



ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ

ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ ΚΑΙ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΑ ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ – ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΡΥΘΜΙΣΤΙΚΕΣ ΑΡΧΕΣ



ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ: ΧΡΗΣΤΟΣ ΤΣΙΚΡΙΤΕΑΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΧΡΗΣΤΟΣ ΓΚΟΓΚΟΣ

ΙΟΥΝΙΟΣ 2015

ΕΥΧΑΡΙΣΤΙΕΣ

Καταρχήν, θα ήθελα να εκφράσω τις ολόθερμες ευχαριστίες μου στον επιβλέποντα καθηγητή μου κ. Γκόγκο Χρήστο για την αμέριστη βοήθεια που μου προσέφερε κατά την διάρκεια της εκπόνησης της συγκεκριμένης εργασίας με τις εύστοχες παρατηρήσεις και καθοδηγήσεις που μου έδινε συνεχώς προκειμένου να την ολοκληρώσω επιτυχώς.

Επίσης, θα ήθελα να εκφράσω τις ευχαριστίες μου και προς το υπόλοιπο εκπαιδευτικό προσωπικό του τμήματος Λογιστικής και Χρηματοοικονομικής του Τ.Ε.Ι. ΗΠΕΙΡΟΥ για τις ολοκληρωμένες οικονομικές και λοιπές γνώσεις που μου παρείχαν αφειδώς κατά την διάρκεια των σπουδών μου.

Τέλος, θα ήθελα να ευχαριστήσω και την οικογένειά μου για την ηθική στήριξη που μου προσέφερε όλο αυτό το χρονικό διάστημα μέχρι να ολοκληρώσω την πτυχιακή μου εργασία.

ΠΕΡΙΛΗΨΗ

Μέσα σε ένα παγκόσμιο περιβάλλον, όπου η δυνατότητα για ανταλλαγή παντός είδους πληροφοριών και σε τεράστιο όγκο αποτελεί δεδομένη δυνατότητα για τη συντριπτική πλειοψηφία του παγκόσμιου πληθυσμού, είναι προφανές ότι πλέον έχουμε περάσει στη λεγόμενη εποχή των Μεγάλων Δεδομένων.

Υπό αυτό το πρίσμα, θα πρέπει να μεταβληθεί και ο τρόπος προσέγγισης διαφόρων εννοιών με κύρια της έννοιας της ιδιωτικότητας, προκειμένου αυτή να μπορέσει να περιλάβει και όλες εκείνες τις συνιστώσες που μπορεί να αποδειχτούν απειλητικές όσον αφορά στη διαφύλαξη της ιδιωτικότητας των προσωπικών δεδομένων με βάση και την ψηφιακή συνιστώσα.

Ταυτόχρονα, οι διάφορες περιοχές και χώρες ανά τον κόσμο, καλούνται να επικαιροποιούν συνεχώς το νομοθετικό τους πλαίσιο προκειμένου αυτό να μπορεί να προσαρμόζεται συνεχώς στις απαιτήσεις της τεχνολογικής εξέλιξης και να εξασφαλίζει στο μέγιστο δυνατό την προστασία των προσωπικών δεδομένων.

Σε κάθε όμως περίπτωση, το άτομο ως αυτόνομη μονάδα θα είναι αυτό που τόσο στο παρόν όσο και στο μέλλον, *καλείται* να διαδραματίσει πρωτεύοντα ρόλο στο πως μπορεί να προστατέψει την ιδιωτική του ζωή και τις πληροφορίες που σχετίζονται με αυτή, θέτοντας ταυτόχρονα τα προσωπικά του όρια όσον αφορά στην έκταση και το είδος των πληροφοριών που θα γνωστοποιεί σε διαδικτυακά περιβάλλοντα.

ABSTRACT

In a global environment, where the vast majority of the world population has the ability to share all kinds of information and in huge amount, it is clear that we have passed today to the so-called era of Big Data.

Within this framework, the approach of various concepts, like the main concept of privacy it should be changed so as to allow it to include all those components that may prove threatening with regard to safeguarding the privacy of personal data.

Simultaneously, the different regions and countries around the world are invited to constantly update their legislative framework so that it can be adapted continuously to the demands of technological developments and to ensure the greatest possible protection of personal data and personal information.

But, in any case, the individual as an autonomous unit both in present and future, has to play a major role in how to protect the privacy and the information associated with it, both by setting personal limits concerning the extent and type of information that would disclose in online environments.

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ	1
ΠΕΡΙΛΗΨΗ	2
ABSTRACT	3
ΠΕΡΙΕΧΟΜΕΝΑ ΣΧΗΜΑΤΩΝ	6
ΕΙΣΑΓΩΓΗ	7
ΚΕΦΑΛΑΙΟ 1	12
ΤΙ ΕΙΝΑΙ ΤΑ ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ	12
1.1 ΓΕΝΙΚΑ	12
1.2 ΤΑ BIG DATA ΣΗΜΕΡΑ	12
1.3 ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ BIG DATA	14
1.3.1 Όγκος των δεδομένων	15
1.3.2 Ποικιλία των δεδομένων	17
1.3.3 Ταχύτητα των δεδομένων	18
1.4 ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ ΤΩΝ BIG DATA	19
1.4.1 IT log analytics	20
1.4.2 Ανίχνευση απάτης	21
1.4.3 Κοινωνικά δίκτυα	23
1.4.4 Διασφάλιση της ποιότητας σε τηλεφωνικά κέντρα	24
1.4.5 Συστήματα διαχείρισης ρίσκου	25
1.4.6 Συστήματα ενέργειας	25
ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ	28
2.1 ΓΕΝΙΚΑ	28
2.2 Η ΕΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΖΩΗ	28
2.2.1 Ιδιωτικότητα των προσωπικών δεδομένων	29
2.2.2 Ιδιωτικότητα της διάχυσης πληροφοριών σε σχέση με προσωπικά δεδομένα ...	29
2.2.3 Ιδιωτικότητα των δεδομένων εταιριών και οργανισμών.....	29
2.3 Η ΕΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ	30
2.3.1 Ιδιωτικότητα της επικοινωνίας	30
2.3.2 Ιδιωτικότητα της συμπεριφοράς.....	31
2.3.3 Προστασία της ανωνυμίας	32
2.4 Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΑΜΕΡΙΚΗ ΚΑΙ ΣΤΗΝ ΕΥΡΩΠΗ	33

2.4.1 Η ιδιωτικότητα στην Αμερική.....	33
2.4.2 Η ιδιωτικότητα στην Ευρώπη.....	35
2.4.3 Σύγκριση προσεγγίσεων για την ιδιωτικότητα στον ευρωπαϊκό και στον αμερικάνικο χώρο.....	36
2.5 ΔΙΑΦΟΡΕΤΙΚΕΣ ΠΤΥΧΕΣ ΠΡΟΣΕΓΓΙΣΗΣ ΤΗΣ ΕΝΝΟΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ.....	37
2.6 Η ΑΝΑΓΚΗ ΓΙΑ ΥΠΑΡΞΗ ΜΙΑΣ ΠΑΓΚΟΣΜΙΑΣ ΝΟΜΟΘΕΣΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ.....	38
2.7 ΠΩΣ ΤΕΛΙΚΑ ΜΕΤΑΦΡΑΖΕΤΑΙ Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗ ΣΗΜΕΡΙΝΗ ΨΗΦΙΑΚΗ ΕΠΟΧΗ.....	39
ΚΕΦΑΛΑΙΟ 3.....	40
ΡΥΘΜΙΣΤΙΚΕΣ ΑΡΧΕΣ.....	40
3.1 ΓΕΝΙΚΑ.....	40
3.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ “ΨΗΦΙΑΚΟΥ” ΡΥΘΜΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ.....	40
3.3 ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ.....	42
3.3.1 Το εκτενές μοντέλο.....	42
3.3.2 Το στοχευμένο μοντέλο.....	42
3.3.3 Το αυτορρυθμιζόμενο μοντέλο.....	43
3.3.4 Το μοντέλο του καταναλωτή.....	44
3.4 ΤΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΣΤΗΝ ΕΥΡΩΠΗ ΚΑΙ ΤΗΝ ΑΜΕΡΙΚΗ.....	44
3.4.1 Το μοντέλο της Ευρωπαϊκής Ένωσης.....	45
3.4.2 Το μοντέλο της Αμερικής.....	50
3.5 ΤΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΑΝΑ ΤΟΝ ΚΟΣΜΟ.....	52

ΠΕΡΙΕΧΟΜΕΝΑ ΣΧΗΜΑΤΩΝ

Σχήμα 1.1 Βασικά χαρακτηριστικά των Μεγάλων Δεδομένων.

Σχήμα 1.2 Φαινόμενο τυφλής ζώνης.

Σχήμα 1.3. Παραδοσιακά συστήματα ανίχνευσης απάτης.

Σχήμα 1.4. Συστήματα ανίχνευσης απάτης με τη χρήση εφαρμογών Μεγάλων Δεδομένων.

Σχήμα 1.5. Συσχέτιση των συνιστωσών των Μεγάλων και Ανοικτών Δεδομένων υπό το πρίσμα της έννοιας της ανοικτής διακυβέρνησης.

ΕΙΣΑΓΩΓΗ

Τη σημερινή εποχή, με την αλματώδη εξέλιξη της τεχνολογίας που έχει λάβει χώρα ιδίως τις τελευταίες δύο δεκαετίες, αποτελεί αδιαμφισβήτητο γεγονός ότι ο κόσμος έχει αλλάξει και η τεχνολογία έχει συμβάλει ριζικά ως προς αυτή την κατεύθυνση.

Άλλοι ισχυρίζονται πως ο κόσμος έχει αλλάξει προς το καλύτερο, ενώ κάποιοι άλλοι υποστηρίζουν πως αυτή η τεράστια δυνατότητα για διάχυση της πληροφορίας ως αποτέλεσμα της τεχνολογικής ανόδου, έχει αρνητικά αποτελέσματα τόσο για το ίδιο το άτομο ως αυτόνομη μονάδα, όσο και συνολικά για την παγκόσμια κοινότητα. Ανεξάρτητα με το ποια από τις δύο πλευρές έχει δίκιο, κανείς δεν μπορεί να αμφισβητήσει το γεγονός ότι σήμερα ο άνθρωπος περισσότερο από κάθε άλλη πρότερη περίοδο, έχει τη δυνατότητα να συλλέγει και να ανταλλάσσει πληροφορίες σχετιζόμενες με αυτόν ή με οποιαδήποτε άλλη μονάδα ή σύνολο μονάδων, γρήγορα και σε αυξημένο όγκο.

Μέσα σε ένα τέτοιο διαμορφωθέν περιβάλλον, όπου η δυνατότητα για ανταλλαγή παντός είδους πληροφοριών και σε τεράστιο όγκο αποτελεί δεδομένη δυνατότητα για τη συντριπτική πλειοψηφία του παγκόσμιου πληθυσμού, είναι προφανές ότι πλέον έχουμε περάσει στη λεγόμενη εποχή ‘big data’.

Ενδεικτικά,

- Το 2009, το ψηφιακό παγκόσμιο περιβάλλον αυξήθηκε κατά περίπου 62% σε σχέση με το προηγούμενο έτος, μέγεθος που αντιστοιχεί περίπου σε 800.000 petabytes. Η τιμή αυτή από μόνη της αποτελεί ενδεικτικό μέγεθος της έκτασης της αύξησης που έλαβε χώρα το εν λόγω έτος.
- Το 2010 η αύξηση αυτή έφτασε τα 1.200.000 petabytes σε σχέση με το 2008.
- Το 2020 αναμένεται, το ψηφιακό περιβάλλον να μεγαλώσει κατά 44 φορές σε σχέση με την έκταση που εμφάνιζε το 2009.

Οι παραπάνω τιμές, καταδεικνύουν με τον πιο σαφή τρόπο την έκταση του ψηφιακού κόσμου στο σημερινό παγκόσμιο γίγνεσθαι.

Στο σημείο αυτό βέβαια θα πρέπει να τονιστεί, ότι η έννοια ‘big data’ δε σχετίζεται αποκλειστικά με το μέγεθος και τον όγκο της πληροφορίας που δύναται να διαχέεται καθημερινά σε παγκόσμιο επίπεδο, αλλά πραγματεύεται και σχετίζεται και με τις διαθέσιμες πηγές άντλησης δεδομένων που υπάρχουν σήμερα και απαντώνται σε διάφορες μορφές. Είναι γεγονός άλλωστε, ότι η έκταση του ψηφιακού περιβάλλοντος σε ποσοστό περίπου 70%, καλύπτεται σήμερα από βάσεις δεδομένων e-mail και από δράσεις σχετιζόμενες με social media, γεγονός που αποδεικνύει ότι η ανταλλαγή πληροφοριών μπορεί να γίνει για επαγγελματικούς, ψυχαγωγικούς ή άλλης στόχευσης λόγους.

Σήμερα

- Υπάρχουν παραπάνω από ένα τρισεκατομμύριο διευθύνσεις URL στο ευρετήριο της Google, ενώ καθημερινά λαμβάνουν χώρα πάνω από δύο δισεκατομμύρια αναζητήσεις στη μηχανή αναζήτησης της εταιρίας.
- Υπάρχουν διαθέσιμα 70 εκατομμύρια video στην πλατφόρμα του Youtube, τα οποία κατά μέσο όρο εμφανίζουν επισκεψιμότητα 100 ατόμων ανά ημέρα.
- Δρουν παραπάνω από 133 εκατομμύρια blogs.
- Υπάρχουν 500 εκατομμύρια ενεργοί χρήστες στο Facebook οι οποίοι συνολικά σπαταλούν 700 δισεκατομμύρια λεπτά σε μηνιαία βάση στο εν λόγω δίκτυο, ενώ στο δίκτυο Twitter, έχουν καταγραφεί συνολικά από την πρώτη μέρα λειτουργίας του σχεδόν 29 δισεκατομμύρια tweets με ροπή αύξησης που ανέρχεται στα 3 εκατομμύρια ανά ημέρα.

Αυτός ο τεράστιος όγκος δεδομένων που διακινείται καθημερινά, είναι κάτι παραπάνω από προφανές ότι σε πολλές περιπτώσεις διακινείται άκριτα από τους χρήστες, μιας και δεν είναι δυνατή η πλήρης επεξεργασία του λόγω της τεράστιας έκστασης και της υψηλής ταχύτητας με την οποία διακινείται.

Με βάση την παραπάνω παρατήρηση, εγείρονται και οι πρώτες σοβαρές αντιδράσεις για το κατά πόσον είναι ασφαλής και ωφέλιμη τελικά για τον άνθρωπο αυτή η διαμορφωθείσα κατάσταση.

Ο τομέας της διαφήμισης και της δυνατότητας για αγορά προϊόντων από ένα χρήστη από όλες τις γωνίες της γης, είναι αποδεκτό γεγονός ότι αύξησε τις επιλογές των καταναλωτών και συνετέλεσε στην παγκοσμιοποίηση της αγοράς. Από την άλλη όμως, η διακίνηση προσωπικών στοιχείων για την πραγματοποίηση αυτών των αγορών δημιουργεί από μόνη της ένα επισφαλές περιβάλλον, όπου υπάρχει η δυνατότητα για υποκλοπή προσωπικών στοιχείων των καταναλωτών και χρήση τους για άλλους σκοπούς.

Επιπρόσθετα, η κατηγοριοποίηση των καταναλωτών ανάλογα με την ηλικία τους, το φύλο τους, το εισόδημά τους, την περιοχή που ζουν, τις συνήθειές τους, ακόμα και με βάση τις ιστοσελίδες που επισκέπτονται, αποτελεί ένα δυνατό όπλο στα χέρια των ισχυρών ‘marketers’ ανά τον κόσμο, έτσι ώστε να κατευθύνουν και να διαμορφώνουν κατά το δοκούν τις καταναλωτικές ανάγκες των χρηστών, ωθώντας ουσιαστικά τον παγκόσμιο καταναλωτικό πληθυσμό σε υποκινούμενες καταναλωτικές δράσεις προκειμένου να κερδοσκοπήσουν.

Τέλος, δε θα πρέπει να ξεχνάμε ότι η αυξημένη δυνατότητα που παρέχεται σήμερα για συλλογή πληροφοριών, δε χρησιμοποιείται μόνο από φορείς που εξυπηρετούν σκοπούς σαν τους προαναφερθέντες, αλλά και από επίσημους φορείς που σκοπό έχουν την προστασία του πολίτη. Και σε αυτές τις περιπτώσεις βέβαια, η σύγκρουση μεταξύ των εννοιών της “ιδιωτικότητας” και της “κοινωνικής ασφάλειας” είναι αναπόφευκτη. Για παράδειγμα, πλέον είναι ευρέως διαδεδομένη η χρήση καμερών και συστημάτων CCTV σε σημεία δρόμων από πολλές κυβερνήσεις ανά τον κόσμο, με σκοπό την καταγραφή δεδομένων που σχετίζονται με την ομαλή ροή κυκλοφορίας ή την εύρεση υπόπτων σε περίπτωση παραβατικής συμπεριφοράς.

Σε κάθε περίπτωση, το σίγουρο είναι πως στην εποχή της τεράστιας διακίνησης δεδομένων, όσο πιο ενημερωμένος είναι ο παγκόσμιος πολίτης όσον αφορά στην προστασία της ιδιωτικής του ζωής, τόσο περισσότερο μπορεί να

επιηρεάσει τις πολιτικές προστασίας των προσωπικών δεδομένων και τους κανονισμούς που διέπουν αυτές, προκειμένου η δυνατότητα που προσφέρεται σε αυτόν για γρήγορη και τεραστίου όγκου διακίνηση πληροφοριών να είναι ωφέλιμη και κυρίως ασφαλής.

Σκοπός του παρόντος συγγράμματος, είναι να αναλυθεί η έννοια των Μεγάλων Δεδομένων και επιπρόσθετα να καταγραφούν οι σημαντικότερες παράμετροι που σχετίζονται με τις συνιστώσες της ιδιωτικότητας και των ρυθμιστικών αρχών στο σημερινό ψηφιακό γίγνεσθαι.

Για τη βέλτιστη επίτευξη αυτού του σκοπού, η παρούσα εργασία απαρτίζεται από τρία κύρια κεφάλαια.

Στο πρώτο κεφάλαιο, λαμβάνει χώρα μια ανάλυση της έννοιας των Μεγάλων Δεδομένων, ενώ ταυτόχρονα καταγράφονται τα βασικά χαρακτηριστικά αυτών καθώς και οι περιπτώσεις που απαντάται κύρια η χρήση τους. Πιο συγκεκριμένα, στο πρώτο κύριο χωρίο του κεφαλαίου περιγράφεται η έννοια των Μεγάλων Δεδομένων στο σημερινό παγκόσμιο γίγνεσθαι, ενώ στο δεύτερο κύριο χωρίο γίνεται εκτενής αναφορά στα τρία κύρια χαρακτηριστικά που περιγράφουν τις εφαρμογές Μεγάλων Δεδομένων σήμερα, τα οποία είναι ο όγκος, η ποικιλία και η ταχύτητα. Κατά την περιγραφή της συνιστώσας του όγκου, μεγάλη σημασία δίδεται στην περιγραφή του φαινομένου της τυφλής ζώνης. Τέλος, στο τρίτο και τελευταίο κύριο χωρίο του κεφαλαίου, γίνεται εκτενής αναφορά στις σημαντικότερες περιπτώσεις στις οποίες λαμβάνει χώρα σήμερα η χρήση εφαρμογών Μεγάλων Δεδομένων.

