίδας. Πολλά από τα νέα ΠΣ είναι τα ακόλουθα:

- Αποθήκες Δεδομένων (Data Warehouses)
- Διαχείρισης Επιχειρηματικών Πόρων (ERP)
- Έμπειρα Συστήματα (Expert Systems)

- Μηχανές Αναζήτησης (Search Engines)
- Γεωγραφικά Πληροφοριακά Συστήματα (GIS)


***Εικόνα 1: Πληροφοριακά Συστήματα - Μοντέλο Πυραμίδας***

## *1.2 Ασφάλεια Πληροφοριακών Συστημάτων – Ορισμοί.*

Κατά το σχεδιασμό ασφαλών πολιτικών στα ΠΣ 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 ως στόχο την διασφάλιση του πληροφοριακού συστήματος αλλά και ολόκληρου του οργανισμού που το χρησιμοποιεί 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 ασφαλείας (Γκρίτζαλης 2003).

Η πολιτική ασφάλειας που διέπει τον οργανισμό θα πρέπει να μεριμνά αποτελεσματικά για όλους τους εμπλεκόμενους στη χρήση και τη λειτουργία του ΠΣ. 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. Συνήθως μια πολιτική ασφάλειας περιλαμβάνει διαδικασίες όπως:

- Εφαρμογή πληρότητας αναφορικά με οδηγίες και μέτρα προστασίας των υπηρεσιών που προσφέρονται καθώς και των λειτουργιών που εκτελούνται,
- Εφαρμογή επικαιρότητας αναφορικά με τρέχουσες τεχνολογικές εξελίξεις,
- Εφαρμογή γενικευσιμότητας αναφορικά με επιπρόσθετες παρεμβάσεις, τροποποιήσεις ή προσθήκες που μπορεί να γίνουν στο ΠΣ.

Η επιτυχία εφαρμογής μίας πολιτικής ασφάλειας εξαρτάται πρωτίστως από τη διάθεση και συμμετοχή των εμπλεκόμενων φορέων. Προς το σκοπό αυτό θα πρέπει η εταιρία ή οργανισμός να παρέχει συνεχή και αδιάλειπτη εκπαίδευση των χρηστών, να αξιολογείται η πρόσβαση, η αμεσότητα και η ευκολία αυτής και να διενεργούνται τακτικά δοκιμές αντοχής (stress tests). Με τη συνεχή αξιολόγηση σε τακτά χρονικά διαστήματα της πολιτικής ασφαλείας του ΠΣ μπορεί να διαγνωσθεί το επίπεδο ετοιμότητας ως προς την αντιμετώπιση και εξουδετέρωση οποιασδήποτε απειλής (Φωτεινόπουλος 2016).

## *1.3 Βασικοί Άξονες Ασφάλειας των ΠΣ*

Κατά τον Krause (1998) οι χαρακτηριστικοί παράγοντες στους οποίους βασίζεται η ασφάλεια των ΠΣ όπως καταγράφονται και από τον Φωτεινόπουλο (2016) είναι οι παρακάτω:

- **Ακεραιότητα (Integrity):** Είναι υψηλής σημασίας η διατήρηση των δεδομένων του ΠΣ σε μία γνώριμη κατάσταση, αναλλοίωτα, χωρίς να μπορούν να υποστούν οποιουδήποτε είδους τροποποίηση, αφαίρεση ή προσθήκη από άτομα εντός και εκτός του οργανισμού που δεν είναι εξουσιοδοτημένα για τις παραπάνω διαδικασίες. Κατά αυτή την έννοια ένας οργανισμός ή μια υπηρεσία θα πρέπει να καθορίζουν με αυστηρό τρόπο την επιλογή των ατόμων που θα έχουν πρόσβαση σε ευαίσθητες λειτουργίες του ΠΣ. Επίσης θα πρέπει να αποτρέπεται η πρόσβαση στη χρήση μη εξουσιοδοτημένων ατόμων. *Παράδειγμα ακεραιότητας θα μπορούσε να αποτελεί ένας οργανισμός μέσων μαζικής ενημέρωσης όπου θα πρέπει τα άρθρα που δημοσιεύονται στο διαδίκτυο να είναι ασφαλή από οποιαδήποτε τροποποίηση και εισαγωγή κειμένων - πληροφοριών από χρήστες πέραν του αρθρογράφου.*

- **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 υπό 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)
  - την πιστοποίηση δεδομένων (data authentication).

  Με τον πρώτο πυλώνα εξασφαλίζεται ότι κάθε οντότητα στο ΠΣ είναι αυτή που ισχυρίζεται και δεν υπάρχει κάποια πλαστοπροσωπία. Με το δεύτερο πυλώνα εξασφαλίζεται η

τοποθεσία, η 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 ως το άθροισμα της Ακεραιότητας και τη Αυθεντικότητας

- **Μοναδικότητα (Uniqueness):** Είναι η αδυναμία αντιγραφής και αναπαραγωγής της πληροφορίας χωρίς εξουσιοδότηση.

## *1.4 Πληροφοριακά Συστήματα στην Ηλεκτρονική Διακυβέρνηση.*

Στις μέρες μας παραδείγματα ΠΣ που συναντώνται στην καθημερινότητα είναι τα συστήματα που σχετίζονται με την Ηλεκτρονική Διακυβέρνηση (e – Government). Ο όρος χρησιμοποιείται για την περιγραφή της εφαρμογής Τεχνολογιών Πληροφοριών και Επικοινωνιών (ΤΠΕ) σε διαδικασίες και υπηρεσίες της Δημόσιας Διοίκησης.

Η χρήση των ΤΠΕ στην Ηλεκτρονική Διακυβέρνηση βέβαια δεν αποτελεί σήμερα κάτι καινούργιο ή καινοτόμο, αφού εφαρμόζεται αρκετές δεκαετίες τώρα σε διάφορους επιμέρους τομείς ή διαδικασίες της Δημόσιας Διοίκησης. Ο συγκεκριμένος όρος αν και εμφανίστηκε στα τέλη της δεκαετίας του 1990, η αλληλεπίδραση προϋπήρχε, σχεδόν από την εμφάνιση των πρώτων Πληροφοριακών Συστημάτων (Grönlund & Horan, 2005) & (Danziger & Andersen, 2002).

Μια τυπική υπηρεσία (ΠΣ) Ηλεκτρονικής Διακυβέρνησης έχει τα ακόλουθα χαρακτηριστικά, τα οποία τη διαφοροποιούν από μία διαδικασία ή απλή διεργασία ενός φορέα (Διακονικολάου & Μυλωνόπουλος, 2004),

- Έχει τελικό χρήστη ο οποίος είναι συνήθως ο πολίτης, η επιχείρηση ή άλλος φορέας της Δημόσιας Διοίκησης.

- Έχει τελικό παραδοτέο που πρέπει να είναι αυτοτελές και ο τελικός χρήστης που το παραλαμβάνει να είναι σε θέση να το αξιοποιήσει χωρίς να απαιτούνται επιπλέον διεργασίες ή συναλλαγές.

- Έχει πάροχο που είναι κάποια μονάδα της Δημόσιας Διοίκησης αρμόδια για την παροχή της συγκεκριμένης ηλεκτρονικής υπηρεσίας.

- Έχει ρυθμιστή που είναι μία, κατ' ελάχιστον, μονάδα της Δημόσιας Διοίκησης, αρμόδια για το ρυθμιστικό πλαίσιο της ηλεκτρονικής υπηρεσίας.

Συνολικά, τα χαρακτηριστικά των ΠΣ στην Ηλεκτρονική Διακυβέρνηση συνοψίζονται:

- Παροχή υπηρεσιών που βασίζονται στις τεχνολογίες Διαδικτύου
- Αξιοποίηση των ΤΠΕ σε όλες τις δραστηριότητες της Δημόσιας Διοίκησης
- Μετασχηματισμός διαδικασιών της Δημόσιας Διοίκησης

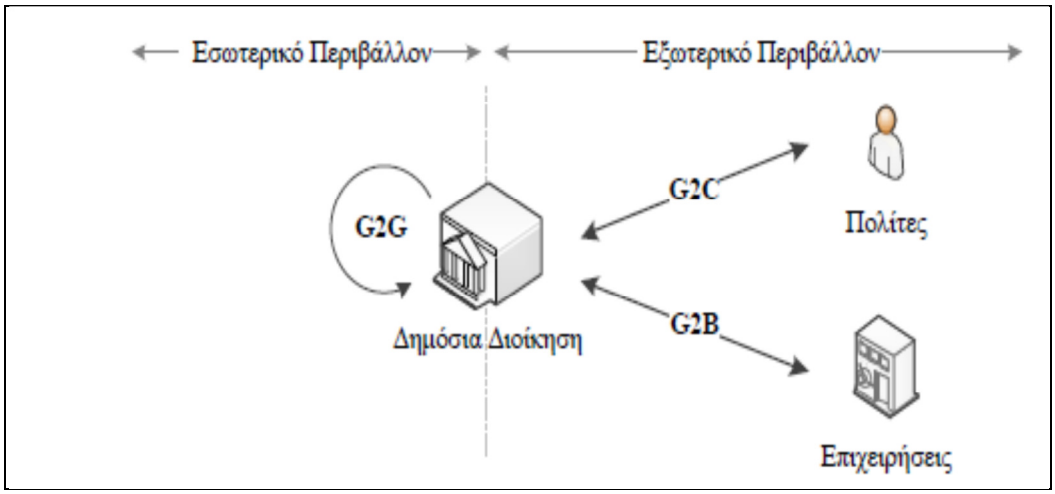
Σύμφωνα με την αναφορά των Ηνωμένων Εθνών (United Nations, 2003), οι βασικές αρχές (*Principles*) για την ανάπτυξη ενός ολοκληρωμένου και επιτυχημένου περιβάλλοντος ΠΣ εφαρμογής Ηλεκτρονικής Διακυβέρνησης είναι:

- υποστήριξη, δέσμευση και συμμετοχή της κεντρικής κυβέρνησης στον στρατηγικό σχεδιασμό και την υλοποίηση των στόχων,
- αποτελεσματικότητα και αποδοτικότητα της κεντρικής κυβέρνησης στην υλοποίηση των απαιτούμενων αλλαγών,
- διασφάλιση απαιτούμενης και επαρκούς χρηματοδότησης,
- καλλιέργεια και ανάπτυξη της απαραίτητης κουλτούρας στη Δημόσια Διοίκηση,
- προγραμματισμός και συντονισμός των απαιτούμενων δράσεων,
- διαμόρφωση κατάλληλου νομικού και κανονιστικού πλαισίου,

Η ανάπτυξη ενός ΠΣ στο πλαίσιο της ΗΔ αποτελείται από διαδικασίες που σχετίζονται όχι μόνο με το εξωτερικό, αλλά και με το εσωτερικό περιβάλλον της Δημόσια Διοίκησης. Κατά αυτή την έννοια οι βασικότεροι τομείς (*Domains*) ενός περιβάλλοντος ΗΔ προκύπτουν από την αναγνώριση των εμπλεκόμενων μελών (*Actors*) στις αλληλεπιδράσεις με τη Δημόσια Διοίκηση. Οι πιο συνήθεις εμπλεκόμενοι είναι i) οι πολίτες, ii) οι επιχειρήσεις και iii) η ίδια η Δημόσια Διοίκηση. Έτσι προκύπτουν οι ακόλουθες αλληλεπιδράσεις:

- ***Government to Citizen (G2C)*:** περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ μεμονωμένων πολιτών και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική υποβολή φορολογίας εισοδήματος φυσικών προσώπων)
- ***Government to Business (G2B)*:** περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ επιχειρήσεων και οργανισμών του ιδιωτικού τομέα και της Δημόσιας Διοίκησης. (π.χ. ηλεκτρονική προμήθεια για δημόσιους φορείς)
- ***Government to Government (G2G)***: περιλαμβάνει όλες τις αλληλεπιδράσεις μεταξύ φορέων και οργανισμών που εμπίπτουν στη δικαιοδοσία της Δημόσιας Διοίκησης (π.χ. ηλεκτρονική ανταλλαγή πληροφοριών φορέων του Δημοσίου).

Οι τομείς του G2B και G2C χαρακτηρίζονται ως "Εξωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*external e-Government*) ενώ ο τομέας G2G χαρακτηρίζεται ως "Εσωτερικό Περιβάλλον Ηλεκτρονικής Διακυβέρνησης" (*Internal e-Government*). Σε αρκετές περιπτώσεις πραγματοποιείται και ένας επιπλέον διαχωρισμός στο εσωτερικό περιβάλλον, προκειμένου να περιγραφούν οι αλληλεπιδράσεις της Δημόσιας Διοίκησης με Δημόσιους Φορείς άλλων κρατών (Δρογκάρης Π., 2013) . Στο Σχήμα 2-1 που ακολουθεί, απεικονίζονται οι τομείς αυτοί.




***Εικόνα 2: Τομείς Ηλεκτρονικής Διακυβέρνησης (Δρογκάρης Π. 2013).***

## *1.5 Χαρακτηριστικά ενός ΠΣ στην ΗΔ.*

Κατά τους ερευνητές (Διακονικολάου & Μυλωνόπουλος, 2004), ο τελικός χρήστης μίας υπηρεσίας του ΠΣ σε εφαρμογή της Ηλεκτρονικής Διακυβέρνησης θα πρέπει να διαθέτει τα παρακάτω χαρακτηριστικά ώστε το ΠΣ να θεωρηθεί επιτυχημένο κατά τη λειτουργία του:

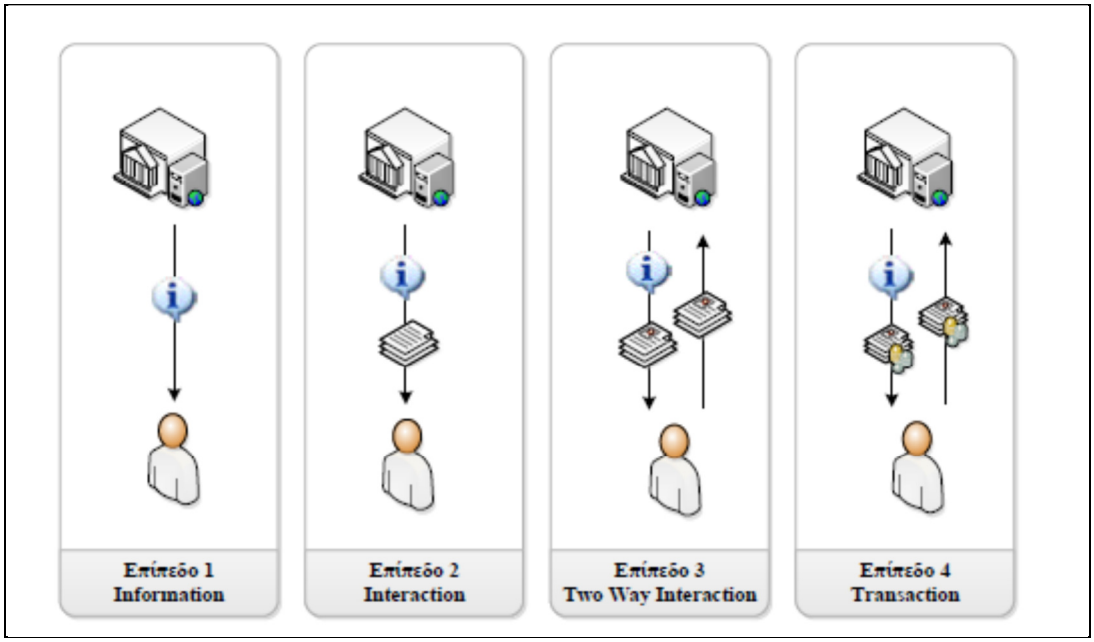
- Δεν απαιτείται να γνωρίζει ή να είναι εξοικειωμένος με τον τρόπο λειτουργίας, τη δομή και τις αρμοδιότητες των οργανωτικών μονάδων της Δημόσιας Διοίκησης που εμπλέκονται για την εξυπηρέτησή του.
- Πρέπει να έρχεται σε επαφή αποκλειστικά με το σημείο εκκίνησης της υπηρεσίας (κέντρο εξυπηρέτησης, δημόσιο πληροφοριακό σύστημα) και να παραλαμβάνει το αποτέλεσμα της υπηρεσίας από ένα σημείο εξόδου, χωρίς να ε-μπλέκεται σε ενδιάμεσα στάδια εξυπηρέτησης (*One Stop Shop*).
- Πρέπει να έχει συνεχή ενημέρωση για τη ροή της πληροφορίας και τη λήψη των αποφάσεων που αφορούν την υπόθεση που διεκπεραιώνει ηλεκτρονικά.

Για να ικανοποιούνται οι παραπάνω απαιτήσεις, θα πρέπει οι ηλεκτρονικές υπηρεσίες που παρέχονται από ένα Π.Σ. να ξεπερνούν τα όρια ενός φορέα, καθώς και να συνδυάζουν περιεχόμενο και λειτουργίες από τις επιμέρους διαδικτυακές υπηρεσίες των εμπλεκόμενων φορέων, με τρόπο διαφανή για τον τελικό χρήστη κάθε υπηρεσίας. Προς την κατεύθυνση αυτή στρέφονται οι προσπάθειες για την κατασκευή διαδικτυακών πυλών ενημέρωσης και εξυπηρέτησης, που καλύπτουν ένα ευρύ φάσμα φορέων της Δημόσιας Διοίκησης (π.χ. Οικονομικές Υπηρεσίες) ή, στη βέλτιστη περίπτωση, το σύνολο της Δημόσιας Διοίκησης. Οι διαδικτυακές αυτές πύλες είναι γνωστές με τον όρο Κυβερνητικές Δικτυακές Πύλες (*e-Government Portals*).

Οι ηλεκτρονικές υπηρεσίες του ΠΣ της ΗΔ κατατάσσονται στις ακόλουθες κατηγορίες-επίπεδα, ανάλογα με το βαθμό ολοκλήρωσης (*Online Sophistication*) της υπηρεσίας που μπορεί να επιτευχθεί ηλεκτρονικά:

- ***Επίπεδο 1:*** *Πληροφοριακές Υπηρεσίες (****Information****):* Παροχή πληροφοριακού υλικού σχετικά με τον τρόπο διεκπεραίωσης της υπηρεσίας. Το υλικό αυτό α-φορά: στα δικαιολογητικά που πρέπει να προσκομιστούν, στους φορείς που εμπλέκονται για την ολοκλήρωση της υπηρεσίας, στη διαδοχή εκτέλεσης των συναλλαγών που περιλαμβάνει η υπηρεσία, κλπ.

- ***Επίπεδο 2:*** *Επικοινωνιακές Υπηρεσίες (**Interaction**):* Παροχή πληροφοριακού υλικού για τον τρόπο διεκπεραίωσης της υπηρεσίας, καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων, κ.λπ.), το οποίο οι χρήστες μπορούν να εξασφαλίσουν με αξιοποίηση του Διαδικτύου, να το εκτυπώσουν και να το χρησιμοποιήσουν κατά τη συναλλαγή τους με το φορέα σε φυσικό επίπεδο.
- ***Επίπεδο 3****: Δια δραστικές Υπηρεσίες (**Two-way interaction**):* Πέραν του πληροφοριακού υλικού που παρέχεται σε αυτό το επίπεδο, προσφέρονται on-Line φόρμες για συμπλήρωση και ηλεκτρονική αποστολή στην αρμόδια υπηρεσία-φορέα.
- ***Επίπεδο 4****: Συναλλακτικές Υπηρεσίες (**Transactions**):* Επιπλέον των φορμών α-αποστολής στοιχείων, οι ηλεκτρονικές υπηρεσίες που εντάσσονται σε αυτό το επίπεδο υποστηρίζουν λειτουργίες, όπου ο χρήστης ολοκληρώνει τις συναλλαγές που περιλαμβάνει η υπηρεσία. Το γεγονός ότι μία ηλεκτρονική υπηρεσία παρέχει τη δυνατότητα ολοκλήρωσης οικονομικών συναλλαγών, συνεπάγεται τη δυνατότητα πλήρους υποκατάστασης της αντίστοιχης μη-ηλεκτρονικής υπηρεσίας.
- ***Επίπεδο 5****:Προληπτική και στοχευμένη παροχή υπηρεσιών* (*Proactive Personalization*). Το συγκεκριμένο επίπεδο περιλαμβάνει την αυτοματοποιημένη παροχή ηλεκτρονικών υπηρεσιών, κατά την οποία ο δημόσιος φορέας προβαίνει προληπτικά σε δράσεις με στόχο να βελτιώσει την ποιότητα της παρεχόμενης υπηρεσίας και το βαθμό φιλικότητάς της προς το χρήστη (Gapgemini, 2007). Επιπρόσθετα, περιλαμβάνει και την αυτόματη εκτέλεση συγκεκριμένων ηλεκτρονικών υπηρεσιών, απαλλάσσοντας από τις αντίστοιχες ενέργειες τον πολίτη ή την επιχείρηση. Το 5ο στάδιο ψηφιακής ολοκλήρωσης μιας υπηρεσίας υφίσταται μόνον για ορισμένες ηλεκτρονικές υπηρεσίες και εκφράζει τις ακόλουθες δύο διαστάσεις:




***Εικόνα 3: Επίπεδα Ολοκλήρωσης Υπηρεσιών ΗΔ. (Δρογκάρης Π. 2013)***

- Την προληπτική παροχή υπηρεσιών *(proactive automated service deliv-ery)*, όπου η Δημόσια Διοίκηση προχωρά προληπτικά σε δράσεις για να αναβαθμίσει την παροχή μιας ηλεκτρονικής υπηρεσίας και τη φιλικότητά της προς το χρήστη. Παραδείγματα τέτοιων δράσεων αποτελούν η έγκαιρη ειδοποίηση του πολίτη / χρήστη σε περίπτωση που πρέπει να προβεί σε κάποια ενέργεια, η προ- συμπλήρωση δεδομένων σε αιτήσεις του χρήστη προς το Δημόσιο, κ.α.
- Την αυτοματοποιημένη παροχή υπηρεσιών *(automated service provision)*, όπου η Δημόσια Διοίκηση παρέχει αυτόματα συγκεκριμένες υπηρεσίες χωρίς να απαιτείται αντίστοιχη αίτηση από τον πολίτη ή τις επιχειρήσεις..

