ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Privacy by Design

και η τεχνολογική διάσταση της προστασίας προσωπικών πληροφοριών στο Σχέδιο Κανονισμού της Ευρωπαϊκής Ένωσης

Θεογνωσία Αζά

M3110021

Αθήνα, Φεβρουάριος 2013

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)

στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Privacy by Design

και η τεχνολογική διάσταση της προστασίας προσωπικών πληροφοριών στο Σχέδιο Κανονισμού της Ευρωπαϊκής Ένωσης

Αζά Θεογνωσία

M3110021

Επιβλέπων Καθηγητής: Λίλιαν Μήτρου

Εξωτερικός Κριτής: Μαριάνθη Θεοχαρίδου

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Αθήνα, Φεβρουάριος 2013

Ευχαριστίες

Σε αυτό το σημείο θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στην επίκουρη καθηγήτρια και επιβλέπουσα της διπλωματικής μου εργασίας, κα Λίλιαν Μήτρου για την πολύτιμη βοήθεια και υποστήριξη που μου παρείχε σε όλη τη διάρκεια της εκπόνησης της παρούσας εργασίας.

Επίσης ιδιαίτερες ευχαριστίες θα ήθελα να δώσω σε όλους τους καθηγητές του Μεταπτυχιακού Προγράμματος Σπουδών του Οικονομικού Πανεπιστημίου Αθηνών στα Πληροφοριακά Συστήματα για τις πολύτιμες γνώσεις που αποκόμισα καθ' όλη τη διάρκεια των σπουδών μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου για την αδιάλειπτη στήριξη της σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περίληψη

Στη σύγχρονη κοινωνία, η ραγδαία αύξηση στη χρήση του διαδικτύου, την κινητή τηλεφωνία και στις εφαρμογές κοινωνικής δικτύωσης καθώς και η αυξημένη χρήση των νέων τεχνολογιών στη καθημερινότητα, κάνουν επιτακτική την ανάγκη για προστασία της ιδιωτικότητας. Σε αυτή την κοινωνία ο χρήστης θα πρέπει να μπορεί να προστατέψει τα δεδομένα του, και τις πληροφορίες του από τη συγκέντρωση και επεξεργασία που μπορούν να υποστούν από τρίτους.

Η ιδιωτικότητα είναι ένα σημαντικό συστατικό της ελευθερίας και παίζει σημαντικό ρόλο στην προστασία των θεμελιωδών δικαιωμάτων του ανθρώπου. Όμως γίνεται όλο και πιο δύσκολο να αγνοήσουμε το γεγονός ότι χωρίς τα κατάλληλα επίπεδα της ιδιωτικότητας, τα δικαιώματα ενός ατόμου μειώνονται.

Οι χρήστες θέλουν να προστατεύσουν την ιδιωτικότητα τους, ιδιαίτερα σε τομείς όπως τα κοινωνικά δίκτυα, ωστόσο όμως οι χρήστες κοινωνικών δικτύων σπάνια ξέρουν πώς να προστατεύουν την ιδιωτικότητα τους.

Αυτό που απαιτείται είναι μια νέα προσέγγιση που να παρέχει στους χρήστες νόμιμο έλεγχο πάνω στις προσωπικές τους πληροφορίες, διατηρώντας παράλληλα και τα πλεονεκτήματα της χρήσης διαδικτυακών υπηρεσιών όπως τα κοινωνικά δίκτυα. Ο καλύτερος τρόπος για να επιτευχθεί αυτό είναι οι πληροφορίες του κάθε ατόμου να συλλέγονται μόνο όταν αυτό κρίνεται απαραίτητο.

Αρχικά, αυτή η προσέγγιση ήταν οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs). Πρόκειται για λογισμικά και συστήματα που επιτρέπουν στα άτομα να αποκρύψουν τα πραγματικά τους στοιχεία από τη λειτουργία αυτών των ηλεκτρονικών συστημάτων ή από την παροχή υπηρεσιών μέσω αυτών και να αποκαλυφθούν μόνο όταν είναι απολύτως απαραίτητο. Οι τεχνολογίες αυτές συμβάλλουν στην ελαχιστοποίηση των πληροφοριών που συλλέγονται για τα άτομα και περιλαμβάνουν ανώνυμα προγράμματα περιήγησης στον παγκόσμιο ιστό, ειδικευμένες υπηρεσίες ηλεκτρονικού ταχυδρομείου και ψηφιακό χρήμα

Μια άλλη προσέγγιση είναι η «Privacy by Design (PbD)» η οποία θα μπορέσει να μετριάσει τα πολλά από τα ζητήματα της ιδιωτικότητας σε πληροφοριακά συστήματα που κάνουν χρήση διαδικτύου και θα μπορούσε να είναι και ένας πιθανός τρόπος για τη προστασία των προσωπικών δεδομένων των χρηστών. Αυτό επιτυγχάνεται με την

άμεση ενσωμάτωση της ιδιωτικότητας στο σχεδιασμό και τη λειτουργία των συστημάτων.

Σκοπός της παρούσας διπλωματικής είναι η ανάλυση της αναγκαιότητας και της χρησιμότητας της προστασίας της ιδιωτικότητας καθώς και των προσωπικών δεδομένων. Θα πρέπει να γίνει κατανοητή η έννοια της ιδιωτικότητας και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αφού πρώτα αναπτυχθεί η έννοια των προσωπικών δεδομένων καθώς και οι βασικές αρχές τους.

Στη συνέχεια θα γίνει αναφορά στις απειλές κατά της Ιδιωτικότητας έτσι να μπορέσει να γίνει κατανοητό το τι θα πρέπει να αποτρέπουν τα μέτρα προστασίας της ιδιωτικότητας. Ακόμη ένα ζήτημα το οποίο πρέπει να γίνει κατανοητό είναι η συσχέτιση Ιδιωτικότητας και Ασφάλειας και γιατί οι δύο αυτές έννοιες είναι διαφορετικές.

Ακόμη ένα θέμα που αναπτύσσεται στην παρούσα διπλωματική είναι οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (PETs), ο σκοπός δημιουργίας τους, οι λειτουργίες τους καθώς επίσης και η έννοια της Privacy by Design ο σκοπός της και ο τρόπος με τον οποίο συμπεριλαμβάνονται στον κύκλο ζωής ανάπτυξης των συστημάτων.

Τέλος, θα αναλυθεί η πραγμάτευση στο Σχέδιο Κανονισμού της Ευρωπαϊκής Ένωσης, Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα καθώς και το αντίστοιχο νομοθετικό πλαίσιο της Ελλάδος (2472/1997), δίνοντας έμφαση στα άρθρα 16 και 17 της Οδηγίας 95/46/ΕΚ και στο άρθρο 10 του νόμου 2472/1997 καθώς και στη συσχέτιση τους με τη Privacy by Design. Επίσης, θα σχολιαστούν οι τροποποιήσεις που πραγματοποιούνται στο νομοθετικό πλαίσιο βάση των τεχνολογικών εξελίξεων καθώς και η Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία δεδομένων και το άρθρο 17 το οποίο προβλέπει το «δικαίωμα στη λήθη».

Abstract

In modern society, the rapid increase in the use of Internet, mobile phones and social networking applications as well as the increased use of new technologies in everyday life, make a compelling case for privacy protection. In this society the user should be able to protect their data, and the information from the collection and processing that they can suffer from third parties.

Privacy is an important component of liberty and plays an important role in the protection of fundamental human rights. But it is becoming increasingly difficult to ignore the fact that without adequate levels of privacy, the rights of an individual are reduced.

Users want to protect their privacy, particularly in areas such as social networks, however though social networks users rarely know how to protect their privacy.

What is needed is a new approach that can provide users with legitimate control over their personal information, while maintaining the advantages of using Web services like social networks. The best way to achieve this is each person's information is collected only when that judge necessary.

Originally this approach was the privacy enhancing technologies (PETs). It is software and systems that allow individuals to conceal their real details from the operation of these systems or the provision of services through these, and are disclosed only when absolutely necessary. These technologies contribute to minimizing information collected for individuals and include anonymous Web browsing programs, specialized email services and digital cash

Another approach is the "Privacy by Design (PbD)" which will be able to mitigate many of the issues of privacy in information systems that make use of the Internet and could be a potential way for the protection of personal data of users. This is accomplished with the direct integration of privacy in design and operation of systems.

The aim of this diploma thesis is the analysis of the necessity and usefulness of the protection of privacy and personal data. You need to understand the concept of

privacy and the processing of personal data, after first developing the concept of personal data as well as the fundamentals.

Then I made reference to the threats to privacy so we can understand what we need to prevent privacy measures. Another issue which needs to be understood is the correlation between security and Privacy, and why these two concepts are different.

Yet it is a matter of developing the present diploma is Privacy enhancing technologies (PETs), the purpose of their creation and their functions as well as the concept of privacy by design the purpose and the way in which are included in the life cycle of systems development.

Finally, the discussion on the draft regulation of the European Union, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the relevant legal framework in Greece (2472/1997). with an emphasis in articles 16 and 17 of Directive 95/46/EC and in article 10 of law 2472/1997 as well as in association with the Privacy by design also made amendments to the legislative framework against technological developments as well as the Proposal for a regulation proposal of the European Parliament and of the Council on data protection and article 17 which provides for the "right to be forgotten".

Περιεχόμενα

Εισαγωγή 10

Ιδιωτικότητα 13

2.1 Οι μορφές της έννοιας της ιδιωτικότητας 14

2.2 Εννοιολογικό πλαίσιο 15

2.2.1 Προσωπικά Δεδομένα 15

2.2.2 Ευαίσθητα προσωπικά δεδομένα 16

2.2.3 Πληροφορία και Δεδομένο 16

2.2.4 Υποκείμενο των δεδομένων 17

2.2.5 Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα 17

2.2.6 Υπεύθυνος επεξεργασίας 17

2.3 Προσωπικά Δεδομένα 17

2.3.1 Βασικές αρχές των προσωπικών δεδομένων 18

2.3.2 Προσωπικά Δεδομένα στο Διαδίκτυο 19

2.4 Απειλές ιδιωτικότητας 20

2.5 Ιδιωτικότητα και Ασφάλεια 22

Τεχνολογίες για Προστασία της Ιδιωτικότητας 25

3.1 Ιστορία των PETs 25

3.1.1 Τι είναι οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs); 26

3.1.2 Περαιτέρω εξελίξεις των PETs 30

3.1.3 Εργαλεία Προστασίας της Ιδιωτικότητας 34

3.2 Τεχνολογίες για τη διασφάλιση της ιδιωτικότητας των χρηστών 35

3.2.1 TOR 35

3.2.2 Anonymizer 35

3.2.3 Anonymous remailer 35

3.2.4 P3P 36

3.2.5 Pretty Good Privacy 36

3.2.6 SSL 37

3.4 Τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs) και Ιδιωτικότητα βάση σχεδιασμού (PbD) 37