Το δεύτερο κεφάλαιο της εργασίας, επεξεργάζεται την έννοια της ιδιωτικότητας μέσα από τη νέα τάξη πραγμάτων που έφερε η αλματώδης εξέλιξη της τεχνολογίας και η μετάβαση στην εποχή των Μεγάλων Δεδομένων. Μέσα σε ένα τέτοιο πλαίσιο, αρχικά καθορίζεται η έννοια της ιδιωτικότητας στην καθημερινή ζωή έτσι ώστε εν συνεχεία να λάβει χώρα η ανάλυση της έννοιας της ιδιωτικότητας με κύρια βάση στην ψηφιακή παράμετρο, προκειμένου ο αναγνώστης να μπορεί να κατανοήσει τις διαφορές που επέφερε η μετάβαση στην ψηφιακή εποχή. Το επόμενο βήμα αποτελεί η καταγραφή των προσεγγίσεων για

την ιδιωτικότητα στην Αμερική και στην Ευρώπη, ενώ εν συνεχεία λαμβάνει χώρα μια γενική καταγραφή των διαφορετικών πτυχών προσέγγισης της έννοιας της ιδιωτικότητας που απαντώνται σήμερα στο παγκόσμιο κοινωνικό γίγνεσθαι. Το πέμπτο κύριο χωρίο του εν λόγω κεφαλαίου, καταδεικνύει με βάση την πρότερη ανάλυση την ανάγκη για την ύπαρξη μιας παγκόσμιας νομοθεσίας για την προστασία της ιδιωτικότητας, ενώ το έκτο και τελευταίο χωρίο αποτελεί την τελική απομάστευση για το πώς τελικά μεταφράζεται η έννοια της ιδιωτικότητας στη σημερινή ψηφιακή εποχή.

Το τρίτο κεφάλαιο της εργασίας, αποτελεί μια επισκόπηση των ρυθμιστικών αρχών και πλαισίων δράσης που απαντώνται σήμερα ανά τον κόσμο σε σχέση με την προστασία της ιδιωτικότητας των πληροφοριών, εστιάζοντας κύρια στο ρυθμιστικό πλαίσιο που χαρακτηρίζει την Ευρωπαϊκή Ένωση. Κατά τη διάρθρωση του εν λόγω κεφαλαίου, αρχικά λαμβάνει χώρα μια ιστορική αναδρομή του “ψηφιακού” ρυθμιστικού πλαισίου, ενώ εν συνεχεία αναλύονται τα σημαντικότερα ρυθμιστικά μοντέλα προστασίας της ιδιωτικότητας που απαντώνται σήμερα ανά τον κόσμο. Ακολουθεί μια εκτενής αναφορά στα ρυθμιστικά μοντέλα που χαρακτηρίζουν σήμερα την Ευρώπη και την Αμερική, με κύρια εστίαση στον ευρωπαϊκό χώρο, ενώ τέλος λαμβάνει χώρα μια επισκόπηση των ρυθμιστικών μοντέλων που απαντώνται σήμερα στις διάφορες περιοχές και χώρες ανά τον κόσμο και αφορούν στην προστασία της ιδιωτικότητας των πληροφοριών και των προσωπικών δεδομένων.

ΚΕΦΑΛΑΙΟ 1

ΤΙ ΕΙΝΑΙ ΤΑ ΜΕΓΑΛΑ ΔΕΔΟΜΕΝΑ

1.1 ΓΕΝΙΚΑ

Στο πρώτο κεφάλαιο, λαμβάνει χώρα μια ανάλυση της έννοιας των Μεγάλων Δεδομένων, ενώ ταυτόχρονα καταγράφονται τα βασικά χαρακτηριστικά αυτών καθώς και οι περιπτώσεις που απαντάται κύρια η χρήση τους.

Πιο συγκεκριμένα, στο πρώτο κύριο χωρίο του κεφαλαίου περιγράφεται η έννοια των Μεγάλων Δεδομένων στο σημερινό παγκόσμιο γίνεσθαι, ενώ στο δεύτερο κύριο χωρίο γίνεται εκτενής αναφορά στα τρία κύρια χαρακτηριστικά που περιγράφουν τις εφαρμογές Μεγάλων Δεδομένων σήμερα, τα οποία είναι ο όγκος, η ποικιλία και η ταχύτητα. Κατά την περιγραφή της συνιστώσας του όγκου, μεγάλη σημασία δίδεται στην περιγραφή του φαινομένου της τυφλής ζώνης.

Τέλος, στο τρίτο και τελευταίο κύριο χωρίο του κεφαλαίου, γίνεται εκτενής αναφορά στις σημαντικότερες περιπτώσεις στις οποίες λαμβάνει χώρα σήμερα η χρήση εφαρμογών Μεγάλων Δεδομένων.

1.2 ΤΑ BIG DATA ΣΗΜΕΡΑ

Από τις παραστάσεις και τεχνολογικές δράσεις που διακρίνει κάθε άνθρωπος γύρω του καθημερινά, είναι προφανές ότι σήμερα βιώνουμε μια περίοδο που η έννοια και οι εφαρμογές των Μεγάλων Δεδομένων βρίσκονται σε πλήρη ισχύ και εφαρμογή.

Πιο συγκεκριμένα, μέσω της χρήσης κατάλληλων οργάνων (instrumentation) είμαστε σε θέση σήμερα να “επικοινωνήσουμε” με περισσότερα πράγματα και σε μεγαλύτερο εύρος, με αποτέλεσμα να υπάρχει και η δυνατότητα για αποθήκευση μεγαλύτερου εύρους δεδομένων όπως αυτή ανακύπτει από την δυνατότητα για επεξεργασία μεγαλύτερου όγκου πρώτης ύλης.

Επιπρόσθετα, μέσω της αυξημένης δυνατότητας για επικοινωνία μέσω της ανάπτυξης των αντίστοιχων τεχνολογιών, οι άνθρωποι και οι πληροφορίες σήμερα είναι δυνατό να βρίσκονται σε πλήρη και συνεχή διασύνδεση (interconnection) και διάδραση (interaction) .

Υπό αυτό το πρίσμα, έχουμε πλέον φτάσει σε μια δυνατότητα για διασυνδεσιμότητα τύπου Machine to Machine, με τη διασύνδεση να παρουσιάζει χαρακτηριστικά διασύνδεσης όμοια με αυτά δύο τυποποιημένων μηχανών, δηλαδή, συνέχεια, αυξημένη διακίνηση πληροφορίας και αυξημένη δυνατότητα για ανάδραση. Αυτή η δυνατότητα άλλωστε είναι υπεύθυνη για τα γεωμετρικώς αυξανόμενα ποσοστά αποθήκευσης που παρατηρούνται κάθε χρόνο όσον αφορά στα δεδομένα και κυρίως στα ψηφιακά δεδομένα.

Προχωρώντας ένα βήμα πιο πέρα, με την αλματώδη ανάπτυξη της τεχνολογίας που έχει επιτελεστεί, πλέον υπάρχει δυνατότητα για αγορά σημαντικών διατάξεων που σχετίζονται άμεσα με εφαρμογές διακίνησης και ανταλλαγής πληροφοριών, με εξέχουσες τα ολοκληρωμένα κυκλώματα, σε πολύ χαμηλές τιμές.

Αυτή η παράμετρος δίνει τη δυνατότητα να προστεθεί η έννοια της ευφυΐας σχεδόν σε κάθε εφαρμογή και δράση, με επακόλουθο να βελτιστοποιείται ακόμη περισσότερο η διαδικασία της ανταλλαγής και αποθήκευσης πληροφοριών και δεδομένων.

Με βάση την παραπάνω παρατήρηση, καταλήγουμε στη βασική διαπίστωση η οποία καθορίζει σήμερα την έννοια των Μεγάλων Δεδομένων στις παγκόσμιες εφαρμογές και δράσεις. Σύμφωνα με αυτή, στο σημερινό παγκόσμιο γίγνεσθαι, παρατηρούμε συνεχείς ενέργειες και αλληλεπιδράσεις στους διάφορους τομείς της ανθρώπινης δραστηριότητας, όπου η ταχύτητα ανταλλαγής πληροφοριών και δεδομένων, ο όγκος αυτών των ποσοτήτων, καθώς και η ποικιλία που τις χαρακτηρίζει, καθορίζουν σήμερα το βαθμό συνθετότητας και τις παραμέτρους της έννοιας των Μεγάλων Δεδομένων.

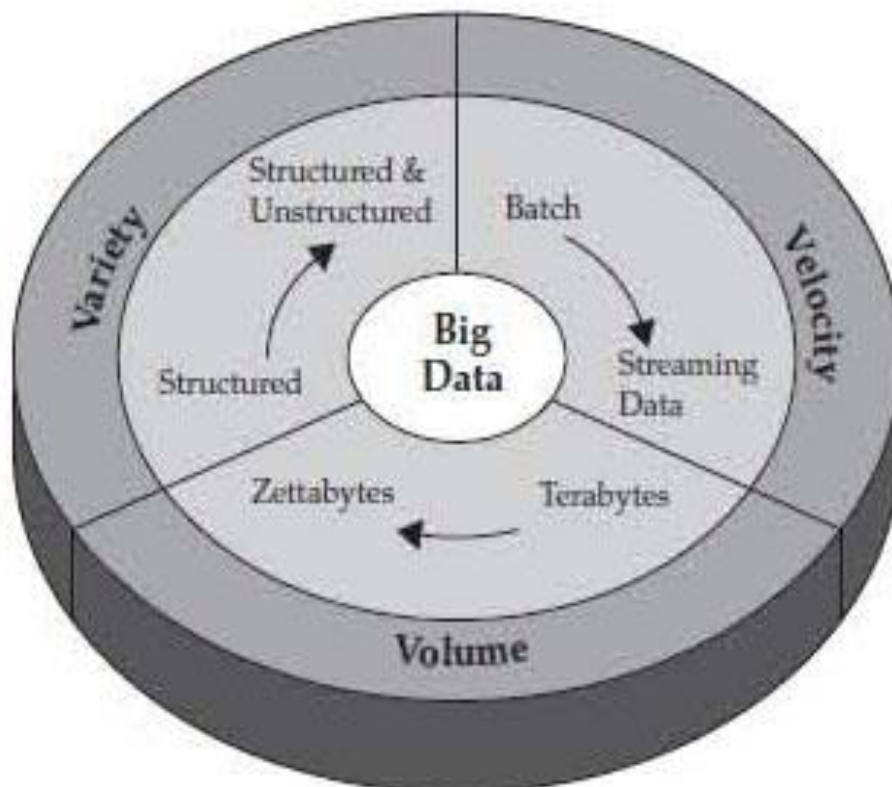
\

1.3 ΤΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΩΝ BIG DATA

Εν γένει, τρία είναι τα βασικά γνωρίσματα που χαρακτηρίζουν τα Μεγάλα Δεδομένα και τις ιδιαίτερες πτυχές και προεκτάσεις αυτών σε μια εφαρμογή. Αυτά τα γνωρίσματα είναι ο όγκος, η ποικιλία και η ταχύτητα.

Η συγκεκριμένη ομάδα χαρακτηριστικών αποτελεί σήμερα το κύριο κριτήριο για την επιλογή και τον χαρακτηρισμό δράσεων που σχετίζονται με Μεγάλα Δεδομένα στα διάφορα τεχνολογικά και οικονομικά πεδία, ενώ η ορθή επιλογή των εν λόγω χαρακτηριστικών, καθορίζει σε μεγάλο βαθμό και τα αποτελέσματα καθώς και το βαθμό επιτυχίας των αντίστοιχων εγχειρημάτων.

Από τα παραπάνω, εύκολα αντιλαμβάνεται κανείς τον σημαίνοντα ρόλο των εννοιών του όγκου, της ποικιλίας και της ταχύτητας των δεδομένων στο σημερινό ψηφιακό γίγνεσθαι.



Σχήμα 1.1 Βασικά χαρακτηριστικά των Μεγάλων Δεδομένων.

Θα προχωρήσουμε τώρα ξεχωριστά στην ανάλυση καθενός από αυτά τα χαρακτηριστικά γνωρίσματα που καθορίζουν τη δυναμικότητα των Μεγάλων Δεδομένων.

1.3.1 Όγκος των δεδομένων

Ο όγκος των δεδομένων που αποθηκεύονται σήμερα αυξάνεται αλματωδώς και καθημερινά. Προκειμένου να συνειδητοποιήσουμε αυτή την αλματώδη αύξηση που λαμβάνει χώρα, ενδεικτικά μπορεί να αναφερθεί ότι το έτος 2000 ο όγκος των δεδομένων που αποθηκεύτηκαν ανέρχονταν στα 800.000 petabytes, όταν το έτος 2020 ο αντίστοιχος όγκος αναμένεται να ανέλθει στα 35 zetabytes. Βέβαια, στο σημείο αυτό θα πρέπει να αναφερθεί ότι, από τον τεράστιο αυτό όγκο διακίνησης δεδομένων, δεν είναι δυνατό να αναλυθούν και να επεξεργαστούν όλες οι πληροφορίες που περιλαμβάνονται σε αυτά, γεγονός το οποίο αποτελεί ένα σημαντικό πρόβλημα όσον αφορά στο πεδίο των Μεγάλων Δεδομένων.

Σε ένα περιβάλλον δράσης, όπου είναι δυνατό να αποθηκευτούν και να αποκωδικοποιηθούν πληροφοριακά σχεδόν τα πάντα, από ατομικές πληροφορίες μικρότερης σημασίας μέχρι περιβαλλοντικά δεδομένα, οικονομικά δεδομένα, ιατρικά δεδομένα και δεδομένα κατασκοπείας τα οποία μπορεί να είναι αυξημένης βαρύτητας και σε μερικές περιπτώσεις να καθορίζουν σημαντικές πολιτικές, οικονομικές και περιβαλλοντικές ισορροπίες σε παγκόσμιο επίπεδο, η εξόρυξη από ένα πλήθος πληροφοριών, των πιο σημαντικών εξ’ αυτών και η μείωση του ρίσκου να χαθεί μια πληροφορία που μπορεί να είναι πολύ σημαντική, αποτελούν μια παρά πολύ σημαντική συνιστώσα προς επισήμανση.

Προχωρώντας ένα βήμα πιο πέρα προς αυτή την κατεύθυνση, όπως συνάγεται από τον όρο "Big Data", οι οργανισμοί και οι εταιρίες σήμερα έχουν να διαχειριστούν τεράστιες ποσότητες δεδομένων και πληροφοριών, με αποτέλεσμα οργανισμοί και εταιρίες που δεν ξέρουν πώς να διαχειριστούν αυτά τα δεδομένα να πρέπει να αναζητήσουν άμεσα τρόπους να ξεπεράσουν αυτή την πολύ σημαντική δυσκολία, η οποία μπορεί να έχει σημαντικές επιπτώσεις στη συνολική τους αποδοτικότητα, παραγωγικότητα και κερδοφορία μέσα σε ένα άκρως ανταγωνιστικό περιβάλλον δράσης.

Σε αντίθετη περίπτωση και λαμβάνοντας υπόψη ότι η ποσότητα των πληροφοριών και δεδομένων που έχει να διαχειριστεί η εταιρία αυξάνεται αλματωδώς, ενώ ταυτόχρονα το ποσοστό των δεδομένων που μπορεί να κατανοήσει, να αναλύσει και να επεξεργαστεί μειώνεται, οδηγούμαστε στη δημιουργία και κλιμάκωση του φαινομένου της τυφλής ζώνης.

Σύμφωνα με το εν λόγω φαινόμενο, αυξάνεται το εύρος των πληροφοριών που δεν επεξεργάζονται και αναλύονται, με αποτέλεσμα να αυξάνεται η πιθανότητα να χαθεί μια σημαντική πληροφορία ή δεδομένο που μπορεί να βρίσκεται εντός αυτού του εύρους, το οποίο αποκαλείται “τυφλή ζώνη”.

Σε ένα πλήρως ανταγωνιστικό περιβάλλον, όπου μια σημαντική πληροφορία που μπορεί να κρύβεται οπουδήποτε, είναι δυνατό να αποβεί εξόχως σημαντική και να προσδώσει ανταγωνιστικό πλεονέκτημα σε μια εταιρία στην αγορά δράσης της, αποτελεί παράμετρο μείζονος σημασίας για τους οργανισμούς και τις επιχειρήσεις η εξεύρεση τρόπων και λύσεων για την όσο το δυνατόν μεγαλύτερη μείωση του εύρους της τυφλής ζώνης.



Σχήμα 1.2 Φαινόμενο τυφλής ζώνης.

1.3.2 Ποικιλία των δεδομένων

Σύμφωνα με την ανάλυση που έλαβε χώρα στο προηγούμενο χωρίο του παρόντος συγγράμματος, ο όγκος πληροφοριών που σχετίζεται σήμερα με φαινόμενα ‘Big Data’ εμφανίζεται μεγαλύτερος παρά ποτέ. Το γεγονός αυτό σε συνδυασμό με την αλματώδη τεχνολογική εξέλιξη, οδηγεί σε νέες προκλήσεις που σχετίζονται κύρια με την έννοια της ποικιλίας των πληροφοριών που μπορεί κάποια αυτόνομη μονάδα ή κάποιος οργανισμός να αποθηκεύσει, να αναλύσει και να επεξεργαστεί σήμερα.

Με την εκτεταμένη πλέον χρήση παντός είδους αισθητήρων και έξυπνων συσκευών σε κάθε τεχνολογική δράση και ενέργεια, η επεξεργασία των δεδομένων έχει καταστεί πιο περίπλοκη διότι πλέον οι σχέσεις των δεδομένων αυτών δεν καθορίζονται με βάση τις παραδοσιακές νόρμες οι οποίες διακρίνονταν από μια αυξημένη ‘ομοιομορφία’, αλλά πλέον περιλαμβάνεται και πλήθος, πρωτογενών, ημιδομημένων αλλά και μη δομημένων δεδομένων που κυρίως η εξόρυξή τους γίνεται μέσω:

- Απλών ιστοσελίδων από το διαδίκτυο,
- Ιστοσελίδων όπου απαιτείται πρόσβαση,
- Καταλόγους αναζήτησης,
- Σελίδων κοινωνικής δικτύωσης
- Μηνυμάτων ηλεκτρονικού ταχυδρομείου
- Δεδομένων που προέρχονται από ενεργητικά και παθητικά συστήματα.

Οι συγκεκριμένες νέες κατηγορίες πληροφοριών διακρίνονται από μεγάλη ποικιλία και απαιτούν εκτεταμένη ανάλυση και επεξεργασία την οποία τα παλιά συμβατικά συστήματα δεν μπορούν να επιτελέσουν ή και στην περίπτωση που μπορούν, αυτό γίνεται ελλειμματικά και με κίνδυνο να αυξηθεί η τυφλή ζώνη.

Με βάση τα παραπάνω, η έννοια της ποικιλίας όσον αφορά στον τομέα των Μεγάλων Δεδομένων έγκειται κυρίως στην αλλαγή που έχει λάβει χώρα όσον αφορά στους τύπους των δεδομένων προς επεξεργασία που απαντώνται σήμερα και περιλαμβάνει όλους εκείνους τους τύπους δεδομένων και πληροφοριών –

πρωτογενείς, ημιδομημένες και μη δομημένες – οι οποίες απαιτούν διαφορετικές και πιο πολύπλοκες διαδικασίες για την επεξεργασία και ανάλυσή τους σε σχέση με αυτές που περιλαμβάνουν τα συμβατικά παραδοσιακά συστήματα.

Λαμβάνοντας υπόψη το γεγονός ότι η σημερινή διάχυση της πληροφορίας περιλαμβάνει σε ποσοστό κοντά στο 80% μη δομημένη ή στην καλύτερη περίπτωση δομημένη πληροφορία, με μεγάλο εύρος πληροφορίας να διαχέεται μέσω δεδομένων ήχου, εικόνας και μεταδεδομένων υψηλής ταχύτητας και ανομοιομορφίας, η υιοθέτηση σύγχρονων συστημάτων επεξεργασίας της πληροφορίας από το σύνολο των οργανισμών φαντάζει σήμερα αναγκαία και απαραίτητη για τη βιωσιμότητά τους.