## *1.6 Βασικές Αρχές Δια λειτουργικότητας των ΠΣ στην ΗΔ.*

Σύμφωνα με την αναφορά των Ηνωμένων Εθνών (United Nations, 2003), οι βασικές αρχές (*Principles*) για την ανάπτυξη ενός ολοκληρωμένου και επιτυχημένου περιβάλλοντος Ηλεκτρονικής Διακυβέρνησης είναι:

- συνεχής παρακολούθηση και αξιολόγηση,
- προώθηση και ανάδειξη των πλεονεκτημάτων στο ευρύ κοινό και εγκαθίδρυση του απαιτούμενο επιπέδου εμπιστοσύνης.
- υποστήριξη, δέσμευση και συμμετοχή της κεντρικής κυβέρνησης στον στρατηγικό σχεδιασμό και την υλοποίηση των στόχων,
- αποτελεσματικότητα και αποδοτικότητα της κεντρικής κυβέρνησης στην υλοποίηση των απαιτούμενων αλλαγών,
- διασφάλιση απαιτούμενης και επαρκούς χρηματοδότησης,
- καλλιέργεια και ανάπτυξη της απαραίτητης κουλτούρας στη Δημόσια Διοίκηση,
- προγραμματισμός και συντονισμός των απαιτούμενων δράσεων,
- διαμόρφωση κατάλληλου νομικού και κανονιστικού πλαισίου,

Η έννοια της δια λειτουργικότητας (*Interoperability*) αφορά στα ΠΣ που αξιοποιούνται για την ολοκλήρωση διαδικασιών της Δημόσιας Διοίκησης, και συνδέεται άμεσα με την ΗΔ, επιτρέποντας τη μεταφορά και χρήση πληροφορίας με ενιαίο και αποτελεσματικό τρόπο από και προς διαφορετικά ΠΣ. Η δια λειτουργικότητα σε Π.Σ. Ηλεκτρονικής Διακυβέρνησης διακρίνεται σε οργανωτική, σημασιολογική και τεχνική, ανάλογα με το αντικείμενο στο οποίο αναφέρεται:

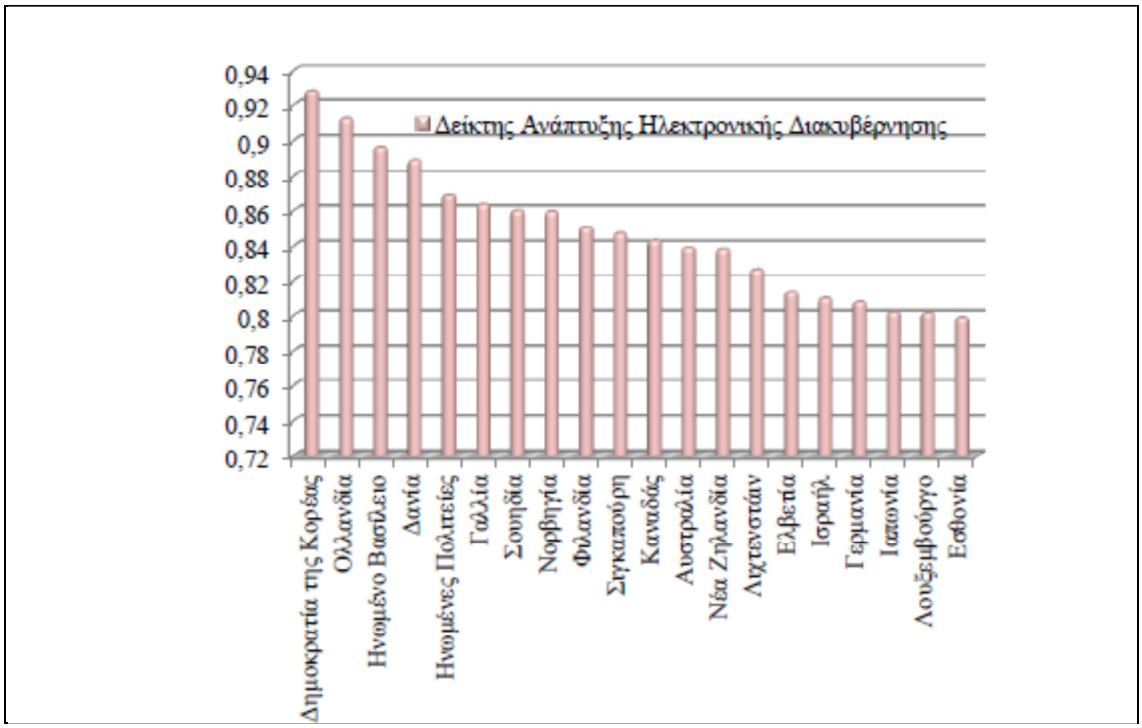
- *Οργανωτική δια λειτουργικότητα (Organisational Interoperability)*: σχετίζεται με τον καθορισμό κοινών στόχων, τη διαμόρφωση διαδικασιών και στην δημιουργία διαύλων συνεργασίας μεταξύ των τμημάτων της Δημόσιας Διοίκησης, με διαφορετικές δομές και διαδικασίες, που επιζητούν την αμοιβαία ανταλλαγή πληροφορίας

- *Σημασιολογική δια λειτουργικότητα (Semantic Interoperability)*: σχετίζεται με τον ορισμό μιας σαφώς προσδιορισμένης και κοινά αποδεκτής περιγραφής της ανταλλασσόμενης πληροφορίας ώστε να είναι κατανοητή και αξιοποιήσιμη από οποιαδήποτε εφαρμογή. Μέσω της δημιουργίας προτύπων διασφαλίζεται κοινή ορολογία και λεξιλόγιο, επιτρέποντας στα Π.Σ. να συνδυάζουν και να επεξεργάζονται πληροφορίες από άλλα Π.Σ.

- *Τεχνική δια λειτουργικότητα (Technical Interoperability)*: σχετίζεται με τη μεταφορά και αξιοποίηση της πληροφορίας σε πραγματικό χρόνο μέσω κατάλληλων φυσικών *(Physical)* και δικτυακών *(Network)* διασυνδέσεων.

## *1.5 Εξέλιξη Ηλεκτρονικής Διακυβέρνησης ανά τον κόσμο.*

Η έκθεση των Ηνωμένων Εθνών για το 2012 για την ανάπτυξη της Ηλεκτρονικής Διακυβέρνηση σε παγκόσμιο επίπεδο (United Nations, 2012), επικεντρώνεται στην έννοια των ενοποιημένων - ολοκληρωμένων υπηρεσιών που αξιοποιούν διασυνδέσεις μεταξύ διαφόρων δημόσιων υπηρεσιών και θεματικά παρόμοιων διαδικτυακών πυλών μίας στάσης, που μπορούν να αναμορφώσουν την ηλεκτρονική παροχή δημόσιων υπηρεσιών τόσο στο εμπρόσθιο τμήμα (*Front-end*) όσο και στο οπίσθιο (*Back-end*), να αυξήσουν την λειτουργική παραγωγικότητα, καθώς και τη βελτίωση των διαδικασιών και μηχανισμών διακυβέρνησης σε διάφορους τομείς της Δημόσιας Διοίκησης. Και οι 20 χώρες που σημειώνουν τους υψηλότερους δείκτες ανάπτυξης, συμπεριλαμβάνονται στις υψηλά ανεπτυγμένες οικονομίες. Από αυτές, οι 14 είναι στη Βόρεια Αμερική και την Ευρώπη, 3 στην Ανατολική Ασία (Δημοκρατία της Κορέας, Σιγκαπούρη και Ιαπωνία), 2 στην Ωκεανία (Αυστραλία και Νέα Ζηλανδία και 1 στη Δυτική Ασία (Ισραήλ). Στη συνέχεια δίνεται μια εικόνα των δεικτών ανάπτυξης για καθεμία από αυτές τις 20 χώρες.

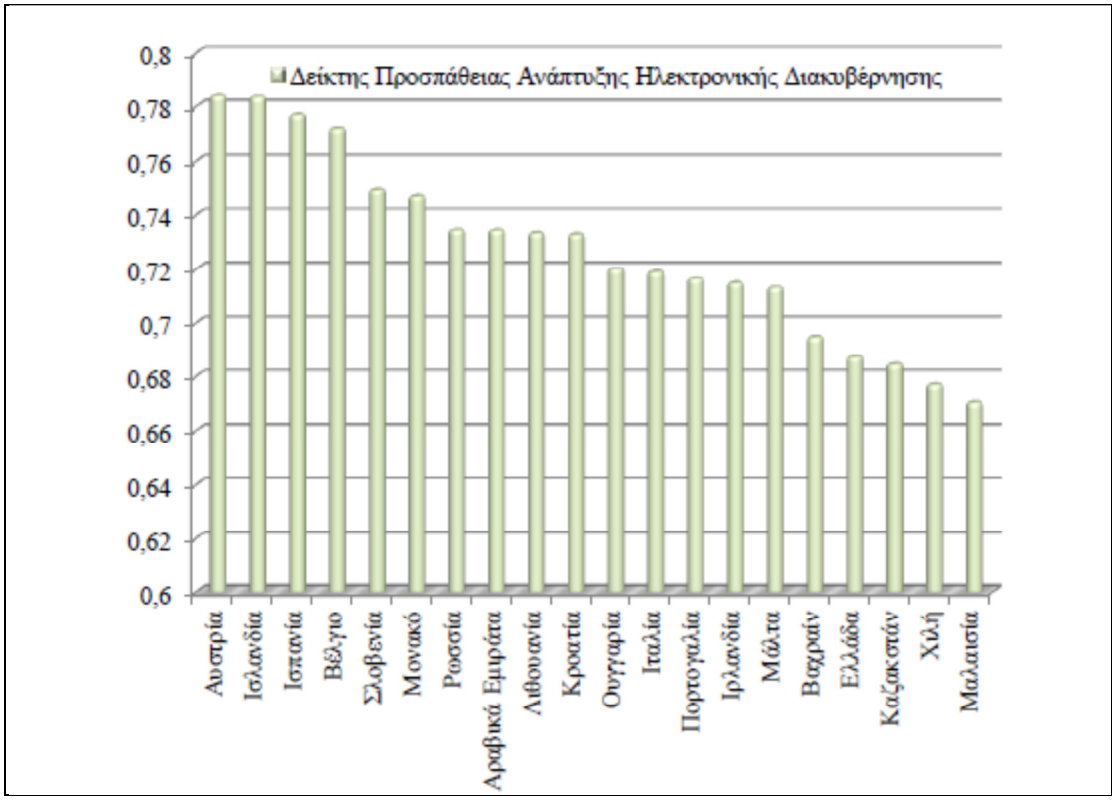



***Εικόνα 4: Δείκτης Ανάπτυξη Ηλεκτρονικής Διακυβέρνησης (Δρογκάκης Π. 2013)***

Η Δημοκρατία της Κορέας είναι ο παγκόσμιος ηγέτης στην ανάπτυξη (0,9283), ακολουθούμενη από την Ολλανδία (0,9125), το Ηνωμένο Βασίλειο (0,8960) και τη Δανία (0.8889), με τις Ηνωμένες Πολιτείες, τον Καναδά, τη Γαλλία, τη Νορβηγία, τη Σιγκαπούρη και Σουηδία να βρίσκονται πιο πίσω. Σε σύγκριση με την αντίστοιχη έκθεση του 2010 (United Nations, 2010) παρατηρείται μία σταθερή βελτίωση των δεικτών ανάπτυξης σε

παγκόσμιο επίπεδο, κάτι που οδήγησε στην αύξηση του μέσου όρου από 0,4406 σε 0,4877. Αυτή η αύξηση έρχεται να επιβεβαιώσει την αυξημένη προσπάθεια που παρατηρείται τα τελευταία χρόνια για παροχή υπηρεσιών Ηλεκτρονικής Διακυβέρνησης. Παρόλα αυτά όμως, παραμένει αρκετά μεγάλο το χάσμα που παρατηρείται μεταξύ των οικονομικά ανεπτυγμένων και μη κρατών, ιδιαίτερα στις χώρες της Αφρικής. Αυτή η διαφορά αποδίδεται κατά μεγάλο βαθμό στην έλλειψη τεχνολογικής υποδομής και διάδοσης της ευρυζωνικότητας (*Broadband*).

Αμέσως μετά τις χώρες που κατατάσσονται πρώτες σε παγκόσμιο επίπεδο, βρίσκονται οι λεγόμενοι "αναδυόμενοι ηγέτες", όπως παρουσιάζονται στο Σχήμα 2-4 παρακάτω. Ως τέτοιες χαρακτηρίζονται οι χώρες εκείνες που έχουν σημειώσει σημαντική βελτίωση σε σχέση με προηγούμενες εκθέσεις. Πρώτη σε αυτή την κατάταξη είναι η Αυστρία (0,7840) και ακολουθούν η Ισλανδία (0,7835), η Ισπανία (0,7770) και το Βέλγιο (0,7718). Σημαντική αύξηση παρατηρείται στους δείκτες της Ρωσίας (0,7345), των Ηνωμένων Αραβικών Εμιράτων (0,7344) και της Σαουδικής Αραβίας (0,6658) καθώς επίσης στην περίπτωση της Ιταλίας (0,7190) και της Πορτογαλίας (0,7165). Τέλος, αξιοσημείωτη είναι και η πρόοδος που σημείωσε η Ελλάδα (0.6872) σε σχέση με τον δείκτη του 2010 (0,5708).




***Εικόνα 5: Δείκτης προσπάθειας Ανάπτυξης Υπηρεσιών ΗΔ (United Nations 2013).***

Η προσπάθεια της Ελληνικής Δημόσιας Διοίκησης για την μετάβαση στην Ηλεκτρονική Διακυβέρνηση και την Κοινωνία της Πληροφορίας ξεκίνησε στο 1994 με την υποστήριξη των Κοινοτικών Πλαισίων Στήριξης (ΚΠΣ) (Markellos, et al., 2007). Αρχικά οι προσπάθειες αφορούσαν στην ανάπτυξη κυβερνητικών ιστότοπων για την παροχή πληροφοριακού, κυρίως, υλικού. Το 1999 διαμορφώθηκε η εθνική στρατηγική προσέγγιση στην Ηλεκτρονική Διακυβέρνηση και την Κοινωνία της Πληροφορίας, με έμφαση στο σχεδιασμό για όλους και στην ποιότητα των παρεχόμενων υπηρεσιών, με απώτερο σκοπό να διασφαλιστεί η κοινωνική συνοχή και η βελτίωση του βιοτικού επιπέδου (Gouscos, et al.,

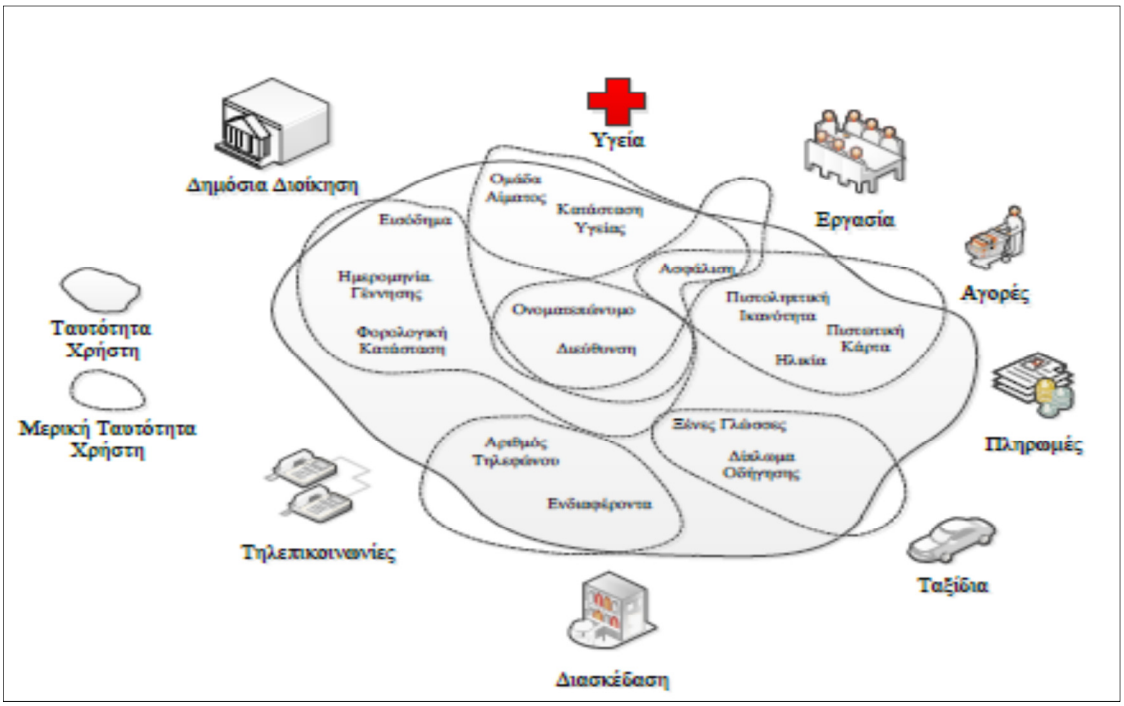
2000). Από το 2000 και έπειτα ξεκινά η παροχή ορισμένων υπηρεσιών Ηλεκτρονικής Διακυβέρνησης (Hahamis, et al., 2005). Όμως, ο Δημόσιος Τομέας στην Ελλάδα χαρακτηρίζεται από ιδιαίτερη πολυπλοκότητα, χαμηλή απόδοση, έλλειψη μηχανογράφησης και τεχνολογικών υποδομών καθώς και από μικρό ποσοστό δαπανών για ΤΠΕ, χαρακτηριστικά τα οποία καθιστούν δύσκολη την εφαρμογή της ΗΔ (Κιοσσέ, 2011).

# 2. *Μέθοδοι Ταυτοποίησης με κάρτες – κωδικούς.*

Στο πλαίσιο εργασίας εντός ενός Πληροφοριακού Συστήματος (ΠΣ) απαιτείται σχεδόν πάντα η ταυτοποίηση των ατόμων που κάνουν χρήση των πόρων ή γενικότερα αλληλεπιδρούν με αυτό μέσα από διαδικασίες. Στο κεφάλαιο αυτό δίνονται μερικά από τα είδη και τις μεθόδους ταυτοποίησης όπως η ψηφιακή ταυτότητα

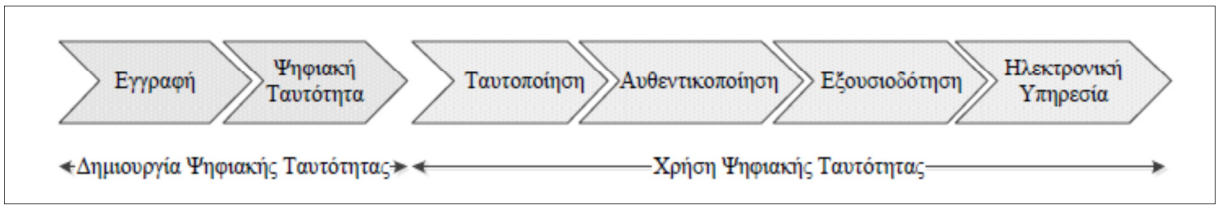
## *2.1 Ψηφιακή Ταυτότητα.*

Η ταυτότητα κάθε ατόμου απαρτίζεται από ένα πλήθος χαρακτηριστικών γνωρισμάτων ικανών να τον αναγνωρίσουν μοναδικά είτε μόνα τους, είτε σε συνδυασμό μεταξύ τους (Buell & Sandhu, 2003). Ανάλογα την περίπτωση, το πλαίσιο και το ρόλο που θέλει να αναλάβει το συγκεκριμένο άτομο, επιλέγει να χρησιμοποιήσει και να αποκαλύψει κάποιο υποσύνολο της ταυτότητάς τους, το οποίο αποτελεί μία μερική ταυτότητα (Clauß & Köhntopp, 2001). Το σύνολο των μερικών ταυτοτήτων αποτελούν την ταυτότητα του κάθε ατόμου, όπως απεικονίζονται και στο Σχήμα 4-1. Η ραγδαία ανάπτυξη και διάδοση των τεχνολογιών Διαδικτύου και των καινούργιων μηχανισμών ολοκλήρωσης των παραδοσιακών συναλλαγών ηλεκτρονικά, εισήγαγε την έννοια της ψηφιακής ταυτότητας (Corradini, et al., 2007). Υπό τη στενή έννοια του όρου, όπως αυτή γίνεται αντιληπτή από τα Π.Σ., αυτή νοείται ως "*ηλεκτρονικά αναγνωρίσιμη αντιπροσώπευση μιας ανθρώπινης ταυτότητας*" (Camp, 2004). Σκοπός της είναι να συνδέσει μία συγκεκριμένη συναλλαγή ή ένα σύνολο δεδομένων από ένα Π.Σ. με ένα αναγνωρίσιμο άτομο. Η χρήση της επιτρέπει την ταυτοποίηση και εξουσιοδότηση του συγκεκριμένου ατόμου για τη χρήση υπολογιστικών πόρων ή ηλεκτρονικών υπηρεσιών.