3.5 Τι είναι η προσέγγιση Privacy by Design; 38

3.5.1 Οι 7 θεμελιώδεις αρχές του Privacy by Design 39

3.5.2 Privacy by design στο κύκλο ζωής των συστημάτων 40

3.5.3 Αρχές Privacy By Design ως Privacy By Default 41
3.6 Privacy By Default 41
Κοινωνία της Πληροφορίας -Αυτορρύθμιση 43
4.1 Κοινωνία της Πληροφορίας 43
4.1.1 Δίκαιο στη κοινωνία της Πληροφορίας 44
4.2Αυτορύθμιση 44
4.2 Πλεονεκτήματα –Μειονεκτήματα Αυτορρύθμισης 45
4.2.1 Πλεονεκτήματα 45
4.2.2 Μειονεκτήματα 46
4.3 Η ανάγκη ύπαρξης Ρυθμίσεων 46
Νομοθετικό πλαίσιο 48
5.1 Διεθνές νομοθετικό πλαίσιο 48
5.1.1 Οδηγία 95/46/ΕΚ 50
5.2 Νομοθετικές Διατάξεις στην Ελλάδα 54
5.2.1 Νόμος 2472/97 55
5.2.2 Νόμος 3471/06 58
5.3 Πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία δεδομένων. 59
5.4Νομοθετικές Διατάξεις και Privacy by Design 61
5.4.1 Privacy by design στο Διεθνές Νομοθετικό πλαίσιο. 63
5.4.2 Privacy by design στο Ελληνικό δίκαιο 65
5.5 Δικαίωμα στη λήθη 66
Επίλογος 69
ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ 74

1

Εισαγωγή

Στη σημερινή κοινωνία παρατηρούνται αλλαγές σε όλες τις πτυχές της καθημερινής ζωής. Κάθε αλλαγή μπορεί να επιφέρει θετικά αποτελέσματα, αλλά όπως και στο κάθε τι, θα υπάρξουν και αρνητικά συνεπακόλουθα. Για παράδειγμα, παράλληλα με την ανάπτυξη της τεχνολογίας, πληθαίνουν και οι ανάγκες για ανάπτυξη και σε άλλους τομείς, οι οποίοι είναι αλληλένδετοι. Οι μεγάλες αλλαγές στον τεχνολογικό τομέα, τα μέσα κοινωνικής δικτύωσης, καθώς και η αύξηση της χρήσης του διαδικτύου, συνεπάγεται με τη διακίνηση μεγαλύτερου όγκου προσωπικών δεδομένων. Επισημαίνεται ότι η συλλογή, όσο περισσότερων προσωπικών δεδομένων για το κάθε άτομο ξεχωριστά, μπορεί να μην έχουν το επιθυμητό αποτέλεσμα. Η συλλογή τους χωρίς την προσωπική έγκριση από τον χρήστη, μπορεί να χρησιμοποιηθεί για σκοπό διαφορετικό από τον αρχικό του.

Αναμφίβολα, η αξιοποίηση της πληροφορίας συμβάλλει καταλυτικά όχι μόνο στην οικονομική ανάπτυξη αλλά και στη βελτίωση των συνθηκών σε σημαντικούς τομείς της ζωής μας, στην εκπαίδευση, την έρευνα, την εργασία, την υγεία και ασφάλιση, τις μεταφορές και τις κοινωνικές σχέσεις.

Οι τεχνολογικές αλλαγές επιφέρουν μεγαλύτερη ευκολία στην αποθήκευση δεδομένων και στην επεξεργασία τους, αφού πλέον η επεξεργασία είναι μια αυτοματοποιημένη διαδικασία. Η ανάπτυξη της υπολογιστικής ισχύς, όπως επίσης και η μείωση του κόστους στην αποθήκευση δεδομένων, επιτρέπουν τη γρήγορη επεξεργασία μεγάλου όγκου δεδομένων καθώς και τη συσχέτιση διαφόρων αρχείων. Αυτό μπορεί να εξελιχθεί σε ένα πολύ μεγάλο πρόβλημα εις βάρος της κοινωνίας του σήμερα.

Λαμβάνοντας υπόψη τα πιο πάνω, παρατηρείται η ανάγκη για την προστασία της ιδιωτικότητας του ατόμου. Αρχικά, το πρώτο μεγάλο (σημαντικό) βήμα προς την επίτευξη αυτού του στόχου, είναι ο περιορισμός των προσωπικών δεδομένων που διακινούνται στο διαδίκτυο, όπως και το δικαίωμα των χρηστών να επιλέγουν ποια από τα δεδομένα τους θα γνωστοποιούνται και για πιο σκοπό.

Για πάνω από τριάντα χρόνια, ο δημόσιος και ο ιδιωτικός τομέας είχαν στραφεί για την προστασία της ιδιωτικότητας στην τήρηση των αρχών της πρακτικής της δίκαιας πληροφόρησης ("FIPPs"- Fair Information Practice Principles). Οι τοπικές οδηγίες, τα διεθνή μέσα, η συνολική και η τομεακή νομοθεσία καθώς και τα έγγραφα καθοδήγησης σε όλο το κόσμο διαμορφώθηκαν με βάση αυτές τις αρχές.
Μέχρι πρόσφατα, η τήρηση των πολιτικών βασισμένων στις FIPPs μέσω της ενσωμάτωσης στις θεσμικές πολιτικές και διαδικασίες εθεωρείτο σε μεγάλο βαθμό επαρκής για την αντιμετώπιση των προβληματισμών που προκύπτουν από τη συλλογή δεομένων στον ιδιωτικό τομέα[1].

Ενώ το μοντέλο FIPPs της προστασίας της ιδιωτικότητας, καθώς και η θεωρία της «Πληροφοριακής αυτοδιάθεσης» στην οποία στηρίζεται συνεχίζει να συμβαδίζει με τις προκλήσεις της ιδιωτικότητας σε πολλούς τομείς της οικονομίας και των ρυθμιστικών αρχών σε όλο τον κόσμο, έχουν αρχίσει να απαιτούνται περισσότερα από τις επιχειρήσεις, ιδιαίτερα σε εταιρείες που ανήκουν στους τομείς της τεχνολογίας πληροφοριών και επικοινωνιών.

Το αυξανόμενο ενδιαφέρον που παρουσιάζεται για τις σελίδες κοινωνικής δικτύωσης και τις πλατφόρμες κοινωνικής αλληλεπίδρασης σε ένα ευρύ φάσμα, όπως η επικοινωνία και η αλληλεπίδραση μεταξύ ατόμων και ομάδων, αποτελούν πρόκληση σε αυτό το μοντέλο προστασίας της ιδιωτικότητας. Μια μεγάλη αύξηση σφαλμάτων για την προστασία της ιδιωτικότητας στις σελίδες κοινωνικής δικτύωσης και τις πλατφόρμες οδηγεί στην αναζήτηση για εύρεση νέων κανονιστικών προσεγγίσεων. Πολλά από αυτά τα σφάλματα ιδιωτικότητας έχουν σχέση με τις αλληλεπιδράσεις μεταξύ των χρηστών.

Οι Ρυθμιστικές αρχές προστασίας προσωπικών δεδομένων σε όλο τον κόσμο γίνονται ολοένα και πιο απαιτητικές έτσι ώστε οι FIPPs να ενημερώνουν το σχεδιασμό τεχνικών συστημάτων. Στο παρελθόν οι FIPPs είχαν σε μεγάλο βαθμό απορροφηθεί μέσω της υιοθέτησης πολιτικών και διαδικασιών εντός των επιχειρήσεων γιατί η προστασία της ιδιωτικότητας ήταν στη «δικαιοδοσία» των νομικών.

Πλέον, με τις τεχνολογίες ενίσχυσης της ιδιωτικότητας στις εφαρμογές οι οποίες μπορούν να οριοθετήσουν τη συλλογή δεδομένων, όπως και την ανεπιθύμητη επεξεργασία τους καθώς και με τη λογική της «ιδιωτικότητας από το σχεδιασμό» (Privacy by Design) για τη χάραξη πολιτικής, ζητούν από τον ιδιωτικό τομέα να

γίνεται χρήση των ξεχωριστών ιδιοτήτων του κώδικα για μεγαλύτερη προστασία της ιδιωτικότητας. Η πρόσκληση για την προστασία της ιδιωτικότητας βάσει σχεδιασμού, δηλαδή την πρακτική ενσωμάτωσης της προστασίας της ιδιωτικότητας σε προϊόντα και υπηρεσίες στη φάση σχεδιασμού και όχι αργότερα, είναι να αναγνωριστεί η ισχύς της τεχνολογίας όχι μόνο στην εφαρμογή αλλά και στη διευθέτηση της πολιτικής μέσα από την αρχιτεκτονική, τις διεπαφές, τη διαμόρφωση (configuration) και τις προεπιλεγμένες ρυθμίσεις[2].

Σκοπός της παρούσας εργασίας είμαι ο καθορισμός της ιδιωτικότητας και των κινδύνων που αντιμετωπίζει η ιδιωτικότητα κάθε ατόμου από την ανάπτυξη των τεχνολογιών καθώς επίσης και το κατά πόσο οι οδηγίες/νόμοι της Ευρωπαϊκής ένωσης και της Ελλάδας συμβαδίζουν με τις τεχνολογικές εξελίξεις.

Στη συνέχεια θα μελετηθούν οι τεχνολογίες ενίσχυσης της ιδιωτικότητας και η Privacy by Design. Επιπλέον, θα μελετηθεί το πώς οι τεχνολογίες αυτές μπορούν να βοηθήσουν στη διατήρηση της ιδιωτικότητας.

Τέλος θα δούμε αν οι τεχνολογίες αυτές υποστηρίζονται από τους νόμους και τις οδηγίες της Ευρωπαϊκής Ένωσης.

2

Ιδιωτικότητα

Η ιδιωτικότητα είναι μια έννοια που αν και χρησιμοποιείται συχνά στην καθημερινή μας ζωή και σε διαφόρους επιστημονικούς κύκλους (τεχνολογικούς, νομικούς), δεν έχει ένα μοναδικό ορισμό που να την καλύπτει. Η ιδιωτικότητα είναι το δικαίωμα ενός ατόμου να αποφασίζει μόνο του σε κάθε περίπτωση πότε, κάτω από ποιες συνθήκες και ποια από τα προσωπικά του δεδομένα θα αποκαλυφθούν και θα μπορούν να χρησιμοποιηθούν και από άλλους. Επίσης η ιδιωτικότητα είναι στενά συνδεδεμένη με την ελευθερία του ατόμου να διατηρεί το προσωπικό του χώρο.

Η ιδιωτικότητα είναι θεμελιώδες ανθρώπινο δικαίωμα. Αποτελεί το ουσιώδες συστατικού της αξιοπρέπειας και της ελευθερίας μας. Η ιδιωτική και οικογενειακή ζωή κάθε ατόμου είναι απαραβίαστη. Όσο συνειδητοποιούμε την αξία της ύπαρξης της και αποκτούμε επίγνωση των απειλών εναντίον αυτής, καταλαβαίνουμε την αναγκαιότητα για την προστασία της.

Συμφώνα με τον Samuel D. Warren και τον Louis D. Brandeis στο άρθρο τους «The Right to Privacy»(1890), η ιδιωτικότητα καθορίζεται ως «*το δικαίωμα της απομόνωσης*»[3]. Αργότερα το 1967 ο Alan Westin (Columbia University) ορίζει την ιδιωτικότητα ως «την *αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των* προσωπικών τους δεδομένων»[4].

Η Ruth Gavison αναγνωρίζει τρία στοιχεία της ιδιωτικότητας: τη μυστικότητα (secrecy), την ανωνυμία (anonymity) και τη μοναξιά (solitude), υπογραμμίζοντας ότι πρόκειται για μια ρευστή κατάσταση η οποία, ανάλογα με τις επιλογές κάθε ατόμου, μπορεί να χαθεί[5]. Ο Edward Bloustein κρίνει το δικαίωμα της ιδιωτικότητας ως απαραίτητη προϋπόθεση για την ανθρώπινη αξιοπρέπεια[6].

Με τα παραπάνω διαπιστώνουμε ότι η ιδιωτικότητα δεν έχει ένα μοναδικό ορισμό που να την καλύπτει ολοκληρωτικά.