Στο σημείο αυτό βέβαια θα πρέπει να αναφερθεί ότι ένας οργανισμός ή μια εταιρία για να μπορεί να ανταποκριθεί με τον καλύτερο δυνατό τρόπο στη διαχείριση των πληροφοριών και δεδομένων που πραγματεύεται, θα πρέπει να υιοθετεί ένα συνδυασμό παραδοσιακών και σύγχρονων συστημάτων έτσι ώστε να μπορεί να επεξεργαστεί παντός είδους πληροφορία ανεξάρτητα από τον τύπο ή την προέλευση της.

Με την υιοθέτηση αυτής της αρχής, μια εταιρία μπορεί να μειώσει την τυφλή της ζώνη που όπως ήδη έχει αναφερθεί, αποτελεί παράγοντα μείζονος σημασίας για την αποδοτικότητα μιας επιχείρησης ή ενός οργανισμού.

1.3.3 Ταχύτητα των δεδομένων

Όπως ακριβώς έχουν αλλάξει τα δεδομένα όσον αφορά στους δύο προηγούμενους παράγοντες, δηλαδή τον όγκο και την ταχύτητα, με την τεχνολογική εξέλιξη και τη διεύρυνση των διαδικτυακών δυνατοτήτων, κάτι ανάλογο ισχύει και με τον τρίτο παράγοντα χαρακτηρισμού των Μεγάλων Δεδομένων που δεν είναι άλλος από την ταχύτητα.

Η ταχύτητα, σύμφωνα με μια συμβατική διατύπωση που μπορεί να αποδοθεί όσον αφορά στη συγκεκριμένη συνιστώσα, είναι το μέγεθος μέσω του οποίου μπορεί να περιγραφεί το πόσο γρήγορα τα δεδομένα φθάνουν στο σημείο προορισμού τους

και αποθηκεύονται σε αυτά, καθώς και το πόσο γρήγορα τα δεδομένα αυτά μπορούν να ανακτηθούν. Στην πραγματικότητα βέβαια και όσον αφορά στο πεδίο των Μεγάλων Δεδομένων, η έννοια της ταχύτητας περιλαμβάνει σαφώς περισσότερες πτυχές και παράγοντες καθορισμού σε σχέση με αυτές που περιλαμβάνει η προηγούμενη συμβατική διατύπωση.

Οι ταχύτητες με τις οποίες διακινούνται σήμερα τα δεδομένα καθώς και ο αυξημένος όγκος αυτών, σε συνδυασμό με τη χρήση όλο και πιο εξελιγμένων μορφών αισθητήρων που οδηγούν σε ακόμα μεγαλύτερες δυνατότητες διάχυσης της πληροφορίας, έχουν καταστήσει ουσιαστικά σήμερα τα παραδοσιακά συστήματα διαχείρισης δεδομένων ανέκτα να τα διαχειριστούν επαρκώς και αποδοτικά.

Είναι γεγονός στο σημερινό επιχειρησιακό γίγνεσθαι, ότι μερικές φορές, το να εξασφαλίσει μια εταιρία ανταγωνιστικό πλεονέκτημα και να αυξήσει κατακόρυφα την αποδοτικότητά της, μπορεί να είναι θέμα μερικών δευτερολέπτων ή να απορρέει ως αποτέλεσμα του γεγονότος ότι μια εταιρία εξέλαβε και πραγματεύτηκε γρηγορότερα μια πληροφορία σε σχέση με τον ανταγωνισμό. Επιπρόσθετα, στη σημερινή πραγματικότητα, οι πληροφορίες, ακόμα και οι πιο σημαντικές, διακρίνονται από πολύ μικρό χρόνο ζωής.

Με βάση τις τελευταίες δύο παρατηρήσεις, είναι προφανής η τεράστια σημασία που έχει για τους φορείς σήμερα η ικανότητα να μπορούν να λαμβάνουν και να επεξεργάζονται τις πληροφορίες και τα δεδομένα γρήγορα και αποδοτικά. Μέσα σε ένα τέτοιο πλαίσιο, η αποτελεσματική διαχείριση των Μεγάλων Δεδομένων απαιτεί την επεξεργασία της τεράστιας ποικιλίας και όγκου αυτών, όχι μόνο όταν φτάνουν σε κατάσταση ηρεμίας, αλλά, αν είναι δυνατόν ακόμα και όταν αυτά βρίσκονται σε κίνηση.

1.4 ΠΕΡΙΠΤΩΣΕΙΣ ΧΡΗΣΗΣ ΤΩΝ BIG DATA

Εν γένει, σήμερα απαντώνται 6 κύριες χρήσεις όσον αφορά στα Μεγάλα Δεδομένα. Αυτές σχετίζονται με τα πεδία των:

- IT log analytics,
- της ανίχνευσης απάτης,
- των κοινωνικών δικτύων,
- της διασφάλισης της ποιότητας στα τηλεφωνικά κέντρα,
- των συστημάτων διαχείρισης ρίσκου και
- των συστημάτων ενέργειας.

1.4.1 IT log analytics

Το πεδίο των IT log analytics αποτελεί ένα σημαντικό πεδίο όσον αφορά στη χρήση των Μεγάλων Δεδομένων. Σε αυτή την περίπτωση, η αναφορά στην έννοια των Μεγάλων Δεδομένων έχει να κάνει κυρίως με τα δεδομένα που συσσωρεύονται ως “ρύποι” και προκύπτουν μετά την επεξεργασία των δεδομένων κύριου ενδιαφέροντος μέσω των εφαρμογών IT.

Οι εταιρίες εμφανίζουν καθημερινά σημαντική ποσότητα τέτοιου τύπου δεδομένων, με τις περισσότερες εξ’ αυτών να θεωρούν αυτά τα δεδομένα ανάξια χρήσης και να προχωρούν στην άμεση διαγραφή τους, θεωρώντας ότι η περαιτέρω αποθήκευσή τους αποτελεί σπατάλη αποθηκευτικού χώρου χωρίς ιδιαίτερο λόγο, ενώ η προσπάθεια για επεξεργασία τους αποτελεί μια οικονομικά και χρονικά απαιτητική διαδικασία που δε θα αποφέρει καμία σημαντική πληροφορία.

Η συγκεκριμένη ενέργεια, αποτελεί αποδεδειγμένα σήμερα μια λανθασμένη δράση μιας και η αξία των “ρύπων” μπορεί να είναι σε πολλές περιπτώσεις σημαντική ακόμα και όταν δεν είναι εμφανής με την πρώτη ματιά. Μέσα σε αυτή την πλειάδα δεδομένων που εκ πρώτης όψεως φαίνεται ότι στερείται χρησιμότητας, μπορεί να υπάρχει μια πληροφορία που σε μια μελλοντική περίπτωση, να απαντά σε ένα πολύ σημαντικό ζήτημα που έχει να αντιμετωπίσει μια εταιρία και να προσφέρει άμεσες λύσεις.

Εξαιτίας αυτού του γεγονότος, οι εταιρίες σήμερα αρχίζουν να κατανοούν όλο και περισσότερο την αξία των προς απόρριψη δεδομένων, με αποτέλεσμα να αναζητούν συνεχώς νέους τρόπους έτσι ώστε να αυξήσουν τη δυνατότητά τους για

αποθήκευση δεδομένων, καθώς και να βελτιστοποιήσουν τη δυνατότητα για ανάκτηση και επεξεργασία δεδομένων που έχουν αποθηκευτεί σε παρελθοντικό χρόνο, τόσο από οικονομική όσο και από χρονική σκοπιά.

Παράλληλα με αυτή την τάση, οι εταιρίες τεχνολογικής αιχμής, εκμαιεύοντας άμεσα αυτή τη νέα ροπή των εταιριών σε σχέση με την εκμετάλλευση των “ρύπων”, κινούνται προς την κατεύθυνση της δημιουργίας κατάλληλων συστημάτων αποθήκευσης και επεξεργασίας αυτού του είδους δεδομένων.

1.4.2 Ανίχνευση απάτης

Στο σημερινό γίγνεσθαι, εΐθισται η έννοια της απάτης να συνδέεται συνήθως με συναλλαγές οικονομικού περιεχομένου, αλλά στην πραγματικότητα φαινόμενα απάτης μπορούν να απαντηθούν σε πλήθος τομέων της ανθρώπινης δραστηριότητας όπως στις διαδικτυακές συναλλαγές και δημοπρασίες, σε ασφαλιστικές απαιτήσεις κ.α. Η χρήση εφαρμογών Μεγάλων Δεδομένων μπορούν να μειώσουν αισθητά την ύπαρξη τέτοιων φαινομένων στις διάφορες συναλλαγές και δράσεις.

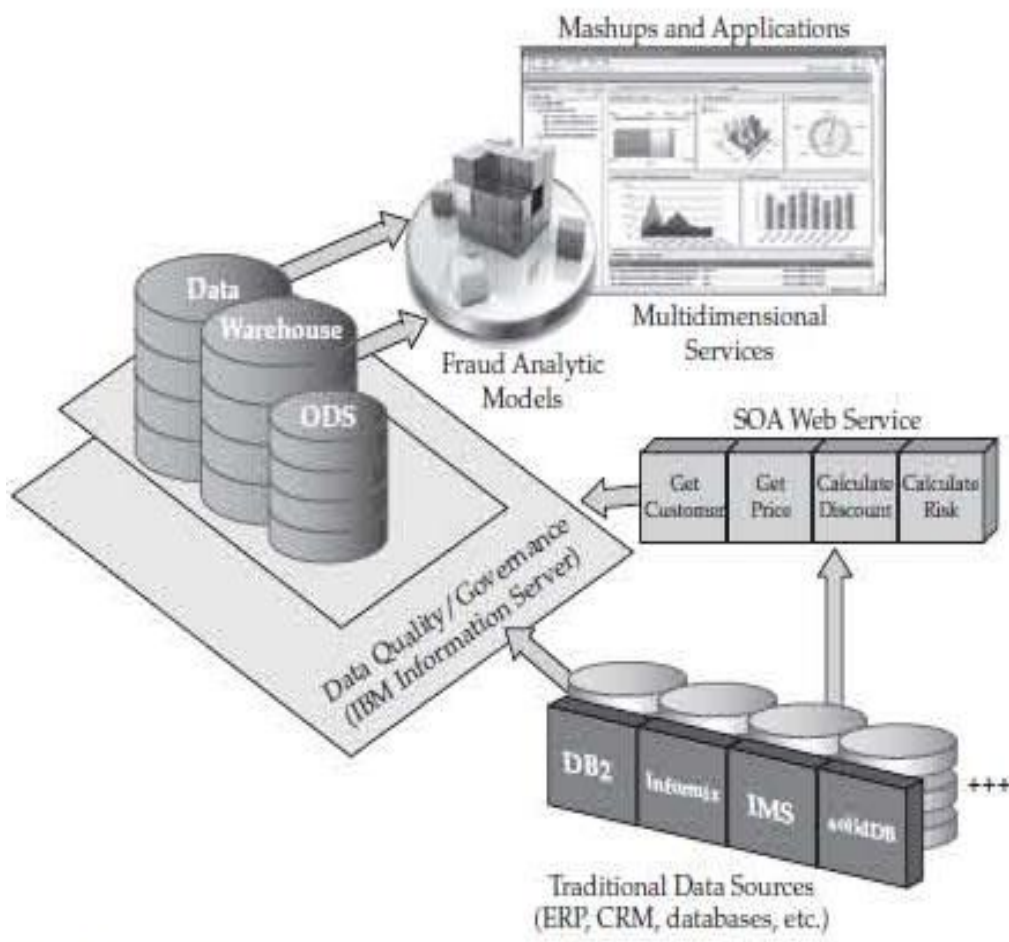
Μέχρι σήμερα, η προσπάθεια για αντιμετώπιση φαινομένων απάτης στηρίζεται σχεδόν αποκλειστικά σε συμβατικά συστήματα επεξεργασίας δεδομένων τα οποία όμως παρουσιάζουν σημαντικούς περιορισμούς όσον αφορά στη δυνατότητα για αποθήκευση και γρήγορη επεξεργασία δεδομένων, με αποτέλεσμα, τις περισσότερες φορές τα φαινόμενα απάτης να μην γίνονται αντιληπτά ή να γίνονται αντιληπτά με σημαντική καθυστέρηση.

Ενδεικτικά, η πλειοψηφία των παραδοσιακών συστημάτων μπορεί να επεξεργαστεί περίπου το 20% της διακινούμενης πληροφορίας, με αποτέλεσμα, η διάδοση φαινομένων απάτης να έχει ένα σημαντικό εύρος ‘ανεπεξεργαστης’ πληροφορίας για να κινηθεί.

Με βάση την παραπάνω παρατήρηση, εύκολα αντιλαμβάνεται κανείς, ότι τα παραδοσιακά συστήματα για την αντιμετώπιση της απάτης λειτουργούν περισσότερο δειγματοληπτικά και με συγκεκριμένους αλγόριθμους, με αποτέλεσμα κάποιος

κυβερνοεγκληματίας αυξημένων δυνατοτήτων, να μπορεί εύκολα να βρει τρόπους να αποφεύγει αυτές τις ελεγκτικές δράσεις.

Η παραπάνω διαπίστωση καταγράφει με τον πιο περιεκτικό τρόπο την αδυναμία των παραδοσιακών συστημάτων να αντιμετωπίσουν τα φαινόμενα της ηλεκτρονικής απάτης σήμερα και καταδεικνύει με τον πιο εμφανή τρόπο την ανάγκη εισαγωγής των εφαρμογών των Μεγάλων Δεδομένων στην αντιμετώπιση αυτού του είδους απάτης.

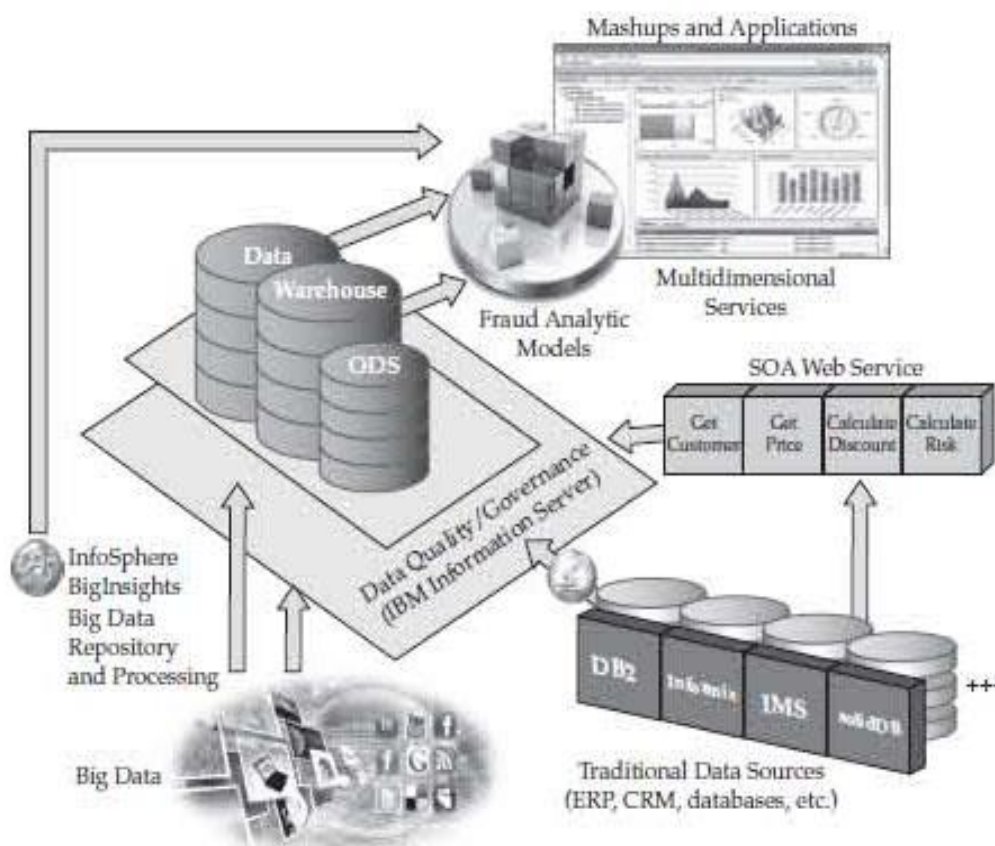


Σχήμα 1.3. Παραδοσιακά συστήματα ανίχνευσης απάτης.

Η χρήση εφαρμογών και συστημάτων Μεγάλων Δεδομένων, μπορεί να βοηθήσει ουσιαστικά προς αυτή την κατεύθυνση, εξαιτίας της αυξημένης δυνατότητας που αυτά παρουσιάζουν σε σχέση με τη συνιστώσα της μοντελοποίησης και επεξεργασίας δεδομένων. Στην περίπτωση αυτών των συστημάτων, μπορεί να επεξεργαστεί ένα ποσοστό κοντά στο 80 % των δεδομένων που διακινούνται, ενώ

λόγω των συνδυασμένων λειτουργικών δυνατοτήτων που παρουσιάζουν, λαμβάνει χώρα μια πολυδιάστατη – και όχι μονοδιάστατη όπως στη περίπτωση των συμβατικών συστημάτων – διαδικασία για την ανίχνευση της απάτης.

Κατά τη διαδικασία αυτή, δεν αφήνεται κανένα είδος πληροφορίας να ξεφύγει χωρίς έλεγχο, ενώ επιπρόσθετα, δεδομένα και πληροφορίες που εμφανίζονται ως ‘ύποπτες’ μέσω μιας διαδικασίας ανάδρασης επιστρέφουν στο σημείο ελέγχου προκειμένου να ελεγχθούν ξανά. Υπό αυτό το πρίσμα, η πιθανότητα για ανίχνευση πιθανής απάτης αυξάνεται σημαντικά.



Σχήμα 1.4. Συστήματα ανίχνευσης απάτης με τη χρήση εφαρμογών Μεγάλων Δεδομένων.

1.4.3 Κοινωνικά δίκτυα

Σε μια περίοδο όπου η κυριαρχία των κοινωνικών δικτύων δεν μπορεί να αμφισβητηθεί από κανέναν, είναι προφανές ότι τα Μεγάλα Δεδομένα και οι εφαρμογές αυτών, διαδραματίζουν σημαντικό ρόλο στο συγκεκριμένο πεδίο συναλλαγής τεράστιου και συνεχούς όγκου πληροφοριών και δεδομένων.

Η κυριότερη εφαρμογή των δυνατοτήτων των Μεγάλων Δεδομένων σήμερα όσον αφορά στα κοινωνικά δίκτυα, έγκειται στον τομέα της πώλησης. Υπό αυτό το πρίσμα, εταιρίες κατά κύριο λόγο εξαιτίας της μεγαλύτερης οικονομικής δυνατότητας που παρουσιάζουν σε σχέση με τους μεμονωμένους χρήστες, χρησιμοποιούν συστήματα Μεγάλων Δεδομένων, τα οποία λόγω της συνδυαστικής δυνατότητας για επεξεργασία και ανάλυση των πληροφοριών που παρουσιάζουν, παρέχουν πληροφορίες σε αυτές σε σχέση με τις ανάγκες των καταναλωτών (μέσω της παρακολούθησης για παράδειγμα των ιστοσελίδων που επισκέπτονται). Έτσι, οι εταιρίες μπορούν πιο εύκολα και στοχευόμενα να καθορίσουν τη στρατηγική προώθησης των προϊόντων τους με βάση τις λαμβανόμενες πληροφορίες.

Και το σημαντικότερο, οι πληροφορίες που διακινούνται στα κοινωνικά δίκτυα, αποτελούν πληροφορίες χωρίς φίλτρα και επεξεργασία, με αποτέλεσμα να παρέχουν επακριβώς το σφυγμό και τις ανάγκες των χρηστών / καταναλωτών.