***Εικόνα 6. Είδη Ταυτοτήτων***

Στο πλαίσιο των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης, οι συγκεκριμένοι πόροι μπορεί να αφορούν υπηρεσίες είτε προς τους πολίτες (*G2C*) είτε προς τις επιχειρήσεις (*G2B*). Προκειμένου να δοθεί πρόσβαση σε κάποιον χρήστη για μία συγκεκριμένη ηλεκτρονική υπηρεσία, θα πρέπει να προηγηθούν αρκετά στάδια επεξεργασίας. Το πρώτο στάδιο περιλαμβάνει τη δημιουργία της ψηφιακής ταυτότητας του χρήστη που μπορεί να αποτελείται από έναν συνδυασμό ονόματος χρήστη (*Username*) και συνθηματικού (*Password*), ένα ψηφιακό πιστοποιητικό (*Digital Certificate*) ή ένα ανώνυμο διακριτικό διαπιστευτήριο (*Anonymous*). Προτού ολοκληρωθεί η διαδικασία δημιουργίας, θα πρέπει να προηγηθεί η διαδικασία της εγγραφής (*Registration*), κατά την οποία ο εκδότης της ψηφιακής ταυτότητας ελέγχει, αν αυτή εκδίδεται για το σωστό πρόσωπο, αν πληροί όλες τις προϋποθέσεις και αν δικαιούται τη συγκεκριμένη μορφή ψηφιακής ταυτότητας. Στην Εικ.7 δίνονται τα στάδια από την δημιουργία έως τη χρήση της ηλεκτρονικής υπηρεσίας (Δρογκάρης π 2013).




***Εικόνα 7: Ψηφιακή Ταυτότητα για χρήση Ηλεκτρονικής Υπηρεσίας (Δρογκάρης Π.2013)***

Τα στάδια που περιλαμβάνονται στη χρήση της ηλεκτρονικής υπηρεσίας και αφορούν τον έλεγχο πρόσβασης του χρήστη (*Access Control*), είναι τα ακόλουθα:

- ***Ταυτοποίηση (Identification)*:** Ο χρήστης ισχυρίζεται την ύπαρξη συγκεκριμένης ψηφιακής ταυτότητας, παρέχοντας π.χ. ένα όνομα χρήστη
- ***Αυθεντικοποίησή (Authentication)*:** Ο χρήστης επαληθεύει την ύπαρξη της προ-αναφερθείσας ψηφιακής ταυτότητας παρέχοντας π.χ. ένα συνθηματικό και ο συνδυασμός τους επαληθεύεται από τον πάροχο της ηλεκτρονικής υπηρεσίας
- ***Εξουσιοδότηση (Authorization):*** Ο πάροχος προσδιορίζει τα δικαιώματα του χρήστη για τη συγκεκριμένη ηλεκτρονική υπηρεσία

## *2.2 Διαχείριση Ψηφιακής Ταυτότητας.*

Οι βασικότεροι ορισμοί που αποδίδονται στον όρο Ηλεκτρονική Διαχείρισης Ταυτότητας (*electronic Identity Management*) είναι "*το σύνολο των διαδικασιών που επιτρέπουν την δημιουργία, διατήρηση και κατάργηση των πληροφοριών που ορίζουν μοναδικά κάθε χρήστη ενός συνόλου πληροφοριακών συστημάτων*" (Rosenberg, 1992) και "*το σύνολο των διαδικασιών, εργαλείων και κοινωνικών συμβολαίων που προσδιορίζουν την δημιουργία, διατήρηση και κατάργηση της ψηφιακής ταυτότητας ατόμων για την ασφαλή πρόσβαση σ' ένα διευρυμένο σύνολο συστημάτων και εφαρμογών*" (Pato, 2003). Τα κύρια σημεία των δύο αυτών ορισμών, σύμφωνα και με (Πουλούδη, et al., 2007), είναι:

- Ο προσδιορισμός των επιχειρηματικών διαδικασιών που απαιτούν ταυτοποίηση των χρηστών,
- Ο βαθμός απαίτησης για την ταυτοποίηση των χρηστών, το πόσο ισχυρή είναι η ταυτότητα που δημιουργείται από το σύστημα και αν είναι ανθεκτική σε αντι-γραφή ή κακή χρήση της,
- Η διακριτική προσπέλαση των χρηστών σε διάφορες υπηρεσίες και

- Η επιλογή εκείνων των εργαλείων που θα διαχειρίζονται αποτελεσματικά τις ταυτότητες των χρηστών και θα δημιουργούν ένα ασφαλές περιβάλλον χωρίς προβλήματα

Τα συστήματα διαχείρισης ταυτότητας απαρτίζονται από μια σειρά υπηρεσιών και επιμέρους συστημάτων, τα οποία έχουν ως στόχο μια συνολική αντιμετώπιση της έκδοσης, διαχείρισης και κατάργησης των δεδομένων που συγκροτούν την ταυτότητα των χρηστών. Τα επιμέρους στοιχεία ενός τυπικού συστήματος διαχείρισης ταυτότητας περιγράφονται από τον (Pato, 2003).


***Εικόνα 8: Κυριότερα μέρη συστημάτων ηλεκτρονικής διαχείρισης ταυτοτήτων (Pato 2003).***

Κομβικό ρόλο κάθε συστήματος διαχείρισης ταυτότητας επιτελεί το Ψηφιακό Αποθετήριο (*Data Digital Repository*), όπου αποθηκεύονται τα δεδομένα του συστήματος (*Logical data*), και το Μοντέλο δεδομένων ταυτότητας (*Identity data model*). Επιπλέον, στο τμήμα αυτό αποθηκεύονται και οι κανόνες που ορίζουν την πρόσβαση και διαχείριση της πληροφορίας. Το σύστημα διαχείρισης ταυτότητας διαρθρώνεται σε τρία επίπεδα. Κάθε ένα από αυτά τα επίπεδα αποσκοπεί στη ρύθμιση εκείνων των στοιχείων που σχετίζονται με τους κανόνες δημιουργίας και διαχείρισης των δεδομένων και την πρόσβαση στο σύστημα των κατόχων αυτών.

Τα επίπεδα αυτά, σύμφωνα με (Pato, 2003) και (Πουλούδη, et al., 2007), είναι:

- ***Βάση (Foundation)*:** πρόκειται για το επίπεδο που ρυθμίζει τους κανόνες πρόσβασης στα δεδομένα που τηρούνται στο σύστημα
- ***Κύκλος ζωής (Lifecycle)*:** εδώ ρυθμίζονται όλα εκείνα στοιχεία που αφορούν στην έκδοση ηλεκτρονικών ταυτοτήτων, καθώς και στη διαχείριση των δεδομένων που τις απαρτίζουν
- ***Πρόσβαση & χρήση (Consumable)*:** στο επίπεδο αυτό ορίζεται ο τρόπος πρόσβασης και προσπέλασης των δεδομένων στο σύστημα.

Σε κάθε ένα από αυτά τα επίπεδα, διάφορα τμήματα του συστήματος ταυτότητας αλληλοεπιδρούν, με στόχο τη συλλογή και αποτελεσματική διαχείριση των δεδομένων, που θα επιτρέψει την απρόσκοπτη χρήση των υπηρεσιών του από τον τελικό χρήστη. Η βάση ενός συστήματος διαχείρισης ταυτότητας, σύμφωνα πάλι με (Pato, 2003), αποτελείται από τα εξής μέρη:

- ***Πάροχος Αυθεντικοποίησης (Authentication Provider):*** είναι υπεύθυνος για την αρχική αυθεντικοποίησή κάθε οντότητας που θα συνδεθεί με συγκεκριμένη ψηφιακή ταυτότητα. Παράγει ένα διακριτικό αυθεντικοποίησης (*Token Authenticator*), που επιτρέπει στις υπόλοιπες συνιστώσες του συστήματος (components) να γνωρίζουν ότι η αρχική αυθεντικοποίησή έχει ολοκληρωθεί επιτυχώς. Αυτές οι τεχνικές περιλαμβάνουν μηχανισμούς, όπως επαλήθευση συνθηματικών, επαλήθευση διακριτικών έξυπνων καρτών (*Smart Cards*), σαρώσεις βιομετρικών δεδομένων κ.α. Κάθε ταυτότητα μπορεί να σχετίζεται με περισσότερους από έναν παρόχους αυθεντικοποίησης. Οι μηχανισμοί που χρησιμοποιούνται από τον κάθε πάροχο, διαφέρουν ως προς την αποτελεσματικότητα και την ασφάλειά τους. Έτσι, ανάλογα με το πλαίσιο χρήσης ενός συστήματος διαχείρισης ταυτότητας, είναι δυνατόν να απαιτούνται συγκεκριμένοι μηχανισμοί αυθεντικοποίησης.

- ***Έλεγχος Πολιτικής (Policy Control):*** Η πρόσβαση και χρήση των δεδομένων και πληροφοριών που σχετίζονται με την ηλεκτρονική ταυτότητα, διέπετέ από μια σειρά κανόνων. Οι πολιτικές εξουσιοδότησης προσδιορίζουν τον τρόπο διαχείρισης, διαχείρισης και εκχώρησης της πληροφορίας. Έλεγχοι αυτών των πολιτικών μπορεί να εγείρουν ελέγχους σε συγκεκριμένα περιστατικά (*Events*), καθώς και να ενημερώσουν το υποκείμενο της ταυτότητας για προσπέλαση των δεδομένων του.

- ***Έλεγχος (Auditing):*** Οι διαδικασίες ελέγχου αποτελούν το μηχανισμό επίβλεψής για τον τρόπο με τον οποίο η πληροφορία δημιουργείται, μεταβάλλεται και χρησιμοποιείται. Με αυτό τον τρόπο καθίσταται δυνατός ο εντοπισμός περιπτώσεων παραβίασης των πολιτικών του συστήματος.

Τα συστατικά του κύκλου ζωής ενός συστήματος διαχείρισης ταυτότητας είναι τα εξής:

- *Παροχή (Provisioning)*: Αφορά την αυτοματοποίηση όλων των διαδικασιών και των εργαλείων διαχείρισης του κύκλου ζωής μιας ταυτότητας και περιλαμβάνει τη δημιουργία ενός αναγνωριστικού (*Identifier*) για την ψηφιακή ταυτότητα, τη διασύνδεση με τους παρόχους αυθεντικοποίησης, τον προσδιορισμό και τη μεταβολή των χαρακτηριστικών αλλά και των προνομίων καθώς και την κατάργηση της ταυτότητας.

- *Διάρκεια (Longevity)*: Αφορά τη δημιουργία εγγραφών ιστορικού κάθε διακριτής ταυτότητας, καθώς και την εξέλιξη και διαφοροποίησή της με την πάροδο του χρόνου.

Το επίπεδο πρόσβασης και χρήσης του συστήματος περιλαμβάνει τα ακόλουθα στοιχεία:

- *Ενιαία πρόσβαση (Single Sign-On)*: με τον τρόπο αυτό η ταυτότητα του χρήστη πιστοποιείται μια φορά κατά την πρόσβασή του σε μια υπηρεσία του συστήματος ταυτότητας. Στη συνέχεια, μπορεί να έχει πρόσβαση σε όλες τις υπηρεσίες και τα συστήματα που έχουν διασυνδεθεί και απαρτίζουν το ευρύτερο περιβάλλον που διαχειρίζεται το σύστημα διαχείρισης ταυτότητας.
- *Εξατομίκευση (Personalization)*: τα εργαλεία αυτά επιτρέπουν, πληροφορίες που αφορούν στις εφαρμογές που χρησιμοποιεί ο χρήστης, καθώς και γενικές πληροφορίες

να διασυνδεθούν με μια συγκεκριμένη ταυτότητα. Αυτά τα εργα-λεία επιτρέπουν αφενός στον χρήστη να έχει μια εμπειρία, κατά την χρήση του συστήματος, προσαρμοσμένη στις προτιμήσεις του. Αφετέρου, επιτρέπουν στις επιχειρήσεις που διαχειρίζονται το σύστημα, να συγκεντρώνουν χρήσιμες πληροφορίες που μπορούν στη συνέχεια να χρησιμοποιήσουν για εμπορικούς σκοπούς.

- *Διαχείριση Πρόσβασης (Access Management)*: Επιτρέπει την πρόσβαση στους πόρους του συστήματος με βάση τα δικαιώματα και τους κανόνες που έχουν αποθηκευτεί στο αποθετήριο.

## *2.3 Διαχείριση Ψηφιακής Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση.*

Συνήθως τα ζητήματα θέματα που σχετίζονται με την έννοια της ταυτότητας σε ένα ηλεκτρονικό περιβάλλον, κυρίαρχα στο Διαδίκτυο (Πουλούδη, et al., 2007), (Stefanova, et al., 2010), είναι τα παρακάτω:

- αυξημένη ανάγκη ταυτοποίησης των συναλλασσόμενων
- επιθυμία των χρηστών να διατηρήσουν τις συνήθειες του «πραγματικού» κόσμου δηλαδή να διατηρούν την ανωνυμία τους στις συναλλαγές
- επικράτηση μιας κουλτούρας, όπου ο κάθε χρήστης, όχι μόνο δεν αποκαλύπτει την ταυτότητά του κατά την περιήγησή του στο Διαδίκτυο, αλλά χρησιμοποιεί ένα ή περισσότερα ψευδώνυμα
- δυνατότητα εταιρειών να συλλέξουν σημαντικές πληροφορίες για τις συνήθειες των συναλλασσόμενων.

Στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, το ζήτημα της ηλεκτρονικής διαχείρισης ταυτότητας (*electronic Identity Management - eIdM*) είναι σαφώς υψηλότερης σημασίας καθώς αποτελεί βασικό παράγοντα και προϋπόθεση για την ασφαλή και αποτελεσματική χρήση ηλεκτρονικών υπηρεσιών και εμπορικών συναλλαγών. Οι βασικές ανησυχίες των πολιτών αφορούν κυρίως στα δεδομένα που το κάθε κράτος επιλέγει να απαρτίζουν την πληροφοριακή τους ταυτότητα (*Informational Identity*).

Για παράδειγμα στο ηλεκτρονικό εμπόριο *(e-commerce)*, η ψηφιακή ταυτότητα του ατόμου διαμορφώνεται εν μέρει με τη δική του συμβολή. Στην Ηλεκτρονική Διακυβέρνηση κάτι τέτοιο δεν είναι εφικτό, αφού η Δημόσια Διοίκηση είναι αυτή που προσδιορίζει τις πληροφοριακές ανάγκες. Οι ανησυχίες που εγείρει η διαχείριση ταυτότητας στο πλαίσιο της Ηλεκτρονικής Διακυβέρνησης, σχετίζονται κυρίως με τους φορείς ταυτοποίησης και αυθεντικοποίησης, οι οποίοι συγκεντρώνουν ευαίσθητα και μοναδικά στοιχεία του ατόμου, για τα οποία, φορέας διαχείρισης ήταν το ίδιο το άτομο (Πουλούδη, et al., 2007).

Σήμερα, όλα τα Κράτη-Μέλη της ΕΕ, έχουν υιοθετήσει συστήματα διαχείρισης ηλεκτρονικών ταυτοτήτων στο πλαίσιο του εκσυγχρονισμού των ηλεκτρονικά παρεχόμενων υπηρεσιών τους (Λαζαρίδης, 2011). Η εφαρμογή και διαχείριση ηλεκτρονικών ταυτοτήτων συνεχίζει όμως να αποτελεί πρόκληση, δεδομένου ότι περιλαμβάνει εκ των πραγμάτων τη διαχείριση προσωπικών δεδομένων και επομένως ενέχει κινδύνους παραβίασης της ιδιωτικότητας (του προσωπικού απορρήτου) από τη μη εξουσιοδοτημένη πρόσβαση, συλλογή και επεξεργασία προσωπικών ή και ευαίσθητων δεδομένων. Είναι λοιπόν πολύ σημαντικό κάθε λύση ηλεκτρονικής ταυτοποίησης να λαμβάνει πολύ σοβαρά υπόψη θέματα ιδιωτικότητας και να διασφαλίζει την ασφάλεια και προστασία των προσωπικών δεδομένων (Κουντζέρης, 2011). Σύμφωνα και με το Άρθρο 8 του Ευρωπαϊκού Συμφώνου Ανθρωπίνων Δικαιωμάτων (*European Convention on Human Rights*), τα παραπάνω αποτελούν βασικό ανθρώπινο δικαίωμα και η Ευρωπαϊκή Οδηγία 95/46/ΕΚ προβλέπει συγκεκριμένους

περιορισμούς για τη διαχείριση προσωπικών δεδομένων. Καθοριστικός παράγοντας, προς αυτή την κατεύθυνση, αποτελεί η σχετική ελευθερία των χωρών να προσδιορίσουν τις ειδικές συνθήκες κάτω από τις οποίες η διαχείριση προσωπικών δεδομένων είναι αποδεκτή και νόμιμη, τις εγγυήσεις που παρέχονται για την προστασία της ιδιωτικότητας, και τις συνθήκες κάτω από τις οποίες είναι επιτρεπτή η πρόσβαση σε προσωπικά δεδομένα. Όλα αυτά τα θέματα συνήθως ρυθμίζονται μέσω του νομικού και κανονιστικού πλαισίου (Κουντζέρης, 2010).

## *2.4 Μέθοδοι Ταυτοποίησης - Αναγνωριστικά.*

Οι προσεγγίσεις ταυτοποίησης οντοτήτων σε περιβάλλοντα ΗΔ συνήθως διαχωρίζονται σε δύο βασικές κατηγορίες με βάση την αξιοποίηση ενός καθολικού μοναδικού αναγνωριστικού για όλες τις υπηρεσίες, ή εναλλακτικά, διαφορετικών μοναδικών αναγνωριστικών (πολλαπλά αναγνωριστικά ή τομεακά αναγνωριστικά) ανά υπηρεσία ή φορέα παροχής υπηρεσιών (Κουντζέρης, 2010). Είναι προφανές ότι η χρήση ενός καθολικού μοναδικού αναγνωριστικού γενικής χρήσης (*National ID Number*) για όλες τις ηλεκτρονικές υπηρεσίες διευκολύνει τη διαχείριση της ταυτοποίησης και αυθεντικοποίησης στις υπηρεσίες αυτές. Σε αρκετές περιπτώσεις, όμως, τίθενται περιορισμοί από το εκάστοτε εθνικό νομικό και κανονιστικό πλαίσιο, κυρίως σε ζητήματα διασύνδεσης μεταξύ όλων των προσωπικών δεδομένων ενός πολίτη, εγείροντας σημαντικούς περιορισμούς και προβλήματα αναφορικά με την προστασία της ιδιωτικότητας του (Μήτρου, 2010).

Για παράδειγμα σήμερα οι υπηρεσίες της ΑΑΔΕ πέρα από τη φορολογική ενημερότητα των πολιτών δίνουν τη δυνατότητα στους πολίτες με χρήση ενός και μόνο συνθηματικού να εισέρχονται σε πλατφόρμες σχετικές με τη μισθοδοσία (Ενιαία Αρχή Πληρωμών), ασφαλιστικά ταμεία (ΗΔΙΚΑ), ενημερώσεις συντάξεων κλπ.

### *2.4.1. Αυθεντικοποίησή Ψηφιακών Ταυτοτήτων.*

Με τον όρο «αυθεντικοποίησή» νοείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της. Σε καμία περίπτωση δε θα πρέπει η αυθεντικοποίησή ενός χρήστη να συγχέεται με την παροχή εξουσιοδότησης (*Authorization*) στους πόρους του Π.Σ.

Οι μηχανισμοί αυθεντικοποίησης συνιστώνται από συστήματα που είναι δυνατό να κατηγοριοποιηθούν με βάση τη μέθοδο, η οποία αξιοποιείται για την πιστοποίηση της ταυτότητας ενός χρήστη. Οι μέθοδοι αυτοί διαχωρίζονται (Burr, et al., 2011) με βάση τα εξής χαρακτηριστικά:

- Κάτι που γνωρίζει (*Something Known*) ο χρήστης, για παράδειγμα ένα συνθηματικό
- Κάτι που κατέχει (*Something Possessed*) ο χρήστης, για παράδειγμα μία έξυπνη κάρτα (*Smart Card*)
- Κάποιο χαρακτηριστικό γνώρισμα (*Something Inherent*), για παράδειγμα βιομετρικές μέθοδοι
- Συνδυασμός κάποιων εκ των ανωτέρω χαρακτηριστικών γνωρισμάτων

Οι μηχανισμοί αυθεντικοποίησης, ανεξάρτητα από τα χαρακτηριστικά που υιοθετούν, αξιοποιούν δύο τύπους κλειδιών:

- Μυστικά κλειδιά: Σε αυτά συμπεριλαμβάνονται τα συνθηματικά, οι κωδικοί και τα συμμετρικά κλειδιά.
- Ασύμμετρα κλειδιά: Σε αυτά συμπεριλαμβάνονται ζεύγη κλειδιών, από τα οποία το ένα είναι δημόσια γνωστό - δημόσιο κλειδί, ενώ το άλλο παραμένει μυστικό - ιδιωτικό κλειδί. Για παράδειγμα ασύμμετρα κλειδιά χρησιμοποιούνται από τις τράπεζες στις οποίες οι ηλεκτρονικές συναλλαγές γίνονται σε δύο βήματα. Πρώτα ο χρήστης δίνει την ταυτότητά του (User ID) που είναι φανερή και στη συνέχεια δίνει το συνθηματικό του (password) καλυμμένα.