2.1 Οι μορφές της έννοιας της ιδιωτικότητας

- Πληροφοριακή ιδιωτικότητα (informational privacy). Ανεβαίνει στο προσκήνιο το ’60 και το ’70 όταν οι κυβερνήσεις ανακαλύπτουν την αυτοματοποιημένη επεξεργασία δεδομένων ως αποτελεσματικό μέσο για την καταλογράφηση πολιτών. Η Πληροφοριακή ιδιωτικότητα περιλαμβάνει τη θέσπιση κανόνων που διέπουν τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως χρηματοπιστωτικές πληροφορίες, ιατρικά και κυβερνητικά αρχεία. Είναι αυτή η πτυχή την οποία αποκαλούμε και «προστασία προσωπικών δεδομένων».

  Αναμφισβήτητα, η νομική προστασία της πληροφοριακής ιδιωτικότητας σε ένα τοπίο συνεχών τεχνολογικών αλλαγών, κρύβει κινδύνους για την καταπάτηση του δικαιώματος και την προσβολή της προσωπικότητας του ατόμου με την προβολή ή τη χρήση προσωπικών δεδομένων. Η ανάγκη των ανθρώπων για την προάσπιση της ιδιωτικότητας οδήγησε πολλά κράτη στη θέσπιση νόμων προστασίας δεδομένων.
- Σωματική ιδιωτικότητα (bodily privacy), αφορά την προστασία του φυσικού εαυτού των ανθρώπων ενάντια σε επεμβατικές διαδικασίες, όπως γενετικοί και φαρμακευτικοί έλεγχοι ή σωματική ψηλάφηση.
- Τηλεπικοινωνιακή ιδιωτικότητα (communications privacy), η οποία καλύπτει την ασφάλεια και την ιδιωτικότητα αλληλογραφίας, τηλεφωνικών συνδιαλέξεων, ηλεκτρονικών μηνυμάτων (email) και άλλων μορφών επικοινωνίας.
- Εδαφική ιδιωτικότητα (territorial privacy), που αφορά την οριοθέτηση ιδιωτικών χώρων, αλλά και χώρων όπως το περιβάλλον εργασίας ή η δημόσια σφαίρα [7].

Η ιδιωτικότητα των ατόμων γίνεται όλο και περισσότερο πιο σημαντική σε μια όλο και περισσότερο δικτυωμένη κοινωνία και πρέπει να προστατευθεί με μερικά μέσα. Η προστασία της ιδιωτικότητας δεν μπορεί να επιτευχθεί μόνο με την επιβολή και εφαρμογή των νόμων για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, οι οποίοι προωθούνται από την κυβέρνηση.

Για να μπορέσει να επιτευχθεί θα πρέπει να υπάρχουν τα ακόλουθα:

- εκπαίδευση των επαγγελματιών Πληροφορικής, σχετικά με την ιδιωτικότητα και την υιοθέτηση χρήσης τεχνολογιών ενίσχυσής της. Τα ζητήματα περί ιδιωτικότητας πρέπει να αποτελούν ένα σημαντικό μέρος της εκπαίδευσης των επιστημόνων υπολογιστών. Η ιδιωτικότητα πρέπει να αποτελεί ένα αναπόσπαστο κριτήριο στο σχεδιασμό συστημάτων. Έμφαση πρέπει να δίνεται στο σχεδιασμό συστημάτων που «αποδέχονται» και διαφυλάσσουν την ιδιωτικότητα του ατόμου. Οι επιστήμονες των υπολογιστών πρέπει να είναι εξοικειωμένοι με τις νομικές απαιτήσεις της προστασίας των δεδομένων και πώς να τις επιβάλουν.

- εκτεταμένη ενημέρωση των καταναλωτών σχετικά με την ιδιωτικότητα και τη χρήση τεχνολογιών ενίσχυσής της. Οι χρήστες και οι πελάτες χρειάζονται πληροφόρηση και εκπαίδευση για τα δικαιώματά τους, για την αξία των προσωπικών στοιχείων τους, για τους κινδύνους υπονόμευσης της ιδιωτικότητας και τις δυνατότητες προστασίας από τεχνολογίες ενίσχυσης ιδιωτικότητας (PETs – Privacy Enhancing Technologies).

- Επίσης, απαραίτητη είναι και η αυτορρύθμιση από τους κώδικες δεοντολογίας σχετικά με τις δίκαιες πρακτικές πάνω σε πληροφορίες, που προωθούνται από τις επιχειρήσεις. Η αυτορρύθμιση (self-regulation) βασίζεται στο γεγονός ότι οι οργανώσεις και η βιομηχανία θα περιορίσουν τις πρακτικές τους σύμφωνα με τις αρχές πληροφοριών. Για να είναι αποτελεσματική επιβολή της αυτορρύθμισης πρέπει να υπάρχει επαρκής έλεγχος.

Όσον αφορά τους νόμους περί προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων θα αναφερθούμε εκτενέστερα σε επόμενο κεφάλαιο.

2.2 Εννοιολογικό πλαίσιο

2.2.1 Προσωπικά Δεδομένα

Με την έννοια Προσωπικά Δεδομένα ή «δεδομένα προσωπικού χαρακτήρα», εννοούνται όλες οι πληροφορίες που αναφέρονται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί. Ως πρόσωπο του οποίου η ταυτότητα

μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη.

2.2.2 Ευαίσθητα προσωπικά δεδομένα

Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.

2.2.3 Πληροφορία και Δεδομένο

Συχνά παρατηρείται η ταυτόχρονη χρήση και εναλλαγή των όρων «πληροφορία» (information) και «δεδομένο» (data). Η «πληροφορία» δηλώνει το αποτέλεσμα της ερμηνείας των δεδομένων, καθώς και ότι τα δεδομένα αναδείχθηκαν και καθιερώθηκαν ως ξεχωριστός όρος σε συνάρτηση με την επεξεργασία δεδομένων και κυρίως με την ανάπτυξη και διάδοση της αυτοματοποιημένης επεξεργασίας δεδομένων. Η συσχέτιση του όρου δεδομένο με την τεχνολογία αναδεικνύει τον τεχνικό του χαρακτήρα και το προσδιορίζει ως στοιχείο μιας «επεξεργασμένης» πληροφορίας [8].

Η έννοια της πληροφορίας παραπέμπει αυτόματα στην πληροφοριακή αξία της, γεγονός που δεν ισχύει με την έννοια του δεδομένου. Ενώ στην έννοια του δεδομένου προσδίδεται μία ουδετερότητα όσον αφορά τον σκοπό, η έννοια της πληροφορίας συσχετίζεται με τη χρησιμότητά της. Η πληροφορία (information) είναι το αποτέλεσμα που προκύπτει από κάποια κατάλληλη επεξεργασία δεδομένων. Η πληροφορία αυξάνει τη γνώση και η διάθεσή της συμβάλει στη λήψη αποφάσεων. Οι πληροφορίες που παίρνουμε από την επεξεργασία δεδομένων μπορεί να χρησιμοποιηθούν ως νέα δεδομένα για περαιτέρω επεξεργασία και να δώσουν ως αποτελέσματα νέες πληροφορίες. Έτσι, πολλές φορές, ο όρος επεξεργασία πληροφοριών χρησιμοποιείται ως ταυτόσημος της επεξεργασίας δεδομένων. Μάλιστα, από τη δεκαετία του `80 ο όρος επεξεργασία πληροφοριών επικράτησε

γιατί οι υπολογιστές μπορούν πλέον να επεξεργάζονται πληροφορίες αντί των στοιχειωδών δεδομένων.

2.2.4 Υποκείμενο των δεδομένων

Ορίζεται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική[9].

2.2.5 Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Με την έννοια «Επεξεργασία» εννοούμε κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα. Σε αυτές συγκαταλέγονται η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή.

2.2.6 Υπεύθυνος επεξεργασίας

Κάθε φυσικό ή νομικό πρόσωπο του δημόσιου ή ιδιωτικού τομέα που τηρεί και επεξεργάζεται προσωπικά δεδομένα. Επιπλέον καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

2.3 Προσωπικά Δεδομένα

Σύμφωνα με το άρθρο 9Α του αναθεωρημένου το 2001 ελληνικού Συντάγματος, το δικαίωμα στην προστασία των προσωπικών δεδομένων ορίζεται ως εξής: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως ο νόμος ορίζει» [10].

Επίσης σύμφωνα με απόφαση του Γερμανικού Συνταγματικού Δικαστηρίου το κάθε άτομο έχει το δικαίωμα της πληροφοριακής αυτοδιάθεσης. Παρέχεται, δηλαδή σε κάθε φυσικό προσώπου το δικαίωμα του να κρίνει και να αποφασίζει αν επιθυμεί την αποκάλυψη ή/και την επεξεργασία των προσωπικών του δεδομένων. Κάθε πολίτης έχει δικαίωμα να επιτρέπει ή να απαγορεύει τη χρήση των δεδομένων που τον αφορούν. Οι προϋποθέσεις υπό τις οποίες μπορεί να ασκήσει αυτό το δικαίωμα, προβλέπονται από τη νομοθεσία για την προστασία των προσωπικών δεδομένων. Επίσης καθένας έχει δικαίωμα να ζητήσει πρόσβαση στις πληροφορίες που τηρεί άλλος γι' αυτόν, καθώς και να ζητήσει την διόρθωσή τους, εφόσον δεν είναι ακριβείς.

Η προστασία των δεδομένων του ατόμου έχει σκοπό τη διασφάλιση της ιδιωτικότητας. Παρόλα αυτά η ιδιωτικότητα, δεν παύει να είναι ένα οροθετημένο δικαίωμα, καθώς μπορεί να έρθει σε σύγκρουση με άλλα δικαιώματα ή νομικές αξίες. Επιπλέον, η συμμετοχή των ατόμων στη κοινωνία χωρίς την αποκάλυψη ενός μέρους των προσωπικών τους δεδομένων δεν είναι εφικτή. Οι νόμοι περί Προστασίας της Ιδιωτικότητας και των Δεδομένων τίθενται σε εφαρμογή μόνο σε περιπτώσεις συλλογής και επεξεργασίας των δεδομένων.

2.3.1 Βασικές αρχές των προσωπικών δεδομένων

Σε αυτό το σημείο, θα μελετηθούν οι βασικές αρχές των προσωπικών δεδομένων, οι οποίες πρέπει να τηρούνται για να υπάρχει η θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα. Λόγο των εξελίξεων στις τεχνολογίες πληροφορικής και επικοινωνιών, οι ρυθμίσεις από μόνες τους δεν μπορούν να εξασφαλίσουν την τήρηση των αρχών αυτών γιατί αλλάζει ριζικά ο τρόπος με τον οποίο θα πρέπει να εξασφαλιστούν. Λύση σε αυτό το πρόβλημα έρχεται να δώσει η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, που αποσκοπεί στη διασφάλιση της εφαρμογής αυτών των αρχών, αφού πλέον η προστασία των δεδομένων δεν είναι μόνο θεσμικό ζήτημα, αλλά και τεχνολογικό.

- Αρχή της νομιμότητας

Η συλλογή και επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται με δίκαιο και νόμιμο τρόπο.

- Αρχή του περιορισμού του σκοπού

Τα προσωπικά δεδομένα πρέπει να συλλέγονται και να τυγχάνουν επεξεργασίας για προσδιορισμένο, σαφή και νόμιμο σκοπό και να μην υφίστανται μεταγενέστερη επεξεργασία ασυμβίβαστη με το σκοπό αυτό.

- Αρχή της αναλογικότητας

Τα προσωπικά δεδομένα που υπόκεινται σε επεξεργασία πρέπει να είναι κατάλληλα και συναφή με το σκοπό της επεξεργασίας και όχι περισσότερα από όσα χρειάζονται.