1.4.4 Διασφάλιση της ποιότητας σε τηλεφωνικά κέντρα

Η χρήση εφαρμογών Μεγάλων Δεδομένων έχει συντελέσει και συνεχίζει να συντελεί στη βελτίωση της αποδοτικότητας και δυνατότητας για ανάκτηση δεδομένων όσον αφορά στην περίπτωση των τηλεφωνικών κέντρων.

Σε μια εποχή όπου συνεχώς και καθημερινά το σύνολο των πολιτών δέχεται κλήσεις από τηλεφωνικά κέντρα διαφόρων εταιριών παροχής υπηρεσιών και προϊόντων, με την ανταλλαγή πληροφοριών να είναι συνεχής και ογκώδης, είναι σύνηθες φαινόμενο να εμφανίζονται φαινόμενα δυσαρέσκειας κυρίως από την πλευρά των καταναλωτών είτε ως προς τον τρόπο προώθησης, είτε ως προς την κάλυψη των παραμέτρων τυχόν συμφωνίας.

Η δυνατότητα που προσφέρουν τα Μεγάλα Δεδομένα για μεγαλύτερο χρόνο αποθήκευσης των πληροφοριών και για ευκολότερη ανάκτηση και γρηγορότερη επεξεργασία αυτών, αποτελεί σήμερα τη βάση επίλυσης συγκεκριμένων τύπων διαφορών.

1.4.5 Συστήματα διαχείρισης ρίσκου

Η διαχείριση του κινδύνου αποτέλεσε και αποτελεί ένα από τα σημαντικότερα ζητήματα που καλούνται να αντιμετωπίσουν οι ανά τον κόσμο επιχειρήσεις και οργανισμοί. Η υιοθέτηση κατάλληλων συστημάτων και δράσεων στο πεδίο της διαχείρισης κινδύνου, μπορεί να αποδειχθεί πολλές φορές σημαντική ακόμα και για την ίδια τη βιωσιμότητα μιας εταιρίας σε ένα πλήρως ανταγωνιστικό περιβάλλον.

Όπως αναφέρθηκε και στη περίπτωση της ανίχνευσης απάτης, τα παραδοσιακά συστήματα επεξεργασίας δεδομένων μπορούν να επεξεργαστούν ένα ποσοστό μέχρι 20% της διακινούμενης πληροφορίας. Στην περίπτωση της διαχείρισης κινδύνου, που αποτελεί ένα ιδιαίτερα απαιτητικό πεδίο, είναι προφανές ότι τα παραδοσιακά συστήματα δεν μπορούν να λάβουν υπόψη όλους εκείνους τους παράγοντες και συνιστώσες, και επιπρόσθετα να προβούν στους απαραίτητους συνδυασμούς, προκειμένου να παράσχουν ικανοποιητικά αποτελέσματα στο πεδίο αυτό.

Με βάση την παραπάνω παρατήρηση, εύκολα αντιλαμβάνεται κανείς ότι η διαχείριση κινδύνου στο πλαίσιο εταιριών και οργανισμών αποτελεί ένα κλασικό παράδειγμα εφαρμογής Μεγάλων Δεδομένων, λόγω του πολύ μεγάλου και πολυεπίπεδου όγκου πληροφοριών που πρέπει να ληφθούν υπόψη – για παράδειγμα, ένα οικονομικό γεγονός στην Κίνα, μπορεί να επηρεάσει μια εταιρία στην Ελλάδα, οπότε πρέπει να ληφθεί υπόψη – και της πολυδιάστατης ανάλυσης που πρέπει να λάβει χώρα.

1.4.6 Συστήματα ενέργειας

Ο τομέας της ενέργειας αποτελεί κατεξοχήν πεδίο εφαρμογής των Μεγάλων Δεδομένων ένεκα του πλήθους των δεδομένων και πληροφοριών που διακινούνται στα διάφορα συστήματα ενέργειας, εξαιτίας του μεγάλου όγκου αισθητήρων που αυτά φέρουν.

Για παράδειγμα, μια τυπική πλατφόρμα γεώτρησης πετρελαίου μπορεί να φέρει από 20.000 έως 40.000 αισθητήρες ανάλογα με τον τύπο και τη δυναμικότητά

της. Το γεγονός αυτό, καταδεικνύει από μόνο του τον τεράστιο όγκο δεδομένων μέσω σημάτων που διακινούνται από αυτούς τους αισθητήρες. Εύκολα λοιπόν μπορεί να συμπεράνει κανείς, το βαθμό που θα μπορούσε να βελτιστοποιήσει τη λειτουργία και την αποδοτικότητα μιας τέτοιας πλατφόρμας, η ύπαρξη ενός συστήματος διαχείρισης πληροφοριών Μεγάλων Δεδομένων, όπου η δυνατότητα επεξεργασίας και ανάλυσης θα ήταν τέσσερις φορές μεγαλύτερη (80% έναντι 20%) από αυτή που ισχύει για τα συμβατικά συστήματα.

Είναι προφανές, πως η διαπίστωση αυτή μπορεί να επεκταθεί για ένα οποιοδήποτε σύστημα ενέργειας.

Προχωρώντας ένα βήμα πιο πέρα, τα συστήματα Μεγάλων Δεδομένων μπορούν να δώσουν σημαντικές λύσεις και όσον αφορά στην παράμετρο του θορύβου, η οποία αποτελεί μια πολύ σημαντική συνιστώσα για αυτά τα συστήματα και απαιτεί προσεκτική διαχείριση.

Η αυξημένη δυνατότητα διαχείρισης που παρουσιάζουν τα συστήματα Μεγάλων Δεδομένων, είναι λογικό να επιφέρει και αυξημένες δυνατότητες διαχωρισμού, με αποτέλεσμα να παράγονται σήματα υψηλότερης ποιότητας, αφού επιτυγχάνεται καλύτερος διαχωρισμός αυτών από τις προσμίξεις θορύβου.

Τέλος, η χρήση συστημάτων Μεγάλων Δεδομένων, μπορεί να βελτιώσει γεωμετρικά την απόδοση συστημάτων σχετιζόμενων με εναλλακτικές πηγές ενέργειας, οι οποίες αποτελούν σήμερα την πιο ελπιδοφόρα μορφή ενέργειας η οποία εξασφαλίζει προστασία του περιβάλλοντος με ταυτόχρονη αυξημένη απόδοση ενέργειας.

Η σημαντικότερη εφαρμογή σε αυτή την περίπτωση, μπορεί να λάβει χώρα στον τομέα των ανεμογεννητριών, μιας και εκεί απαιτείται συνδυαστική χρήση πολλών παραμέτρων για τη βέλτιστη λειτουργία της, όπως η θερμοκρασία, η καθίζηση, η ταχύτητα του αέρα, η υγρασία, η ατμοσφαιρική πίεση και η μεταβολή των ειδικών παραμέτρων και χαρακτηριστικών της περιοχής τοποθέτησης. Τα συμβατικά συστήματα μπορεί να ανταποκρίνονται σήμερα σε τέτοιες κατασκευές,

αλλά σε καμία περίπτωση δεν προσφέρουν τη βελτιστοποίηση που μπορεί να προσφέρει ένα σύστημα Μεγάλων Δεδομένων.

ΚΕΦΑΛΑΙΟ 2

ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

2.1 ΓΕΝΙΚΑ

Το δεύτερο κεφάλαιο της εργασίας, επεξεργάζεται την έννοια της ιδιωτικότητας μέσα από τη νέα τάξη πραγμάτων που έφερε η αλματώδης εξέλιξη της τεχνολογίας και η μετάβαση στην εποχή των Μεγάλων Δεδομένων.

Μέσα σε ένα τέτοιο πλαίσιο, αρχικά καθορίζεται η έννοια της ιδιωτικότητας στην καθημερινή ζωή έτσι ώστε εν συνεχεία να λάβει χώρα η ανάλυση της έννοιας της ιδιωτικότητας με κύρια βάση στην ψηφιακή παράμετρο, προκειμένου ο αναγνώστης να μπορεί να κατανοήσει τις διαφορές που επέφερε η μετάβαση στην ψηφιακή εποχή.

Το επόμενο βήμα αποτελεί η καταγραφή των προσεγγίσεων για την ιδιωτικότητα στην Αμερική και στην Ευρώπη, ενώ εν συνεχεία λαμβάνει χώρα μια γενική καταγραφή των διαφορετικών πτυχών προσέγγισης της έννοιας της ιδιωτικότητας που απαντώνται σήμερα στο παγκόσμιο κοινωνικό γίγνεσθαι.

Το πέμπτο κύριο χωρίο του εν λόγω κεφαλαίου, καταδεικνύει με βάση την πρότερη ανάλυση την ανάγκη για την ύπαρξη μιας παγκόσμιας νομοθεσίας για την προστασία της ιδιωτικότητας, ενώ το έκτο και τελευταίο χωρίο αποτελεί την τελική απομάστευση για το πώς τελικά μεταφράζεται η έννοια της ιδιωτικότητας στη σημερινή ψηφιακή εποχή.

2.2 Η ΕΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΚΑΘΗΜΕΡΙΝΗ ΖΩΗ

Γενικά η έννοια της ιδιωτικότητας όσον αφορά στις καθημερινές δραστηριότητες και ενέργειες των ανθρώπων μπορεί να ταξινομηθεί σε τρεις κύριες κατηγορίες: στην ιδιωτικότητα των προσωπικών δεδομένων, στην ιδιωτικότητα της

διάχυσης των πληροφοριών σε σχέση με προσωπικά δεδομένα και στην ιδιωτικότητα των δεδομένων εταιριών και οργανισμών.

2.2.1 Ιδιωτικότητα των προσωπικών δεδομένων

Η συγκεκριμένη μορφή ιδιωτικότητας σχετίζεται με την εισβολή στα δεδομένα του ατόμου που έχουν να κάνουν με τη φυσική υπόσταση αυτού, τα υπάρχοντά του καθώς και τον προσωπικό του χώρο.

Στις περισσότερες χώρες σήμερα, η νομοθεσία προστατεύει σε μεγάλο βαθμό φαινόμενα όπως, η πραγματοποίηση παράνομων ερευνών στον προσωπικό χώρο των πολιτών, φαινόμενα κατασχέσεων καθώς και δράσεις που προσβάλουν εμφανώς την προσωπική υπόσταση και αξιοπρέπεια των πολιτών.

2.2.2 Ιδιωτικότητα της διάχυσης πληροφοριών σε σχέση με προσωπικά δεδομένα

Ο εν λόγω τύπος ιδιωτικότητας σχετίζεται με την αποτροπή φαινομένων διάχυσης προσωπικών ευαίσθητων πληροφοριών και δεδομένων των ατόμων οι οποίες για διάφορους λόγους, συλλέγονται και αποθηκεύονται σε διάφορες βάσεις δεδομένων (π.χ. ιατρικά δεδομένα ασθενών στις βάσεις δεδομένων των νοσοκομειακών ιδρυμάτων).

Και σε αυτή την περίπτωση, τα περισσότερα κράτη έχουν μεριμνήσει έτσι ώστε να απαγορεύεται σε σημαντικό βαθμό η διάχυση προσωπικών ευαίσθητων πληροφοριών που σχετίζονται κύρια με οικονομικά και ιατρικά δεδομένα των πολιτών, με σαφή προσανατολισμό την αποτροπή άσκοπης διάχυσης αυτών μέσω του διαδικτύου.

2.2.3 Ιδιωτικότητα των δεδομένων εταιριών και οργανισμών

Σε μια εποχή έντονου ανταγωνισμού στο επιχειρηματικό γίγνεσθαι, είναι προφανές ότι πολλές επιχειρήσεις ανά τον κόσμο θέλουν να κρατούν ενέργειες και πληροφορίες μυστικές από τον ανταγωνισμό, γιατί μπορεί αυτές να τους εξασφαλίζουν ή να δύναται να τους εξασφαλίσουν μελλοντικά ανταγωνιστικό πλεονέκτημα (για παράδειγμα τα χαρακτηριστικά μιας πατέντας ενός καινοτόμου

προϊόντος, ή η συνταγή ενός πολύ πετυχημένου προϊόντος, με χαρακτηριστικό παράδειγμα την Coca – Cola).

Σε αυτή την περίπτωση, η νομοθεσία δεν είναι τόσο εκτεταμένη όσο στην περίπτωση της διασφάλισης των προσωπικών δεδομένων, αλλά οι ίδιες οι εταιρίες, έχοντας ισχυρά νομικά τμήματα, κινούνται αποδοτικά με ίδιες δράσεις προς την κατεύθυνση της προστασίας των δεδομένων τους.

2.3 Η ΕΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

Εισάγοντας στις δράσεις της καθημερινής ζωής την έννοια της ψηφιοποίησης, με τις τεράστιες δυνατότητες που προσφέρει αυτή όσον αφορά κυρίως στη διάχυση των πληροφοριών, είναι προφανές ότι οι παραπάνω κατηγορίες ταξινόμησης της έννοιας της ιδιωτικότητας θα πρέπει να μεταβληθούν προκειμένου να μπορέσουν να περιλάβουν όλες εκείνες τις συνιστώσες που μπορεί να αποδειχτούν απειλητικές όσον αφορά στη διαφύλαξη της ιδιωτικότητας των προσωπικών δεδομένων.

Έτσι, με βάση την ψηφιακή παράμετρο, η έννοια της ιδιωτικότητας μπορεί να ταξινομηθεί στις εξής κατηγορίες:

- ιδιωτικότητα της επικοινωνίας,
- ιδιωτικότητα της συμπεριφοράς και
- προστασία της ανωνυμίας.

2.3.1 Ιδιωτικότητα της επικοινωνίας

Η πλειοψηφία των ατόμων σήμερα, θεωρεί πως η καθημερινή ανταλλαγή πληροφοριών μέσω e-mail, κινητών τηλεφώνων ή άλλων μέσων ανταλλαγής δεδομένων είναι ασφαλής, με αποτέλεσμα να προβαίνει σχεδόν απρόσκοπτα σε τέτοιου είδους ενέργειες.

Στην πραγματικότητα όμως η αλήθεια είναι λίγο διαφορετική. Η αλματώδης αύξηση της τεχνολογίας με τη δημιουργία συνεχώς εξελισσόμενων συσκευών συνεχούς παρακολούθησης, σε συνδυασμό με τις αμφιλεγόμενες πολιτικές

προστασίας του απορρήτου που υπάρχουν σήμερα, οδηγούν στο συμπέρασμα ότι το γεγονός ότι στην πλειοψηφία τους οι επικοινωνίες μεταξύ ατόμων δεν παρακολουθούνται, οφείλεται σε έλλειψη ενδιαφέροντος και όχι στη δυσκολία του εγχειρήματος για μια τέτοια παρακολούθηση.

Υπό αυτό το πρίσμα, η υιοθέτηση δράσεων για την προστασία της ιδιωτικότητας της επικοινωνίας από την πλευρά των νομοθετών κάθε κράτους, φαντάζει ως μια ενέργεια ουσιαστικά χωρίς ιδιαίτερη σημασία μιας και δεν μπορεί να οδηγήσει στην αποτροπή, με αποτέλεσμα, να εξαρτάται περισσότερο από το ίδιο το άτομο ο βαθμός στον οποίο αυτό μπορεί να προστατεύσει τον εαυτό του από φαινόμενα υποκλοπής προσωπικών δεδομένων μέσω των καθημερινών του επικοινωνιών (για παράδειγμα με την αποφυγή αποστολής προσωπικών δεδομένων όπως στοιχεία ταυτότητας ή ΑΦΜ μέσω ηλεκτρονικού ταχυδρομείου).

2.3.2 Ιδιωτικότητα της συμπεριφοράς

Μέχρι πριν λίγα χρόνια, η προσωπική συμπεριφορά και επιλογές σε σχέση με συνιστώσες όπως πως αρέσει σε ένα άτομο να διασκεδάζει, τι του αρέσει να αγοράζει κτλ. αποτελούσαν γνώση που κινούνταν στα στενά οικογενειακά και φιλικά πλαίσια.

Σήμερα, με τη συνεχή ανταλλαγή πληροφοριών που λαμβάνει χώρα μεταξύ ατόμων, μεταξύ ατόμων και ομάδων ατόμων, μεταξύ ατόμων και εταιριών κτλ. σε μια παγκόσμια ακτίνα μέσω του διαδικτύου, είναι κάτι παραπάνω από απλό για κάποιον που ενδιαφέρεται, να διαμορφώσει το καταναλωτικό προφίλ και το προφίλ συμπεριφοράς ατόμων ακόμα και αν δεν έχει έρθει ποτέ σε προσωπική επαφή με αυτά. Μια τέτοια δράση μπορεί να ενισχύσει κερδοσκοπικές επιδιώξεις από πλευράς πωλητών του διαδικτύου, αλλά ακόμα και να οδηγήσει σε παραβατικές δράσεις, όπου ομάδες ατόμων με παραβατική συμπεριφορά, μέσω του διαδικτύου ανιχνεύουν άτομα με όμοιες συμπεριφορές και καλούν αυτά να ενσωματωθούν στην ομάδα τους.

Και σε αυτή την περίπτωση, το άτομο είναι αυτό που μπορεί να προστατεύσει τον εαυτό του προκειμένου να αποφύγει καταστάσεις σαν τις προαναφερθείσες. Ο ρόλος του κράτους σε αυτή την περίπτωση μπορεί να είναι περισσότερο συμβουλευτικός και ενημερωτικός.

2.3.3 Προστασία της ανωνυμίας

Κάθε άτομο, ακόμα και αν καθημερινά υποβάλλεται σε μια συνεχή διαδικασία ανταλλαγής πληροφοριών μέσω του διαδικτύου και των μέσων κοινωνικής δικτύωσης, κατέχει το δικαίωμα για τη διατήρηση μιας σχετικής ανωνυμίας στην κοινωνία στην οποία δρα και παράγει.

Αυτή η διατήρηση της σχετικής ανωνυμίας στην ψηφιακή εποχή αποτελεί μια διαδικασία πιο δύσκολη από ποτέ μιας και φαινόμενα όπως, η ανάρτηση μίας φωτογραφίας σε ένα μέσο κοινωνικής δικτύωσης ή η καταγραφή μίας κίνησης από μια εφαρμογή εύρεσης τοποθεσιών ή μια κάμερα στο δρόμο, αποτελούν καθημερινές δράσεις που αντιστέκονται σθεναρά προς την κατεύθυνση της διατήρησης της προσωπικής ανωνυμίας.

Στη συγκεκριμένη περίπτωση, το άτομο μπορεί να προστατευτεί μόνο από ενέργειες που είναι ενήμερο (όπως η ανάρτηση μίας φωτογραφίας με ίδια ενέργεια σε ένα μέσο κοινωνικής δικτύωσης), σε καμία όμως περίπτωση δεν μπορεί να προστατευτεί από μια καταγραφή του προσώπου του για παράδειγμα από μια κάμερα τράπεζας ή μια κάμερα τροχαίας στο δρόμο.

Με βάση την ανάλυση που έλαβε χώρα στο συγκεκριμένο χωρίο, γεννάται το ερώτημα για το πώς η νομοθεσία και οι αρχές προστασίας προσωπικών δεδομένων μπορούν να προστατεύσουν σε μεγαλύτερο βαθμό πολίτες που δεν μπορούν από μόνοι τους να αντιληφτούν τους κινδύνους.

Η απάντηση σε αυτό το ερώτημα είναι ότι πέρα από τη δυσκολία ενός τέτοιου εγχειρήματος ένεκα της αδυναμίας για παρακολούθηση όλων των ενεργειών σε παγκόσμιο επίπεδο σε πραγματικό χρόνο, συναντάται και το εμπόδιο από τα ίδια τα άτομα, τα οποία επιζητούν μεν προστασία, αλλά σε καμία περίπτωση δε θέλουν να ‘θυσιάσουν’ ούτε στο ελάχιστο τις τεράστιες δυνατότητες για εργασία και ψυχαγωγία που απολαμβάνουν μέσω εφαρμογών όπως το ηλεκτρονικό ταχυδρομείο και τα μέσα κοινωνικής δικτύωσης.