Τα συστήματα αυθεντικοποίησης μπορούν να χαρακτηριστούν ως μονοδιάστατα ή πολυδιάστατα, ανάλογα με τα διαφορετικά χαρακτηριστικά που αξιοποιούν, ώστε να εξασφαλίσουν το επιθυμητό επίπεδο βεβαιότητας για την ταυτότητα κάποιας ηλεκτρονικής οντότητας. Για παράδειγμα, η χρήση ενός ιδιωτικού κλειδιού ως διακριτικού αυθεντικοποίησης, που προστατεύεται από το συνθηματικό του χρήστη, αντιπροσωπεύει ένα χαρακτηριστικό παράδειγμα δισδιάστατου συστήματος αυθεντικοποίησης.

### *2.4.2 Διακριτικά Αυθεντικοποίησης.*

Τα διακριτικά αυθεντικοποίησης αξιοποιούνται για τον έλεγχο της ορθότητας της ψηφιακής ταυτότητας των χρηστών ενός Π.Σ.. Ανάλογα με το επιθυμητό επίπεδο ασφάλειας υιοθετείται και ο αντίστοιχος συνδυασμός χαρακτηριστικών και κλειδιών αυθεντικοποίησης (Ferguson & Schneier, 2003).,

- Τα συνθηματικά (*Passwords*) αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του, κάνοντας χρήση ενός μυστικού που είναι γνωστό μόνο σε αυτόν. Ο χρήστης πρέπει να απομνημονεύσει το μυστικό κωδικό και να μην τον αποκαλύπτει σε τρίτες οντότητες.

  - Τα διακριτικά συνθηματικών μιας χρήσης (*One-time Password Tokens*) είναι συσκευές υλικού οι οποίες αξιοποιούνται για τη δημιουργία συνθηματικών, τα οποία δεν απαιτείται να απομνημονεύει ο χρήστης και τα οποία χρησιμοποιούνται μόνο μια φορά. Η παραγωγή των συνθηματικών στηρίζεται σε συγκεκριμένους αλγόριθμους κρυπτογράφησης. Η επαναχρησιμοποίηση ενός κωδικού για μελλοντική αυθεντικοποίησή του χρήστη δεν είναι δυνατή.

- Τα διακριτικά χαλαρής αποθήκευσης (*Soft Tokens*) αναφέρονται σε μυστικά κλειδιά, τα οποία αποθηκεύονται σε κάποιο μέσο αποθήκευσης όπως σκληρός δίσκος, CD, USB token κ.λπ. Τα κλειδιά είναι αποθηκευμένα σε κρυπτογραφημένη μορφή, ενώ η προσπέλασή τους είναι δυνατή μόνο με τη χρήση του κατάλληλου συνθηματικού.

- Τα διακριτικά υλικού σκληρής αποθήκευσης (*Hard Tokens*) αναφέρονται σε συσκευές υλικού, οι οποίες αποθηκεύουν τα απαιτούμενα μυστικά κλειδιά και προσφέρουν απαραβίαστη (*Tamper Proof*) προστασία. Όλες οι κρυπτογραφικές διαδικασίες πραγματοποιούνται εσωτερικά στη συσκευή και συνεπώς δεν υπάρχει καμία δυνατότητα ανάγνωσης των κλειδιών από εξωτερικές οντότητες. Για την ενεργοποίηση των κλειδιών συνηθίζεται η χρήση κάποιου συνθηματικού.

## *2.5 Ομόσπονδες Ταυτότητες*

Ως Ομοσπονδία (*Federation*) ορίζεται "*το σύνολο δύο ή περισσοτέρων επιχειρηματικών συνεργατών που έχουν κοινούς χρήστες και στοχεύουν στην αναβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών ταυτόχρονα με τη μείωση του κόστους διαχείρισης των ψηφιακών ταυτοτήτων τους*" (Buecker, et al., 2008). Ως αποτέλεσμα δημιουργίας της ομοσπονδίας, οι συμμετέχοντες μπορούν να αναπτύξουν και να αξιοποιήσουν εφαρμογές βασισμένες στην ψηφιακή ταυτότητα των χρηστών τους (*Identity-Based Applications*), διευκολύνοντας και απλοποιώντας την πρόσβαση σε υπηρεσίες και πληροφορίες χωρίς την ανάγκη για δημιουργία ή εκ νέου αντιστοίχιση των ψηφιακών ταυτοτήτων μέσα στην ομοσπονδία (Baldoni, 2012). Η εγκαθίδρυση μίας ομοσπονδίας βασίζεται στην εγκαθίδρυση αμοιβαίων σχέσεων εμπιστοσύνης. Οι σχέσεις αυτές δημιουργούνται χρησιμοποιώντας νομικές συμφωνίες (*Agreement s*) μεταξύ των συμμετεχόντων, και είναι απαραίτητο να ισχύσουν πριν την έναρξη λειτουργίας της. Τέτοιες συμφωνίες συνήθως περιλαμβάνουν και τις τεχνολογίες – μεθοδολογίες, που θα υποστηρίζουν την ομοσπονδία, και περιλαμβάνουν κατ' ελάχιστον τις δυνατότητες διαχείρισης της ομοσπονδίας και της μεταξύ τους εμπιστοσύνης, την κρυπτογραφική υποστήριξη, καθώς και τα πρωτόκολλα και τις επιχειρηματικές διαδικασίες βάσει των οποίων πραγματοποιείται μία συναλλαγή.

Στην τεχνολογία πληροφορίας (*IT*), η ομόσπονδη ταυτότητα (*Federated Identity*) έχει δύο βασικές έννοιες (Buecker, et al., 2008):

- Τη διαδικασία αυθεντικοποίησης ενός χρήστη, διαμέσου διαφορετικών Π.Σ. ή οργανισμών.
- Την εικονική ένωση (*Assembled Identity*) των πληροφοριών ενός χρήστη (ή μιας αρχής), που είναι αποθηκευμένες σε πολλαπλά διακριτά συστήματα διαχείρισης ταυτότητας. Τα δεδομένα συνενώνονται μεταξύ τους χρησιμοποιώντας ένα κοινό στοιχείο, συνήθως το όνομα του χρήστη.

### *2.5.1 Διαχείριση Ομόσπονδης Ταυτότητας*

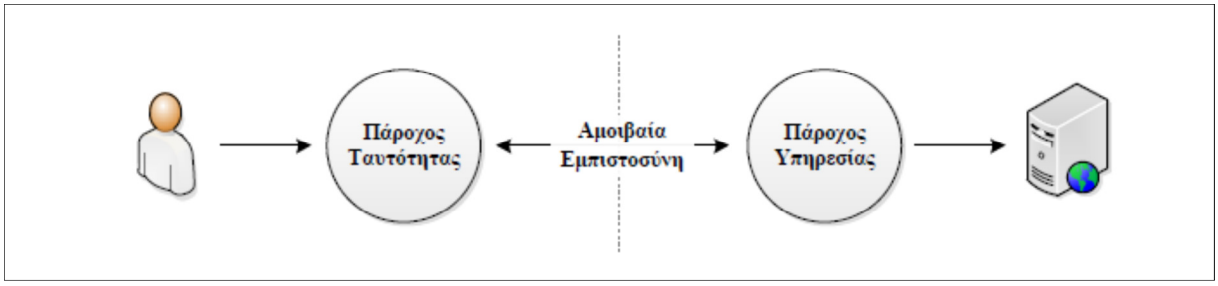
Μία βασική απαίτηση για την εγκαθίδρυση και ομαλή λειτουργία μίας ομοσπονδίας είναι η αποτελεσματική και συνεπής διαχείριση των ψηφιακών ταυτοτήτων. Η συγκεκριμένη διαδικασία - *Federated Identity Management* (Pfitzmann & Waidner, 2003, Baldwin, et al., 2008) εστιάζει στον προσδιορισμό :

- των διαδικασιών και υπηρεσιών που απαιτούν ταυτοποίηση των χρηστών,
- του βαθμού βεβαιότητας για την πραγματική ταυτότητα του χρήστη,
- της διακριτικής προσπέλασης των χρηστών από τις παρεχόμενες υπηρεσίες και
- των εργαλείων που θα διαχειρίζονται τις ψηφιακές ταυτότητες των χρηστών.

Σύμφωνα με τους (Jøsang & Pope, 2005), η διαχείριση ομόσπονδων ταυτοτήτων ορίζεται ως "*ένα σύνολο συμφωνιών, προτύπων και τεχνολογιών που επιτρέπουν σε μια ομάδα παροχών ηλεκτρονικών υπηρεσιών να αναγνωρίσουν τα αναγνωριστικά χρήστη και δικαιώματα από άλλους παρόχους υπηρεσιών που συμμετέχουν στην ομοσπονδία*". Οι σημαντικότεροι ρόλοι (*Roles*) σε μια ομοσπονδία είναι ο πάροχος ταυτότητας (*Identity Provider*) και ο πάροχος υπηρεσίας (*Service Provider*) (Buecker, et al., 2008).

Ο πάροχος ταυτότητας είναι υπεύθυνος για τη διαχείριση των χρηστών και των ταυτοτήτων τους, για την έκδοση πιστοποιητικών, την αυθεντικοποίησή τους, και εγγυάται για την ταυτότητα των χρηστών. Ο πάροχος υπηρεσιών είναι υπεύθυνος για τον έλεγχο πρόσβασης σε υπηρεσίες, επικυρώνει τις πληροφορίες των ταυτοτήτων για τον πάροχο

ταυτότητας, παρέχει πρόσβαση βασιζόμενος στις ταυτότητες και διαχειρίζεται μόνο τοπικά χαρακτηριστικά των χρηστών και όχι ολόκληρο το προφίλ τους. Η αμοιβαία εμπιστοσύνη μεταξύ των δύο παροχών που δημιουργείται σε μία ομοσπονδία παρουσιάζεται στην Εικ.9.




***Εικόνα 9: Λειτουργία ομοσπονδίας με πάροχο ταυτότητας και πάροχο υπηρεσιών (Buecker et al. 2008)***

## *2.6 Έξυπνες Κάρτες.*

Πριν περίπου μια δεκαετία η τεχνολογία υπέδειξε τη χρήση των λεγόμενων έξυπνων καρτών ως κυρίαρχη για τα συστήματα ελέγχου πρόσβασης. Τα εξελιγμένα χαρακτηριστικά τους, όπως ο αυξημένος βαθμός ασφάλειας, η ευχρηστία και η λειτουργικότητά τους, αποτέλεσαν το βασικό λόγο για τη διαφαινόμενη επικράτησή τους, ανάμεσα σε άλλες τεχνολογίες.

Ωστόσο οι κατασκευαστές έξυπνων καρτών, στην προσπάθειά τους να προσφέρουν ακόμα μεγαλύτερη λειτουργικότητα, παραμελούν μερικές φορές την ασφάλεια. Συγκεκριμένα, επιλέγουν να κατασκευάζουν συσκευές ανάγνωσης καρτών (readers), που παρακάμπτουν τους ενσωματωμένους στην κάρτα μηχανισμούς ασφαλείας και αντί αυτών να διαβάζουν μόνο το σειριακό αριθμό της κάρτας (Card's Serial Number), γνωστότερο και ως CSN. Όμως, πρέπει να γίνει κατανοητό ότι η χρήση μόνο του CSN δεν εξασφαλίζει προστασία και ακυρώνει τους μηχανισμούς ασφάλειας.

Πολλές φορές η πρακτική αυτή παρομοιάζεται με την εγκατάσταση μιας ακριβής πόρτας ασφαλείας, χωρίς όμως ανάλογο μηχανισμό κλειδώματος. Η λαθεμένη χρήση των καρτών ασφαλείας, πρέπει να επισημανθεί σε όλους τους εμπλεκόμενους στην κατασκευή και χρήση συστημάτων ελέγχου πρόσβασης, ώστε να μπορέσουν να αντιμετωπίσουν το πρόβλημα και τελικά να επιτύχουν το στόχο τους, που δεν πρέπει να είναι άλλος από τη μεγιστοποίηση της ασφάλειας. Γιατί, ομολογουμένως, εάν χρησιμοποιηθούν σωστά οι έξυπνες κάρτες, αποτελούν μία από τις εξελιγμένες και αποτελεσματικές τεχνολογίες ταυτοποίησης των εισερχόμενων προσώπων σε ένα συγκεκριμένο χώρο.

### *2.6.1 Πλεονεκτήματα των έξυπνων καρτών.*

Ο τρόπος κατασκευής των σύγχρονων έξυπνων καρτών, ενσωματώνει τις πλέον προηγμένες τεχνολογίες ασφάλειας. Πριν την επίτευξη διασύνδεσης μεταξύ μιας κάρτας και μιας συσκευής ανάγνωσης, λαμβάνει χώρα μία διαδικασία αμοιβαίας αναγνώρισης, ώστε να εξασφαλιστεί ότι και οι δύο συσκευές είναι ασφαλείς, τηρούν όλα τα εχέγγυα γνησιότητας και δεν είναι προϊόντα παραποίησης. Μετά το πέρας αυτής της διαδικασίας και αφού

διασφαλιστεί ότι η κάρτα δεν είναι προϊόν παραποίησης, τότε μόνο επιτρέπεται η επικοινωνία μεταξύ των συσκευών και ο αναγνώστης μπορεί να έχει πρόσβαση στα στοιχεία που είναι αποθηκευμένα στην κάρτα. Συνήθως, τα δεδομένα αυτά προστατεύονται από διάφορους κρυπτογραφικούς αλγόριθμους και «κλειδιά», έτσι ώστε, ακόμα και αν κάποιος πετύχει με κάποιο τρόπο να εξάγει από την κάρτα τα αποθηκευμένα δεδομένα, να είναι δύσκολο να τα αποκρυπτογραφήσει και τελικά να τα χρησιμοποιήσει.

Όπως και με τις Proximity κάρτες, οι έξυπνες κάρτες δεν είναι απαραίτητο να τοποθετηθούν μέσα σε μηχανισμό ανάγνωσης. Το μόνο που χρειάζεται, είναι ο χρήστης να πλησιάσει την κάρτα του κοντά σε ένα μηχανισμό ανάγνωσης- χωρίς να είναι απαραίτητη ούτε καν η οπτική επαφή. Αυτό σημαίνει πρακτικά, ότι δεν χρειάζεται να τη βγάλει από την τσέπη του ή από το πορτοφόλι του (οπότε μειώνεται ο χρόνος για την ταυτοποίηση του προσώπου) και επιπρόσθετα μειώνεται η φθορά των συγκεκριμένων καρτών σε σχέση με τις κάρτες επαφής. Σημαντικό χαρακτηριστικό των έξυπνων καρτών που ενισχύει την ευχρηστία τους, είναι η δυνατότητά τους να υποστηρίζουν πολλαπλές εφαρμογές. Παραδείγματος χάρη, μία κάρτα μπορεί να χρησιμοποιηθεί για το άνοιγμα μιας θύρας αλλά και την ενεργοποίηση ενός υπολογιστή.

Άλλο ένα τεχνικό χαρακτηριστικό που ενισχύει τη λειτουργικότητα των έξυπνων καρτών είναι η αυξημένη ποσότητα μνήμης που διαθέτουν, επιτρέποντας τη συνεργασία τους με απαιτητικότερες εφαρμογές, όπως βιομετρικά συστήματα πρόσβασης. Αυτές οι αυξημένες δυνατότητες των έξυπνων καρτών, ελαχιστοποιούν την πιθανότητα να χρησιμοποιεί την κάρτα κάποιος, ο οποίος δεν έχει την ανάλογη εξουσιοδότηση, όταν βέβαια χρησιμοποιούνται σωστά.

### *2.6.2 Επίπεδα Ασφαλείας των έξυπνων καρτών.*

Σήμερα, στην αγορά συστημάτων ασφαλείας έχουν επικρατήσει ορισμένες τεχνολογίες καρτών πρόσβασης, οι οποίες προσφέρουν διαφορετικά επίπεδα ασφάλειας. Για παράδειγμα οι κάρτες μαγνητικής ταινίας διαθέτουν το χαμηλότερο επίπεδο ασφάλειας, ενώ ακολουθούν με την εξής σειρά: οι έξυπνες κάρτες που χρησιμοποιούν το CSN (Card's Serial Number), οι proximity κάρτες και τέλος, οι πιο ασφαλείς, είναι οι έξυπνες κάρτες που χρησιμοποιούν κρυπτογραφικούς αλγορίθμους για ταυτοποίηση. Σημαντικό στοιχείο για την παραπάνω κατάταξη των καρτών, αποτελεί ο αριθμός των δεδομένων που απαιτείται για την παράνομη αντιγραφή ή ανάγνωση μιας κάρτας. Φυσικό είναι, όσο μεγαλύτερος είναι ο αριθμός τόσο δυσκολότερη να είναι η αντιγραφή της κάρτας και άρα να προσφέρει μεγαλύτερα επίπεδα ασφάλειας.

Αναλυτικότερα, οι κάρτες μαγνητικών ταινιών διαθέτουν το χαμηλότερο επίπεδο ασφάλειας, επειδή η κατασκευή τους βασίζεται σε συγκεκριμένα ISO πρότυπα, τα οποία είναι καταγεγραμμένα και άρα προσβάσιμα, ενώ επιπλέον χρησιμοποιούν ελάχιστες δικλείδες ασφαλείας. Άλλος ένας κίνδυνος είναι ότι κυκλοφορούν ειδικές συσκευές, που μπορούν με επιτυχία να αντιγράψουν και να αναπαράγουν τις κάρτες αυτής της κατηγορίας.

Όμως και οι έξυπνες κάρτες που χρησιμοποιούν το CSN, διαθέτουν χαμηλό επίπεδο ασφάλειας, καθώς και εδώ υπάρχει πλήρης κωδικοποίηση μέσω των ISO προτύπων. Επίσης, υπάρχει και εδώ το πρόβλημα της εύκολης εύρεσης συσκευών αντιγραφής αυτών των καρτών. Αντιθέτως, οι Proximity κάρτες παίρνουν υψηλό βαθμό σε ό,τι αφορά στο επίπεδο ασφαλείας που προσφέρουν και ο κύριος λόγος είναι ότι οι τεχνικές πληροφορίες για τη συγκεκριμένη τεχνολογία δεν έχουν κωδικοποιηθεί σε μεγάλο βαθμό και ούτε αποτελούν αντικείμενο κάποιων ISO προδιαγραφών. Κάθε κατασκευαστής χρησιμοποιεί δική του μέθοδο για την προστασία των δεδομένων, στοιχείο που δυσχεραίνει σημαντικά το έργο των επίδοξων αντιγραφέων.

Εντούτοις, στην κορυφή της βαθμολογίας σχετικά με την ασφάλεια που προσφέρουν, βρίσκονται οι έξυπνες κάρτες, όταν όμως είναι κατάλληλα εφοδιασμένες με τους ειδικούς κρυπτογραφικούς μηχανισμούς και με τα μυστικά κλειδιά και όταν αυτοί οι μηχανισμοί χρησιμοποιούνται και δεν παρακάμπτονται.

Τίθεται το ερώτημα για την ουσιαστική ασφάλεια που παρέχει η χρήση του σειριακού αριθμού (CSN) των έξυπνων καρτών. Η απάντηση στο παραπάνω ερώτημα προϋποθέτει καταρχήν την κατανόηση των μηχανισμών με τους οποίους λειτουργούν οι έξυπνες κάρτες, εστιάζοντας σε δύο ειδικούς όρους: CSN και anti-collision.

Ο αριθμός CSN είναι ο σειριακός αριθμός μιας συγκεκριμένης κάρτας. Σε κάθε κάρτα αντιστοιχεί ένας μόνο σειριακός αριθμός, μήκους 32 έως 64 bits, σύμφωνα με τις προδιαγραφές 14443 και 15693 του ISO. Τον αριθμό αυτό (CSN) μπορεί να βρει κανείς και με άλλες ονομασίες, όπως UID ( Unique ID), PUPI (Pseudo Unique Proxcard Identifier), CUID ( Card Unique ID). Είναι σημαντικό να σημειωθεί ότι ο CSN, σύμφωνα πάντα με τις προδιαγραφές ISO, μπορεί να αναγνωστεί χωρίς να χρειάζεται οποιαδήποτε ασφάλεια ή ταυτοποίηση. Μια πιο εκλαϊκευμένη προσέγγιση, είναι η παρομοίωση του CSN με έναν αριθμό σπιτιού. Είναι σημαντικό για τον οποιοδήποτε να είναι σε θέση να διαβάσει το συγκεκριμένο αριθμό, ώστε να μπορεί εύκολα και γρήγορα να εντοπίσει το σπίτι. Ομοίως, το CSN χρησιμοποιείται για να προσδιορίσει μεμονωμένα μία κάρτα, όταν εκτίθενται περισσότερες από μία κάρτες σε έναν αναγνώστη, συγχρόνως. Επιπροσθέτως, κανένας δεν μπορεί να μπει στο σπίτι ή αντίστοιχα να «διαβάσει» μια έξυπνη κάρτα, χωρίς τη χρήση του σωστού κλειδιού.

Η διεργασία anti-collision χρησιμοποιείται από τις έξυπνες κάρτες, ώστε να είναι εφικτή η ταυτοποίηση μιας συγκεκριμένης κάρτας, όταν παρουσιάζονται στον αναγνώστη ταυτόχρονα περισσότερες από μία κάρτες Είναι ιδιαίτερα χρήσιμη στους αναγνώστες μεγάλης εμβέλειας. Τα πρότυπα ISO απαιτούν κάθε κάρτα να έχει ένα μοναδικό CSN και παράλληλα περιγράφουν διάφορες μεθόδους για την υλοποίηση του anti-collision. Εδώ όμως είναι το σημαντικό σημείο που αξίζει να τονιστεί, καθώς σύμφωνα με τα πρότυπα ISO, η χρήση του CSN απαιτείται μόνο για την εφαρμογή του στη διαδικασία του anti-collision και για κανέναν άλλο σκοπό (ταυτοποίηση στοιχείων).