- Αρχή της χρονικά πεπερασμένης διάρκειας τήρησης

Τα δεδομένα πρέπει να είναι ακριβή και να υποβάλλονται σε ενημέρωση επίσης τα δεδομένα πρέπει να διατηρούνται μόνο για όσο διάστημα χρειάζονται για την επίτευξη του σκοπού.

- Αρχή της ασφάλειας και της ακρίβειας

Θα πρέπει να ληφθούν οι κατάλληλοι μηχανισμοί απέναντι σε κινδύνους για να εξασφαλιστεί η προστασία των προσωπικών δεδομένων. Έτσι να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες. Θα πρέπει να διασφαλίζονται η εμπιστευτικότητα και ακεραιότητα των δεδομένων. Τα προσωπικά δεδομένα θα πρέπει να κρατούνται ακριβή, κατάλληλα και επικαιροποιημένα, διαρκώς [11].

Θα πρέπει να αναφερθεί ότι για να μπορέσει να πραγματοποιηθεί θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα προϋποθέτετε ότι το υποκείμενο των δεδομένων θα έχει δόση τη συγκατάθεση του.

2.3.2 Προσωπικά Δεδομένα στο Διαδίκτυο

Με τη διαρκή εξέλιξη του Διαδικτύου τα τελευταία χρόνια, την ευρεία χρήση και αποδοχή του από όλες σχεδόν τις πληθυσμιακές ομάδες και τις νέες υπηρεσίες που παρέχει, η ανάγκη προστασίας των προσωπικών δεδομένων αυξάνετε σημαντικά. Η επεξεργασία των προσωπικών μας δεδομένων στο Διαδίκτυο είναι πλέον συνεχής και ουσιαστικά αναπόφευκτη.

Τα προβλήματα προστασίας προσωπικών δεδομένων στο Διαδίκτυο είναι ιδιαίτερα σημαντικά, δεδομένου ότι διαπιστώνεται κυκλοφορία προσωπικών δεδομένων σε

μεγάλη έκταση, αφού ακόμη και μια απλή περιήγηση στο Διαδίκτυο δεν παραμένει ανώνυμη όσο αναφορά το χρήστη.

Στο διαδίκτυο μέσω των διάφορων αναζητήσεων, συναλλαγών και γενικά των δραστηριοτήτων που πραγματοποιούνται από τους χρήστες γίνετε αποκάλυψη δεδομένων προσωπικών και μη. Μερικά παραδείγματα στα οποία γίνετε αποκάλυψη δεδομένων είναι οι ηλεκτρονικές συναλλαγές, οι εγγραφές σε κάποιες ιστοσελίδες ή σε άλλες παροχές του διαδικτύου κ.α.

Με την επεξεργασία των δεδομένων που αποκαλύπτονται μπορεί να δημιουργηθεί μια «εικόνα» του χρήστη με τα ενδιαφέροντα του, τις συνήθειες του και τις προτιμήσεις του. Αυτά τα δεδομένα στη συνέχεια μπορούν να χρησιμοποιηθούν για εμπορικούς σκοπούς, για την αποκάλυψη της ταυτότητας του χρήστη, για διαφημιστικούς σκοπούς κ.α.

Ακόμη ένα ζήτημα για της προστασία της ιδιωτικότητας είναι η διασυνοριακή ροή των πληροφοριών. Μέσω του διαδικτύου τα προσωπικά δεδομένα μπορούν να μεταφέρονται και να τυγχάνουν επεξεργασίας σε άλλες χώρες και όχι σε αυτές που έγινε η συλλογή τους. Το κρισιμότερο σημείο τις διασυνοριακής ροής εντοπίζετε όταν τα δεδομένα μεταφέρονται σε χώρες όπου δεν προσφέρετε επαρκή επίπεδο προστασίας. Σε αυτές τις περιπτώσεις είναι πολύ δύσκολο να υπάρξει έλεγχος της επεξεργασίας.

Συμπερασματικά, η λάθος χρήση του διαδικτύου μπορεί να γίνει η αιτία για την αποκάλυψη των προσωπικών δεδομένων ενός ατόμου και να επιφέρει μεγάλο πλήγμα στην ιδιωτικότητα του.

2.4 Απειλές ιδιωτικότητας

Ο σύγχρονος τρόπος ζωής βασίζεται στο διαδίκτυο, την κινητή τηλεφωνία και στις εφαρμογές κοινωνικής δικτύωσης που είναι συνδεδεμένα σε παγκόσμιο επίπεδο. Αντικαθιστούνται οι συναλλαγές πρόσωπο με πρόσωπο καθώς και εξ αποστάσεως συναλλαγές μέσω καθιερωμένων συμβατικών μέσων, με συστήματα εικονικών συναλλαγών. Οι άνθρωποι κάνουν συναλλαγές μέσω διαδικτύου για διάφορα θέματα όπως αναψυχή, υγεία, την εκπαίδευση και την εργασία.

Οι χρήστες αν και ανησυχούν για προστασία της ιδιωτικότητας τους, αποκαλύπτουν σημαντικό μέρος προσωπικών τους δεδομένων και χωρίς να λαμβάνουν τα απαραίτητα μέτρα για την προστασία τους.

Μερικές απειλές για την ιδιωτικότητα είναι: α) Η υποκλοπή περιεχομένου και δεδομένων κίνησης και θέσης ηλεκτρονικών επικοινωνιών β) Η επιτήρηση, παρακολούθηση με τη βοήθεια ψηφιακών μέσων (monitoring systems) γ) κλοπή στοιχείων και δεδομένων επαλήθευσης ταυτότητας χρηστών ή μελών δ) απώλεια ελέγχου χρήσης και διανομής στοιχείων ταυτότητας ε) Αθέμιτη χρήση δεδομένων επικοινωνίας (spam) στ) Δημιουργία μορφοτύπων χρηστών, μελών ζ) Δημιουργία πληροφοριακού πέπλου.

Οι απειλές αυτές μπορούν να πραγματοποιηθούν αν δεν υπάρχει η απαιτούμενη ασφάλεια. Ένας από τους τρόπους παραβίασης της ιδιωτικότητας είναι η χρήση μη ασφαλών τεχνολογιών. Δηλαδή κατά πόσο τα τεχνικά και οργανωτικά μέτρα/μηχανισμοί ασφάλειας μπορούν να διασφαλίσουν την προστασία προσωπικών δεδομένων. Συγκεκριμένες επιθέσεις που μπορεί να πραγματοποιηθούν σε περιπτώσεις τέτοιων αδυναμιών είναι: οι επιθέσεις Δούρειου ίππου(Trojan horse), επιθέσεις σκουληκιών (worms), address spoofing κ.α. Επίσης υπάρχουν προγράμματα που έχουν εγκατασταθεί και εν αγνοία του χρήστη έχουν πρόσβαση στα προσωπικά του δεδομένα και μπορούν μέσο δικτύου να τα αποστείλουν σε τρίτους.

Ένας άλλος τρόπος για παραβίαση της ιδιωτικότητας μπορεί να είναι σε επίπεδο επικοινωνίας. Σε αυτή τη κατηγορία θα εντάσσαμε της πληροφορίες που μπορεί να συλλέξει ο πάροχος υπηρεσιών του χρήστη και τα "Cookies" τα οποία παρακολουθούν την πρόσβαση των χρηστών στις διάφορες ιστοσελίδες.

Επιπρόσθετος κίνδυνος για την ασφάλεια της ιδιωτικότητας στη σημερινή κοινωνία που πρέπει να ληφθεί υπόψη είναι η διασυνοριακή ροή των δεδομένων. Τα προσωπικά δεδομένα καθώς και τα ευαίσθητα προσωπικά δεδομένα εύκολα πλέον μπορούν να αποσταλούν σε χώρες οι οποίες δεν έχουν το απαραίτητο επίπεδο ασφάλειας.

Συμπερασματικά, υπάρχουν πολλοί σοβαροί κίνδυνοι για την ιδιωτικότητα και θα πρέπει οι τεχνολογίες και τα μέτρα προστασία να συμβαδίζουν με τις εξελίξεις.

Επίσης θα πρέπει και οι κανονισμοί για την Ιδιωτικότητα να εναρμονιστούν με τις τεχνολογικές εξελίξεις για να μπορέσει να υπάρξει ένα ικανοποιητικό επίπεδο προστασίας.

2.5 Ιδιωτικότητα και Ασφάλεια

Η ασφάλεια αποτελεί την πρώτη γραμμή άμυνας για την προστασία της ιδιωτικότητας, παρά το γεγονός ότι οι δυο αυτές έννοιες δεν ταυτίζονται.

Για τον όρο «Ασφάλεια» μπορούν να αποδοθούν πολλές ερμηνείες. Κάθε μια από αυτές, μπορεί να αποδώσει με ακρίβεια διαφορετικές καταστάσεις. Σύμφωνα με τον ορισμό του λεξικού της Οξφόρδης, «ασφάλεια είναι η ελευθερία από τον κίνδυνο ή το φόβο». Άλλοι ορισμοί που μπορούν να χρησιμοποιηθούν για να προσδιορίσουν την «ασφάλεια» είναι οι παρακάτω:

• Η κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, εκεί όπου αισθάνεται κανείς ότι δεν απειλείται.

• Η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας.

Η ασφάλεια σχετίζεται με το τεχνικό μέρος των υπολογιστών. Αφορά στην επινόηση, κατασκευή και εφαρμογή τεχνικών, όπως η χρήση κωδικών πρόσβασης ή η κρυπτογραφία, προκειμένου η προσπέλαση στα δεδομένα να γίνετε από εξουσιοδοτημένα άτομα και να εξασφαλίζετε και η ασφαλείς μετάδοση δεδομένων. Στην Κοινωνία της πληροφορίας ένας άνθρωπος είναι ασφαλής, όταν είναι ασφαλή τα δεδομένα που σχετίζονται με αυτόν.

Η έννοια της ιδιωτικότητας και η έννοια της ασφάλειας είναι διαφορετικές. Ενώ η ιδιωτικότητα αφορά περισσότερο την κακή χρήση της πληροφορίας για ένα πρόσωπο, η ασφάλεια έχει να κάνει με τον αποκλεισμό απόκτησης και χρησιμοποίησης της πληροφορίας από τρίτους.

Οι Τεχνολογίες Πληροφοριών και Επικοινωνιών έχουν ήδη χρησιμοποιηθεί ως μέσο για παράνομη δραστηριότητα όπως η παραβίαση προσωπικών δεδομένων, με σχετικά μεγάλη ευκολία που παρέχει η τεχνολογία.

Αξίζει να γίνει αναφορά σε τρείς περιπτώσεις παραβίασης της ασφάλειας προσωπικών δεδομένων οι οποίες σχετίζονται με ΤΠΕ.

- Κακόβουλη Πρόθεση: με την αποθήκευση πληροφοριών δίνεται η δυνατότητα σε επιτήδειους παραβάτες να αποσπάσουν πληροφορίες και προσωπικά δεδομένα, χωρίς να γίνονται συνήθως αντιληπτοί.
- Πνευματική Ιδιοκτησία: με τη ανάπτυξη των ηλεκτρονικών υπολογιστών και των συστημάτων ψηφιακής πληροφορίας έχει πάρει ανεξέλεγκτες διαστάσεις η αναπαραγωγή και η διακίνηση κειμένων, εικόνας, μουσικής κ.α. Αν αυτή η δραστηριότητα γίνεται χωρίς την έγκριση του ιδιοκτήτη, αποτελεί εκμετάλλευση της προσωπικής τους ιδιοκτησίας και παραβίαση της προσωπικής του ασφάλειας.
- Ασφάλεια Συστημάτων: Καθώς στην εποχή μας οι περισσότεροι ηλεκτρονικοί υπολογιστές ανήκουν σε κάποιο δίκτυο, είναι πολύ πιο εύκολη η παραβίαση των συστημάτων ασφαλείας τους. Έτσι γεννιέται η ανάγκη για την ανάπτυξη πιο εξελιγμένων και αποδοτικών συστημάτων ασφαλείας για την προστασία δεδομένων.