2.4 Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗΝ ΑΜΕΡΙΚΗ ΚΑΙ ΣΤΗΝ ΕΥΡΩΠΗ

Η έννοια της ιδιωτικότητας και της προστασίας αυτής, αποτέλεσε και αποτελεί μια δυναμική και συνεχώς εξελισσόμενη έννοια που πρέπει να προσαρμόζεται στις ανάγκες της κάθε εποχής και στα χαρακτηριστικά αυτής.

Υπό αυτό το πρίσμα, τόσο στον αμερικάνικο όσο και στο ευρωπαϊκό χώρο, οι κυβερνήσεις των κρατών προσπαθούν συνεχώς προκειμένου να δημιουργούν ένα πλαίσιο δράσης και προστασίας της ιδιωτικότητας το οποίο θα συνάδει με τα ιδιαίτερα χαρακτηριστικά και τις ιδιαιτερότητες της κοινωνίας.

Η αλματώδης εξέλιξη της τεχνολογίας σε συνδυασμό με την τεράστια δυνατότητα για ανταλλαγή πληροφοριών ακόμα και σε πραγματικό χρόνο που προσφέρει αυτή, αποτελεί σήμερα τη σημαντικότερη συνιστώσα που πρέπει να ληφθεί υπόψη προκειμένου να καθοριστούν τα πλαίσια δράσης για την προστασία της ιδιωτικότητας των δεδομένων και των πληροφοριών των πολιτών.

2.4.1 Η ιδιωτικότητα στην Αμερική

Οι Ηνωμένες Πολιτείες Αμερικής, ανιχνεύοντας από πολύ νωρίς τις ανακατατάξεις που μπορεί να επιφέρει η ραγδαία αύξηση της τεχνολογίας και της δυνατότητας για άμεση ανταλλαγή πληροφοριών στο πεδίο της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων, άρχισαν ήδη να προβαίνουν σε ενέργειες προς αυτή την κατεύθυνση με την εμφάνιση των πρώτων τεχνολογιών αυτού του είδους.

Ήδη από το 1960, ο William Prosser, κορυφαίος νομικός της εποχής, καθόρισε τέσσερις νέους τύπους ιδιωτικότητας, έτσι ώστε να περιλάβει και την παράμετρο της διάχυσης της πληροφορίας και των επιπτώσεων που αυτή μπορεί να επιφέρει στην προστασία των προσωπικών δεδομένων. Οι τέσσερις αυτές κατηγορίες περιγράφονται από τις ακόλουθες καταστάσεις:

- Εισβολή στις προσωπικές υποθέσεις του ατόμου.
- Δημοσιοποίηση γεγονότων και καταστάσεων που μπορεί να φέρουν σε αμηχανία ή να προσβάλουν το άτομο.
- Δημοσιοποίηση πληροφοριών που δημιουργούν μια ψευδή – συνήθως αρνητική – δημόσια εικόνα για το άτομο στο οποίο αναφέρονται οι πληροφορίες.
- Εκμετάλλευση πληροφοριών που σχετίζονται με ένα άτομο για επίτευξη οφέλους από ένα άλλο άτομο ή ομάδα ατόμων, χωρίς τη συγκατάθεση αυτού.

Οι τέσσερις αυτές κατηγορίες ιδιωτικότητας που προς το παρόν σε μεγαλύτερο βαθμό από ποτέ περιλαμβάνουν την ψηφιακή παράμετρο, επικρατούν με μικρές παραλλαγές στις Ηνωμένες Πολιτείες μέχρι και σήμερα και είναι αυτές πάνω στις οποίες στηρίζεται το αμερικανικό δικαστικό σύστημα προκειμένου να καθορίσει το πλαίσιο δράσης του σε σχέση με την προστασία της ιδιωτικότητας.

Γενικά, το αμερικανικό δικαστικό σύστημα σε σχέση με τις παραμέτρους που περιλαμβάνει για την προστασία της ιδιωτικής ζωής στην ψηφιακή εποχή, θεωρείται ιδιαίτερα άκαμπτο και χωρίς ευελιξία με αποτέλεσμα να παρατηρούνται συνεχώς νέες νομοθετικές δράσεις για τη βελτίωση αυτής της συνιστώσας.

Χαρακτηριστικό παράδειγμα αποτελεί η προσφάτως εισαχθείσα νομοθεσία για την Προστασία των Προσωπικών Δεδομένων η οποία για πρώτη φορά καθορίζει σαφή όρια για τη χρήση και διάχυση προσωπικών πληροφοριών.

Παρόλες όμως τις προσπάθειες που γίνονται για αύξηση της ευελιξίας του αμερικανικού δικαστικού συστήματος σε σχέση με την προστασία της ιδιωτικότητας, το εν λόγω σύστημα μέχρι και σήμερα καθορίζει τις δράσεις του κυρίως με βάση σταθερές αξίες, όπως η αξία της διατήρησης ενός συστήματος ελεύθερης αγοράς, και ελευθερίες, όπως η ελευθερία της επιλογής των θρησκευτικών πεποιθήσεων και η ελευθερία της έκφρασης.

Υπό αυτό το πρίσμα, το σύστημα των ΗΠΑ ζυγίζει τα ζητήματα που αφορούν στην προστασία της ιδιωτικής ζωής μέσα από ένα φίλτρο ελευθερίας, με αποτέλεσμα ο περιορισμός των ομοσπονδιακών και πολιτειακών εξουσιών σε σχέση με το θέμα ενασχόλησης να είναι κάτι παραπάνω από ορατή.

2.4.2 Η ιδιωτικότητα στην Ευρώπη

Εν γένει, η έννοια της ιδιωτικότητας στον ευρωπαϊκό χώρο έγκειται στην ανάγκη για προστασία της ανθρώπινης τιμής και αξιοπρέπειας στη δημόσια σφαίρα και με βάση αυτή την επιταγή καθορίζονται όλα τα πλαίσια δράσεων για την προστασία της ιδιωτικότητας στα διάφορα κράτη ανά την Ευρώπη.

Η Ευρώπη δείχνει μια μικρότερη ανοχή στην ελευθερία διάχυσης προσωπικών πληροφοριών σε σχέση με την Αμερική, ενώ αναγνωρίζει σε απόλυτο βαθμό στο άτομο τη δυνατότητα να καθορίζει αυτό το εύρος και τον τύπο των πληροφοριών που θα διατίθενται προς διάχυση σε σχέση με αυτό.

Προχωρώντας ένα βήμα πιο πέρα, η ευρωπαϊκή νομοθεσία διακρίνεται από μεγάλη αυστηρότητα σε θέματα όπου μπορεί να απαντώνται ζητήματα προσβολής σχετιζόμενα με τις έννοιες της θρησκείας και της εθνικότητας. Υπό αυτό το πρίσμα, χώρες όπως η Γερμανία, η Αυστρία, το Βέλγιο, η Σουηδία, η Νορβηγία, η Γαλλία και η Βρετανία εμφανίζουν νομοθεσίες πάνω σε ζητήματα διάχυσης πληροφοριών με προσβλητικό περιεχόμενο για κάποιο άτομο ή για μια ομάδα ατόμων σε σχέση με τις συνιστώσες της θρησκείας και της εθνικότητας.

Με βάση την ευρωπαϊκή προσέγγιση, τα μέσα μαζικής ενημέρωσης και το διαδίκτυο μπορούν να θέσουν σε κίνδυνο τη δημόσια αξιοπρέπεια ενός ατόμου και επομένως θα πρέπει να καθορίζονται σαφή όρια δράσης αυτών, ενώ θα πρέπει να λαμβάνουν χώρα ενέργειες συγκράτησης όταν ξεπερνιούνται αυτά τα όρια.

Με βάση την ανάλυση που έλαβε χώρα σε σχέση με την ευρωπαϊκή και αμερικανική προσέγγιση πάνω στο ζήτημα της ιδιωτικότητας των προσωπικών

πληροφοριών, μπορούμε τώρα να προβούμε σε μια συγκριτική αποτίμηση των δύο αυτών προσεγγίσεων.

2.4.3 Σύγκριση προσεγγίσεων για την ιδιωτικότητα στον ευρωπαϊκό και στον αμερικάνικο χώρο

Όπως ήδη αναφέρθηκε, οι Ηνωμένες Πολιτείες Αμερικής διακρίνονται από μια μεγαλύτερη ελευθερία όσον αφορά στη δυνατότητα για διακίνηση προσωπικών πληροφοριών σε σχέση με τις ευρωπαϊκές χώρες.

Στο αμερικάνικο σύστημα, η προστασία της προσωπικής ελευθερίας αποτελεί την πρώτη προτεραιότητα, ακόμα και αν μερικές φορές το γεγονός αυτό μπορεί να οδηγήσει σε απώλεια της ιδιωτικότητας του ατόμου.

Από την άλλη, στο ευρωπαϊκό σύστημα, δίδεται πρώτη προτεραιότητα στην προστασία της ιδιωτικότητας των προσωπικών δεδομένων, με αποτέλεσμα να περιορίζεται αν κριθεί αναγκαίο ως ένα βαθμό η ελευθερία του ατόμου. προκειμένου να εξασφαλιστεί στο βέλτιστο δυνατό βαθμό αυτή η προστασία. Στο ευρωπαϊκό σύστημα, η προστασία των προσωπικών δεδομένων, είναι άμεσα συνυφασμένη με τις έννοιες της ανθρώπινης τιμής και αξιοπρέπειας, με αποτέλεσμα όλα τα πλαίσια δράσης να καθορίζονται με βάση αυτές τις δύο έννοιες.

Βέβαια, και στις δύο προσεγγίσεις, ξεκαθαρίζεται σαφώς ότι η ιδιωτικότητα των προσωπικών δεδομένων θα πρέπει να είναι απαραβίαστη, αλλά διαφέρει ο τρόπος με τον οποίο επιδιώκεται η εξασφάλιση αυτής της επιταγής.

Τα Μέσα Μαζικής Ενημέρωσης και ο τρόπος που δρουν αντίστοιχα στον ευρωπαϊκό και στο αμερικάνικο χώρο, καταδεικνύουν με τον πιο σαφή τρόπο τη διαφορετικότητα των προσεγγίσεων των δύο αυτών χώρων όσον αφορά στον τρόπο που εκλαμβάνουν την έννοια της ιδιωτικότητας του ατόμου. Υπό αυτό το πρίσμα, ένα αμερικάνικο τηλεοπτικό δίκτυο, μπορεί κάλλιστα και χωρίς ιδιαίτερους ενδοιασμούς να προβάλλει εικόνες και σκηνές ισχυρής βίας, χωρίς να λαμβάνει μέτρα προστασίας των προσωπικών δεδομένων των ατόμων (κάλυψη προσώπου κτλ.) που λαμβάνουν χώρα σε αυτές. Από την άλλη, στα ευρωπαϊκά δίκτυα, η προβολή τέτοιων

σκηνών γίνεται πάντα μετά από τη χρήση πολλαπλών φίλτρων και πάντα με την κάλυψη των προσωπικών δεδομένων των ατόμων που λαμβάνουν χώρα σε αυτές, στα πλαίσια της αυξημένης βάσης που δίνει το ευρωπαϊκό σύστημα σύμφωνα με τα προηγούμενα, στις έννοιες της ανθρώπινης αξιοπρέπειας και τιμής ακόμα και όταν το άτομο συμμετέχει σε κακουργηματικές πράξεις.

2.5 ΔΙΑΦΟΡΕΤΙΚΕΣ ΠΤΥΧΕΣ ΠΡΟΣΕΓΓΙΣΗΣ ΤΗΣ ΕΝΝΟΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Η προηγούμενη ανάλυση που έλαβε χώρα και κατέδειξε τη διαφορετικότητα με την οποία προσεγγίζεται η έννοια της ιδιωτικότητας στην ψηφιακή εποχή από τις Ηνωμένες Πολιτείες Αμερικής και τις ευρωπαϊκές χώρες, μπορεί να επεκταθεί ώστε να καταδείξει τις διαφορετικές πτυχές μέσα από τις οποίες διάφορες χώρες και περιοχές προσεγγίζουν την έννοια της ιδιωτικότητας, ακόμα και αν ο σκοπός είναι ίδιος και δεν είναι άλλος από την προστασία της ιδιωτικότητας του ατόμου και των προσωπικών πληροφοριών που σχετίζονται με αυτό, στο μέγιστο δυνατό βαθμό.

Οι επιρροές στον τρόπο προσέγγισης αλλά και στην προσδοκία για προστασία της ιδιωτικότητας εν γένει εξαρτώνται από παράγοντες όπως, η ιστορία της χώρας ή της περιοχής, ο πολιτισμός τους καθώς και οι κοινωνικές και ηθικές νόρμες που επικρατούν στην χώρα ή την περιοχή.

Μέσα σε ένα τέτοιο πλαίσιο, σε καταπιεστικά καθεστάτα όπως η Κίνα, η Ρωσία ή η Συρία οι κάτοικοι εμφανίζουν χαμηλότερες προσδοκίες σε σχέση με την προστασία της ιδιωτικής τους ζωής, ενώ σε πιο δημοκρατικά καθεστάτα οι προσδοκίες αυτές αυξάνουν με αποτέλεσμα το όλο σύστημα – κοινωνικό και πολιτικό – να κινούνται πιο σθεναρά προς αυτή την κατεύθυνση.

Με βάση την τελευταία παρατήρηση, είναι φανερό ότι ο τρόπος με τον οποίο μια περιοχή ή χώρα προσεγγίζει την έννοια της ιδιωτικότητας, καθώς και οι προσδοκίες των πολιτών για την προστασία της ιδιωτικότητάς τους, καθορίζουν σε μεγάλο βαθμό και τους νόμους και πολιτικές που θα ακολουθηθούν από την πλευρά της πολιτείας.

Ακόμα όμως και σήμερα, οι απόψεις για την έννοια της ιδιωτικότητας των προσωπικών δεδομένων ποικίλλουν, ενώ όσον αφορά στον τρόπο που αυτή πρέπει να προστατεύεται, αυτός αποτελεί ζήτημα για περαιτέρω ζύμωση και πραγμάτευση ακόμα και στο εσωτερικό χωρών, όπου η όσμωση χαρακτηριστικών θεωρείται δεδομένη.

2.6 Η ΑΝΑΓΚΗ ΓΙΑ ΥΠΑΡΞΗ ΜΙΑΣ ΠΑΓΚΟΣΜΙΑΣ ΝΟΜΟΘΕΣΙΑΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Αποτελεί αδιαπραγμάτευτο γεγονός σήμερα ότι η διάχυση οποιασδήποτε πληροφορίας μπορεί να λάβει χώρα από τη μια άκρη του κόσμου στην άλλη σε μερικές στιγμές και χωρίς να μεσολαβήσει οποιοδήποτε μέσο μεταφοράς παρά ένας ηλεκτρονικός υπολογιστής και μια σύνδεση στο διαδίκτυο.

Υπό αυτό το πρίσμα, ένας τέτοιος τύπος πληροφορίας είναι προφανές δεν μπορεί να υπόκειται στους κανόνες και νόμους κάποιας συγκεκριμένης χώρας μιας και ουσιαστικά μεταφέρεται σε παγκόσμιο επίπεδο.

Ενδεικτικά, πολλές μεγάλες εταιρίες μεταφέρουν πληροφορίες μέσω ευρωπαϊκών διακομιστών και τις παραδίδουν σε αποδέκτες που εδρεύουν στην αμερικανική ήπειρο ή και το αντίθετο, με αποτέλεσμα να γεννάται το ερώτημα για το ποια νομοθεσία πρέπει να αποτελέσει τη βάση πραγμάτευσης εφόσον διαπιστωθεί κάποια παραβατική συμπεριφορά σε σχέση με τη διαχεόμενη πληροφορία.

Καταστάσεις σαν την προαναφερθείσα, καθιστούν κάτι παραπάνω από επιτακτική την ανάγκη για υιοθέτηση μιας κοινής νομοθεσίας σε παγκόσμιο επίπεδο σε σχέση με τη διάχυση και προστασία της ιδιωτικότητας των προσωπικών δεδομένων.

Ένα τέτοιο εγχείρημα βέβαια μόνο εύκολο δεν είναι. Πολλές χώρες και κυρίως οι ισχυρότερες εξ αυτών, θα προσπαθήσουν να επιβάλουν στο μεγαλύτερο βαθμό τη δική τους νομοθεσία στην προσπάθεια αυτή με βάση τις ιδιαίτερες επιδιώξεις και χαρακτηριστικά τους, με αποτέλεσμα μέχρι και σήμερα, ένα τέτοιο

εγχείρημα να αποτελεί ουσιαστικά μια ιδέα που θα πρέπει να συζητηθεί εκτενέστερα και πιο ουσιαστικά στο μέλλον. Η σύγκρουση ιδεών μεταξύ των χωρών σίγουρα αποτελεί και θα αποτελέσει ένα σημαντικό εμπόδιο για τη δημιουργία ενός κοινού παγκόσμιου πλαισίου νομοθετικής δράσης.

Η σύγκρουση της προσήλωσης στην προστασία της αξιοπρέπειας και της τιμής του ατόμου με βάση την ευρωπαϊκή προσέγγιση, με την προτεραιότητα στην εξασφάλιση της ατομικής ελευθερίας με βάση την αμερικανική νόρμα, θα αποτελέσει το βασικό παράγοντα για την δημιουργία αυτού του παγκόσμιου πλαισίου με τη δημιουργία αυτή να εξαρτάται σε μεγάλο βαθμό από τη δυνατότητα για εξεύρεση λύσεων για τη γεφύρωση αυτού του χάσματος.

2.7 ΠΩΣ ΤΕΛΙΚΑ ΜΕΤΑΦΡΑΖΕΤΑΙ Η ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΗ ΣΗΜΕΡΙΝΗ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

Με βάση την ανάλυση που έλαβε χώρα στο δεύτερο κεφάλαιο του παρόντος συγγράμματος, είναι προφανές ότι η αλματώδης τεχνολογική ανάπτυξη που έχει επιτελεστεί, ώθησε στην επανεξέταση των εννοιών της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων.

Πλέον, το άτομο ως αυτόνομη μονάδα είναι αυτό που καλείται να διαδραματίσει πρωτεύοντα ρόλο στο πως μπορεί να προστατέψει την ιδιωτική του ζωή και τις πληροφορίες που σχετίζονται με αυτή, θέτοντας ταυτόχρονα τα προσωπικά του όρια όσον αφορά στην έκταση και του είδους των πληροφοριών που θα γνωστοποιεί σε διαδικτυακά περιβάλλοντα.

Υπό αυτό το πρίσμα, εν τέλει οι αυτόνομες μονάδες είναι αυτές που στην ψηφιακή εποχή καλούνται να μεταφράσουν κατά το δοκούν την έννοια της ιδιωτικότητας για λογαριασμό τους και με βάση τις προσωπικές τους αντιλήψεις, διαμορφώνοντας ταυτόχρονα και το ανάλογο προσωπικό πλαίσιο δράσης για την προστασία των προσωπικών τους δεδομένων.

ΚΕΦΑΛΑΙΟ 3

ΡΥΘΜΙΣΤΙΚΕΣ ΑΡΧΕΣ

3.1 ΓΕΝΙΚΑ

Το τρίτο κεφάλαιο της εργασίας, αποτελεί μια επισκόπηση των ρυθμιστικών αρχών και πλαισίων δράσης που απαντώνται σήμερα ανά τον κόσμο σε σχέση με την προστασία της ιδιωτικότητας των πληροφοριών, εστιάζοντας κύρια στο ρυθμιστικό πλαίσιο που χαρακτηρίζει την Ευρωπαϊκή Ένωση.