Οι αναγνώστες CSN είναι συσκευές που χρησιμοποιούν το CSN μιας έξυπνης κάρτας, αντί των στοιχείων ταυτοποίησης που είναι αποθηκευμένα στην ασφαλή περιοχή της κάρτας. Όταν μία κάρτα εκτεθεί στον αναγνώστη, αυτός διαβάζει το CSN και το μετατρέπει σε ένα κατάλληλα κωδικοποιημένο format ώστε στη συνέχεια η πληροφορία να μεταβιβάζεται σε μία συσκευή, που μπορεί να είναι ένα απλό πάνελ ή ένας κεντρικός υπολογιστής. Οι περισσότεροι αναγνώστες που χρησιμοποιούνται για τις εφαρμογές ελέγχου πρόσβασης διαβιβάζουν τα στοιχεία τους, χρησιμοποιώντας το πρωτόκολλο Wiegand. Ο συνηθέστερα χρησιμοποιούμενος τύπος αποτελείται από στοιχεία των 26 bits και περιλαμβάνει ένα πεδίο κωδικού χώρου (8-bits) και ένα πεδίο για τον αριθμό της κάρτας (16-bits) και δύο bits ισοτιμίας (parity) που χρησιμοποιούνται για τον έλεγχο λαθών.

Το πεδίο κωδικού χώρου (συχνά αναφέρεται και ως κωδικός εγκατάστασης), είναι συνήθως το ίδιο για όλες τις κάρτες επί ενός δεδομένου χώρου και χρησιμοποιείται για να εξασφαλίσει ότι κάρτες από διαφορετικές εγκαταστάσεις, που βρίσκονται στην ίδια γεωγραφική περιοχή, μπορούν να διακριθούν μεταξύ τους. Χωρίς αυτό το πεδίο, οι κάτοχοι κάρτας με τον ίδιο αριθμό μπορεί να είχαν πρόσβαση σε εγκαταστάσεις, για τις οποίες κανονικά δεν είχαν άδεια εισόδου. Το πεδίο για τον αριθμό της κάρτας προσδιορίζει μεμονωμένα κάθε κάτοχο κάρτας. Στην περίπτωση που χρησιμοποιείται το πρωτόκολλο Wiegand των 26 bits, το δεκαεξάμπιτο πεδίο του αριθμού της κάρτας εξάγεται από το CSN και το πεδίο κωδικού χώρου δημιουργείται συνήθως από έναν προγραμματισμένο εκ των πρότερων αριθμό, που αποθηκεύεται στον αναγνώστη.

Καθώς οι κατασκευαστές καρτών προγραμματίζουν εκ των πρότερων το CSN, η χρήση μόνο ενός μικρού τμήματος του CSN αυξάνει την πιθανότητα ότι θα υπάρξουν διπλοί αριθμοί καρτών. Στατιστικά, από κάθε 65.535 κάρτες, θα υπάρξει τουλάχιστον ένα αντίγραφο. Γι' αυτό το λόγο, είναι προτιμότερο να χρησιμοποιείται ένα format με μεγαλύτερο πεδίο για τον αριθμό της κάρτας. Τέτοιο format είναι το HID Corporate 1000, που εκτός του μεγαλύτερου πεδίου για τον αριθμό της κάρτας, χρησιμοποιεί και ένα επιπρόσθετο OEM πεδίο, μαζί με το πεδίο του κωδικού χώρου. Και πάντα πρέπει να λαμβάνουμε υπόψη ότι το θέμα της ύπαρξης διπλών αριθμών καρτών δεν περιορίζεται μόνο στο πρωτόκολλο Wiegand, αλλά εμφανίζεται σε οποιοδήποτε πρωτόκολλο χρησιμοποιεί ένα μειωμένο αριθμό bits από το CSN.

Στην προσπάθεια για τη δημιουργία ενός χαμηλού κόστους αναγνώστη και ικανού να διαβάσει κάρτες προερχόμενες από οποιονδήποτε κατασκευαστή, υιοθετείται η λύση της ανάγνωσης του CSN. Η προσθήκη του chip που περιέχει τους αλγόριθμους ασφαλείας, επιφέρει μεγαλύτερο κόστος παραγωγής, ενώ επίσης μπορεί να απαιτείται και η καταβολή αμοιβής για τη χρήση των δικαιωμάτων των συγκεκριμένων αλγόριθμων. Επιπροσθέτως, μπορεί και τα κλειδιά ασφαλείας για ορισμένες έξυπνες κάρτες, να μην είναι διαθέσιμα. Χρησιμοποιώντας όμως μια χαμηλού κόστους συσκευή ανάγνωσης – και ικανής να λειτουργήσει με όλες τις κάρτες που κυκλοφορούν – αναιρούνται όλα εκείνα τα τεχνικά χαρακτηριστικά ασφάλειας, που διασφαλίζουν την ασφάλεια των εγκαταστάσεων και των χώρων. Όπως προαναφέρθηκε, οι τρεις σημαντικότεροι λόγοι για τη χρήση των έξυπνων καρτών είναι η ασφάλεια, η ευχρηστία και η λειτουργικότητα.

## *2.7 Προβλήματα κατά τη χρήση του CSN.*

Το CSN αποτελείται από μια αλληλουχία μη διαδοχικών αριθμών, τοποθετημένων σε τυχαία σειρά. Επομένως, χρησιμοποιώντας για την ταυτοποίηση ενός κατόχου μιας κάρτας, το CSN, δεν μπορούμε παραδείγματος χάρη, να ομαδοποιήσουμε τους υπαλλήλους που αντιστοιχούν στους αριθμούς καρτών από 1 έως 100. Επίσης, εάν χρησιμοποιούνται – όπως πρέπει – όλα τα διαθέσιμα bits για την απεικόνιση του CSN, ένας αριθμός 32 bits θα χρειαζόταν να απεικονισθεί τουλάχιστον με 10 ψηφία, ενώ ένας αριθμός CSN 64 bits θα απαιτούσε τη χρησιμοποίηση τουλάχιστον 20 ψηφίων. Ακόμη και εάν χρησιμοποιούσαμε το δεκαεξαδικό σύστημα για την απεικόνιση του CSN , θα χρειαζόταν η εισαγωγή 16 ψηφίων για την προσθήκη μιας νέας κάρτας ή την αλλαγή μιας υφιστάμενης. Με τη χρήση μιας συσκευής ανάγνωσης, η διαδικασία εισαγωγής μιας κάρτας σε ένα σύστημα μπορεί θεωρητικά να απλοποιηθεί, καθώς πλέον, το CSN διαβάζεται αντί να εισάγεται.

Όμως, πλέον αυξάνεται ο βαθμός πολυπλοκότητας του συστήματος, καθώς απαιτείται αύξηση της ισχύος τόσο σε επίπεδο Software όσο και σε επίπεδο hardware. Επιπλέον, στην περίπτωση που πρέπει να αλλάξουν τα δικαιώματα πρόσβασης ενός κατόχου κάρτας, τότε η συσκευή ανάγνωσης δεν μπορεί να βοηθήσει, εάν η κάρτα δεν είναι διαθέσιμη. Καθώς η ανάγνωση μόνο του CSN μιας έξυπνης κάρτας απαιτεί λιγότερη ισχύ, έχουμε ως αποτέλεσμα να μη χρειάζεται να έρθουν κοντά η κάρτα με τη συσκευή ανάγνωσης. Και αυτό συμβαίνει, γιατί τα πιο απαιτητικά σε ισχύ κυκλώματα των κρυπτογραφικών αλγορίθμων δεν χρησιμοποιούνται. Οπότε, οι μεγαλύτερες αποστάσεις, σε συνδυασμό με την έλλειψη μηχανισμών ταυτοποίησης ή ασφάλειας, καθιστούν τις κάρτες λιγότερο ασφαλείς και τα στοιχεία που είναι αποθηκευμένα, περισσότερο ευάλωτα. Πολλοί είναι λοιπόν εκείνοι που παραπλανούνται και θεωρούν ότι η απόδοση των συσκευών ανάγνωσης CSN είναι μεγαλύτερη από την πραγματική. Συμπέρασμα λανθασμένο, που μπορεί να παραπλανήσει διπλά τους χρήστες, καθώς θεωρούν ότι κερδίζουν διπλά από τους απλούς αναγνώστες CSN, αφού έχουν υψηλότερη απόδοση, ενώ και το κόστος τους είναι χαμηλότερο.

Σύμφωνα με μια έκθεση της κυβέρνησης των Η.Π.Α., συνιστάται η αποφυγή της χρήσης του σειριακού αριθμού ως μέσου ταυτοποίησης. Επίσης και ο Διεθνής Οργανισμός Πολιτικής Αεροπορίας προειδοποιεί ότι «η χρήση του CSN δεν παρέχει προστασία, επειδή αυτό εισάγεται στο λογισμικό του τσιπ από τους κατασκευαστές και μπορεί με εξωτερική επέμβαση να αλλάξει.» Στο ίδιο συμπέρασμα καταλήγουν και πολλοί ειδικοί της βιομηχανίας των συστημάτων ασφαλείας, τονίζοντας τους κινδύνους σε θέματα ασφαλείας, που εγκυμονεί η χρήση του σειριακού αριθμού.

Σύμφωνα με το David Engberg της Corestreet LTD «ο σειριακός αριθμός δεν παρέχει καμία προστασία είτε με τη μορφή κρυπτογραφικού κώδικα είτε σε επίπεδο πρωτοκόλλου, ώστε να αποτρέψει κάποια προσπάθεια αντιγραφής της κάρτας". Συμφωνεί και ο Bruno Charrat της Inside Contacless, ενώ και ο Klaus Finkenzeller της Giesecke & Devrient GmbH's επαυξάνει, αναφέροντας ότι όλες οι έξυπνες κάρτες έχουν ενσωματωμένους προγραμματιζόμενους μικροεπεξεργαστές με λειτουργικό σύστημα και άρα μπορεί να γίνει επέμβαση και να αλλάξει ο CSN. Ενδιαφέρον παρουσιάζει η άποψη του Greq Young, διευθυντή πωλήσεων της RFI Communications & Security Systems, "Οι έξυπνες κάρτες μπορούν μεν να αποτελούν τον ασφαλέστερο τρόπο, χωρίς όμως αυτό να εξασφαλίζει ότι στην πράξη είναι ο ασφαλέστερος. Πολλοί κατασκευαστές συσκευών ανάγνωσης ισχυρίζονται ότι τα προϊόντα τους έχουν τη δυνατότητα ανάγνωσης ποικίλων τύπων έξυπνων καρτών, ενώ πραγματικά, αυτό που διαβάζουν είναι ο σειριακός αριθμός της κάρτας. Μόνο στην περίπτωση που είναι απόλυτα εξασφαλισμένο ότι οι πληροφορίες που διαβάζονται προέρχονται από έναν ασφαλή τομέα της κάρτας, ο οποίος μπορεί να κρυπτογραφηθεί, τότε υπάρχει μεγαλύτερη ασφάλεια από τις proximity κάρτες".

Ακόμα και η χρήση των κρυπτογραφημένων CSN δεν παρέχει καμία προστασία, ενώ ένα ερώτημα που τίθεται είναι τι γίνεται με τους τυχαία επιλεγόμενους σειριακούς αριθμούς. Για το συγκεκριμένο θέμα, οι προδιαγραφές ISO αναφέρουν ότι ο CSN είναι ένας μοναδικός σταθερός αριθμός ή ένας δυναμικά παραγόμενος αριθμός, που δημιουργείται από την έξυπνη κάρτα. Ο Finkenzeller, συγγραφέας του βιβλίου "RFID handbook" αναφέρει ότι σε αντίθεση με τις κάρτες τύπου Α, ο σειριακός αριθμός των καρτών τύπου Β δεν είναι απαραίτητα σταθερός, αλλά μπορεί να είναι ένας τυχαία παραγόμενος αριθμός, ο οποίος να αλλάζει ύστερα από μια διακοπή της ηλεκτρικής τροφοδοσίας του κυκλώματος. Όμως είναι σαφές, ότι σύμφωνα με το παραπάνω στοιχείο δεν μπορεί να λειτουργήσει ένας συγκεκριμένος αναγνώστης με έξυπνες κάρτες που χρησιμοποιούν μεταβαλλόμενους CSN, καθώς είναι πιθανό, κάθε φορά που οι κάρτες εκτίθενται στον αναγνώστη, ο σειριακός τους αριθμός να είναι διαφορετικός και να μην μπορεί να επιτευχθεί διασύνδεση. Ακόμα και το συμπέρασμα στο οποίο πολλοί καταλήγουν αβίαστα, ότι από τη στιγμή που ο CSN είναι ένας μοναδικός σειριακός αριθμός που καταγράφεται μόνιμα στη μνήμη του μικροεπεξεργαστή κατά τη διαδικασία της παραγωγής και άρα δεν μπορεί να αλλάξει, δεν είναι πάντα απόλυτα σωστό.

Εκεί που μπορούν να φανούν χρήσιμες οι απλές συσκευές ανάγνωσης των CSN είναι σαν μια προσωρινή λύση όταν υπάρχει μετάβαση από έναν τύπο καρτών ενός κατασκευαστή, σε άλλο σύστημα. Ένας απλός αναγνώστης μπορεί να χρησιμοποιηθεί τόσο για τις υφιστάμενες κάρτες, όσο και για τις καινούριες, οι οποίες θα διαθέτουν όλα τα προηγμένα χαρακτηριστικά ασφάλειας και ταυτοποίησης. Με αυτόν τον τρόπο εξασφαλίζεται ένα περιθώριο χρόνου για την ολοκλήρωση της αντικατάστασης. Όταν όλες οι κάρτες αντικατασταθούν, τότε μπορεί να απενεργοποιηθεί η δυνατότητα ανάγνωσης του CSN από τον αναγνώστη. Και όπως είναι εύκολα αντιληπτό, η παραπάνω περίοδος αντικατάστασης πρέπει να είναι όσον το δυνατό συντομότερη, για λόγους ασφαλείας.

Αποδεικνύεται λοιπόν ότι η χρήση του CSN για λειτουργίες που δεν συμπεριλαμβάνονται στο αρχικό σκεπτικό του σχεδιασμού, απλώς συμβάλλουν στη μείωση της ασφάλειας. Οπότε, οι υπεύθυνοι ασφάλειας κατά την υλοποίηση και ανάπτυξη ενός συστήματος έξυπνων καρτών, πρέπει να λαμβάνουν υπόψη τα ακόλουθα:

1. Οι έξυπνες κάρτες είναι πολύ ασφαλείς, όταν όμως χρησιμοποιούνται κατάλληλα.

2. Η χρήση του CSN μιας έξυπνης κάρτας, ουσιαστικά παρακάμπτει τους μηχανισμούς ασφαλείας που είναι ενσωματωμένοι εκ κατασκευής στις κάρτες.

3.Η τεχνολογία Proximity προσφέρει μεγαλύτερη ασφάλεια, συγκρινόμενη με εκείνη των έξυπνων καρτών, όταν όμως χρησιμοποιείται το CSN ως μέσο ταυτοποίησης.

4. Η κατανόηση των ενδεχόμενων κινδύνων που συνδέονται με τη χρήση του CSN, αντί των στοιχείων που προστατεύονται από τους μηχανισμούς ασφάλειας, συνεισφέρει στην ουσιαστική προστασία των εγκαταστάσεων, των υλικών υποδομών, αλλά και του προσωπικού. https://www.itsecuritypro.gr/nees-prokliseis-gia-tis-lyseis-iam/

# *3. Ιδιωτικότητα και Προσωπικά Δεδομένα.*

Με την έννοια «Προσωπικά Δεδομένα» στις μέρες μας νοείται μια ευρεία γκάμα επιμέρους χαρακτηριστικών της προσωπικότητας του ατόμου που δραστηριοποιείται στο διαδίκτυο, τα οποία μπορεί να διαφοροποιούνται κατά ένα ποσοστό ανάμεσα στις χώρες και ταξινομείται σε κατηγορίες ανάλογα με το είδος και τη φύση των δεδομένων αυτών. Στο διαδίκτυο η κατηγοριοποίηση των προσωπικών δεδομένων γίνεται με διάφορους τρόπους, ενώ αντίστοιχα η έννοια της ιδιωτικότητας και των προσωπικών δεδομένων συχνά είναι συνυφασμένες.

## *3.1 Ορισμός των Προσωπικών Δεδομένων.*

Σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), στα προσωπικά δεδομένα περιλαμβάνεται κάθε πληροφορία που χαρακτηρίζει και ταυτοποιεί ένα φυσικό πρόσωπο, όπως για παράδειγμα το όνομα, η διεύθυνση, το τηλέφωνο, τα ενδιαφέροντα, οι φωτογραφίες και οι προσωπικές απόψεις. Ορισμένα προσωπικά δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής ζωής του ατόμου, όπως το θρήσκευμα, οι πολιτικές πεποιθήσεις, η κατάσταση της υγείας του ή η ερωτική ζωή του.

Στην Ελλάδα ειδικότερα , τα λεγόμενα "απλά" προσωπικά δεδομένα είναι τα εξής:

- Το ονοματεπώνυμο,
- Ο τόπος κατοικίας,
- Το επάγγελμα,
- Το μορφωτικό επίπεδο,
- Οι καταναλωτικές συνήθειες,
- Η ταξιδιωτική δραστηριότητα,
- Η οικογενειακή κατάσταση,
- Η περιουσιακή κατάσταση,
- Ο μισθός και οι τραπεζικοί λογαριασμοί.

Αντίστοιχα, στα "ευαίσθητα" προσωπικά δεδομένα συγκαταλέγονται στοιχεία που αφορούν τον "σκληρό πυρήνα" της ιδιωτικής ζωής του καθενός. Σε κάθε χώρα η έννοια της ιδιωτικής ζωής ή αλλιώς της ιδιωτικότητας, διαφοροποιείται. Στη χώρα μας, τα ευαίσθητα προσωπικά δεδομένα σχετίζονται με:

- Την φυλετική ή εθνική καταγωγή,
- Τα πολιτικά φρονήματα,
- Τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
- Τη συμμετοχή σε συνδικαλιστική οργάνωση, τη συμμετοχή σε ενώσεις προσώπων που σχετίζονται με ευαίσθητα προσωπικά δεδομένα (π.χ. σωματείο ομοφυλόφιλων),
- Την υγεία, χρόνιες ασθένειες παθήσεις,
- Την κοινωνική πρόνοια,
- Την ερωτική ζωή,
- Τις ποινικές διώξεις ή τα αδικήματα που έχει διαπράξει το άτομο (π.χ. ποινικό μητρώο),
- Τα μητρώα και αρχεία της Εθνικής Αρχής Ιατρικώς Υποβοηθούμενης Αναπαραγωγής,
- Τις δηλώσεις και τα στοιχεία των αιτούντων πολιτικό άσυλο,
- Τα δεδομένα των ληπτών και δωρητών ανθρωπίνων ιστών και οργάνων,
- Τα γενετικά δεδομένα

Πρακτικά ο διαχωρισμός των προσωπικών δεδομένων σε απλά και ευαίσθητα σχετίζεται με τη διαδικασία συλλογής και επεξεργασίας αυτών, καθώς για τη νόμιμη επεξεργασία των απλών δεδομένων αρκεί η προφορική συγκατάθεση του υποκειμένου και η γνωστοποίηση στην αρμόδια Αρχή (Αρχή Προστασίας Προσωπικών Δεδομένων – ΑΠΔΠΧ).

Αντίθετα, για τα ευαίσθητα δεδομένα θεσπίζεται η γενική απαγόρευση της επεξεργασίας τους. Κατ' εξαίρεση επιτρέπεται η συλλογή και επεξεργασία τους καθώς και η τήρηση σχετικού αρχείου, κατόπιν λήψης σχετικής άδειας από την ΑΠΔΧ (Αλεξανδροπούλου – Αιγυπτιάδου 2007). Για τη λήψη άδειας από την ΑΠΔΧ, θα πρέπει να συντρέχουν συγκεκριμένοι λόγοι (αρ.7 ν.2472/1997), όπως:

- Η γραπτή συγκατάθεση του υποκειμένου των δεδομένων,
- Η διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του,
- Η αναγκαιότητα αναγνώρισης, άσκησης ή υπεράσπισης δικαιώματος ενώπιων δικαστηρίου ή πειθαρχικού οργάνου (αρ.22 ν.3471/2006),
- Η ιατρική πρόληψη, διάγνωση, περίθαλψη ή διαχείριση υπηρεσιών υγείας (αρ.34 ν.2915/2001),
- Η εθνική ασφάλεια, η διακρίβωση εγκλημάτων, ποινικών καταδίκων ή η λήψη μέτρων ασφάλειας,
- Η προστασία της δημόσιας υγείας, η άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών (αρ.34 ν.2915/2001),
- Η πραγματοποίηση επιστημονικής έρευνας ενώ προβλέπεται και η διενέργεια προληπτικού ελέγχου τήρησης των δεδομένων αυτών (ν.2472/1997).

## *3.2 Η έννοια της Ιδιωτικότητας.*

Σε πολλές περιπτώσεις η έννοια της προστασίας των προσωπικών δεδομένων ταυτίζεται με την έννοια της προστασίας της ιδιωτικής ζωής ή αλλιώς της ιδιωτικότητας, καθώς τα προσωπικά δεδομένα αποτελούν στοιχεία της ιδιωτικότητας ενός ατόμου. Ο όρος ιδιωτικότητα αναφέρεται ως "το δικαίωμα στην απομόνωση" (the right to be let alone) και σχετίζεται με την απομόνωση, την μυστικότητα και την αυτονομία. Αλλιώς, η ιδιωτικότητα χρησιμοποιείται για να περιγράψει την κατάσταση του να μπορεί κάποιος να είναι μόνος και να μην μπορεί κάποιος να τον δει ή να τον ακούσει, καθώς και την κατάσταση του να είναι κάποιος ελεύθερος από τη δημόσια προσοχή (Longman dictionary of Contemporary English). Ο όρος αυτός χρησιμοποιείται στις ΗΠΑ χωρίς διάκριση από την έννοια των προσωπικών δεδομένων για ζητήματα που άπτονται της προστασίας τους. Ο όρος προσωπικά δεδομένα (personal data) χρησιμοποιείται κυρίως στην ευρωπαϊκή νομική ορολογία, στην πράξη όμως οι δύο έννοιες συχνά ταυτίζονται.