Θα πρέπει να καταστήσουμε σαφές ότι οι δύο αυτές έννοιες δεν είναι ταυτόσημες. Κανένα μέτρο ασφάλειας δεν μπορεί να αποτρέψει κάποια εταιρία να εκμεταλλευτεί, παράνομα πολλές φορές, τα δεδομένα που λαμβάνει οικειοθελώς από τους χρήστες της, ενώ δεν είναι λίγες οι περιπτώσεις όπου η ιδιωτικότητα και ασφάλεια αποτελούν έννοιες αντικρουόμενες.

Για παράδειγμα εάν μια εφαρμογή ή ένα σύστημα είναι ασφαλές, δεν σημαίνει ότι μπορεί να προστατευτεί και την ιδιωτικότητα ενός ατόμου. Σε πολλές εφαρμογές/ συστήματα, ο χρήστης μπορεί να δώσει προσωπικά του δεδομένα /πληροφορίες. Στην περίπτωση που το σύστημα δεν είναι ασφαλές, δεν ακολουθεί κάποια πρότυπα ασφάλειας, αυτά τα δεδομένα μπορεί να αποκαλυφθούν, να αλλοιωθούν ή ακόμη και να διαγραφούν. Ακόμη και να υπάρχει ασφάλεια στο σύστημα τα προσωπικά δεδομένα του ατόμου μπορούν να χρησιμοποιηθούν για άλλους σκοπούς και όχι για τους αρχικούς, για τους οποίους τα έδωσε ο χρήστης και έλαβε γνώση για αυτούς.

Συμπερασματικά θα λέγαμε ότι μπορεί να γίνει παραβίαση της Ιδιωτικότητας του υποκειμένου ακόμη και αν υπάρχουν ισχυρά μέτρα ασφάλειας. Έτσι βλέπουμε ότι η ασφάλεια και η Ιδιωτικότητα συμβαδίζουν, αλλά δεν είναι τα ίδια, ούτε το ένα αντικαθιστά ή υποκαθιστά το άλλο.

3

Τεχνολογίες για Προστασία της Ιδιωτικότητας

Η ιδιωτικότητα αποτελεί θεμελιώδη ανάγκη και βασικό δικαίωμα του κάθε ατόμου. Ωστόσο, συχνά διαφαίνεται πως η χρήση διαφόρων συσκευών επικοινωνίας έχει αρνητικό αντίκτυπο στην ιδιωτικότητα.

Στη δεκαετία του 1990, άρχισε να γίνετε σαφές ότι η προσέγγιση για την προστασία της ιδιωτικότητας, η οποία βασιζόταν στο ότι η ιδιωτικότητα και η τεχνολογία ήταν εκ διαμέτρου αντίθετα, δεν είχε μέλλον. Η ανάπτυξη της τεχνολογίας δεν μπορούσε και δεν έπρεπε να σταματήσει, επομένως επιβαλλόταν να βρεθεί κάποιος τρόπος ούτος ώστε η ιδιωτικότητα να μπορεί να προστατευτεί.

Αυτό οδήγησε στην ανάπτυξη των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (PETs), οι οποίες βασίζονται στην ιδέα υποστήριξης της τεχνολογίας για την ενίσχυση της ιδιωτικότητας και όχι στην προσβολή της.

Η ιδέα αναπτύχτηκε, εν μέρει, από την αίσθηση ότι οι τεχνολογίες κρυπτογράφησης θα μπορούσαν να βοηθήσουν τα άτομα και τους οργανισμούς να προστατέψουν τις προσωπικές τους πληροφορίες ενόψει της ευρείας διάδοσης των προσωπικών υπολογιστών και την εμφάνιση του διαδικτύου ως ένα νέο μέσο επικοινωνίας [12].

3.1 Ιστορία των PETs

Ο όρος «Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας» χρησιμοποιήθηκε για πρώτη φορά στην έκθεση «Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας: ο δρόμος προς την ανωνυμία» που δημοσιεύθηκε το 1995. Η έκθεση αυτή ήταν το αποτέλεσμα ενός κοινού έργου που είχε συσταθεί από την ολλανδική Αρχή Προστασίας Δεδομένων και την Επίτροπο Πληροφοριών του Οντάριο. Σε αυτό το έργο διερευνούταν μια νέα προσέγγιση για την προστασία της ιδιωτικότητας, με μια σειρά από μελέτες περιπτώσεων (case studies), για να αποδειχτεί ότι τα συστήματα χωρίς προσωπικά δεδομένα ή τουλάχιστον με πολύ λιγότερα, θα μπορούσε να έχει τις ίδιες λειτουργίες. Η έκθεση αυτή απέδειξε ότι η τεχνολογία θα μπορούσε να χρησιμοποιηθεί ως μέσο

για την προστασία των ατόμων από την κατάχρηση των προσωπικών τους δεδομένων, μειώνοντας την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Δημοσιεύτηκε στη Βόρεια Αμερική και την Ευρώπη την ίδια ημέρα, και στη συνέχεια παρουσιάστηκε στο Διεθνές Συνέδριο Προστασίας Δεδομένων και των Επιτρόπων Προστασίας Προσωπικών Δεδομένων στην Κοπεγχάγη[13].

Οι τεχνολογίες ενίσχυσης της Ιδιωτικότητας μπορούσαν να θεωρηθούν ως ένα ισχυρό εμπορικό σήμα, και υπήρξαν διάφορες εταιρίες και οργανισμοί που κατέβαλαν προσπάθειες για να επωφεληθούν από τη φήμη τους, συμπεριλαμβάνοντας άλλες τεχνολογίες, οι οποίες δεν ήταν κατ' ανάγκη «Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας», αλλά «επιβολής της ιδιωτικότητας» (privacy enforcing)ή «ενεργοποίησης της ιδιωτικότητας» (privacy enabling).

Οι PETs έχουν ήδη επιτύχει μια σημαντική θέση στο πρακτικό και θεωρητικό σύνολο των μέσων προστασίας της ιδιωτικότητας στις περισσότερες, αν όχι σε όλες, χώρες όπου οι νόμοι περί προστασίας των δεδομένων και των συστημάτων είναι ήδη ενεργοί ή δημιουργούνται. Οι PETs έχουν βρεθεί στο επίκεντρο της προσοχής σε διάφορες χώρες και κυρίως στις ΗΠΑ, όπου οι νομοθετικές διατάξεις για την προστασία των δεδομένων είναι περιορισμένες ή ανεπαρκείς. Μερικές φορές οι PETs θεωρούνται ως υποκατάστατα για τα άλλα μέσα προστασίας της ιδιωτικότητας, όπως οι νόμοι και οι ρυθμιστικοί φορείς που επιβάλλουν την εφαρμογή της νομοθεσίας. Η αντίληψη αυτή δεν είναι παραγωγική. Είναι καλύτερο να θεωρούνται ως συμπληρωματικές τεχνολογίες προς τα άλλα μέσα με τα οποία πρέπει να συνεργάζονται για να παρέχουν μια ισχυρή μορφή προστασίας της ιδιωτικότητας. Το μέσο στο οποίο βασίζονται οι PETs είναι ο νόμος γιατί μέσω αυτού θα ενσωματωθούν στις νομικές αρχές οι τεχνικές προδιαγραφές.

3.1.1 Τι είναι οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs);

Οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) προσφέρουν λύσεις για τη προστασίας της ιδιωτικότητας των χρηστών, των καταναλωτών και των πολιτών. Η εφαρμογή των ΤΠΕ για την προστασία της ιδιωτικότητας έχει γίνει ευρέως γνωστή με το όνομα Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (PETs ή PET). Οι τεχνολογίες ενίσχυσης της ιδιωτικότητας (Privacy-Enhancing Technologies-PETs) αναπτύχθηκαν προκειμένου να ενισχύσουν την προστασία της ιδιωτικότητας στα σύγχρονα

πληροφοριακά και επικοινωνιακά συστήματα, τα οποία υποστηρίζουν υπηρεσίες ή υποδομές. Οι PETs είναι ένα ολοκληρωμένο σύστημα μέτρων ΤΠΕ που προστατεύουν την ιδιωτικότητα εξαλείφοντας ή περιορίζοντας προσωπικά δεδομένα ή εμποδίζοντας την περιττή ή/και ανεπιθύμητη επεξεργασία προσωπικών δεδομένων, με τη παροχή εργαλείων για την ενίσχυση του ελέγχου του ατόμου πάνω στα προσωπικά του στοιχεία, και όλα αυτά χωρίς να χαθεί η λειτουργικότητα του πληροφοριακού συστήματος.

Οι τεχνολογίες αυτές θεωρούνται τεχνικά και οργανωσιακά πρότυπα. Ως οργανωσιακά πρότυπα, οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας (PETs) συνίστανται από ένα σύνολο οδηγιών στον επιχειρηματικό τομέα με στόχο την προστασία της ιδιωτικότητας. Από τεχνική άποψη οι PETs είναι συγκεκριμένα δικτυακά εργαλεία που χρησιμοποιούνται για τον έλεγχο της ποσότητας των προσωπικών δεδομένων που αποκαλύπτονται κατά την χρήση δικτύων ηλεκτρονικών υπολογιστών. Αν και αυτός είναι ο κύριος στόχος των PETs, μια από τις πιο αποτελεσματικές εφαρμογές τους είναι η κρυπτογράφηση, που χρησιμοποιείται για την προστασία των περιεχομένων ηλεκτρονικών μηνυμάτων.

Σήμερα, οι PETs υλοποιούνται σε μια ποικιλία εφαρμογών, όπως:

- Προγράμματα ασφάλειας που ενημερώνουν τους χρήστες για τις πολιτικές διασφάλισης προσωπικών δεδομένων εμπορικών διαδικτυακών εταιρειών και εγγυώνται την αξιοπιστία τους.
- Ειδικά εργαλεία που δίνουν την δυνατότητα στους χρήστες να επιλέξουν ποια προσωπικά τους στοιχεία θα γνωστοποιηθούν κατά την πλοήγησή τους στο Διαδίκτυο.
- Προγράμματα προστασίας του περιεχομένου των μηνυμάτων που ανταλλάσσονται μέσω διαδικτύου.
- Εφαρμογές που επιτρέπουν στους χρήστες να πλοηγούνται στο Διαδίκτυο «ανώνυμα» ή με «ψευδώνυμο».

Οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας είναι ένας τρόπος προστασίας για τους χρήστες του διαδικτύου, παρέχοντας την δυνατότητα ελέγχου του βαθμού μετάδοσης των προσωπικών τους δεδομένων. Προσφέρουν επιλογές διαχείρισης σχετικά με το

ποια δεδομένα επιθυμούν να γνωστοποιηθούν και ποια όχι στην μετάδοση και αποκάλυψη προσωπικών δεδομένων.

Στον δημόσιο λόγο έχουν αναπτυχθεί δύο βασικά επιχειρήματα από δύο κύριες ομάδες με αντικρουόμενα συμφέροντα. Ομάδες καταναλωτών και συνήγοροι της ιδιωτικότητας υποστηρίζουν ότι απαιτείται ισχυρότερο νομικό πλαίσιο προστασίας των προσωπικών δεδομένων των χρηστών του διαδικτύου, ενώ από την άλλη, ηλεκτρονικές εμπορικές εταιρίες ασκούν πίεση για να νομοθετηθεί ο ατομικός εθελοντικός έλεγχος των προσωπικών δεδομένων και η αυτό- διευθέτηση και ρύθμιση των σχετικών θεμάτων από τις ίδιες τις εταιρείες.