Κατά τη διάρθρωση του εν λόγω κεφαλαίου, αρχικά λαμβάνει χώρα μια ιστορική αναδρομή του “ψηφιακού” ρυθμιστικού πλαισίου, ενώ εν συνεχεία αναλύονται τα σημαντικότερα ρυθμιστικά μοντέλα προστασίας της ιδιωτικότητας που απαντώνται σήμερα ανά τον κόσμο.

Ακολουθεί μια εκτενής αναφορά στα ρυθμιστικά μοντέλα που χαρακτηρίζουν σήμερα την Ευρώπη και την Αμερική, με κύρια εστίαση στον ευρωπαϊκό χώρο, ενώ τέλος λαμβάνει χώρα μια επισκόπηση των ρυθμιστικών μοντέλων που απαντώνται σήμερα στις διάφορες περιοχές και χώρες ανά τον κόσμο και αφορούν στην προστασία της ιδιωτικότητας των πληροφοριών και των προσωπικών δεδομένων.

3.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ “ΨΗΦΙΑΚΟΥ” ΡΥΘΜΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ

Ουσιαστικά, η προσέγγιση της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων που σχετίζονται με αυτή με βάση και την ψηφιακή παράμετρο, αρχίζει να λαμβάνει χώρα τη δεκαετία του 1970, όπου πλέον οι νομοθετικές προσεγγίσεις και δράσεις αρχίζουν να λαμβάνουν σοβαρά υπόψη τις επιδράσεις της ψηφιακής εποχής και της τεχνολογικής εξέλιξης, και να διαμορφώνονται σε σημαντικό βαθμό με βάση και αυτές.

Η πρώτη νομοθετική δράση για την προστασία των προσωπικών δεδομένων που περιείχε σαφή προσανατολισμό στην ψηφιακή παράμετρο έλαβε χώρα στο Hesse

της Γερμανίας το 1970, ενώ ακολούθησαν και άλλες χώρες όπου περιέλαβαν στην εθνική τους νομοθεσία νόμους για την προστασία των προσωπικών δεδομένων σε σχέση με την ψηφιακή συνιστώσα, όπως η Σουηδία το 1973, οι Ηνωμένες Πολιτείες το 1974, η Γερμανία το 1977 και η Γαλλία το 1978.

Στη δεκαετία του 1980, πλέον αρχίζουν να κάνουν την εμφάνισή τους αναλυτικές κατευθυντήριες γραμμές από σημαντικούς φορείς ανά τον κόσμο, για την προστασία των προσωπικών δεδομένων η οποία θα πρέπει να συμβαδίζει με την ψηφιακή έκρηξη.

Τα σημαντικότερα παραδείγματα πλαισίων τέτοιων κατευθυντήριων γραμμών αποτέλεσαν:

- Η οδηγία για την προστασία των ατόμων σε σχέση με την Αυτοματοποιημένη Διαδικασία των Προσωπικών Δεδομένων (Convention for the Protection of Individuals with regard to the Automatic Process of Personal Data) – Συμβούλιο της Ευρώπης, Στρασβούργο, 1981.
- Η οδηγία για την προστασία της ιδιωτικής ζωής και των διασυνοριακών συναλλαγών δεδομένων Προσωπικού Χαρακτήρα (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data – Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), 1980

Οι συγκεκριμένες οδηγίες και κατευθυντήριες γραμμές αποτέλεσαν τη βάση για τη δημιουργία του νομοθετικού πλαισίου για την προστασία των προσωπικών δεδομένων στην πλειοψηφία των χωρών της Ευρώπης, με την κάθε χώρα να λαμβάνει υπόψη όπως είναι φυσικό τα ιδιαίτερα πολιτισμικά, κοινωνικά και ιστορικά χαρακτηριστικά της προκειμένου να διαμορφώσει το καταλληλότερο νομοθετικό πλαίσιο δράσης.

3.3 ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Σήμερα, απαντώνται τέσσερα βασικά ρυθμιστικά μοντέλα προστασίας της ιδιωτικότητας σε σχέση με την ψηφιακή παράμετρο, τα οποία καλύπτουν ουσιαστικά το σύνολο των ρυθμιστικών μοντέλων που απαντώνται στις διάφορες χώρες ανά τον κόσμο. Τα μοντέλα αυτά είναι:

- Το εκτενές μοντέλο.
- Το στοχευόμενο μοντέλο.
- Το αυτορρυθμιζόμενο μοντέλο.
- Το μοντέλο του καταναλωτή.

3.3.1 Το εκτενές μοντέλο

Στο συγκεκριμένο μοντέλο, η γενική νομοθεσία των χωρών είναι υπεύθυνη για τη συλλογή και χρήση των ιδιωτικών πληροφοριών τόσο στον ιδιωτικό όσο και στο δημόσιο τομέα, με την ταυτόχρονη ύπαρξη ενός οργάνου εποπτείας αυτών των διαδικασιών το οποίο εξασφαλίζει τη συμμόρφωση στους προβλεπόμενους κανόνες.

Η πλειοψηφία των χωρών της Ευρωπαϊκής Ένωσης χρησιμοποιεί το συγκεκριμένο ρυθμιστικό μοντέλο, ενώ ο Καναδάς και η Αυστραλία χρησιμοποιούν μια παραλλαγή αυτού του μοντέλου, κατά την οποία οι ίδιες οι βιομηχανίες που ενδιαφέρονται για την ανταλλαγή δεδομένων, συλλέγουν τα δεδομένα και καθορίζουν τους κανόνες προστασίας των ιδιωτικών δεδομένων, με την όλη διαδικασία να επιβλέπεται από έναν οργανισμό προστασίας της ιδιωτικότητας.

3.3.2 Το στοχευόμενο μοντέλο

Όσον αφορά στο εν λόγω μοντέλο, οι χώρες που το ακολουθούν, υιοθετούν συγκεκριμένες ομάδες νόμων για συγκεκριμένα στοιχεία, όπως για παράδειγμα τη χρηματοοικονομική προστασία της ιδιωτικής ζωής, τη διάδοση προσωπικών αρχείων πολυμέσων κτλ., με την επιβολή αυτών των νόμων να επιτυγχάνεται με μια σειρά μηχανισμών και δράσεων όπως, μέσω ρυθμιστικών οργανισμών, μέσω

ομοσπονδιακών και πολιτειακών καταστατικών ή ακόμα και μέσω της αυτοαστυνόμευσης.

Το συγκεκριμένο μοντέλο διακρίνεται από σημαντική ευελιξία μιας και μπορεί ανά πάσα στιγμή να εισαχθεί μια νέα νομοθεσία κάθε φορά που μια νέα τεχνολογία εγείρει ζητήματα και ανησυχίες όσον αφορά στην προστασία της ιδιωτικής ζωής.

Σε πολλές χώρες, το συγκεκριμένο μοντέλο χρησιμοποιείται συνδυαστικά με τη γενική νομοθεσία προκειμένου να στοχεύσει στο βέλτιστο δυνατό βαθμό σε συγκεκριμένες πιο ευρείες κατηγορίες όπως οι τηλεπικοινωνίες, ή να αποκτήσει πρόσβαση σε σημαντικά αρχεία όπως τα αρχεία της αστυνομίας ή τα πιστωτικά αρχεία.

Στο σημείο αυτό, θα πρέπει να σημειωθεί ότι το συγκεκριμένο μοντέλο εφόσον χρησιμοποιείται σε χώρες όπου η πνευματική ιδιοκτησία αποτελεί σημαντική οικονομική δύναμη, μπορεί να οδηγήσει σε σύγκρουση μεταξύ των προμηθευτών της τεχνολογίας και των κατόχων πνευματικών δικαιωμάτων, μιας και οι δεύτεροι αποστρέφονται το συνδυασμό των νέων ψηφιακών τεχνολογιών και του δικαιώματος της ανωνυμίας που μπορεί να οδηγήσει σε φαινόμενα πειρατείας με αποτέλεσμα σημαντικά διαφυγόντα κέρδη. Η Αμερική αποτελεί το χαρακτηριστικότερο παράδειγμα προς αυτή την κατεύθυνση.

3.3.3 Το αυτορρυθμιζόμενο μοντέλο

Στο συγκεκριμένο μοντέλο, απαντώνται πολλές και διαφορετικές μορφές αυτορρύθμισης των κανόνων δράσης ανάλογα με την κατηγορία ενδιαφέροντος.

Πιο συγκεκριμένα, οι εταιρίες ανάλογα με τον κλάδο στον οποίο ανήκουν, καθορίζουν από μόνες τους το ρυθμιστικό πλαίσιο και τις πρακτικές δράσεις, ενώ για την επίβλεψη των διαδικασιών υιοθετούν τη δράση της αυτοαστυνόμευσης.

Το βασικό μειονέκτημα αυτού το μοντέλου, είναι ότι πολύ εύκολα μπορεί να ανακύψουν συγκρούσεις συμφερόντων μεταξύ των εταιριών μιας και δεν υπάρχει ένα γενικότερο πολιτειακό πλαίσιο επίβλεψης, με αποτέλεσμα πολύ συχνά οι εταιρίες να καταλήγουν για την επίλυση των διαφορών τους στα δικαστήρια.

3.3.4 Το μοντέλο του καταναλωτή

Με βάση το συγκεκριμένο μοντέλο, η προστασία των προσωπικών δεδομένων επαφίεται σε μεγάλο βαθμό στον ίδιο τον πολίτη / καταναλωτή, ο οποίος με τη χρήση ψηφιακών εργαλείων προστασίας της ιδιωτικότητας που κυκλοφορούν στο εμπόριο, καλείται να προστατέψει τα προσωπικά του δεδομένα σε μικρότερο ή μεγαλύτερο βαθμό.

Παραδείγματα τέτοιων εργαλείων αποτελούν οι κωδικοποιητές για την ασφαλή μεταφορά μηνυμάτων ηλεκτρονικού ταχυδρομείου, δεδομένων φωνής / εικόνας, τα εργαλεία αποτροπής αποδοχής των λεγόμενων cookies κτλ.

Στο σημείο αυτό βέβαια, θα πρέπει να τονιστεί ότι τέτοια εργαλεία σε καμία περίπτωση δεν εξασφαλίζουν πλήρως αποδοτική προστασία όσον αφορά σε θέματα προστασίας των προσωπικών δεδομένων, αλλά αποτελούν βοηθητικά στοιχεία για την εξασφάλιση επιπρόσθετων αποδείξεων για την πιο αποδοτική εφαρμογή της νομοθεσίας.

Με βάση την παραπάνω παρατήρηση, είναι φανερό ότι το συγκεκριμένο μοντέλο μπορεί να χρησιμοποιηθεί μεμονωμένα από τους πολίτες για να εξασφαλίσει μια επιπλέον προστασία των προσωπικών τους δεδομένων στην ψηφιακή εποχή, αλλά σε καμία περίπτωση δεν μπορεί να αντικαταστήσει τις γενικότερες νομοθετικές δράσεις προς αυτή την κατεύθυνση.

3.4 ΤΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΣΤΗΝ ΕΥΡΩΠΗ ΚΑΙ ΤΗΝ ΑΜΕΡΙΚΗ

Στο χωρίο αυτό της εργασίας, θα γίνει μια εκτενής αναφορά στα ρυθμιστικά μοντέλα όσον αφορά στην προστασία της ιδιωτικότητας και των προσωπικών

δεδομένων, που υιοθετούνται σήμερα τόσο στην Ευρώπη όσο και στις Ηνωμένες Πολιτείες Αμερικής.

3.4.1 Το μοντέλο της Ευρωπαϊκής Ένωσης

Η Ευρωπαϊκή Ένωση θεωρείται πρωτοπόρος όσον αφορά στη θέσπιση αυστηρών πολιτικών για την προστασία της ιδιωτικής ζωής και των δεδομένων που σχετίζονται με αυτή, καθώς και για την υιοθέτηση νόμων που ευνοούν το άτομο και της προστασία της ιδιωτικότητας αυτού.

Το δικαίωμα στην ιδιωτική ζωή αποτελεί αναπόσπαστο μέρος των συνταγμάτων σχεδόν του συνόλου των χωρών της Ευρωπαϊκής Ένωσης με πρωτοπόρες χώρες προς αυτή την κατεύθυνση, τη Γερμανία και την Ισπανία.

Η ρητή και θεμελιώδης στήριξη της Ευρωπαϊκής Ένωσης στο δικαίωμα της ιδιωτικής ζωής καταγράφεται στην Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία αποτελεί μια διεθνή συνθήκη σχετιζόμενη με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά στον ευρωπαϊκό χώρο.

Η επικύρωση της εν λόγω συνθήκης έλαβε χώρα το 1953, με τη συνθήκη αυτή να αποτελεί τον πρώτο θεμέλιο λίθο για την ενίσχυση των θεμελιωδών δικαιωμάτων του ατόμου όσον αφορά στην προστασία της προσωπικής του ζωής, υπό το πρίσμα των αλλαγών και των τεχνολογικών εξελίξεων.

Χαρακτηριστικό άρθρο της εν λόγω συνθήκης αποτελεί το άρθρο 8 του χωρίου 1, σύμφωνα με το οποίο:

‘Κάθε άτομο έχει το δικαίωμα του σεβασμού της ιδιωτικής και της οικογενειακής του ζωής, καθώς και του σεβασμού της ανταλλαγής πληροφοριών σε σχέση με αυτή’.

Όπως ήδη αναφέρθηκε και νωρίτερα, κατευθυντήριες γραμμές όσον αφορά στην προστασία της ιδιωτικότητας έλαβαν χώρα στις αρχές της δεκαετίας του 80, οι

οποίες ήρθαν να συμπληρώσουν την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου.

Τα σημαντικότερα παραδείγματα πλαισίων τέτοιων κατευθυντήριων γραμμών αποτέλεσαν:

- Η οδηγία για την προστασία των ατόμων σε σχέση με την Αυτοματοποιημένη Διαδικασία των Προσωπικών Δεδομένων (Convention for the Protection of Individuals with regard to the Automatic Process of Personal Data) – Συμβούλιο της Ευρώπης, Στρασβούργο, 1981.
- Η οδηγία για την προστασία της ιδιωτικής ζωής και των διασυνοριακών συναλλαγών δεδομένων Προσωπικού Χαρακτήρα (Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data – Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), 1980

Στην τελευταία οδηγία, ήρθαν να ενσωματωθούν το 1995 από την Ευρωπαϊκή Ένωση 8 βασικές αρχές, προκειμένου η οδηγία να αποκτήσει έναν πιο συγκεκριμένο και στοχευμένο χαρακτήρα.

Οι 8 αυτές αρχές είναι:

1. Περιορισμός στη συλλογή προσωπικών πληροφοριών:

Σύμφωνα με αυτή την αρχή, θα πρέπει να υπάρχει περιορισμός όσον αφορά στη δυνατότητα για συλλογή προσωπικών πληροφοριών, οι οποίες θα πρέπει να συλλέγονται νόμιμα και με πλήρη επίγνωση του ατόμου στο οποίο ανήκουν τα προσωπικά δεδομένα.

2. Ποιότητα των προσωπικών δεδομένων:

Τα προσωπικά δεδομένα θα πρέπει να χρησιμοποιούνται μόνο για τον αρχικό σκοπό για τον οποίο εξορύχτηκαν, ενώ θα πρέπει να διακρίνονται από ακρίβεια και

να περιλαμβάνουν όλη την σύγχρονη (up-to-date) απαιτούμενη πληροφορία για τον εν λόγω σκοπό.

3. Καθορισμός του σκοπού χρήσης των προσωπικών δεδομένων:

Πριν λάβει χώρα οποιαδήποτε ενέργεια ή προσπάθεια εξόρυξης ή ανταλλαγής προσωπικών δεδομένων και πληροφοριών, θα πρέπει να καθορίζεται επακριβώς ο σκοπός για τον οποίο προορίζονται αυτά τα δεδομένα ή οι πληροφορίες καθώς και τα χαρακτηριστικά αυτού. Σε περίπτωση που αυτός ο σκοπός αλλάξει, θα πρέπει άμεσα να λάβει χώρα επισήμανση αυτής της αλλαγής στο πεδίο των δεδομένων.

4. Περιορισμός στη χρήση των προσωπικών δεδομένων:

Τα προσωπικά δεδομένα θα πρέπει να διακινούνται και να επεξεργάζονται πάντα μέσα στα αυστηρά όρια που καθορίζει ο αρχικός σκοπός και δεν θα πρέπει σε καμία περίπτωση να λαμβάνει χώρα παρέκκλιση ως προς αυτή την αρχή, εκτός και αν παρεμβαίνει δικαστική αρχή.

5. Ύπαρξη δικλίδων ασφαλείας:

Σύμφωνα με αυτή την αρχή, θα πρέπει να εξασφαλίζεται η προστασία των προσωπικών δεδομένων από πιθανή κατάχρηση.

6. Διαφάνεια:

Η διαδικασία της συλλογής των προσωπικών δεδομένων θα πρέπει να χαρακτηρίζεται από πλήρη διαφάνεια και να καθορίζει πλήρως τον τρόπο με τον οποίο θα συλλεχθούν τα προσωπικά δεδομένα, το σκοπό για τον οποίο θα γίνει αυτή η συλλογή, τον τρόπο που θα χρησιμοποιηθούν, καθώς και τον τρόπο με τον οποίο θα διακινηθούν και θα επεξεργαστούν.

7. Ατομική συμμετοχή:

Το άτομο στο οποίο αναφέρονται τα δεδομένα, έχει το αναφαίρετο δικαίωμα να είναι πλήρως ενημερωμένο για το ποιος συλλέγει και χρησιμοποιεί τα προσωπικά

του δεδομένα, ενώ ανά πάσα στιγμή θα πρέπει να έχει πρόσβαση σε αυτά, προκειμένου να μπορεί να προβαίνει ανά πάσα στιγμή σε επιθυμητές αλλαγές.

8. Λογοδοσία:

Οι συλλέκτες προσωπικών δεδομένων θα πρέπει να λογοδοτούν στις αρχές και να εξασφαλίζουν την άδεια των αρχών των συστημάτων συλλογής δεδομένων που χρησιμοποιούν με τις προβλεπόμενες αρχές.

Με την πάροδο των ετών και σύμφωνα με τις εξελίξεις στον τεχνολογικό τομέα, έλαβαν χώρα και άλλες οδηγίες στον ευρωπαϊκό χώρο προκειμένου να εξασφαλίζεται στο βέλτιστο δυνατό βαθμό η προστασία των προσωπικών δεδομένων.

Η οδηγία για την Προστασία των Προσωπικών Δεδομένων που διακινούνται μέσω των Τηλεπικοινωνιών που εκδόθηκε το 1997, αποτέλεσε ουσιαστικά την πρώτη οδηγία στην οποία συζητήθηκαν ειδικότερα οι υποχρεώσεις των φορέων παροχής υπηρεσιών τηλεπικοινωνιών σε σχέση με την προστασία των διακινούμενων προσωπικών πληροφοριών και την εξασφάλιση του απορρήτου των επικοινωνιών μεταξύ των πολιτών.

Το 2002, η παραπάνω οδηγία αναθεωρήθηκε και εμπλουτίστηκε έτσι ώστε να περιλάβει και δραστηριότητες προστασίας που σχετίζονται με το διαδίκτυο.

Πιο συγκεκριμένα, η νέα οδηγία περιελάμβανε κατευθύνσεις για την προστασία των προσωπικών δεδομένων σε σχέση με τις ακόλουθες τρεις κατηγορίες διακίνησης πληροφοριών μέσω του διαδικτύου: traffic data, spam και cookies.