## *3.3 Η διαδικτυακή ιδιωτικότητα (Internet Privacy)*

Η διαδικτυακή ιδιωτικότητα (Internet privacy) αναφέρεται στο δικαίωμα της διατήρησης της προσωπικής ιδιωτικότητας σε σχέση με την αποθήκευση, μετατροπή, διάθεση σε τρίτους και επίδειξη πληροφοριών οι οποίες αφορούν ένα άτομο, μέσω του διαδικτύου. Η ιδιωτικότητα στο διαδίκτυο αποτελεί μέρος της λεγόμενης ιδιωτικότητας των πληροφοριών (information privacy), η οποία αναφέρεται στη γενική απαίτηση των ατόμων να μην είναι διαθέσιμα τα προσωπικά τους δεδομένα σε άλλα άτομα και οργανισμούς. Στην περίπτωση

που ένα τρίτο μέρος κατέχει τα προσωπικά δεδομένα κάποιου ατόμου, η ιδιωτικότητα αναφέρεται στη δυνατότητα του ατόμου να ασκεί ένα σημαντικό βαθμό ελέγχου σχετικά τη χρήση των προσωπικών του δεδομένων (Clarke 1998).

Σύμφωνα με τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ, 2013), τα προσωπικά δεδομένα στο διαδίκτυο ορίζονται ως οποιαδήποτε πληροφορία σχετίζεται με την ταυτοποίηση ενός ατόμου (υποκειμένου δεδομένων) (OECD Privacy Guidelines, 2013). Ο ορισμός αυτός είναι ευρύς και περιλαμβάνει τους εξής τύπους προσωπικών δεδομένων:

- Περιεχόμενο το οποίο έχει δημιουργηθεί από τον χρήστη, συμπεριλαμβανομένων των προσωπικών ιστολογιών (blogs) και ο σχολιασμός, οι φωτογραφίες, τα βίντεο,

- Δραστηριότητα ή δεδομένα συμπεριφοράς, συμπεριλαμβανομένων των αναζητήσεων στον ιστό, τις διαδικτυακές αγορές. τα ποσά και τον τρόπο πληρωμής,

- Κοινωνικά δεδομένα, συμπεριλαμβανομένων των επαφών και φίλων στα μέσα κοινωνικής δικτύωσης,

- Δεδομένα τοποθεσίας, στα οποία περιλαμβάνονται η διεύθυνση κατοικίας, και ο προσδιορισμός της θέσης και τοποθεσίας του ατόμου (GPS), μέσω του κινητού τηλεφώνου ή της διεύθυνσης IP (IP address),

- Δημογραφικά δεδομένα στα οποία συμπεριλαμβάνεται η ηλικία, το φύλο, η φυλή, το εισόδημα, οι σεξουαλικές προτιμήσεις, οι πολιτικές πεποιθήσεις, κλπ.,

- Αναγνώριση δεδομένων επίσημης φύσης, όπως το όνομα, οι οικονομικές πληροφορίες και οι αριθμοί τραπεζικών λογαριασμών, ο αριθμός μητρώου ασφαλισμένων και τα ποινικά μητρώα,

Η ερευνητική βιβλιογραφία έχει επιπλέον κατηγοριοποιήσει τα προσωπικά δεδομένα με διάφορους τρόπους. Για παράδειγμα, ο Schneier (2010) έχει αναπτύξει μια ταξινόμηση των προσωπικών δεδομένων χρησιμοποιώντας τα κοινωνικά δίκτυα και ξεχώρισε έξι τύπους:

- Δεδομένα εξυπηρέτησης (service data), τα οποία καταχωρούνται για τη δημιουργία ενός λογαριασμού (π.χ. το όνομα, η διεύθυνση και ο αριθμός πιστωτικής κάρτας),

- Δεδομένα γνωστοποίησης (disclosed data), τα οποία καταχωρούνται εθελοντικά από τον χρήστη,

- Εμπιστευτικά δεδομένα (entrusted data), για παράδειγμα τα σχόλια που γίνονται στις καταχωρήσεις άλλων προσώπων,

- Συμπωματικά δεδομένα (incidental data), τα οποία αφορούν κάποιον συγκεκριμένο χρήστη αλλά έχουν καταχωρηθεί από άλλο πρόσωπο,

- Δεδομένα συμπεριφοράς (behavioural data), τα οποία περιλαμβάνουν πληροφορίες για τη δραστηριότητα των χρηστών μιας ιστοσελίδας και δύναται να χρησιμοποιηθούν για τη δημιουργία στοχοποιημένης διαφήμισης,

- Συναγόμενα δεδομένα (inferred data), τα οποία προκύπτουν από τα δεδομένα γνωστοποίησης κάποιου, το προφίλ ή τις διαδικτυακές του δραστηριότητες.

Τα προσωπικά δεδομένα συχνά κατηγοριοποιούνται και σύμφωνα με τη χρήση τους. Είναι κοινή τακτική η διάκριση ανάμεσα στα δεδομένα που συλλέγονται από έναν συγκεκριμένο φορέα προκειμένου να χρησιμοποιηθούν για μια τρέχουσα - προσωρινή διαδικτυακή εργασία και σε αυτά που τα οποία αποθηκεύονται για χρήση και ανάλυση και/ή πωλούνται σε τρίτα μέρη (FTC, 2009).

Στη δεύτερη κατηγορία, τα είδη των εμπλεκόμενων προσωπικών δεδομένων μπορούν να ταξινομηθούν βάση της φύσης τους σε δύο μεγάλες κατηγορίες:

- Πληροφορίες που δεν αναμένεται να αλλάξουν δραματικά κατά την πάροδο του χρόνου, οι οποίες αναφέρονται ως στατικές προσωπικές πληροφορίες (static private information). Τέτοιες πληροφορίες αφορούν το οικονομικό ιστορικό, το ιατρικό ιστορικό, τα προσωπικά πιστεύω και η διασύνδεση με ομάδες ανθρώπων, καθώς και τα προσωπικά αρχεία.
- Πληροφορίες οι οποίες αλλάζουν δραματικά με την πάροδο του χρόνου, παρόλα αυτά όμως δύναται να συλλεχθούν και να αναλυθούν κατά τρόπο που να μπορεί να δημιουργηθεί ένα καλά ενημερωμένο προφίλ του ατόμου. Οι πληροφορίες αυτές αναφέρονται ως δυναμικές προσωπικές πληροφορίες, όπως το ιστορικό δραστηριότητας (στο διαδίκτυο) και το ιστορικό περιεχομένου. (H. Wang, M. K.O. Lee, and C. Wang 1998).

Η ιδιωτικότητα στην πληροφορία (information privacy), δηλαδή η δυνατότητα του ατόμου να ελέγχει το πότε, πώς και σε ποιο βαθμό οι προσωπικές του πληροφορίες κοινοποιούνται σε άλλους, αποτελεί ένα από τα πιο σημαντικά ηθικά, νομικά, κοινωνικά και πολιτικά ζητήματα της εποχής της πληροφορίας (Culnan and Bies 2003; Milberg et al. 2000). Οι ανησυχίες για το ενδεχόμενο παράβασης των ιδιωτικών πληροφοριών μέσω του διαμοιρασμού της χρήσης υπολογιστικών συστημάτων εκφράστηκαν από την απαρχή του διαδικτύου (David E. E & Fano, R. M .,1965).

Η αύξηση των ψηφιακών προσωπικών πληροφοριών και η πρόοδος των τεχνολογιών του διαδικτύου έθεσαν νέες προκλήσεις στην ιδιωτικότητα των πληροφοριών των καταναλωτών και χρηστών του διαδικτύου (Angst and Agarwal 2009; Malhotra et al. 2004; Ward et al. 2005). Τα προσωπικά δεδομένα γίνονται στις μέρες του Web 2.0 πιο ευάλωτα, καθώς, από την μία πλευρά, οι προσωποποιημένες διαδικτυακές υπηρεσίες και τα λογισμικά επιχειρηματικής ευφυίας απαιτούν τη συλλογή και εξόρυξη ενός πρωτοφανούς σε μέγεθος όγκου δεδομένων προσωπικών πληροφοριών (Li and Sarkar 2006) και από την άλλη πλευρά, οι ίδιοι οι χρήστες του διαδικτύου προμηθεύουν τα διαδικτυακά blogs και τις σελίδες κοινωνικής δικτύωσης με περιεχόμενα τα οποία αφορούν την ιδιωτική τους ζωή.

## *3.4 Δεδομένα προσωπικής και μη προσωπικής ταυτοποίησης του χρήστη.*

Μια ευρέως χρησιμοποιούμενη διάκριση που γίνεται αναφορικά με τα προσωπικά δεδομένα των χρηστών του διαδικτύου είναι αυτή ανάμεσα στα δεδομένα προσωπικής ταυτοποίησης (Personally Identifiable Information - PII) και τα δεδομένα μη προσωπικής ταυτοποίησης (non - PII).

Στα δεδομένα προσωπικής ταυτοποίησης περιλαμβάνονται πληροφορίες οι οποίες απευθείας ταυτοποιούν ένα πρόσωπο. Στην άλλη κατηγορία περιλαμβάνονται πληροφορίες όπως το ιστορικό αναζήτησης του χρήστη, η επισκεψιμότητα σε διάφορες ιστοσελίδες και η διαδικτυακή συμπεριφορά του εν γένει, οι οποίες δεν ταυτοποιούν απ' ευθείας τον χρήστη με κάποιο συγκεκριμένο πρόσωπο.

Για παράδειγμα, στις πληροφορίες προσωπικής ταυτοποίησης τυπικά περιλαμβάνονται το όνομα και η διεύθυνση, το ΑΦΜ και άλλοι μοναδικοί αριθμοί ταυτοποίησης. Στις πληροφορίες μη προσωπικής ταυτοποίησης τυπικά περιλαμβάνονται δεδομένα που σχετίζονται με τους όρους αναζήτησης που έχουμε χρησιμοποιήσει, τις ιστοσελίδες που έχουμε επισκεφθεί, τις αγορές που έχουμε πραγματοποιήσει διαδικτυακά και τους τρόπους πληρωμής που έχουμε χρησιμοποιήσει (OECD, 2013).

Υπάρχει έντονη αβεβαιότητα σχετικά με την κατηγοριοποίηση ορισμένων τύπων πληροφοριών, όπως η γεωγραφική θέση και η διεύθυνση IP. Η αβεβαιότητα αυτή ενισχύεται καθώς βελτιώνονται οι μέθοδοι ανάλυσης δεδομένων και παρέχεται η δυνατότητα καλύτερου συνδυασμού των μερών της πληροφορίας που είναι μη ταυτοποιήσιμες οι οποίες όταν συνδυαστούν οδηγούν στην ταυτοποίηση ενός χρήστη. Στις μέρες μας οι τεχνικές που χρησιμοποιούνται δίνουν συχνά τη δυνατότητα συσχετισμού των δεδομένων μη προσωπικής ταυτοποίησης που συλλέγονται από τις αναζητήσεις όρων, την επίσκεψη ιστοσελίδων, τις γεωγραφικές θέσεις και τη διεύθυνση IP, με ένα συγκεκριμένο άτομο. Όταν όμως ένα δεδομένο μη προσωπικής ταυτοποίησης συσχετισθεί με την πραγματική ταυτότητα ενός ατόμου, η ανωνυμία και η ιδιωτικότητα του χρήστη παύει πλέον να υφίσταται (Narayanan and Shmatikov, 2010).

Επίσης στις καταναλωτικές δραστηριότητες που πραγματοποιούνται στον χώρο του ηλεκτρονικού εμπορίου, η ιδιωτικότητα συνήθως αναφέρεται στα προσωπικά δεδομένα του καταναλωτή και η εισβολή στην ιδιωτική ζωή συνήθως μεταφράζεται σε μη εξουσιοδοτούμενη συλλογή, γνωστοποίηση ή άλλη χρήση των προσωπικών πληροφοριών η οποία προκύπτει ως άμεσο αποτέλεσμα των ηλεκτρονικών - διαδικτυακών του συναλλαγών

## *3.5 Σημασία Προστασίας των Προσωπικών Δεδομένων των Χρηστών.*

Οι Smith, et al. (1996) σημείωσαν τέσσερις διαστάσεις των ανησυχιών σχετικά με τα προσωπικά δεδομένα και τις πρακτικές που ακολουθούνται στο διαδίκτυο:

- Συλλογή προσωπικών πληροφοριών
- Μη εξουσιοδοτημένη δευτερεύουσα χρήση των προσωπικών πληροφοριών
- Λάθη στις προσωπικές πληροφορίες
- Αντικανονική πρόσβαση στις προσωπικές πληροφορίες

Οι διαστάσεις αυτές έχουν επίσης σημειωθεί στις ανησυχίες σχετικά με το διαδικτυακό μάρκετινγκ και τις αγορές μέσω διαδικτύου. Στην περίπτωση του διαδικτυακού μάρκετινγκ οι διαστάσεις της ανησυχίας περιλαμβάνουν:

- Τη συλλογή των προσωπικών δεδομένων
- Τον έλεγχο σχετικά με τη χρήση τους
- Τη γνώση σχετικά με τις πρακτικές και τις χρήσεις που ακολουθούνται για τα προσωπικά τους δεδομένα (Malhotra, et al. 2004).

Ο έλεγχος και η γνώση περιλαμβάνουν τη μη εξουσιοδοτημένη δευτερεύουσα χρήση, την αντικανονική πρόσβαση και τα λάθη. Σύμφωνα με μια έρευνα, οι διαδικτυακοί καταναλωτές δίνουν μεγαλύτερη έμφαση στη γνώση σχετικά με τη χρήση των προσωπικών τους δεδομένων και στον τρόπο με τον οποίο θα μπορούσαν να έχουν άμεσο έλεγχο των δεδομένων τους (Malhotra, et al. 2004). Στις περισσότερες των περιπτώσεων οι καταναλωτές έχουν μικρό έλεγχο των πρακτικών που ακολουθούνται σχετικά με τη διαχείριση των προσωπικών τους δεδομένων από τις επιχειρήσεις ή τους οργανισμούς που συλλέγουν τα δεδομένα τους. Από πλευράς καταναλωτών δίνεται η δυνατότητα επιλογής των επιχειρήσεων

ή οργανισμών εκείνοι μπορούν να εμπιστεύονται προσωπικά τους δεδομένα καθώς και τον τύπο των πληροφοριών που επιλέγουν να παράσχουν (Tsai et. al, 2011).

Για τους χρήστες του διαδικτύου υπάρχει στις μέρες μας εντεινόμενη ανησυχία αναφορικά με την παραβίαση της εμπιστευτικότητας των προσωπικών δεδομένων τόσο σε κοινωνικό όσο και σε οικονομικό επίπεδο ως προς τις πιθανές αρνητικές συνέπειες.

Οι αρνητικές συνέπειες μπορούν να διαβαθμιστούν σε χαμηλό, μέσο και υψηλό επίπεδο. Σε χαμηλό επίπεδο, το αντίκτυπο μιας παραβίασης μπορεί να σχετίζεται με την προσωπική αναστάτωση και βλάβη που προκαλείται στον χρήστη, όπως π.χ. το να αναγκαστεί να προβεί ο χρήστης στην αλλαγή του αριθμού τηλεφώνου του.

Σε ένα μέσο επίπεδο ανεπιθύμητων παρενεργειών θα μπορούσε να αναφερθεί μια πιθανή οικονομική απώλεια – βλάβη που θα μπορούσε να συμβεί με την κλοπή των στοιχείων της ταυτότητάς του, καθώς και το ενδεχόμενο δημόσιας ταπείνωσης ή μεροληψίας ή ακόμα και να πέσει θύμα εκβιασμού.

Στο υψηλότερο επίπεδο κατατάσσονται οι σωματικές βλάβες, οι κοινωνικές ή οικονομικές ζημιές, με πιο σοβαρές συνέπειες όπως η πιθανή απώλεια της ίδιας της ζωής του ατόμου ή η απώλεια της ικανότητας βιοπορισμού του (NIST 2010).

Ως παραδείγματα των παραπάνω ανησυχιών και προβλημάτων – προσωπικών βλαβών των χρηστών του διαδικτύου μπορούν να σημειωθούν οι μηνύσεις σε δημοφιλείς ιστοσελίδες όπως η Google Buzz, η Facebook Beacon και η AOL ValueClick για παραβάσεις της διαδικτυακής ιδιωτικότητας. Έτσι προέκυψε αναγκαστική η δημιουργία νομοθετικών πράξεων για τη διαδικτυακή προστασία των προσωπικών δεδομένων, αποδίδοντας την αυξημένη σημασία και το υψηλό ενδιαφέρον που δίνεται σήμερα στον τομέα της διαδικτυακής ιδιωτικότητας.

Στον τομέα της προστασίας των δεδομένων, υπάρχει η σύσταση αρκετών ερευνητών για την επανεξέταση των ζητημάτων αυτών προκειμένου να αντανακλάται η σύγχρονη δυναμική του προβλήματος (Chen et al. 2008; Malhotra et al. 2004). Υπό τις παρούσες συνθήκες αλλά περισσότερο και για το μέλλον η κατανόηση των ανησυχιών σχετικά με την προστασία των προσωπικών δεδομένων των ατόμων είναι θεμελιώδης ως προς την ελευθεριάζουσα προοπτική χρήσης του διαδικτύου και η επιτυχία των αναδυόμενων διαδικτυακών τεχνολογιών θα πρέπει να συναρτάται στο πνεύμα ελευθερίας χρήσης του διαδικτύου.

## *3.6 Ιστορικό Ιστοσελίδων Κοινωνικής Δικτύωσης.*

Από την εποχή της δημιουργίας του SixDegrees.com, του πρώτου αναγνωρισμένου μέσου κοινωνικής δικτύωσης το 1997, η χρήση των μέσων αυτών έχει επεκταθεί στις μέρες μας σε τρομακτικό βαθμό (D. M. Boyd & N. B. Ellison 2007). Μεταξύ των ετών 1997 και 2001, οι χρήστες του διαδικτύου απέκτησαν τη δυνατότητα δημιουργίας επαγγελματικών και προσωπικών προφίλ σε διάφορα μέσα κοινωνικής δικτύωσης, όπως τα: "Friends, AsianAvenue, BlackPlanet και MiGente". Το 2002 δημιουργήθηκε το Friendster, μέσω του οποίου συνδέονταν οι φίλοι των φίλων με την προοπτική της γνωριμίας και της δημιουργίας ρομαντικών σχέσεων (D. M. Boyd & N. B. Ellison 2007).

Από το 2003 και έπειτα, η επιτυχία των προηγούμενων ιστοσελίδων ώθησε στη δημιουργία ποικίλων ιστοσελίδων κοινωνικής δικτύωσης, οι οποίες έκαναν διαρκώς την εμφάνισή τους, αντιγράφοντας το μοτίβο των πρώτων μέσων κοινωνικής δικτύωσης. Σταδιακά, όλο και περισσότεροι χρήστες του διαδικτύου αποκτούσαν τη δυνατότητα δημιουργίας ενός δημόσιου ή ημί - δημόσιου προφίλ, συνάθροισης φίλων μέσω ενός δικτύου και δημοσίευσης σχολίων, μηνυμάτων, εικόνων και βίντεο στη σελίδα τους (T. Funk 2010). Μέσω του Flickr δόθηκε η δυνατότητα στους χρήστες του να μοιράζονται φωτογραφίες, το

Last.FM παρείχε στους χρήστες του έναν τόπο συζήτησης (forum) διαμοιρασμού μουσικής και το YouTube σχεδιάστηκε προκειμένου να διαμοιράζεται βίντεο.

Το 2003 έκανε την εμφάνισή του το MySpace, το οποίο παρείχε για πρώτη φορά τη δυνατότητα στους χρήστες του να προσωποποιούν τη σελίδα τους και να προσθέτουν χαρακτηριστικά ανάλογα με τη βούλησή τους. Το MySpace αποτέλεσε παγκόσμιο φαινόμενο, καθώς έγινε ιδιαίτερα δημοφιλές ανάμεσα στους εφήβους (D. M. Boyd & N. B. Ellison 2007). Το 2004 ξεκίνησε τη λειτουργία του το Facebook, το οποίο αρχικά σχεδιάστηκε προκειμένου να χρησιμοποιείται αποκλειστικά από φοιτητές κολεγίων. Από το 2006 επιτράπηκε η πρόσβαση στο Facebook σε όλους τους χρήστες του διαδικτύου (D. Kirkpatrick 2010).

Η χρήση των ιστοσελίδων κοινωνικής δικτύωσης όπως το Facebook, το Twitter και το LinkedIn έχει αυξηθεί σημαντικά κατά τα τελευταία χρόνια (J.B. Yeager and R.K. Sisson 2011). Υπολογίζεται ότι το 75% των ατόμων ηλικίας μεταξύ δεκαοκτώ και εικοσιτεσσάρων διαθέτουν προφίλ σε ένα μέσο κοινωνικής δικτύωσης. Αντίστοιχα, το ένα τρίτο των ατόμων μεταξύ τριάντα πέντε και σαράντα τεσσάρων ετών διαθέτουν έναν ενεργό διαδικτυακό λογαριασμό. Επιπλέον, περίπου το είκοσι τις εκατό των ατόμων μεταξύ σαράντα πέντε και πενήντα τεσσάρων ετών διαθέτουν ένα προφίλ στα κοινωνικά δίκτυα (J. E. Grenig and J.S. Kinsler 2011). Οι αριθμοί αυτοί αυξάνονται με την πάροδο του χρόνου, καθώς οι σελίδες κοινωνικής δικτύωσης γίνονται όλο και περισσότερο καθημερινό κομμάτι της ζωής των ανθρώπων.