Αναμφισβήτητα οι PETs είναι ωφέλιμες για την διαχείριση της ιδιωτικότητας. Συγχρόνως, εντοπίζονται περιορισμοί σχετικά με την αποτελεσματικότητα τους. Πρώτον, από τεχνικής πλευράς, δεν θεωρούνται πάντα επαρκείς ώστε να εγγυώνται την ανωνυμία του χρήση κατά την χρήση του διαδικτύου ενώ αμφισβητείται η δραστικότητα τους στο πεδίο της κρυπτογράφησης. Από την άλλη, κυβερνητικοί φορείς έχουν διατυπώσει την ανησυχία πως οι PETs δίνουν τη δυνατότητα σε διάφορα άτομα να αναπτύξουν παράνομες δραστηριότητες στο Διαδίκτυο χωρίς να μπορούν να εντοπιστούν και παρέχουν την ευχέρεια να επικοινωνούν μεταξύ τους με κωδικοποιημένα μηνύματα που πιθανόν δεν μπορούν να αποκωδικοποιηθούν από τις αρμόδιες υπηρεσίες.

Εξετάζοντας την αποτελεσματικότητα των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας από την άποψη της προστασίας των χρηστών, παρατηρείται ότι δεν εξασφαλίζεται πάντοτε η δυνατότητα επιλογής και συναίνεσης, με αποτέλεσμα η ασφάλειά τους να είναι συχνά αμφίβολη. Το πρώτο ζήτημα που προκύπτει είναι κατά πόσο και αν οι χρήστες γνωρίζουν την ύπαρξη και την λειτουργία των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας. Προς το παρόν δεν προβλέπεται ενημέρωση των χρηστών για την ύπαρξη των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας και τον τρόπο διάθεσης τους. Από την στιγμή που οι χρήστες δεν πληροφορούνται την ύπαρξη των Τεχνολογιών Ενίσχυσης Ιδιωτικότητας δεν έχουν την δυνατότητα να επιλέξουν να τις χρησιμοποιήσουν, με αποτέλεσμα να μην ωφελούνται από την προστασία που θα μπορούσαν να τους παρέχουν. Ερωτήματα που προκύπτουν είναι ποιος πρέπει να καταστεί υπεύθυνος για την διανομή των PETs στους χρήστες, αν πρέπει να συμπεριλαμβάνονται υποχρεωτικά στις εφαρμογές Λειτουργικών Συστημάτων, αν

πρέπει οι ηλεκτρονικές εταιρείες να διανέμουν τις PETs στους πελάτες τους και αν είναι λογικό να περιμένουμε από τους χρήστες του διαδικτύου να είναι υπεύθυνοι για την διανομή των PETs. Χαρακτηριστική περίπτωση είναι αυτή της δημοφιλούς εφαρμογής «Pretty Good Privacy» (PGP), που θα δούμε πιο κάτω, όπου προσφερόταν δωρεάν και η ευθύνη για την εγκατάσταση και χρήση του ήταν στη δικαιοδοσία των χρηστών, οι οποίοι έπρεπε πρώτα να το ανακαλύψουν από μόνοι τους, έπειτα να εντοπίσουν την ιστοσελίδα στην οποία βρίσκεται και τέλος, να το κατεβάσουν και να το εγκαταστήσουν στον υπολογιστή τους.

Ένα δεύτερο θέμα που προκύπτει είναι πως, παρόλο που οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας ενδεχομένως παρέχουν στους χρήστες τρόπους ελέγχου των προσωπικών τους δεδομένων σε μια αρχική συναλλαγή στο Διαδίκτυο, δεν μπορούν απαραίτητα να προστατέψουν τους χρήστες από περαιτέρω χρήση των προσωπικών τους δεδομένων. Εκτός από την περιορισμένη δυνατότητα προστασίας προσωπικών δεδομένων που παρέχουν οι PETs και πολιτικές συγκεκριμένων φορέων ή εταιρειών, απαιτείται να εφαρμοστούν διαδικασίες ελέγχου με την μορφή νόμων, στοχεύοντας στην εξασφάλιση μιας ζώνης ιδιωτικότητας και στην προστασία των χρηστών των ΤΠΕ όσον αφορά στην επακόλουθη χρήση προσωπικών δεδομένων που αρχικά αποκαλύπτουν σε πολλαπλές διαδικτυακές δραστηριότητες.

Επιπρόσθετα, στοχεύοντας στην αποσαφήνιση θεμάτων χρήσης και εκμετάλλευσης προσωπικών δεδομένων, έχει διατυπωθεί το επιχείρημα ότι για την περαιτέρω εκμετάλλευση προσωπικών δεδομένων στο Διαδίκτυο δεν πρέπει να ευθύνονται οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας, αλλά οι χρήστες που εκθέτουν τα προσωπικά τους στοιχεία. Σύμφωνα με αυτό το σκεπτικό, το Διαδίκτυο είναι ένα δημόσιος χώρος όπου οι χρήστες γνωστοποιούν με την θέλησή τους πληροφορίες, οι οποίες παύουν πλέον να θεωρούνται ιδιωτικές. Δεν λαμβάνεται όπως υπ’ όψιν ότι η συναίνεση των χρηστών για την χρήση των προσωπικών τους δεδομένων δεν συνεπάγεται την αποδοχή πιθανής κακής εκμετάλλευσης των πληροφοριών αυτών. Επιπλέον, έχει παρατηρηθεί ότι οι ηλεκτρονικές εταιρείες συχνά δεν ενημερώνουν τους πελάτες τους επαρκώς για τον τρόπο με τον οποίο θα χειριστούν τα δεδομένα τους. Αυτό συμβαίνει είτε γιατί οι εταιρείες συλλέγουν από τους χρήστες πληροφορίες χωρίς να έχουν εγκαίρως αποφασίσει πώς ακριβώς θα τις χρησιμοποιήσουν είτε γιατί επιδιώκουν να αποσπάσουν την συγκατάθεσή τους με δόλιο τρόπο.

Ο καλύτερος τρόπος για την προστασία της ιδιωτικότητας των ατόμων είναι η συλλογή των προσωπικών τους πληροφοριών μόνο όταν αυτό κριθεί απαραίτητο.

Συνοψίζοντας βλέπουμε ότι οι PETs είναι ένα σύνολο εργαλείων και τεχνολογιών που επιτρέπουν:

- Την ελαχιστοποίηση ή εξάλειψη της αποκάλυψης και της συλλογής προσωπικών δεδομένων ή δεδομένων αναγνώρισης (personally identifiable data) των χρηστών
- Την διεξαγωγή συναλλαγών χωρίς την αποκάλυψη της ταυτότητας των χρηστών
- Στους χρήστες να ασκήσουν έλεγχο στην διαχείριση των προσωπικών τους δεδομένων
- Στις επιχειρήσεις και οργανισμούς να εφαρμόσουν τις πολιτικές και πρακτικές προστασίας της ιδιωτικότητας (privacy policies and practices)
- την πρόληψη αυτοματοποιημένης συλλογής δεδομένων μέσω των cookies, HTTP κεφαλίδων, spyware κ.α.
- το φιλτράρισμα ανεπιθύμητων μηνυμάτων.

Οι Τεχνολογίες Ενίσχυσης Ιδιωτικότητας, παρόλο που είναι αξιόλογα μέσα προστασίας της ιδιωτικότητας, δεν προστατεύουν ικανοποιητικά τα προσωπικά δεδομένα των χρηστών του διαδικτύου. Απαιτείται λοιπόν η λήψη επιπρόσθετων μέτρων για την ασφάλεια των χρηστών και η θέσπιση σχετικών νόμων σε εθνικό και σε διεθνές πλαίσιο.

3.1.2 Περαιτέρω εξελίξεις των PETs

Μετά την επίτευξη της εφαρμογής των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας η παγκόσμια βιομηχανία ΤΠΕ άρχισε να ενδιαφέρεται για τις δυνατότητές τους. Μετά την ψευδο-ταυτότητα, καθιερώθηκαν νεότερα PETs που οδήγησαν σε μια κατάταξη από επτά αρχές.

Οι Επτά Αρχές PET

1. **Περιορισμός στη συλλογή προσωπικών δεδομένων**

Τα συστήματα ενίσχυσης της ιδιωτικότητας θα πρέπει πρώτα απ 'όλα να είναι σύμφωνα με το άρθρο 6, παράγραφος 1(γ) , της οδηγίας 95/46/ΕΚ. Τα δεδομένα προσωπικού χαρακτήρα που δεν συλλέγονται, δε χρήζουν κανενός μέτρου

προστασίας επειδή δεν μπορεί κανένας να τα επεξεργαστεί. Κατά το σχεδιασμό ενός σχήματος βάσης δεδομένων, τα στοιχεία πρέπει να προστίθενται αν και μόνο αν , η συλλογή τους μπορεί να δικαιολογηθεί εντός του ορισμού του σκοπού του πληροφοριακού συστήματος.

2. Ταυτοποίηση / πιστοποίηση / εξουσιοδότηση

Το άρθρο 16 της οδηγίας 95/46/ΕΚ, μπορεί να ερμηνευτεί κατά τέτοιο τρόπο, που ο χρήστης ενός πληροφορικού συστήματος που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα πρέπει να επεξεργάζεται μόνο προσωπικά δεδομένα που είναι σχετικά με τις ανάγκες του συστήματος.

Αυτή η λειτουργικότητα το πληροφοριακού συστήματος θα μπορούσε να είναι ένα χαρακτηριστικό παράδειγμα όπου ένα οργανωτικό μέτρο τίθεται σε εφαρμογή με τη χρήση των PETs. Ο υπεύθυνος επεξεργασίας θα πρέπει να καθορίσει ένα σύστημα αδειοδότησης. Αυτό το σύστημα θα μπορούσε να έχει την ακόλουθη δομή: αρχικά, τα προφίλ λειτουργίας δημιουργούνται μετά τη σύνδεση των λειτουργιών του πληροφοριακού συστήματος με οργανωτικές λειτουργίες σε αυτό το προφίλ. Στη συνέχεια, σε κάθε επεξεργαστή εντός του οργανισμού δίδεται μια μοναδική ταυτότητα που πρέπει να χρησιμοποιείται όταν κάποιος είναι χρήστης του πληροφοριακού συστήματος. Ως τελευταίο βήμα, η ταυτότητα αυτή του χρήστη εκχωρείται σε ένα προφίλ λειτουργίας. Αν ένας χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί μια συγκεκριμένη λειτουργία του συστήματος, αυτό δεν σημαίνει απαραίτητα ότι αυτό το άτομο έχει τη δυνατότητα να έχει πρόσβαση στα δεδομένα όλων των υποκειμένων των δεδομένων που υποβάλλονται σε επεξεργασία.

3. Τυποποιημένες τεχνικές που χρησιμοποιούνται για την προστασία των προσωπικών δεδομένων

Βάση του άρθρου 6, παράγραφος 1 (β), της οδηγίας 95/46/ΕΚ, οι επιχειρήσεις πρέπει να διασφαλίζουν ότι τα δεδομένα που φυλάσσουν πρέπει να χρησιμοποιηθούν μόνο για τους σκοπούς για τους οποίους έχουν συλλεχθεί. Η καλύτερη εγγύηση επιτυγχάνεται με μετασχηματισμό των δεδομένων με τέτοιο τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να χρησιμοποιηθούν για την αναγνώριση του υποκειμένου των δεδομένων. Η διαδικασία αυτή συχνά αναφέρεται ως ανωνυμοποίηση.