Η συγκεκριμένη οδηγία εν γένει, σχετίζονταν περισσότερο με την προστασία των δεδομένων που διακινούνται μέσω του διαδικτύου και “ανάγκαζε” ουσιαστικά τους παρόχους υπηρεσιών διαδικτύου να εξασφαλίζουν την ασφάλεια των διακινούμενων πληροφοριών, μέσω της δημιουργίας κατάλληλων συστημάτων, όπως συστήματα όπου παρέχεται η δυνατότητα στο χρήστη για διαβαθμισμένη ανταλλαγή πληροφοριών (για παράδειγμα, σε μια συνομιλία, ο χρήστης επιτρέπει τη διακίνηση

δεδομένων ήχου, αλλά όχι τη διακίνηση δεδομένων εικόνας, εκτός και αν δώσει την απαραίτητη συγκατάθεση).

Επίσης, στην αναθεωρημένη μορφή της οδηγίας, προβλέπονταν κατευθύνσεις σε σχέση με την πολιτική των εταιριών παροχής υπηρεσιών διαδικτύου όσον αφορά στη διατήρηση των δεδομένων.

Σύμφωνα με αυτές, ο πάροχος οφείλει να διαγράψει ή τουλάχιστον να εξασφαλίσει την ανωνυμία πληροφοριών, όταν αυτές παύουν πλέον να είναι χρήσιμες.

Ωστόσο, η οδηγία έδινε τη δυνατότητα στα κράτη μέλη να μπορούν να τροποποιούν ως ένα βαθμό τα προβλεπόμενα αυτής, με βάση τις ιδιαίτερες ανάγκες και επιδιώξεις τους.

Το 2006, η Ευρωπαϊκή Ένωση θέσπισε μια νέα οδηγία που σχετίζονταν κύρια με τη συνιστώσα της χρονικής διάρκειας διατήρησης των δεδομένων, ενώ προσπάθησε να επιβάλει την πλήρη εναρμόνιση των κρατών μελών της με την εν λόγω οδηγία.

Ο κύριος λόγος που δημιουργήθηκε αυτή η οδηγία, ήταν οι τρομοκρατικές επιθέσεις που έλαβαν χώρα στο Λονδίνο και στη Μαδρίτη.

Σύμφωνα με αυτή την οδηγία λοιπόν, προβλέπονταν η διατήρηση και αποθήκευση παντός είδους διακινούμενων δεδομένων είτε μέσω διαδικτύου είτε μέσω τηλεπικοινωνιών για χρονικό διάστημα από 6 μήνες έως 2 χρόνια.

Το γεγονός αυτό θεωρήθηκε κατάφορη διάβρωση της αρχής προστασίας των προσωπικών δεδομένων και ξεσήκωσε θύελλα αντιδράσεων από τους πολίτες σχεδόν στο σύνολο των ευρωπαϊκών χωρών.

Μέχρι και σήμερα, η Ευρωπαϊκή Ένωση προβαίνει σε συνεχείς επικαιροποιήσεις των υπαρχόντων οδηγιών προκειμένου να ενισχύει τα δικαιώματα των ατόμων όσον αφορά στην προστασία των προσωπικών τους δεδομένων,

ενισχύοντας όμως ταυτόχρονα και τη δυνατότητα για αστυνομική και ποινική παρέμβαση όταν αυτό κρίνεται αναγκαίο.

Κλείνοντας αυτό το χωρίο, θα πρέπει να τονιστεί ότι από τις απαρχές της, η άποψη της Ευρωπαϊκής Ένωσης όσον αφορά στην προστασία των προσωπικών δεδομένων, είναι ότι αυτή πρέπει να εξασφαλίζεται με κάθε τρόπο, αποτελώντας βασικό ανθρώπινο δικαίωμα.

Υπό αυτό το πρίσμα, η Ευρωπαϊκή Ένωση ενίσχυε και συνεχίζει να ενισχύει και να επικαιροποιεί συνεχώς το νομοθετικό της πλαίσιο, με σκοπό να δημιουργήσει ένα τυποποιημένο παγκόσμιο πλαίσιο δράσης, το οποίο θα μπορούσε να υιοθετηθεί από το σύνολο των χωρών ανά τον κόσμο, με απώτερο σκοπό τη δημιουργία ενός συμπαγούς παγκόσμιου πλαισίου δράσης προς την κατεύθυνση της προστασίας των προσωπικών δεδομένων στην ψηφιακή εποχή.

3.4.2 Το μοντέλο της Αμερικής

Οι Ηνωμένες Πολιτείες Αμερικής δεν διαθέτουν σήμερα ένα ολοκληρωμένο νομοθετικό ρυθμιστικό πλαίσιο δράσης όσον αφορά στην προστασία των προσωπικών δεδομένων στην ψηφιακή εποχή. Εντούτοις, διαθέτουν ένα πολύ αυστηρό ομοσπονδιακό πλαίσιο δράσης όσον αφορά στην προστασία ιδιωτικών πληροφοριών σε σχέση με τις τρεις ακόλουθες κατηγορίες.

- Προστασία πληροφοριών σε σχέση με την παράμετρο της ιατρικής φροντίδας.

Υπάρχει μια σειρά διοικητικών και νομοθετικών ρυθμίσεων που διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα, το βαθμό χρήσης και την προστασία των δεδομένων υγείας, οι οποίες περιλαμβάνονται στο λεγόμενο νόμο HIPAA (Health Information and Portability Accountability Act).

Με βάση τα ισχύοντα του συγκεκριμένου κανόνα, ο καταναλωτής διατηρεί το δικαίωμα να θέτει τους κανόνες όσον αφορά στη διακίνηση πληροφοριών που

σχετίζονται με την υγεία του, τους αποδέκτες των πληροφοριών, καθώς και το περιεχόμενό τους.

- Προστασία των οικονομικών πληροφοριών.

Η προστασία των οικονομικών πληροφοριών καθορίζεται μέσω συνιστωσών που περιλαμβάνονται στο λεγόμενο νόμο GLB (Gramm-Leach-Bliley).

Ο εν λόγω νόμος απαιτεί από τα χρηματοπιστωτικά ιδρύματα και τις εταιρίες παροχής υπηρεσιών και προϊόντων, να εξηγούν τον τρόπο με τον οποίο προστατεύουν τα δεδομένα των πελατών τους, σε ετήσια βάση.

Σύμφωνα με τα προβλεπόμενα για την εν λόγω διαδικασία, κάθε οργανισμός καλείται να συμπληρώνει μια φόρμα διασφάλισης των προσωπικών πληροφοριών και να επιβεβαιώνει γραπτώς ότι θα εφαρμοστούν πλήρως τα προβλεπόμενα στη φόρμα τα οποία εμποδίζουν τη μη εξουσιοδοτημένη πρόσβαση σε «προσωπικές εμπιστευτικές» πληροφορίες.

- Προστασία πληροφοριών σχετιζόμενων με παιδιά κάτω των 13 ετών.

Η προστασία πληροφοριών σχετιζόμενων με παιδιά κάτω των 13 ετών, εξασφαλίζεται μέσω του νόμου COPPA (Children’s Online Privacy Protection Act), ο οποίος απαιτεί από όλες τις ιστοσελίδες που συλλέγουν πληροφορίες από παιδιά κάτω των 13 ετών, να διατηρούν μια σαφή πολιτική για την προστασία της ιδιωτικής αυτής πληροφορίας.

Επιπρόσθετα, ο συγκεκριμένος νόμος σκιαγραφεί πλήρως τις ευθύνες των ιδιοκτητών των ιστοσελίδων που διαθέτουν πληροφορίες προερχόμενες από παιδιά κάτω των 13 ετών, ενώ τονίζει ότι για οποιαδήποτε δράση, απαιτείται πρώτα η συγκατάθεση των γονέων.

Κλείνοντας, όσον αφορά στον αμερικάνικο χώρο, υπάρχει ένας επιπρόσθετος εκτεταμένος αριθμός διατάξεων και ρυθμίσεων, πέραν των παραπάνω, σε σχέση με την προστασία της ιδιωτικότητας των πληροφοριών, που όμως αποτελούν διατάξεις

που αφορούν σε συγκεκριμένες Πολιτείες ή περιοχές και σε καμία περίπτωση δεν μπορούν να ενταχθούν σε ένα γενικότερο, συνολικό κανονιστικό πλαίσιο για την προστασία της προσωπικής πληροφορίας στις Ηνωμένες Πολιτείες Αμερικής.

3.5 ΤΑ ΡΥΘΜΙΣΤΙΚΑ ΜΟΝΤΕΛΑ ΑΝΑ ΤΟΝ ΚΟΣΜΟ

Εν γένει, κάθε χώρα και κάθε περιοχή ανά τον κόσμο, αναγνωρίζει το δικαίωμα στην ιδιωτική ζωή και προστατεύει αυτή είτε μέσω του συντάγματός της, είτε μέσω των δικαστικών αρχών, είτε μέσω της υιοθέτησης διεθνών συμφωνιών.

Για παράδειγμα, όμοια με την Ευρωπαϊκή Ένωση, η Αυστραλία και ο Καναδάς διαθέτουν σήμερα μια ολοκληρωμένη νομοθεσία για την προστασία της ιδιωτικότητας των πληροφοριών.

Προχωρώντας ένα βήμα πιο πέρα, τα 21 κράτη μέλη της συνεργασίας Ασίας – Ειρηνικού, στηρίζουν τις πρωτοβουλίες τους για την προστασία της ιδιωτικής ζωής στο διακρατικό νομοθετικό πλαίσιο που υπογράφηκε το 2004 και συνεχίζει να επικαιροποιείται μέχρι και σήμερα, με σημαντικότερη επικαιροποίηση αυτή που έλαβε χώρα το 2010 και σύμφωνα με την οποία προβλέπονταν εναρμόνιση αρκετών διατάξεων με τις αντίστοιχες διατάξεις του κανονιστικού πλαισίου της Ευρωπαϊκής Ένωσης, προς δημιουργία ενός πιο αυστηρού και παγκοσμιοποιημένου πλαισίου δράσης.

Ένα ιδιαίτερο παράδειγμα προσέγγισης της προστασίας της ιδιωτικότητας της προσωπικής ζωής αποτελεί η Κίνα. Αν θεωρήσουμε ότι η Αμερική αποτελεί ένα παράδειγμα εμπορευματοποίησης της προσωπικής ζωής και η Ευρώπη ένα παράδειγμα προσέγγισης της ιδιωτικής ζωής ως θεμελιώδες δικαίωμα του ατόμου, η Κίνα κάλλιστα μπορεί να θεωρηθεί ως ένα παράδειγμα χώρας, όπου η προστασία της προσωπικής ζωής αποτελεί πεδίο ήσσονος σημασίας.

Πράγματι, στο κινεζικό γίγνεσθαι, απαντάται καθημερινά πλήθος δράσεων παρακολούθησης και διακίνησης προσωπικών πληροφοριών χωρίς την απαιτούμενη συγκατάθεση από το άτομο στο οποίο αναφέρονται οι πληροφορίες, χωρίς

ουσιαστικά να παρεμβαίνει κανείς. Η διαμορφωθείσα αυτή κατάσταση η οποία έχει αντίκτυπο και στο υπάρχον νομοθετικό πλαίσιο δράσης, αποδεικνύει και την αλληλεξάρτηση μεταξύ της διαμόρφωσης των νομοθετικών πλαισίων και της κουλτούρας των λαών.

ΣΥΖΗΤΗΣΗ - ΠΡΟΟΠΤΙΚΕΣ ΣΤΟΝ ΤΟΜΕΑ ΤΩΝ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ

Από την ανάλυση που έλαβε χώρα νωρίτερα, εύκολα μπορεί να συμπεράνει κανείς τον πολύ μεγάλο βαθμό εισχώρησης των Μεγάλων Δεδομένων σε όλους τους τομείς της ανθρώπινης δραστηριότητας σήμερα, με θετικά και αρνητικά αποτελέσματα τόσο για το άτομο ως αυτόνομη μονάδα, όσο και για την κοινωνία ως σύνολο ατόμων.

Η σημαντικότερη παράμετρος που καλούνται σήμερα αλλά και μελλοντικά να αντιμετωπίσουν οι ανά τον κόσμο κυβερνήσεις, είναι η εξεύρεση τρόπων προκειμένου η χρήση των Μεγάλων Δεδομένων να μην επιδρά άμεσα στην ιδιωτικότητα των προσωπικών πληροφοριών των πολιτών και υπό αυτό το πρίσμα, ως ένα βαθμό στο δημοκρατικό δικαίωμα των πολιτών για προστασία της προσωπικής τους ζωής.

Προχωρώντας ένα βήμα πιο πέρα, όπως σαφώς καταδείχτηκε στην ανάλυση των προηγούμενων κεφαλαίων, η νομοθεσία δεν επαρκεί για να καλύψει αυτή την ανάγκη για προστασία των προσωπικών δεδομένων και για διατήρηση της δημοκρατικότητας στο σημερινό ψηφιακό γίγνεσθαι.

Παρά τη συνεχή προσπάθεια που λαμβάνει χώρα στις διάφορες περιοχές του κόσμου ώστε η νομοθεσία τους να προσαρμόζεται συνεχώς στις νέες απαιτήσεις και να προστατεύει στο μέγιστο δυνατό βαθμό την ιδιωτικότητα των δεδομένων, είναι προφανές πως ένεκα της φύσης και της ταχύτητας διάδοσης των Μεγάλων Δεδομένων, τα αποτελέσματα αυτής της προσπάθειας θα υστερούν πάντα όσον αφορά στην πλήρη προστασία των προσωπικών δεδομένων των πολιτών ανά τον κόσμο.

Με βάση τα παραπάνω, η σημαντικότερη πρόκληση που έχουν να αντιμετωπίσουν σήμερα οι κυβερνήσεις ανά τον κόσμο, είναι η εξεύρεση τρόπων και λύσεων προκειμένου να καταστεί δυνατός ο έλεγχος της διάδοσης και επεξεργασίας των δεδομένων έτσι ώστε να εξασφαλίζεται σε μεγαλύτερο βαθμό η προστασία της ιδιωτικότητας των προσωπικών δεδομένων.

Ο συνδυασμός των Μεγάλων Δεδομένων με τα λεγόμενα Ανοικτά Δεδομένα αποτελεί σήμερα τη μεγαλύτερη πρόκληση προς αυτή την κατεύθυνση.

Η έννοια των Ανοικτών Δεδομένων, αποτελεί ουσιαστικά μια νέα έννοια η οποία μπορεί να συνδέεται στενά με την έννοια των Μεγάλων Δεδομένων, αλλά σε καμία περίπτωση δεν ταυτίζεται με αυτή.

Εν γένει, τα Ανοικτά Δεδομένα φέρνουν μια προοπτική που μπορεί να κάνει τα Μεγάλα δεδομένα πιο χρήσιμα, πιο δημοκρατικά και λιγότερο απειλητικά.

Ενώ τα Μεγάλα Δεδομένα ορίζονται από το μέγεθος, την ταχύτητα διάδοσής τους και τη μεγάλη ποικιλία τους, τα Ανοικτά Δεδομένα ορίζονται από τη χρήση τους και από τη σημασία αυτής, με αποτέλεσμα να ισχυροποιείται σε αυτά η έννοια της ποιότητας.

Όπως ήδη καταγράφηκε στα προηγούμενα κεφάλαια του παρόντος συγγράμματος, τα Μεγάλα Δεδομένα αποτελούν όρο που χρησιμοποιείται για να περιγράψει πολύ μεγάλες, πολύπλοκες και ταχέως μεταβαλλόμενες βάσεις δεδομένων.

Αυτές οι κρίσεις όμως είναι υποκειμενικές και εξαρτώνται από την τεχνολογία. Υπό αυτό το πρίσμα, τα σημερινά Μεγάλα Δεδομένα μπορεί να μην φαίνονται τόσο μεγάλα σε μερικά χρόνια, καθώς η ανάλυση των δεδομένων και της τεχνολογίας των υπολογιστών βελτιώνεται συνεχώς και με αλματώδεις ρυθμούς.

Από την άλλη, τα Ανοικτά Δεδομένα αποτελούν προσβάσιμα, δημόσια δεδομένα που οι άνθρωποι, οι εταιρείες και οι οργανισμοί μπορούν να χρησιμοποιήσουν για να δημιουργήσουν νέες επιχειρήσεις, να αναλύσουν σχέδια και τάσεις, να λαμβάνουν αποφάσεις που βασίζονται σε δεδομένα, καθώς και για την επίλυση σύνθετων προβλημάτων, παράμετροι που προσδίδουν στην έννοια των Ανοικτών Δεδομένων μια σαφώς πιο αντικειμενική υφή σε σχέση με την έννοια των Μεγάλων Δεδομένων σύμφωνα και με την προηγούμενη διατύπωση.

Όλοι οι ορισμοί που αποδίδονται σήμερα στην έννοια των Ανοικτών Δεδομένων, περιλαμβάνουν δύο βασικά χαρακτηριστικά:

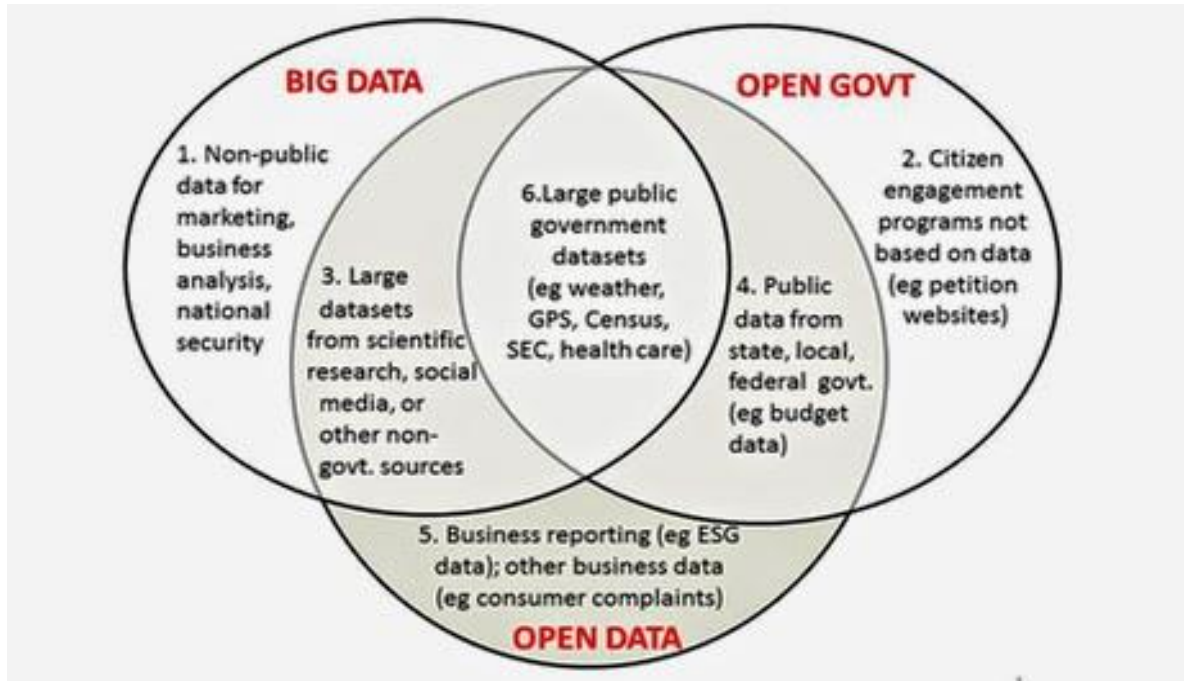
- Τα δεδομένα πρέπει να είναι διαθέσιμα στο κοινό για οποιαδήποτε χρήση, και πρέπει να αδειοδοτούνται με τρόπο που να επιτρέπει την επαναχρησιμοποίησή τους.
- Τα Ανοικτά Δεδομένα πρέπει επίσης να είναι σχετικά εύκολα στη χρήση, αν και υπάρχουν διαβαθμίσεις του "ανοίγματος". Επίσης, υπάρχει γενική συμφωνία ότι τα Ανοικτά Δεδομένα θα πρέπει να διατίθενται δωρεάν ή με ελάχιστο κόστος.