Με το Web 2.0 οι μεταβολές που επήλθαν στο τοπίο των μέσων επικοινωνίας συνοδεύτηκαν από τη μετάλλαξη του χαρακτήρα τόσο της μαζικής όσο και της προσωπικής επικοινωνίας, δημιουργώντας τη λεγόμενη "μαζική – προσωπική επικοινωνία" (J. Pierson 2012). Η μετάλλαξη αυτή απεικονίζεται στον τρόπο που το Web 2.0 και τα κοινωνικά μέσα, δηλαδή οι σελίδες κοινωνικής δικτύωσης και τα μικροϊστολόγια (microblogging) όπως για παράδειγμα το Twitter, ενσωματώθηκαν στην καθημερινότητα των δυτικών κοινωνιών και στην πίστη ότι ο ίδιος ο χρήστης βρίσκεται στη θέση του οδηγού της κοινωνικό - τεχνικής αυτής καινοτομίας.

Παρατηρείται όμως ένα παράδοξο σχετικά με τον χαρακτήρα των ιστοσελίδων αυτών. Από τη μία πλευρά τα εργαλεία και τα μέσα για την ενδυνάμωση των χρηστών μέσω των κοινωνικών δικτύων αναπαράγουν και ενισχύουν την ιδέα ότι με το Web 2.0 συντελείται η ουσιαστική και αποτελεσματική ενδυνάμωση των χρηστών του. Από την άλλη πλευρά διαπιστώνεται στην πράξη ότι η ενδυνάμωση αυτή εκλείπει σε μεγάλο βαθμό και αντίστοιχα με τις ευκαιρίες ενδυνάμωσης διακυβεύεται η αντίστοιχη αποδυνάμωση των χρηστών του Web 2.0 (Van Dijck 2009). Κάτι τέτοιο δείχνει ότι ο κοινωνικός κόσμος ο οποίος εκπροσωπείται εντατικά από τη μαζική - προσωπική επικοινωνία δημιουργεί συνθήκες ευαισθησίας, οι οποίες καθιστούν τα άτομα ευάλωτα, καθώς δεν έχουν πάντα τις απαραίτητες ικανότητες ώστε να κατανοήσουν και να αντιδράσουν με τον καλύτερο δυνατό τρόπο έναντι άλλων ατόμων και οργανισμών προκειμένου να αποκτήσουν μια ισάξια κοινωνική θέση. Το τελευταίο χαρακτηριστικό είναι ιδιαίτερα εμφανές μελετώντας τη σχέση ανάμεσα στα κοινωνικά δίκτυα, την ενδυνάμωση και την ιδιωτικότητα (J. Pierson 2012).

Καθώς ο αριθμός των ατόμων που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης αυξάνεται, οι ανησυχίες για την ιδιωτικότητα επικεντρώνονται όλο και περισσότερο σε αυτά. Το Facebook, το δημοφιλέστερο μέσο κοινωνικής δικτύωσης παγκοσμίως έχει κατηγορηθεί αρκετές φορές για εισβολή στην ιδιωτικότητα των χρηστών του και παράνομη χρήση των προσωπικών δεδομένων του. Στη δίκη για την Ιδιωτικότητα στο Facebook ("In re Facebook Privacy Litigation", 2010) ο ενάγων David Gould κατηγόρησε τη συγκεκριμένη ιστοσελίδα για παραβίαση των προσωπικών του δεδομένων, καθώς σύμφωνα με την Federal Wiretap Act οριζόταν ότι "ένας οργανισμός ο οποίος παρέχει υπηρεσίες ηλεκτρονικής επικοινωνίας στο κοινό δεν θα πρέπει εσκεμμένα να κοινοποιεί τα περιεχόμενα οποιασδήποτε επικοινωνίας...σε

οποιοδήποτε πρόσωπο ή οργανισμό διαφορετικό από τον αποδέκτη ή τον παραλήπτη στον οποίο απευθύνεται το μήνυμα της επικοινωνίας". Η δίκη κατέληξε ότι οι ενάγοντες απέτυχαν να αποδείξουν ότι το Facebook σκόπιμα παρείχε στους διαφημιστές πληροφορίες των χρηστών του (B. Lodge, 2011).

Την ίδια χρονιά (2010) στην υπόθεση κατά της υπηρεσίας "Facebook Beacon" (Lane v. Facebook (N.D. Cal)) το Facebook κατηγορήθηκε για την υπηρεσία Beacon, στην οποία τρίτα μέρη ανέφεραν πληροφορίες σχετικά με τις δραστηριότητες των χρηστών του και το Facebook αναρτούσε τις πληροφορίες αυτές στον πίνακα ανακοινώσεων (newsfeed) χωρίς την ύπαρξη ρητής συγκατάθεσης από την πλευρά των χρηστών του. Στην υπόθεση αυτή το Facebook συμβιβάστηκε για $9,5 εκατομμύρια (Findings of Fact, Conclusions of Law, and Order Approving Settlement at 7, Lane v. Facebook, No. C 08-3845 RS (N.D. Cal. Mar. 17, 2010)), από τα οποία περίπου $2,3 εκατομμύρια δόθηκαν στους δικηγόρους των εναγόντων (Order Re Attorney Fees at 4, Lane v. Facebook, No. C 08-3845 RS (N.D. Cal. May 24, 2010)), και περίπου $25.000 δόθηκαν στους ενάγοντες.

Το υπολοιπόμενο ποσό κατατέθηκε για τη δημιουργία νέου ιδρύματος για την ιδιωτικότητα (Privacy Foundation) (Goldman E. 2012). Στην πιο πρόσφατη υπόθεση κατά αυτού του μέσου κοινωνικής δικτύωσης (Campbell v. Facebook Inc, U.S. District Court, Northern District of California, No.13-5996), ο ενάγων Matthew Campbell κατηγορεί την ιστοσελίδα για παραβίαση των προσωπικών δεδομένων των χρηστών του, καθώς η τελευταία σάρωνε (scan) το περιεχόμενο των μηνυμάτων που έστελναν οι χρήστες μεταξύ τους για διαφημιστικούς λόγους (Reuters, 24/12/2014, last view 12/1/2015). Η μήνυση η οποία κατατέθηκε το 2013 αναφέρει ότι η συγκεκριμένη ιστοσελίδα σάρωνε τα μηνύματα των χρηστών της με σκοπό τον εντοπισμό συνδέσεων (links) σε ιστοσελίδες και στη συνέχεια καταμετρούσε τον αριθμό των "likes" κάθε σύνδεσης. Τα "likes" αυτά στη συνέχεια χρησιμοποιούνταν με σκοπό τη δημιουργία στοχευμένης διαφήμισης. Σύμφωνα με το κατηγορητήριο η συγκεκριμένη πρακτική καταπατούσε τον ομοσπονδιακό νόμο καθώς και τους νόμους της πολιτείας της Καλιφόρνια, στην οποία εδρεύει το Facebook (Techworm, 25/12/2014, last view 12/1/2015).

Όμοια, στην υπόθεση κατά της Google Buzz του καινούργιου μέσου κοινωνικής δικτύωσης της Google, η μήνυση αφορούσε την αποκάλυψη προσωπικών δεδομένων από τους λογαριασμούς Gmail των χρηστών της. Η Google συμβιβάστηκε με το ποσό των $8,5 εκατομμυρίων (Settlement Agreement at 6, In re Google Buzz User Privacy Litigation, No. 5:10-CV-00672-JW (N.D. Cal. Sept. 3, 2010)), από τα οποία οι δικηγόροι μπορούσαν να διεκδικήσουν έως το 30% (περίπου $2.5 εκατομμύρια) και οι ενάγοντες αποζημιώθηκαν με $2,500 ο καθένας (Wendy Davis, 2010). Το υπολοιπόμενο ποσό κατατέθηκε σε οργανισμούς επιμόρφωσης καταναλωτών και οργανισμούς για την ιδιωτικότητα (N.D. Cal. Sep. 20, 2011). Καθώς η διαμάχη σχετικά με το τι θεωρείται ως εισβολή στην ιδιωτικότητα συνεχίζεται, είναι εμφανές ότι η χρήση των μέσων κοινωνικής δικτύωσης έχει διαφοροποιηθεί από τους πρωταρχικούς του σκοπούς της διασύνδεσης των ανθρώπων με παρόμοια ενδιαφέροντα. Παρόλο που αρχικά τα μέσα αυτά σχεδιάστηκαν έχοντας ως επίκεντρό τους τις διαδικτυακές κοινότητες, το επίκεντρο τώρα βρίσκεται στο μεμονωμένο άτομο το οποίο αποτελεί το επίκεντρο της δικής του κοινότητας. Η καινούργια αυτή δομή αναφέρεται ως "εγωκεντρικά δίκτυα" (egocentric networks) (D. M. Boyd & N. B. Ellison 2007).

Τα δίκτυα αυτά καθώς επικεντρώνονται σε ένα άτομο, παρέχουν στους υπόλοιπους τη μοναδική και εύκολη ευκαιρία να πραγματοποιούν έρευνα σχετικά με το άτομο αυτό και ενδεχομένως στο τέλος τα στοιχεία αυτά να χρησιμοποιηθούν εις βάρος του. Παράδειγμα τέτοιας περίπτωσης αποτελεί η δικαστική υπόθεση που απασχόλησε το 2010 δικαστήριο της Boulogne Billancourt στη Γαλλία, με αντικείμενο την απόλυση μιας υπαλλήλου από την εταιρία στην οποία εργαζόταν λόγω των σχολίων που ανάρτησε κατά της επιχείρησης στο Facebook. Το δικαστήριο υιοθέτησε την υπερασπιστική γραμμή του συνηγόρου, σύμφωνα με

την οποία η απόλυση λόγω σχολίων στο Facebook συνιστά απειλή κατά της ιδιωτικής ζωής και τελικά έκρινε την απόλυση παράνομη, κηρύσσοντας παράλληλα αθέμιτη την απαγόρευση διατύπωσης σχολίων, έστω και αυστηρών, σχετικά με την εταιρία απασχόλησης της ενάγουσας (Conseil de prud' hommes de Boulogne Billancourt de departage 19 Novembre 2010).

Η χρήση των μέσων κοινωνικής δικτύωσης όπως το Facebook δύναται να εκθέσει τα ευαίσθητα προσωπικά δεδομένα των χρηστών της με εύκολο τρόπο. Σε μια έρευνα που διεξήχθη με τη συμμετοχή 58.000 εθελοντών χρηστών του δικτύου αυτού, αποδείχθηκε ότι τα Facebook Likes, δηλαδή οι προτιμήσεις των χρηστών της υπηρεσίας αυτής, δύναται να χρησιμοποιηθούν αυτόματα και να προβλέψουν με ακρίβεια ένα εύρος απλών και ευαίσθητων προσωπικών δεδομένων, στα οποία συμπεριλαμβάνονται: η εθνική καταγωγή, το θρήσκευμα, οι προσωπικές και πολιτικές απόψεις, ο σεξουαλικός προσανατολισμός, το επίπεδο ευδαιμονίας, η νοημοσύνη, η οικογενειακή κατάσταση, η χρήση εξαρτησιογόνων ουσιών, η ηλικία και το φύλο (Kosinski et al 2013).

## *3.7 Θέματα Κρατικής Παρακολούθησης.*

Τον Ιούνιο του 2013, ο Edward Joseph Snowden, Αμερικάνος διαχειριστής υπολογιστικών συστημάτων και πρώην εργαζόμενος της Κεντρικής Υπηρεσίας Πληροφοριών των ΗΠΑ (Central Inteligence Agency - CIA), διέρρευσε στον Τύπο απόρρητα έγγραφα της αμερικάνικης Εθνικής Υπηρεσίας Ασφάλειας (National Security Agency - NSA) τα οποία σχετίζονταν με το πρόγραμμα μαζικής - παγκόσμιας παρακολούθησης που εφάρμοζε τα τελευταία χρόνια η NSA. Σύμφωνα με τις αποκαλύψεις του Snowden, η NSA συνέλεγε εκατοντάδες εκατομμύρια λίστες επαφών από προσωπικούς λογαριασμούς ηλεκτρονικών ταχυδρομείων (email) και υπηρεσίες αποστολής άμεσων μηνυμάτων (instant messaging Services). Ενδεικτικά, κατά τη διάρκεια μίας μόνο ημέρας, το Ειδικό Τμήμα Επιχειρήσεων της NSA (Special Source Operations) συνέλεξε 444.743 βιβλία διευθύνσεων από το Yahoo, 105.068 από το Hotmail, 82.857 από το Facebook, 33.697 από το Gmail και 22.881 από άλλους παρόχους. Αυτά τα στοιχεία, τα οποία περιγράφουν μια τυπική ημέρα, αναλογούσαν στη συλλογή 250 εκατομμυρίων βιβλίων διευθύνσεων το έτος. Όμοια, καθημερινά συλλέγονταν 500.000 λίστες επαφών από τις υπηρεσίες ζωντανής συνομιλίας (live chat) (Gellman, Barton, Soltani, Ashkan 1/11/2013).

Η υπηρεσία αφού συνέλεγε τα βιβλία διευθύνσεων στη συνέχεια ερευνούσε τα περιεχόμενα των ηλεκτρονικών ταχυδρομείων προκειμένου να ανακαλύψει πληροφορίες σχετικά με πιθανούς εξωτερικούς κινδύνους για την ασφάλεια των ΗΠΑ (Savage, Charlie 8/8/2013). Παράλληλα, εντόπιζαν και χαρτογραφούσαν τις τοποθεσίες κινητών τηλεφώνων (Gellman, Barton; Soltani, Ashkan 12/12/2013) και ανέπτυξαν προγράμματα υποβάθμισης των τεχνολογιών διαδικτυακής ασφάλειας και κρυπτογράφησης (Ball, Borger, Greenward, 5/9/2013). Η NSA χρησιμοποιούσε τεχνολογία cookies προκειμένου να ενισχυθεί η κυβερνητική παρακολούθηση (Ashkan Soltani, Andrea Peterson, and Barton Gellman December 10, 2013). Χρησιμοποιώντας το "Muscular", ένα ειδικό πρόγραμμα παρακολούθησης, η NSA φαίνεται ότι "μυστικά" εισέβαλε στα κέντρα δεδομένων της Yahoo και της Google προκειμένου να συλλέξει πληροφορίες από εκατοντάδες εκατομμύρια λογαριασμούς χρηστών παγκοσμίως (Gellman, Barton 4/11/2013).

Οι αποκαλύψεις του Snowden, σόκαραν την κοινή γνώμη παγκοσμίως. Σύμφωνα με έρευνα που έγινε τον Ιανουάριο του 2014 στις ΗΠΑ, διαφάνηκε ότι το διαδίκτυο έχασε μέρος της αξιοπιστίας του, καθώς οι άνθρωποι μετέβαλλαν τη διαδικτυακή συμπεριφορά τους, μειώνοντας κατά ένα ποσοστό τις δραστηριότητες που αφορούσαν αγορές, καταχώρηση στοιχείων προσωπικών δεδομένων, διατραπεζικές συναλλαγές και προσωπικές συνομιλίες

(Pew Research Center, 2014). Ίσως η πιο σημαντική προέκταση την επομένη των αποκαλύψεων ήταν η πλήρης έλλειψη της πεποίθησης ότι έχουν τον έλεγχο των προσωπικών τους δεδομένων. Η έλλειψη της εμπιστοσύνης αντικατοπτρίζεται τόσο στις συναλλαγές τους με τις επιχειρήσεις, όσο και με το δημόσιο. Για παράδειγμα:

- Το 91% των ενηλίκων στην έρευνα "συμφωνεί απόλυτα" ή "συμφωνεί πολύ" ότι οι καταναλωτές έχουν χάσει τον έλεγχο του τρόπου με τον οποίο τα προσωπικά τους δεδομένα συλλέγονται και χρησιμοποιούνται από τις επιχειρήσεις,
- Το 88% των ενήλικων "συμφωνούν" ή "συμφωνούν πολύ" ότι θα ήταν πολύ δύσκολο να διαγράψουν ανακριβείς πληροφορίες σχετικά με τους ίδιους στο διαδίκτυο.
- Το 80% αυτών που χρησιμοποιούν μέσα κοινωνικής δικτύωσης δηλώνουν ανήσυχοι σχετικά με τρίτα μέρη όπως διαφημιστές ή επιχειρήσεις οι οποίες εισβάλουν στα δεδομένα που κοινοποιούν στις ιστοσελίδες αυτές.
- Το 70% των χρηστών των ιστοσελίδων κοινωνικής δικτύωσης δηλώνουν ότι είναι ανήσυχοι σχετικά με το ενδεχόμενο πρόσβασης της κυβέρνησης σε μερικά από τα δεδομένα που κοινοποιούν στα μέσα χωρίς να το γνωρίζουν οι ίδιοι.

## *3.8 GDPR Συμμόρφωση – Εφαρμογή.*

Αναφορικά με την επίλυση των παραπάνω προβλημάτων στις μέρες μας ενισχύεται νομοθετικά σε επίπεδο τουλάχιστον ΕΕ η πρακτική χρήσης του διαδικτύου με ένα πλαίσιο κανόνων λειτουργίας του διαδικτύου στο οποίο πρέπει να συμμορφώνονται οι επιχειρήσεις.

Το GDPR είναι ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation GDPR). Στοχεύει να προσφέρει στους πολίτες της ΕΕ μια ενιαία και εναρμονισμένη προσέγγιση όσον αφορά την προστασία της ιδιωτικής ζωής στην Ευρωπαϊκή Ένωση. Επιδιώκει την ενίσχυση του δικαιώματος των πολιτών για την προστασία των δεδομένων τους, όπως ορίζεται στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Μετά από σχεδόν τέσσερα χρόνια συζήτησης και συζήτησης, το GDPR εγκρίθηκε από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016. Η ημερομηνία υποχρεωτικής εφαρμογής του GDPR καθορίστηκε στις 25 Μαΐου 2018 https://www.niriis.gr/gdpr).

Μια από τις πρώτες αλλαγές σχετικά με το GDPR και μια θεμελιώδη αλλαγή από το προηγούμενο πλαίσιο προστασίας δεδομένων (οδηγία της ΕΕ για την προστασία των δεδομένων - οδηγία 95/46 / ΕΕ) είναι ότι, μετά από πολλές συζητήσεις, το κοινοβούλιο της ΕΕ αποφάσισε ότι το νέο πλαίσιο προστασίας της ιδιωτικής ζωής θα δημιουργηθεί τη μορφή κανονισμού και όχι οδηγίας.

Το GDPR αποτελεί έναν κανονισμό, μια δεσμευτική νομοθετική πράξη που εφαρμόζεται άμεσα σε όλα τα κράτη μέλη της ΕΕ, εξαλείφοντας την ανάγκη κατάρτισης τοπικών νομοθετικών πράξεων. Ωστόσο, παρά την ανάγκη τοπικής νομοθεσίας, είναι πιθανό να υπάρξουν διαφορές ως προς τον τρόπο με τον οποίο ο κανονισμός ερμηνεύεται και επιβάλλεται σε διάφορα κράτη μέλη. Εκτός από την ανάγκη για ένα κοινό πλαίσιο προστασίας της ιδιωτικής ζωής, η ΕΕ στέλνει ένα ισχυρό μήνυμα σχετικά με τη δέσμευσή της για την προστασία των προσωπικών δεδομένων των υποκειμένων των δεδομένων της ΕΕ (το υποκείμενο των δεδομένων είναι ένα ζωντανό άτομο στο οποίο αναφέρονται προσωπικά δεδομένα) όχι μόνο από εταιρείες που δραστηριοποιούνται στην ΕΕ και όχι μόνο. Δηλαδή το GDPR απολαμβάνει εκτεταμένη ισχύ που επηρεάζει οντότητες που δεν είναι εγκατεστημένες στην ΕΕ. Φυσικά, πρέπει να πληρούνται ορισμένοι όροι για να εφαρμοστεί η έξω εδαφικότητα. Το GDPR της ΕΕ εφαρμόζεται στην επεξεργασία προσωπικών δεδομένων των προσώπων στα οποία αναφέρονται τα δεδομένα της ΕΕ, ανεξαρτήτως του εάν οι δραστηριότητες επεξεργασίας πραγματοποιούνται στην ΕΕ ή όχι.

Το GDPR της ΕΕ εφαρμόζεται επίσης σε οντότητες που είναι εγκατεστημένες εκτός ΕΕ εάν προσφέρουν αγαθά ή υπηρεσίες σε άτομα στην Ένωση ή αν παρακολουθούν τη συμπεριφορά των ατόμων στην Ένωση (δηλ. Δραστηριότητες σχετικές με τη δημιουργία προφίλ, παρακολούθηση των δραστηριοτήτων των ατόμων στο Διαδίκτυο κ.λπ. .).