4. Ψευδο-ταυτότητα

Πολλά συστήματα αρχειοθέτησης προσωπικών δεδομένων επεξεργάζονται δεδομένα που ανήκουν στη ίδια ομάδα υποκειμένων. Για στατιστικούς σκοπούς, υπάρχει η απαίτηση να συνδεθούν αυτά τα συστήματα, αλλά δεν υπάρχει καμία απαίτηση να διατηρηθεί η ταυτότητα των υποκειμένων των δεδομένων. Η λύση μπορεί να βρεθεί σε ένα συνδυασμό των PETs. Το πρώτο βήμα είναι να δημιουργήσουμε μια ψευδο-ταυτότητα ως αναγνωριστικό. Αυτή η ταυτότητα δημιουργείται σε τρία βήματα: πρώτων, δημιουργείται μια σειρά από τους τρεις πρώτους χαρακτήρες του επωνύμου, την ημερομηνία γέννησης και τον κωδικός που δείχνει το φύλο του υποκειμένου των δεδομένων. Στο επόμενο στάδιο, παράγεται ένας κατακερματισμός (hash) της συμβολοσειράς. Τέλος, η αρχική συμβολοσειρά απομακρύνεται. Η ψευδο-ταυτότητα που δημιουργείται έτσι είναι η ίδια για κάθε ένα από τα συστήματα πληροφοριών πηγής και συνεπώς διασφαλίζεται. Η τρίτη αρχή των PET πρέπει να εφαρμοστεί σε κάθε σύστημα αρχειοθέτησης για να συγχωνευθούν τα αρχεία. Τα μεμονωμένα αρχεία μπορούν τώρα να αποστέλλονται σε μια κεντρική τοποθεσία. Επιπλέον, ασφάλεια (PET) μπορεί να επιτευχθεί με τον ακόλουθο τρόπο: μετά την παραλαβή των φακέλων, η αρχική ψευδο-ταυτότητα κατακερματίζεται για άλλη μια φορά και αντικαθιστά την αρχική ψευδο-ταυτότητα.

5. Κρυπτογράφηση

Η κρυπτογράφηση είναι ένα τυπικό παράδειγμα μιας υπάρχουσας τεχνολογίας που μπορεί να βοηθήσει την προστασία των δεδομένων. Η δήλωση αυτή μπορεί να δώσει την εντύπωση ότι η τεχνολογία κρυπτογράφησης δεν έχει άλλη εφαρμογή από το να χρησιμεύσει ως PET. Αντιθέτως, η κρυπτογράφηση είναι ένα γενικό μέτρο ασφαλείας για την επίτευξη εμπιστευτικότητας. Μια εταιρεία χρησιμοποιεί κρυπτογράφηση για να διασφαλίσει τα μυστικά της (οικονομικά στοιχεία καθώς και πληροφορίες για το προϊόν), ακόμη και αν δεν υπάρχουν προσωπικά δεδομένα σε κίνδυνο. Σε όλες τις περιπτώσεις κατά τις οποίες η «εμπιστοσύνη» είναι ένα θέμα, η «κρυπτογράφηση» θα μπορούσε να είναι η λύση.

Η δύναμη της κρυπτογραφίας μπορεί να χρησιμοποιηθεί για την εφαρμογή PETs προκειμένου να μειωθεί η ποσότητα των προσωπικών δεδομένων προς επεξεργασία, χωρίς να χάσει τη λειτουργικότητα του το πληροφοριακό σύστημα. Πρέπει να υπάρχει ένας υπεύθυνος ο οποίος θα λαμβάνει αποφάσεις σχετικά με τα ακόλουθα:

αποθήκευση, πρόσβαση, δημοσιοποίηση και μεταφορά. Χρησιμοποιώντας κρυπτογραφία μπορεί να ενισχυθούν όλες αυτές οι πτυχές.

6. Βιομετρικά

Η πιστοποίηση του χρήστη είναι ένα πολύ σημαντικό στάδιο στη διαδικασία σύνδεσης. Είστε το πρόσωπο που λέγατε ότι είστε; Είναι γνωστό ότι τους κωδικούς είναι εύκολο να τους μαντέψει κάποιος ή εάν ο κωδικός πρόσβασης είναι καλά επιλεγμένος τότε ο χρήστης δεν μπορεί να τον θυμηθεί ούτε ο ίδιος και ως εκ τούτου το σημειώνει κάπου και τον φυλάσσει κοντά στο πληκτρολογίου του. Σε κάθε περίπτωση οι κωδικοί πρόσβασης δεν μπορούν να εγγυηθούν τη ταυτότητα του χρήστη. Η αναγνώριση του «υλικού του σώματος» μπορεί να πιστοποιήσει τον χρήστη χωρίς εύλογη αμφιβολία.

7. Δυνατότητα ελέγχου (audit)

Το άρθρο 28 της οδηγίας 95/46/ΕΚ δίνει στις Εποπτικές Αρχές (Αρχή προστασίας δεδομένων) εξουσίες έρευνας, όπως η εξουσία πρόσβασης στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας και το δικαίωμα να συλλέγει όλες τις πληροφορίες που είναι αναγκαίες για την εκπλήρωση των εποπτικών καθηκόντων τους. Μερικά από τα δεδομένα που απαιτούνται από τις αρχές για την εκτέλεση των εποπτικών καθηκόντων τους είναι:

1. Οι περιγραφές των αυτοματοποιημένων και μη συστημάτων που χρησιμοποιούνται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

2. Οι πληροφορίες παρακολούθησης (ίχνη ελέγχου) σχετικά με τις δραστηριότητες του χρήστη, ο οποίος επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα.

Η πιο προφανής λύση για τη δημιουργία ιχνών ελέγχου είναι με τη χρήση των PETs . Ένας μηχανισμός κάνει οριοθετούμενη καταγραφή όλων των δραστηριοτήτων στη βάση δεδομένων που χρησιμοποιείται για την αποθήκευση προσωπικών δεδομένων, σε μια βάση δεδομένων σε επίπεδο διακομιστή.

Η αρχή αυτή σχετίζεται στενά με τη δεύτερη αρχή PET. Εάν ο χρήστης του πληροφοριακού συστήματος δεν είναι μονοσήμαντα προσδιορισμένος όταν οι πληροφορίες σύνδεσης του συστήματος εμφανίζεται, η καταγραφή των

δραστηριοτήτων που συνδέονται με αυτόν τον χρήστη έχουν πολύ μικρή χρησιμότητα για την εποπτική αρχή.

3.1.3 Εργαλεία Προστασίας της Ιδιωτικότητας

Τα εργαλεία προστασίας της ιδιωτικότητας στοχεύουν στην απόκρυψη της ταυτότητας του χρήστη, την ελαχιστοποίηση αποκάλυψης προσωπικών δεδομένων και την κάλυψη στις συνδέσεις δικτύου καμουφλάζ, έτσι ώστε να μην αποκαλύπτεται από πού προέρχεται η διεύθυνση πρωτοκόλλου διαδικτύου (IP-Internet Protocol).

Μαθαίνοντας την διεύθυνση πρωτοκόλλου διαδικτύου, κάποιος μπορεί να είναι σε θέση να εντοπίσει τη γεωγραφική θέση από την οποία προέρχεται ή την κοντινότερη πόλη ή ακόμα και την μοναδική αναγνώριση του υπολογιστή. Τα εργαλεία προστασίας της ιδιωτικότητας μπορούν επίσης να πιστοποιήσουν συναλλαγές, όπως πληρωμές, ενώ καθιστούν αδύνατη την ανίχνευση σύνδεσης με το χρήστη.

- Εργαλεία Ανωνυμοποίησης

  Το λογισμικό που ανήκει σε αυτή τη κατηγορία αποκρύπτει τη διεύθυνση πρωτοκόλλου διαδικτύου του εντολέα και σε περιπτώσεις ανώνυμων μηνυμάτων ή μηνυμάτων με χρήση ψευδώνυμου, αποκρύπτει τη πηγή διεύθυνσης του ηλεκτρονικού ταχυδρομείου.

- Πληρωμή ανώνυμα η με χρήση ψευδώνυμου

  Η πληρωμή με ανώνυμο τρόπο είναι μια απλή λειτουργία και συνήθως λειτουργεί με τον τρόπο που θα περιγραφεί στη συνέχεια. Ο χρήστης αγοράζει μια προπληρωμένη κάρτα που προσδιορίζεται με ένα μοναδικό αριθμό. Όταν ο χρήστης θελήσει να κάνει μια αγορά σε ένα διαδικτυακό κατάστημα, η πληρωμή πραγματοποιείται από τον ανώνυμο πάροχο με τη χρήση του μοναδικού αριθμού της κάρτας.

- Εργαλεία ασφάλειας Πληροφοριών

  Υπάρχει ένας αριθμός εφαρμογών για τον τελικό χρήστη που ορισμένες φορές κατηγοριοποιούνται ως τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs), άλλα στη πραγματικότητα είναι Εργαλεία Ασφάλειας Πληροφοριών. Τα εργαλεία αυτά είναι σημαντικά για την προστασία των δεδομένων και της ιδιωτικότητας, αλλά ο πρωταρχικός τους στόχος είναι να αποτρέψουν τη μη

εξουσιοδοτημένη πρόσβαση σε συστήματα, αρχεία ή επικοινωνίες μέσω του δικτύου[14].

3.2 Τεχνολογίες για τη διασφάλιση της ιδιωτικότητας των χρηστών

3.2.1 TOR

Το Tor είναι συντομογραφία του The onion router. Είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο διαδίκτυο. Το λογισμικό Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου δικτύου διακομιστών για να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από κάποιον που διεξάγει διαδικτυακή παρακολούθηση. Έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι δραστηριότητές που διεξάγει στο διαδίκτυο [15].

3.2.2 Anonymizer

Ο anonymizer ή anonymous proxy (όπως αλλιώς ονομάζεται) είναι ένα εργαλείο που προσπαθεί να κάνει τη δραστηριότητα στο διαδίκτυο δύσκολη να εντοπιστεί. Ουσιαστικά πρόκειται για έναν proxy server ο οποίος ενεργεί σαν μια ενδιάμεση και ιδιωτική ασπίδα ανάμεσα στον computer client και στο διαδίκτυο. Ο anonymizer αποκτά πρόσβαση στο παγκόσμιο ιστό εκ μέρους του χρήστη, αποκρύπτοντας πληροφορίες που μπορεί να φανερώσουν την ταυτότητά του. Υπάρχουν πολλοί λόγοι για να χρησιμοποιηθεί ένα τέτοιου είδους εργαλείο, ένας εκ των οποίων είναι η μείωση του κινδύνου που διατρέχει ο χρήστης στο διαδίκτυο. Επίσης βοηθά στην αποφυγή κλοπής προσωπικών στοιχείων, καθώς και στην προστασία κατά της δημοσιοποίησης ιστορικών αναζήτησης χρηστών από τρίτους (κακόβουλους χρήστες).

3.2.3 Anonymous remailer

Anonymous remailer ονομάζεται ένας εξυπηρετητής ο οποίος λαμβάνει τα μηνύματα, με ενσωματωμένες οδηγίες για το που θα σταλούν στη συνέχεια. Αυτά τα μηνύματα στη συνέχεια προωθούνται χωρίς να αποκαλύπτεται η αρχική πηγή προέλευσης τους. Κάθε πακέτο που στέλνεται περιέχει τις IP διευθύνσεις του αποστολέα και των κόμβων παραλαβής. Οι remailers αναλαμβάνουν να αλλάξουν αυτές τις διευθύνσεις

και να τις αντικαταστήσουν πλαστές διευθύνσεις προέλευσης. Έτσι η IP προέλευσης μπορεί να αντικατασταθεί με αυτήν του κεντρικού εξυπηρετητή. Οι remailers μπορεί να μεταβιβάσουν το μήνυμα σε άλλους remailers και μετά από πολλούς κύκλους τελικά να καταλήξει στη διεύθυνση προορισμού.