Με βάση όλα τα παραπάνω, είναι προφανής η ανάγκη για υιοθέτηση των συνιστωσών των Ανοικτών Δεδομένων στην έννοια των Μεγάλων Δεδομένων, προκειμένου αυτά να καταστούν πιο χρήσιμα και λιγότερο απειλητικά.

Η συνδυαστική χρήση αυτών των δύο εννοιών στο άμεσο μέλλον, ίσως αποτελεί τη μοναδική λύση προκειμένου τα Μεγάλα Δεδομένα να συνεχίσουν να εξελίσσονται αποδοτικά και χρήσιμα για το άτομο μεμονωμένα αλλά και για την παγκόσμια κοινωνία..

Σε διαφορετική περίπτωση, είναι ορατός ο κίνδυνος να κυριαρχήσει η αρνητική πλευρά των Μεγάλων Δεδομένων, με αποτέλεσμα αυτά να αποτελέσουν μια συνεχή απειλή για την ατομικότητα των πολιτών, με αυτό τον κίνδυνο να εξαλείφει όλα τα θετικά χαρακτηριστικά των Μεγάλων Δεδομένων και επιπρόσθετα να αποτελεί έναν κίνδυνο τόσο διογκωμένο, που θα είναι σχεδόν αδύνατο να αντιμετωπιστεί.

Το διάγραμμα Βεν αποτελεί σήμερα το πιο εποπτικό μέσο το οποίο χαρτογραφεί τη σχέση μεταξύ των Μεγάλων και Ανοικτών δεδομένων, και καταδεικνύει τον τρόπο που αυτά συνδέονται υπό το πρίσμα της έννοιας της ανοικτής διακυβέρνησης.



Σχήμα 1.5. Συσχέτιση των συνιστωσών των Μεγάλων και Ανοικτών Δεδομένων υπό το πρίσμα της έννοιας της ανοικτής διακυβέρνησης.

Από το παραπάνω διάγραμμα, ανακύπτουν κάποια σημαντικά σημεία τα οποία πρέπει να τονιστούν, προκειμένου να καταδείξουν την αναγκαιότητα εισχώρησης των συνιστωσών των Ανοικτών Δεδομένων στην έννοια των Μεγάλων Δεδομένων και ταυτόχρονα να τονιστεί η σημαντικότητα αυτής της πρόκλησης.

Δεν είναι δημοκρατικό τα μεγάλα δεδομένα να μην είναι ανοιχτά:

Το πρώτο τμήμα του διαγράμματος, περιλαμβάνει όλα τα είδη των Μεγάλων Δεδομένων που φυλάσσονται από το κοινό - όπως τα δεδομένα που κρατούν μεγάλες επιχειρήσεις λιανικού εμπορίου για τους πελάτες τους, ή τα δεδομένα εθνικής ασφάλειας όπως αυτά που συλλέγονται από την NSA.

Αυτό το είδος των Μεγάλων Δεδομένων, δίνει ένα πλεονέκτημα στους ανθρώπους που τα ελέγχουν, αλλά ταυτόχρονα μπορεί να αποδυναμώσει όλους τους υπόλοιπους.

Το συγκεκριμένο είδος Μεγάλων Δεδομένων, αποτελεί σήμερα το πιο αμφιλεγόμενο και με τις μεγαλύτερες ενστάσεις.

Τα ανοιχτά δεδομένα δεν χρειάζεται να είναι μεγάλα δεδομένα για να έχουν σημασία:

Μέτριες ποσότητες δεδομένων, όπως φαίνεται στην ενότητα τέσσερα του διαγράμματος, μπορούν να έχουν μεγάλο αντίκτυπο και να επισύρουν σημαντικά αποτελέσματα, εφόσον η διάδοσή τους γίνει δημόσια και σε κατάλληλο περιβάλλον.

Τα δεδομένα από τις τοπικές κυβερνήσεις για παράδειγμα, μπορούν να βοηθήσουν τους πολίτες να συμμετέχουν στον τοπικό προϋπολογισμό, να επιλέξουν υγειονομική περίθαλψη, να αναλύουν την ποιότητα των τοπικών υπηρεσιών, ή να χτίσουν εφαρμογές που βοηθούν τους ανθρώπους να περιηγηθούν με τα μέσα μαζικής μεταφοράς.

Τα μεγάλα ανοιχτά δεδομένα δεν είναι απαραίτητο να προέρχονται από την κυβέρνηση:

Το συγκεκριμένο συμπέρασμα απορρέει από την ενότητα τρία του διαγράμματος.

Υπό αυτό το πρίσμα, όλο και περισσότεροι επιστήμονες ανά τον κόσμο σήμερα, μοιράζονται και αναπτύσσουν την έρευνά τους στην αστρονομία, στη γονιδιοματική, καθώς και άλλες περιοχές έρευνας και ανάπτυξης σε ένα νέο, συνεργατικό μοντέλο έρευνας.

Προχωρώντας ένα βήμα πιο πέρα, άλλοι ερευνητές, χρησιμοποιούν τα Μεγάλα Δεδομένα που συλλέγονται από τα social media - τα περισσότερα από τα οποία είναι ανοικτά για το κοινό - για να αναλύσουν την κοινή γνώμη και τις τάσεις της αγοράς.

Εισάγοντας τώρα την έννοια της κυβέρνησης, οι εκάστοτε κυβερνήσεις ανά τον κόσμο, όταν μετατρέπουν μεγάλα δεδομένα σε ανοικτά δεδομένα, αποδεικνύονται ιδιαίτερα ισχυρές.

Οι κρατικές υπηρεσίες έχουν την ικανότητα και τους πόρους να συγκεντρώνουν πολύ μεγάλες ποσότητες δεδομένων (όπως τα παραδείγματα των ΗΠΑ στο έκτο τμήμα του διαγράμματος), με το άνοιγμα του συνόλου των δεδομένων αυτών να δύναται να αποφέρει σημαντικά οικονομικά και κυβερνητικά οφέλη.

Ως επίλογο, κλείνοντας το χωρίο της συζήτησης, η εφαρμογή των αρχών των Ανοικτών Δεδομένων σε Μεγάλα Δεδομένα μπορεί να βοηθήσει στην επίλυση των δύσκολων ζητημάτων που έθεσαν τα Μεγάλα Δεδομένα στο σημερινό ψηφιακό γίγνεσθαι.

Η μεγαλύτερη απειλή για την ευημερία των πολιτών όπως έχει ειπωθεί κατά κόρον στο παρόν σύγγραμμα, είναι ο κίνδυνος τα ιδιωτικά, προσωπικά τους δεδομένα να συλλέγονται και να χρησιμοποιούνται χωρίς την έγκρισή τους και χωρίς ελεγχόμενο για τους σκοπούς χρήσης τρόπο. Τα Ανοικτά Δεδομένα, αποτελούν σήμερα την πιο προφανή λύση για την εξάλειψη στο μέγιστο δυνατό βαθμό αυτής της απειλής.

Τα Μεγάλα Δεδομένα αναντίρρητα μας δίνουν πρωτοφανή δύναμη να κατανοήσουμε και να αναλύσουμε τον κόσμο που ζούμε, όμως τα Ανοικτά Δεδομένα είναι αυτά που θα μας εξασφαλίσουν την ταυτόχρονη προστασία των προσωπικών μας δεδομένων κατά την εξέλιξη αυτής της διαδικασίας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά, με την αλματώδη εξέλιξη της τεχνολογίας η οποία έχει επιτελεστεί τα τελευταία χρόνια, αποτελεί αδιαμφισβήτητο γεγονός ότι ο κόσμος έχει αλλάξει και η τεχνολογία έχει συμβάλει ριζικά ως προς αυτή την κατεύθυνση.

Κανείς δεν μπορεί να αμφισβητήσει το γεγονός ότι σήμερα ο άνθρωπος περισσότερο από κάθε άλλη πρότερη περίοδο, έχει τη δυνατότητα να συλλέγει και να ανταλλάσσει πληροφορίες σχετιζόμενες με αυτόν ή με οποιαδήποτε άλλη μονάδα ή σύνολο μονάδων, γρήγορα και σε αυξημένο όγκο.

Μέσα σε ένα τέτοιο διαμορφωθέν περιβάλλον, όπου η δυνατότητα για ανταλλαγή παντός είδους πληροφοριών και σε τεράστιο όγκο αποτελεί δεδομένη δυνατότητα για τη συντριπτική πλειοψηφία του παγκόσμιου πληθυσμού, είναι προφανές ότι πλέον έχουμε περάσει στη λεγόμενη εποχή των Μεγάλων Δεδομένων.

Εν γένει, τρία είναι τα βασικά γνωρίσματα που χαρακτηρίζουν τα Μεγάλα Δεδομένα και τις ιδιαίτερες πτυχές και προεκτάσεις αυτών σε μια εφαρμογή. Αυτά τα γνωρίσματα είναι ο όγκος, η ποικιλία και η ταχύτητα.

Η συγκεκριμένη ομάδα χαρακτηριστικών αποτελεί σήμερα το κύριο κριτήριο για την επιλογή και τον χαρακτηρισμό δράσεων που σχετίζονται με Μεγάλα Δεδομένα στα διάφορα τεχνολογικά και οικονομικά πεδία, ενώ η ορθή επιλογή των εν λόγω χαρακτηριστικών, καθορίζει σε μεγάλο βαθμό και τα αποτελέσματα καθώς και το βαθμό επιτυχίας των αντίστοιχων εγχειρημάτων.

Όσον αφορά στους τομείς εφαρμογής τους, σήμερα απαντώνται 6 κύριες χρήσεις όσον αφορά στα Μεγάλα Δεδομένα. Αυτές σχετίζονται με τα πεδία των IT log analytics, της ανίχνευσης απάτης, των κοινωνικών δικτύων, της διασφάλισης της ποιότητας στα τηλεφωνικά κέντρα, των συστημάτων διαχείρισης ρίσκου και των συστημάτων ενέργειας.

Μέσα σε ένα τέτοιο πλαίσιο, είναι προφανές ότι θα πρέπει να εισαχθεί στις δράσεις της καθημερινής ζωής η έννοια της ψηφιοποίησης, με τις τεράστιες δυνατότητες που προσφέρει αυτή όσον αφορά κυρίως στη διάχυση των πληροφοριών.

Υπό αυτό το πρίσμα, θα πρέπει να μεταβληθεί και ο τρόπος προσέγγισης της έννοιας της ιδιωτικότητας προκειμένου να μπορέσει να περιλάβει και όλες εκείνες τις συνιστώσες που μπορεί να αποδειχτούν απειλητικές όσον αφορά στη διαφύλαξη της ιδιωτικότητας των προσωπικών δεδομένων με βάση και την ψηφιακή συνιστώσα.

Έτσι, με βάση την ψηφιακή παράμετρο, η έννοια της ιδιωτικότητας μπορεί να ταξινομηθεί πλέον στις εξής κατηγορίες: στην ιδιωτικότητα της επικοινωνίας, στην ιδιωτικότητα της συμπεριφοράς και στην προστασία της ανωνυμίας.

Οι Ηνωμένες Πολιτείες Αμερικής διακρίνονται από μια μεγαλύτερη ελευθερία όσον αφορά στη δυνατότητα για διακίνηση προσωπικών πληροφοριών σε σχέση με αυτήν στις ευρωπαϊκές χώρες.

Στο αμερικάνικο σύστημα, η προστασία της προσωπικής ελευθερίας αποτελεί την πρώτη προτεραιότητα, ακόμα και αν μερικές φορές το γεγονός αυτό μπορεί να οδηγήσει σε απώλεια της ιδιωτικότητας του ατόμου.

Από την άλλη, στο ευρωπαϊκό σύστημα, δίδεται πρώτη προτεραιότητα στην προστασία της ιδιωτικότητας των προσωπικών δεδομένων, με αποτέλεσμα να περιορίζεται αν κριθεί αναγκαίο ως ένα βαθμό η ελευθερία του ατόμου. προκειμένου να εξασφαλιστεί στο βέλτιστο δυνατό βαθμό αυτή η προστασία. Στο ευρωπαϊκό σύστημα, η προστασία των προσωπικών δεδομένων, είναι άμεσα συνυφασμένη με τις έννοιες της ανθρώπινης τιμής και αξιοπρέπειας, με αποτέλεσμα όλα τα πλαίσια δράσης να καθορίζονται με βάση αυτές τις δύο έννοιες.

Με βάση τις παραπάνω προτεραιότητες, οι συγκεκριμένες περιοχές καθορίζουν και το νομοθετικό πλαίσιο δράσης για την προστασία της ιδιωτικότητας των πληροφοριών.

Η Ευρωπαϊκή Ένωση θεωρείται πρωτοπόρος όσον αφορά στη θέσπιση αυστηρών πολιτικών για την προστασία της ιδιωτικής ζωής και των δεδομένων που σχετίζονται με αυτή, καθώς και για την υιοθέτηση νόμων που ευνοούν το άτομο και της προστασία της ιδιωτικότητας αυτού.

Το δικαίωμα στην ιδιωτική ζωή αποτελεί αναπόσπαστο μέρος των συνταγμάτων σχεδόν του συνόλου των χωρών της Ευρωπαϊκής Ένωσης με πρωτοπόρες χώρες προς αυτή την κατεύθυνση, τη Γερμανία και την Ισπανία.

Η ρητή και θεμελιώδης στήριξη της Ευρωπαϊκής Ένωσης στο δικαίωμα της ιδιωτικής ζωής καταγράφεται στην Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ), η οποία αποτελεί μια διεθνή συνθήκη σχετιζόμενη με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά στον ευρωπαϊκό χώρο.

Οι Ηνωμένες Πολιτείες Αμερικής από την άλλη, δεν διαθέτουν σήμερα ένα ολοκληρωμένο νομοθετικό ρυθμιστικό πλαίσιο δράσης όσον αφορά στην προστασία των προσωπικών δεδομένων στην ψηφιακή εποχή. Εντούτοις, διαθέτουν ένα πολύ αυστηρό ομοσπονδιακό πλαίσιο δράσης όσον αφορά στην προστασία ιδιωτικών πληροφοριών σε σχέση με τις τρεις ακόλουθες κατηγορίες: την προστασία των πληροφοριών σε σχέση με την παράμετρο της ιατρικής φροντίδας (νόμος HIPAA- Health Information and Portability Accountability Act), την προστασία των οικονομικών πληροφοριών (νόμος GLB - Gramm-Leach-Bliley), την προστασία των πληροφοριών σχετιζόμενων με παιδιά κάτω των 13 ετών (νόμος COPPA - Children’s Online Privacy Protection Act).

Εν γένει, κάθε χώρα και κάθε περιοχή ανά τον κόσμο, αναγνωρίζει το δικαίωμα στην ιδιωτική ζωή και προστατεύει αυτή είτε μέσω του συντάγματός της, είτε μέσω των δικαστικών αρχών, είτε μέσω της υιοθέτησης διεθνών συμφωνιών, ενώ αποτελεί αδιαπραγμάτευτο γεγονός σήμερα ότι η διάχυση οποιασδήποτε πληροφορίας μπορεί να λάβει χώρα από τη μια άκρη του κόσμου στην άλλη σε μερικές στιγμές και χωρίς να μεσολαβήσει οποιοδήποτε μέσο μεταφοράς παρά ένας ηλεκτρονικός υπολογιστής και μια σύνδεση στο διαδίκτυο.

Υπό αυτό το πρίσμα, ένας τέτοιος τύπος πληροφορίας είναι προφανές ότι δεν μπορεί να υπόκειται στους κανόνες και νόμους κάποιας συγκεκριμένης χώρας μιας και ουσιαστικά μεταφέρεται σε παγκόσμιο επίπεδο.

Με βάση την παραπάνω επισήμανση, καθίσταται κάτι παραπάνω από επιτακτική σήμερα η ανάγκη για υιοθέτηση μιας κοινής νομοθεσίας σε παγκόσμιο επίπεδο, σε σχέση με τη διάχυση και προστασία της ιδιωτικότητας των προσωπικών δεδομένων.

Ένα τέτοιο εγχείρημα βέβαια μόνο εύκολο δεν είναι. Πολλές χώρες και κυρίως οι ισχυρότερες εξ αυτών, θα προσπαθήσουν να επιβάλουν στο μεγαλύτερο βαθμό τη δική τους νομοθεσία στην προσπάθεια αυτή με βάση τις ιδιαίτερες επιδιώξεις και χαρακτηριστικά τους, με αποτέλεσμα μέχρι και σήμερα, ένα τέτοιο εγχείρημα να αποτελεί ουσιαστικά μια ιδέα που θα πρέπει να συζητηθεί εκτενέστερα και πιο ουσιαστικά στο μέλλον. Η σύγκρουση ιδεών μεταξύ των χωρών σίγουρα αποτελεί και θα αποτελέσει ένα σημαντικό εμπόδιο για τη δημιουργία ενός κοινού παγκόσμιου πλαισίου νομοθετικής δράσης.

Αλλά ακόμα και αν επιτευχθεί ένα τέτοιο εγχείρημα, το άτομο ως αυτόνομη μονάδα θα είναι αυτό που πάντα θα καλείται να διαδραματίσει πρωτεύοντα ρόλο στο πως μπορεί να προστατέψει την ιδιωτική του ζωή και τις πληροφορίες που σχετίζονται με αυτή, θέτοντας ταυτόχρονα τα προσωπικά του όρια όσον αφορά στην έκταση και του είδους των πληροφοριών που θα γνωστοποιεί σε διαδικτυακά περιβάλλοντα.

Υπό αυτό το πρίσμα, εν τέλει οι αυτόνομες μονάδες είναι αυτές παροντικά και μελλοντικά που στην ψηφιακή εποχή καλούνται να μεταφράσουν κατά το δοκούν την έννοια της ιδιωτικότητας για λογαριασμό τους και με βάση τις προσωπικές τους αντιλήψεις, διαμορφώνοντας ταυτόχρονα και το ανάλογο προσωπικό πλαίσιο δράσης για την προστασία των προσωπικών τους δεδομένων.

Η εφαρμογή των αρχών των Ανοικτών Δεδομένων στα Μεγάλα Δεδομένα μπορεί να βοηθήσει αυτή την προσπάθεια του ατόμου να προστατέψει τα προσωπικά του δεδομένα στη σύγχρονη ψηφιακή εποχή, με τη δράση αυτή να αποτελεί τη

μεγαλύτερη πρόκληση στο πεδίο των Μεγάλων Δεδομένων όσον αφορά στην επίλυση των δύσκολων ζητημάτων που έθεσαν αυτά στο σημερινό ψηφιακό γίγνεσθαι.

Τα Μεγάλα Δεδομένα αναντίρρητα μας δίνουν πρωτοφανή δύναμη να κατανοήσουμε και να αναλύσουμε τον κόσμο που ζούμε, όμως τα Ανοικτά Δεδομένα είναι αυτά που θα μας εξασφαλίσουν την ταυτόχρονη προστασία των προσωπικών μας δεδομένων κατά την εξέλιξη αυτής της διαδικασίας, έτσι ώστε αυτή να καταστεί ωφέλιμη και όχι καταστρεπτική για το άτομο μεμονωμένα και για την παγκόσμια κοινωνία γενικότερα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Craig, T., & Ludloff, M., (2011), ‘Privacy and Big Data’, Sebastopol: O’Reilly Media.
- Zikopoulos, P., et al., (2012), Understanding Big Data, , New York: McGraw Hill.

Διαδίκτυο:

- http://bigdata.csail.mit.edu/Big_Data_Privacy
- <https://epic.org/privacy/big-data/>
- <http://www.ibm.com/big-data/us/en/>
- http://www.sas.com/el_gr/insights/big-data/what-is-big-data.html
- <http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data>