Μία από τις συνέπειες της εξ εδαφικής προσέγγισης είναι ότι οι εταιρείες που δεν είναι εγκατεστημένες στην ΕΕ πρέπει να διορίσουν έναν εκπρόσωπο. Ο εν λόγω αντιπρόσωπος πρέπει να είναι εγκατεστημένος σε κράτος μέλος στο οποίο βασίζονται τα σχετικά πρόσωπα στα οποία αναφέρονται τα δεδομένα. Μόνο μια περιορισμένη παρέκκλιση επιτρέπεται όταν η επεξεργασία είναι περιστασιακή, δεν συνεπάγεται μεγάλης κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων και ο σκοπός και το αποτέλεσμα της επεξεργασίας είναι απίθανο να αποτελούν κίνδυνο για τα άτομα.

### *3.8.1 Μεταφορά Δεδομένων κατά GDPR.*

Κατά τη διαβίβαση δεδομένων, το GDPR επιβάλλει αυστηρούς περιορισμούς στις μεταφορές σε σημεία εκτός της Ευρωπαϊκής Ένωσης. Αυτό γίνεται προκειμένου να διασφαλιστεί η προστασία των δεδομένων προσωπικού χαρακτήρα σε κατάλληλο επίπεδο. Οι μεταφορές δεδομένων προς χώρες εκτός της ΕΕ μπορούν να πραγματοποιηθούν εάν υπάρχουν:

- μια απόφαση επάρκειας της ΕΕ (η ΕΕ έχει αποφασίσει ότι μια συγκεκριμένη χώρα έχει νόμους προστασίας δεδομένων ισοδύναμους με αυτούς της ΕΕ)
- υπάρχουν κατάλληλες διασφαλίσεις (για παράδειγμα, οι συμβάσεις που περιλαμβάνουν τις πρότυπες ρήτρες της ΕΕ για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα)
- ειδικές παρεκκλίσεις (για παράδειγμα, σαφή ενημέρωση από το πρόσωπο στο οποίο αναφέρονται τα δεδομένα).

Οι μεταφορές δεδομένων αποτελούν περίπλοκο τομέα της GDPR, ιδίως επειδή το ζήτημα της συναίνεσης αμφισβητείται από την ΕΕ και η συγκατάθεση χρησιμοποιείται ευρέως για να δικαιολογήσει τη διασυνοριακή μεταφορά προσωπικών δεδομένων. Ως εκ τούτου, οι οργανισμοί που έχουν ιστορικά προστατευθεί μέσω της συγκατάθεσης του χρήστη μπορεί να βρεθούν να χρειαστεί να επεξεργαστούν το πλαίσιο μεταφοράς δεδομένων τους ή να αντιμετωπίσουν υψηλές ποινές.

### *3.8.2 Διατήρηση Ασφαλών Προσωπικών Δεδομένων κατά GDPR.*

Το GDPR της ΕΕ απαιτεί από τις επιχειρήσεις να διατηρούν τα προσωπικά τους δεδομένα ασφαλή, όπως ακριβώς ορίζει και η ισχύουσα οδηγία. Παρόλο που η υποχρέωση αυτή εκφράζεται γενικά, παρέχει ορισμένες ενδείξεις σχετικά με τα μέτρα που αποσκοπούν στην προστασία προσωπικών δεδομένων, όπως:

- κρυπτογράφηση και ψευδονυμοποίηση,
- την εξασφάλιση και διατήρηση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας των συστημάτων πληροφορικής,
- της δυνατότητα αποκατάστασης της διαθεσιμότητας και πρόσβασης σε δεδομένα προσωπικού χαρακτήρα εγκαίρως,
- βοηθώντας τακτικά και δοκιμάζοντας την αποτελεσματικότητα των μέτρων ασφαλείας που εφαρμόζονται για την προστασία των δεδομένων.

Τα προαναφερθέντα μέτρα είναι απλά παραδείγματα - όχι υποχρεωτικά - και θα πρέπει να εφαρμόζονται μόνο "όπου ενδείκνυται". Επομένως, είναι ευθύνη της εταιρείας να αποδείξει ότι τα μέτρα ασφαλείας είναι κατάλληλα. Μια καλή πρακτική όσον αφορά τα μέτρα ασφαλείας θα ήταν το πρότυπο ISO 27001, έτσι οι εταιρείες θα μπορούσαν να το χρησιμοποιήσουν ως σημείο εκκίνησης κατά την οικοδόμηση των μέτρων προστασίας των δεδομένων τους.

Το GDPR της ΕΕ επιβάλλει επίσης νέες κυρώσεις στους μεταποιητές δεδομένων. Πρόκειται για μια μεγάλη απόκλιση από τους προηγούμενους νόμους περί προστασίας δεδομένων, όπου όλες οι υποχρεώσεις επικεντρώνονταν γύρω από τον υπεύθυνο επεξεργασίας δεδομένων. Μεταξύ άλλων, οι επεξεργαστές δεδομένων πρέπει τώρα να τηρούν αρχεία δραστηριοτήτων επεξεργασίας. Όπως και πριν, ένας επεξεργαστής δεδομένων είναι μια οντότητα (όπως ένα νομικό πρόσωπο, μια δημόσια αρχή, ένας οργανισμός ή οποιοσδήποτε άλλος φορέας) που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό ελεγκτή.

Σε μια σημαντική επικαιροποίηση, το GDPR της ΕΕ εισήγαγε νέα δικαιώματα για τα υποκείμενα των δεδομένων. Αυτά είναι:

- δικαιώματα πρόσβασης, διόρθωσης και φορητότητας
- δικαίωμα να αντιταχθεί στην επεξεργασία των δεδομένων του
- δικαιώματα διαγραφής και περιορισμού της επεξεργασίας
- Το πιο υψηλό ζήτημα των αλλαγών είναι το ευρέως συ ζητημένο "Δικαίωμα στη Λήθη" (το οποίο τώρα αποκαλείται "δικαίωμα διαγραφής"). Αυτό το δικαίωμα διαγραφής μπορεί να ενεργοποιηθεί σε ορισμένες συγκεκριμένες καταστάσεις, ακόμη και όταν το υποκείμενο των δεδομένων αποσύρει τη συγκατάθεσή του ή εάν δεν υπάρχει πλέον καμία αιτιολόγηση για την επεξεργασία των προσωπικών δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει να ανταποκρίνεται "χωρίς αδικαιολόγητη καθυστέρηση" κατά τη λήψη αυτών των αιτήσεων και πρέπει να ειδοποιεί όλες τις οντότητες στις οποίες έχει κοινοποιήσει αυτά τα δεδομένα. Είναι σαφές ότι για όλα τα δικαιώματα των προσώπων δεδομένων υπάρχει αυστηρή απαίτηση για τους υπευθύνους επεξεργασίας δεδομένων να καταγράφουν και να χαρτογραφούν τα δεδομένα προσωπικού χαρακτήρα που κατέχονται προκειμένου να είναι σε θέση να ανταποκρίνονται στις αιτήσεις πρόσβασης των υποκειμένων των δεδομένων (σε όλες τις μορφές) "χωρίς αδικαιολόγητη καθυστέρηση".

Σύμφωνα με το GDPR υπάρχει επίσης η υποχρέωση για ορισμένους οργανισμούς να διορίζουν έναν υπεύθυνο προστασίας δεδομένων, αν και μόνο σε συγκεκριμένες περιπτώσεις:

- όταν ο υπεύθυνος επεξεργασίας δεδομένων ή ο μεταποιητής είναι δημόσια αρχή
- όπου οι κύριες δραστηριότητες του υπεύθυνου επεξεργασίας δεδομένων ή του επεξεργαστή είναι η "τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα"
- όπου ο υπεύθυνος επεξεργασίας ή ο υπεύθυνος επεξεργασίας διεξάγει μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (όπως εθνικότητα, φυλετική προέλευση, πολιτικές απόψεις, θρησκευτικές πεποιθήσεις κ.λπ.)

### *3.8.3 Παραβιάσεις Δεδομένων και Ασφάλεια κατά GDPR.*

Εκτός από την εισαγωγή νέων δικαιωμάτων για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, το GDPR της ΕΕ εισάγει επίσης νέους κανόνες για παραβιάσεις δεδομένων. Σε σύγκριση με την προηγούμενη οδηγία, το GDPR επιβάλλει υποχρεώσεις τόσο στους

υπεύθυνους επεξεργασίας δεδομένων όσο και στους επεξεργαστές δεδομένων. Το GDPR προσφέρει επίσης καθοδήγηση και παραδείγματα για να διευκολύνει τους οργανισμούς να μετριάσουν τον κίνδυνο. Μεταξύ αυτών είναι:

1. ψευδονοποίηση δεδομένων προσωπικού χαρακτήρα (δηλαδή επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο που δεν μπορεί πλέον να αποδοθεί σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών)
2. την ικανότητα να αποκαθιστά εγκαίρως τη διαθεσιμότητα (και την πρόσβαση) σε προσωπικά δεδομένα, ύστερα από φυσικά ή τεχνικά περιστατικά
3. την ικανότητα διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της ανθεκτικότητας των συστημάτων επεξεργασίας
4. την προσθήκη διαδικασιών για την εξασφάλιση τακτικού ελέγχου και αξιολόγησης τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας των επεξεργασμένων δεδομένων προσωπικού χαρακτήρα
5. Επιπλέον, οι οργανισμοί πρέπει τώρα να πληρούν τα πρότυπα όταν πρόκειται για παραβιάσεις κοινοποιήσεων. Σε γενικές γραμμές, οι οργανώσεις που έχουν υποστεί παραβίαση δεδομένων πρέπει να ενημερώσουν την εποπτική αρχή (ανεξάρτητη δημόσια αρχή που έχει συσταθεί από ένα κράτος μέλος σύμφωνα με το άρθρο 51 του GDPR) «χωρίς αδικαιολόγητη καθυστέρηση» εκτός εάν η παραβίαση δεν θέτει σε κίνδυνο τα υποκείμενα των δεδομένων. Εάν υπάρχει κίνδυνος για τα επηρεαζόμενα άτομα, οι οργανώσεις πρέπει επίσης να το γνωστοποιήσουν στα ενδιαφερόμενα πρόσωπα στα οποία αναφέρονται, και πάλι "χωρίς αδικαιολόγητη καθυστέρηση".

Η κακή διαχείριση των παραβιάσεων δεδομένων θα τιμωρείται με την υψηλότερη βαθμίδα κυρώσεων βάσει του GDPR. Ένας άλλος τρόπος για το Ευρωπαϊκό Κοινοβούλιο να επιβεβαιώσει τη δέσμευσή του για την προστασία της ιδιωτικής ζωής είναι οι νέες κυρώσεις, οι οποίες είναι σημαντικά υψηλότερες από ό, τι στην προηγούμενη οδηγία. Οι κυρώσεις και τα πρόστιμα μπορούν τώρα να φθάσουν το 4% του συνολικού κύκλου εργασιών της εταιρείας που βρίσκεται σε παραβίαση. Η λογική πίσω από τα τεράστια πρόστιμα που αφορούν την νομοθεσία είναι αρκετά απλή: οι υψηλότερες κυρώσεις για τη μη συμμόρφωση θεωρούνται ότι οδηγούν σε υψηλότερα επίπεδα συμμόρφωσης. Θα γίνει όλο και πιο δύσκολο για τις επιχειρήσεις να αποδεχθούν απλώς ένα ορισμένο επίπεδο κινδύνου όταν χειρίζονται προσωπικά δεδομένα, επειδή οι ποινές είναι τώρα ιδιαίτερα υψηλές.

Οι κυρώσεις στο πλαίσιο του GDPR θα εμπίπτουν σε δύο κατηγορίες όσον αφορά το ύψος του προστίμου:

1. Μέχρι 2% του ετήσιου παγκόσμιου κύκλου εργασιών ή 10 εκατ. Ευρώ, όποιο είναι υψηλότερο, για παραβάσεις σε περιπτώσεις όπου:
   - Υπάρχει αδυναμία αναφοράς παραβίασης δεδομένων
   - Υπάρχει παραβίαση της αρχής του απορρήτου βάσει του σχεδιασμού, όπως ορίζεται στο άρθρο 25 του GDPR
   - Υπάρχει αδυναμία διορισμού αντιπροσώπου (όταν η οντότητα είναι εγκατεστημένη εκτός της ΕΕ)
   - Υπάρχει αδυναμία λήψης συγκατάθεσης κατά την επεξεργασία των δεδομένων παιδιών
   - Υπάρχει αδυναμία θέσπισης κατάλληλων ρητρών προστασίας δεδομένων στις συμβάσεις με τους μεταποιητές
   - Υπάρχει αδυναμία ορισμού υπευθύνου προστασίας δεδομένων
   - Υπάρχει αδυναμία διατήρησης γραπτών αρχείων.

2. Μέχρι 4% του ετήσιου παγκόσμιου κύκλου εργασιών ή 20 εκατ. Ευρώ, όποιο είναι υψηλότερο, για πιο σοβαρά αδικήματα όπως:

- τη μη συμμόρφωση με τις αρχές της νόμιμης επεξεργασίας δεδομένων όπως ορίζονται στο GDPR
- τη μη τήρηση των διατάξεων σχετικά με τις μεταφορές δεδομένων προσωπικού χαρακτήρα εκτός της ΕΕ
- τη μη συμμόρφωση με τα δικαιώματα των υποκειμένων των δεδομένων.

Τα νέα σύνολα κυρώσεων συμπληρώνονται επίσης από πρόσθετες εξουσίες που είναι εύκολα προσπελάσιμες από τις εποπτικές αρχές προστασίας δεδομένων, όπως η έκδοση προειδοποιήσεων για μη συμμόρφωση, η διενέργεια ελέγχων, η απαιτούμενη ειδική αποκατάσταση εντός συγκεκριμένου χρονικού πλαισίου, η παραγγελία διαγραφής δεδομένων και αναστολή της μεταφοράς δεδομένων σε τρίτη χώρα.

Ο αντίκτυπος του GDPR ενδέχεται να είναι ελαφρώς διαφορετικός για τους οργανισμούς που λειτουργούν σε χώρες όπως η Γερμανία, η Γαλλία ή οι Κάτω Χώρες, όπου η νομοθεσία για την προστασία των δεδομένων είναι ιστορικά αυστηρή και, σε ορισμένες περιπτώσεις, ξεπερνούν ακόμη και την υπάρχουσα οδηγία. Η συμμόρφωση με το GDPR θα επιτευχθεί ευκολότερα από εταιρείες που δραστηριοποιούνται σε αυτούς τους τομείς, καθώς οι αρχές εποπτείας στις χώρες αυτές έχουν ήδη επιδείξει επιμέλεια για να προστατεύσουν τα δικαιώματα και τις ελευθερίες του ατόμου. Ωστόσο, για άλλες χώρες όπως η Ελλάδα όπου οι αρχές προστασίας δεδομένων "έμειναν αδρανείς" λόγω έλλειψης διοικητικών εξουσιών και σχεδόν αμελητέων προστίμων, οι οργανώσεις αγνοούσαν τους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, γνωρίζοντας ότι οι εποπτικές αρχές δεν διέθεταν τους πόρους ή τη δύναμη να επιβάλλουν κυρώσεις στους παραβάτες. Συγκεκριμένα, οι επεξεργαστές θα επηρεαστούν σε αυτές τις δικαιοδοσίες, διότι μέχρι στιγμής δεν αποτέλεσαν ποτέ στόχο των ερευνών των αρχών προστασίας δεδομένων.

# 4. Βιβλιογραφία

## 4.1 Ξενόγλωσση βιβλιογραφία


Buell, D. & Sandhu, R., 2003. Identity management. *Internet Computing, IEEE,* 7(6), pp. 26 - 28

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*.

Camp, L., 2004. Digital Identity. *Technology and Society, IEEE,* 23(3), pp. 34 - 41

Chen, H. G., Chen C.C., Lo, L., and Yang, S. C. (2008) "Online Privacy control via anonymity and pseudonym: Cross - cultural implications", *Behaviour & Information Technology* (27:3), pp. 229-242.

Clauß, S. & Köhntopp, M., 2001. Identity management and its support of multilateral security. *Computer Networks, Elsevier,* 37(2), p. 205 – 219

Corradini, F., Paganelli, E. & Polzonetti, A., 2007. The e-Government digital credentials. *Int. J. of Electronic Governance, Inderscience,* 1(1), pp. 17 - 37

Culnan, M. J., and Bies, R. J. (2003) "Consumer Privacy: Balancing economic and Justice Considerations", *Journal of Social Issues* (59:2), pp. 323-342.

Danziger, J. & Andersen, K., 2002. The Impacts of Information Technology on Public Administration: An Analysis of Empirical Research from the "Gloden Age" of Transformation. *International Journal of Public Administration,* 25(5), pp. 591 - 627

Gapgemini, 2007. *The User Challenge Benchmarking the Supply of Online Public Services,* Brussles: Directorate General for Information Society and Media

Gouscos, D., Georgiadis, P. & Sagris, T., 2000. *From Introvert IT Systems to Extrovert eServices, e-Government as an Enabler for e-Citizens and e-Business - A frameowrk of Principles.* Madrid, Proceedings of the Electronic Business and Electronic Work 2000 Conference (EBEW 2000), IOS Press, pp. 866 - 872

Grönlund, Å. & Horan, T., 2005. Introducing e-Gov: History, Definitions, and Issues. *Communications of the Association for Information Systems,* 15(1), pp. 713 - 729.

Hahamis, P., J., I. & Healy, M., 2005. e-Government in Greece: Bridging the Gap between Need and Reality. *Electronic Journal of e-Government,* 3(4), pp. 185 - 192.

Jessup Leonard M. and Joseph S. (2008): *Information Systems Today (3rd ed.)*. Valacich : Pearson Publishing.

Krause M. and Tipton H.F. (1998): *Handbook of Information Security Management*. Auerbach Publications, CRC Press LLC.

Kroenke D.M. ( (2008)): *Experiencing MIS*. Upper Saddle River, NJ: Prentice-Hall.

Laudon K.C. and Laudon J.P. (1988): *Management Information Systems*. 2nd edition. Aufl. Macmillan

Malhotra, N. K., Kim S. S., and Agarwal, J. (2004) "Internet users'information privacy concerns (IUIPC): The construct, the scale and a casual model», *Information Systems Research* (15:4), pp. 336-355.

Markellos, K., Markellou, P., Panayiotaki, A. & Stergianeli, E., 2007. Current State of Greek E-Government Initiatives. *J. of Business Systems, Governance and Ethics,* 2(3), pp 67 - 88.

Milberg, S. J., Smith H. J., and Burke, S. J. (2000) "Information Privacy: Corporate management and National Regulation", *Organization Science* (11:1), pp. 35-37.

Narayanan A. and V. Shmatikov (2010) "Privacy and security Myths and fallacies of Personally identifiable information" *Communications of the ACM* ,vol. 53 (6)

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

Tsai et al. (2011) "The Effect of Online Privacy Information on Purchasing Behavior" *Information Systems Research* 22 (2), pp. 254–268, INFORMS

Zheng J. (2009): *Environment Information PeopleTechnology Input Output Boundary Purpose Processes and Interactions*

## *4.2 Ελληνική βιβλιογραφία*

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία (2007) "Προσωπικά δεδομένα: Η νομική ρύθμιση της ηλεκτρονικής επεξεργασίας τους", Εκδόσεις Αντ. Ν. Σάκκουλα

Γκρίτζαλης Δ.Α.; Γκρίτζαλης Σ. and Κάτσικας Σ. (2003): *Ασφάλεια δικτύων υπολογιστών*. Παπασωτηρίου.

Διακονικολάου, Κ. & Μυλωνόπουλος, Ν., 2004. *Το παρόν και το μέλλον των Ηλεκτρονικών Υπηρεσιών του Κράτους προς τις Επιχειρήσεις (Government to Business) στην Ελλάδα,* Αθήνα: Κοινωνία της Πληροφορίας

Δρογκάρης Κ. Προκόπιος «Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης» Διδακτορική Διατριβή Παν/μιο Αιγαίου, Σχολή Θετικών Επιστημών Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, ΣΑΜΟΣ 2013

Κιοσσέ, Ε., 2011. *Η πορεία της Ηλεκτρονικής Διακυβέρνησης στις χώρες της Ε.Ε. και την Ελλάδα - Οι επιδόσεις των χωρών,* Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας

Φωτεινόπουλος Χ. Αναστάσιος – Μιχαήλ « Τεχνολογίες Ταυτοποίησης με Προστασία της Ιδιωτικότητας η Τεχνολογία PRIVACY-ABCS», Μεταπτυχιακή Διπλωματική Εργασία, Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών Μαθηματικά των Υπολογιστών και των Αποφάσεων, ΠΑΤΡΑ 2016.
Διαθέσιμο

## *4.3 Ιστοσελίδες*

Clarke Roger "Information privacy on the Internet" (2 May 1998). Available at: http://www.rogerclarke.com/DV/IPrivacy.html (Ανάκτηση 17/06/2019)

David E. E and R. M. Fano (1965): "Some Thoughts about the Social Implications of Accessible Computing". *Proceedings 1965 Fall Joint Computer Conference.* Available at: http://www.multicians.org/fjcc6.html (Ανάκτηση 17/06/2019)

FTC (2009), "Self-Regulatory Principles for Online Behavioral Advertising", FTC, Washington DC. Available at: www.ftc.gov/opa/2009/02/behavad.shtm (Ανάκτηση 17/06/2019).

NIST - National Institute of Standards and Technology Special Publication (Apr. 2010) "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - Recommendations of the National Institute of Standards and Technology" 800-122 *Natl. Inst. Stand. Technol. Spec. Publ*. 800-122 http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (Ανάκτηση 22/06/2019)

OECD (2013), "The OECD Privacy Framework", Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Ανάκτηση 17/06/2019)

OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing. Διαθέσιμο : http://dx.doi.org/10.1787/5k486qtxldmq-en (Ανάκτηση 17/06/2019)

Schneier (2010), SecuritySchneier on Security, A blog covering security and security technology. Διαθέσιμο

http://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html