3.2.4 P3P

Το P3P είναι μια ειδική πλατφόρμα προστασίας δεδομένων, η οποία δίνει τη δυνατότητα σε ιστοσελίδες να υλοποιήσουν τις πρακτικές προστασίας προσωπικών δεδομένων σε τυποποιημένη μορφή έτσι ώστε να μπορούν να ανακτηθούν αυτόματα και να ερμηνεύονται εύκολα από τους χρήστες. Στο P3P οι διαχειριστές επιτρέπουν στους χρήστες να ενημερώνονται για νέες πρακτικές και να παίρνουν αυτόματα αποφάσεις. Ως εκ τούτου οι χρήστες δεν χρειάζεται να διαβάζουν τις πολιτικές απορρήτου σε κάθε ιστοσελίδα που επισκέπτονται.

Το P3P χρησιμοποίει μηχανές αναζήτησης συμβατές έτσι ώστε να μπορεί να περιγράψει τα δεδομένα που έχει συλλέξει και να τα χρησιμοποιήσει. Σελίδες που εκτελούν τέτοιες πολιτικές ασφαλείας κάνουν σαφείς τις πρακτικές τους έτσι ώστε να είναι ελεύθερα για δημόσιο έλεγχο. Οι μηχανές αναζήτησης βοηθούν τους χρήστες να κατανοήσουν αυτές τις ιδιωτικές πρακτικές με χρήση διεπαφών (interfaces). Οι πιο σημαντικοί φυλλομετρητές αναπτύσσονται προς αυτήν την κατεύθυνση. Σε περίπτωση κλειδώματος περιεχομένου, όπως μπορεί να γίνει με τα cookies, αυτοί δίνουν πραγματικά κίνητρα ώστε οι σελίδες ηλεκτρονικού εμπορίου να σέβονται και να διασφαλίζουν την ανωνυμία και τα ιδιωτικά δεδομένα του χρήστη.

3.2.5 Pretty Good Privacy

Το Pretty Good Privacy (PGP) είναι πρόγραμμα για κρυπτογράφηση αλλά και για αποκρυπτογράφηση δεδομένων. Παρέχει ιδιωτικότητα και πιστοποίηση αυθεντικότητας για δεδομένα που ανταλλάσσονται μεταξύ χρηστών. Επίσης χρησιμοποιείται για ψηφιακή υπογραφή, κρυπτογράφηση και αποκρυπτογράφηση αρχείων κειμένου, αρχείων ηλεκτρονικού ταχυδρομείου, καταλόγων και ολόκληρων τμημάτων σκληρών δίσκων, έτσι ώστε να αυξήσει την προστασία της επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου. Δημιουργήθηκε το 1991 από τον Phil Zimmermann.

3.2.6 SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) δημιουργήθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο όπως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές. Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ ηλεκτρονικών υπολογιστών, επιτυγχάνοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP και το telnet. Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email).

3.3 Διείσδυση των PETs στην αγορά

Η υποστήριξη των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs) εκφράζεται πλέον και σε κοινοτικό επίπεδο, χωρίς ωστόσο να προσλαμβάνει την ποιότητα κανονιστικής επιταγής. Η Ευρωπαϊκή Επιτροπή με μία δημόσια ανακοίνωση της 2^{ας} Μαΐου 2007 δήλωσε την άμεση υποστήριξή της στις Τεχνολογίες αυτές ώστε να ενισχυθεί η ιδιωτικότητα. Όμως και πάλι οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας δεν κατάφεραν να διεισδύσουν στην αγορά γιατί οι εταιρίες δεν αισθάνονται υποχρεωμένες να χρησιμοποιήσουν αυτές τις τεχνολογίες καθώς ο νομοθέτης δεν απαιτεί την υιοθέτησή τους. Ο νομοθέτης δεν απαιτεί την υιοθέτησή τους γιατί δεν διαπιστώνει την ύπαρξη προσφοράς τέτοιων τεχνολογιών, προσφορά που δεν αναπτύσσεται καθώς οι επιχειρήσεις δεν είναι υποχρεωμένες να την εισάγουν.

3.4 Τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs) και Ιδιωτικότητα βάση σχεδιασμού (PbD)

Η έννοια της Privacy by Design είναι στενά συνδεδεμένη με την έννοια των τεχνολογιών ενίσχυσης της ιδιωτικότητας (PETs). Η Ενσωμάτωση των αρχών τις ιδιωτικότητας στις τεχνολογίες πληροφοριών και συστημάτων σε ένα πρώιμο στάδιο είναι πρωταρχικής σημασίας για την καλύτερη λειτουργία των Τεχνολογιών

Ενίσχυσης της Ιδιωτικότητας. Είναι επίσης σαφές ότι η έννοια των PETs είναι στενά συνδεδεμένη με την αρχή της «ελαχιστοποίησης δεδομένων» και σταδιακά εξελίχθηκε στην αρχή της “Privacy by Design" που δεν είναι σημαντική μόνο για τα πληροφοριακά συστήματα αλλά επίσης και για οργανισμούς και μεθόδους γενικά, και συνεπώς για τις «πιο αποτελεσματικές» αρχές προστασίας δεδομένων. Οι αρχές του PbD μπορούν να χρησιμοποιηθούν για την υιοθέτηση των PETs άμεσα στο επίπεδο σχεδιασμού του συστήματος.

3.5 Τι είναι η προσέγγιση Privacy by Design;

Η Privacy by Design (PBD) είναι μια έννοια που αναπτύχθηκε από την Επίτροπο Πληροφοριών και Προστασίας Προσωπικών Δεδομένων του Οντάριο, Δρ Ann Cavoukian, στη δεκαετία του '90. Η PbD προβλέπει ότι πρέπει να γίνεται άμεση ενσωμάτωση της ιδιωτικότητας στο σχεδιασμό και τη λειτουργία όχι μόνο των διαφόρων τεχνολογιών, αλλά και των επιχειρηματικών διαδικασιών και των υποδομών δικτύου[12]. Με τη έννοια της άμεσης ενσωμάτωσης εννοείται ότι η προστασία της ιδιωτικότητας δεν προστέθηκε εκ των υστέρων, αλλά προϋπήρχε ως μέρος του σχεδιασμού του αντικειμένου για τον τρόπο λειτουργίας του[16].

Ο σκοπός της Privacy by Design είναι να δώσει την απαιτούμενη προσοχή στις ανάγκες της ιδιωτικότητας πριν από την ανάπτυξη νέων εφαρμογών. Με άλλα λόγια, να εξετάσει τον αντίκτυπο ενός συστήματος ή μιας διαδικασίας στην ιδιωτικότητα των ατόμων. Αυτό γίνεται καθ’ όλη τη διάρκεια του κύκλου ζωής των συστημάτων, έτσι ώστε να εξασφαλίζεται η εφαρμογή των κατάλληλων ελέγχων .

Οι διαφορετικές προσεγγίσεις της έννοιας της ιδιωτικότητας αποδίδουν τα ακόλουθα σημεία εκκίνησης σχετικά με το PbD:

- Η προστασία της ιδιωτικότητας αναφέρεται σε διαφορετικούς κύκλους, όπως για παράδειγμα στο σπίτι, την ιδιωτική ζωή και την αλληλογραφία.
- Η προστασία της ιδιωτικότητας αναφέρεται σε ένα ευρύ φάσμα των κοινωνικών αξιών και την προσωπική αυτονομία στην ελευθερία έκφρασης και του συνεταιρίζεσθαι, καθώς και την ισορροπία των εξουσιών.
- Η κοινωνική αξία της ιδιωτικότητας ερμηνεύεται ως το όφελος που λαμβάνει η κοινωνία από την προστασία της (ιδιωτικότητας).

- Προστασία της ιδιωτικότητας είναι η ετοιμότητα για περιορισμό και ο έλεγχος πρόσβασης στο χώρο.

3.5.1 Οι 7 θεμελιώδεις αρχές του Privacy by Design

1. Η προσέγγιση του Privacy by Design χαρακτηρίζεται από ενεργητικά μέτρα και όχι αντιδραστικά. Προβλέπει και εμποδίζει τυχόν παραβιάσεις της ιδιωτικότητας. Η Privacy by Design δεν προσφέρει τρόπους επίλυσης της παραβίασης της ιδιωτικότητας, αλλά έχει ως στόχο να την αποτρέψει από το να συμβεί. Είναι προληπτικό μέτρο και όχι τρόπος επίλυσης.

2. Προστασία Ιδιωτικότητας ως προεπιλεγμένη ρύθμιση. Το Privacy by Design επιδιώκει να επιτύχει το μέγιστο βαθμό της ιδιωτικότητας με την εξασφάλιση ότι τα προσωπικά δεδομένα προστατεύονται αυτόματα σε κάθε σύστημα ή επιχειρηματική πρακτική. Αν ένα άτομο δεν κάνει τίποτα, η προστασία της ιδιωτικότητάς του παραμένει ανέπαφη. Δεν απαιτείται από τη πλευρά του ατόμου καμία ενέργεια για την προστασία της ιδιωτικότητάς του γιατί είναι ενσωματωμένη ως προεπιλογή.

3. Ιδιωτικότητα ενσωματωμένη στο σχεδιασμό. Η Privacy by Design είναι ενσωματωμένη στο σχεδιασμό και την αρχιτεκτονική των συστημάτων και των επιχειρηματικών πρακτικών. Δεν αποτελεί επιπρόσθετο χαρακτηριστικό. Το αποτέλεσμα είναι ότι η προστασία της ιδιωτικότητας γίνεται «απαραίτητο συστατικό» των κύριων λειτουργιών. Η ιδιωτικότητα είναι ενσωματωμένη στο σύστημα, χωρίς να μειώνεται η λειτουργικότητα του.

4. Πλήρης Λειτουργικότητα. Το Privacy by Design αποφεύγει το διαχωρισμό ιδιωτικότητας και ασφάλειας, αποδεικνύοντας ότι είναι δυνατόν να έχουμε και τα δύο.

5. Από άκρο σε Άκρο Ασφάλεια - Πλήρης προστασία στον κύκλο ζωής.
Η Privacy by Design, έχοντας ήδη ενσωματωθεί στο σύστημα πριν από την πρώτη συλλογή του πρώτου στοιχείου πληροφοριών, με ασφάλεια εκτείνεται σε ολόκληρη τη διάρκεια του κύκλου ζωής των σχετικών δεδομένων. Για την ιδιωτικότητα είναι απαραίτητο να παρθούν ισχυρά μέτρα ασφάλειας, από την αρχή μέχρι το τέλος.

Αυτό εξασφαλίζει ότι όλα τα δεδομένα φυλάσσονται με ασφάλεια, και στη συνέχεια καταστρέφονται με ασφάλεια στο τέλος της διαδικασίας. Έτσι, η Privacy by Design εξασφαλίζει από την αρχή έως το τέλος, ασφαλή διαχείριση των πληροφοριών του κύκλου ζωής.

6. Ορατότητα και διαφάνεια. Η Privacy by Design επιδιώκει να διαβεβαιώσει όλους τους ενδιαφερόμενους ότι ανεξάρτητα από την επιχειρηματική πρακτική ή τις τεχνολογίες που εμπλέκονται, στην πραγματικότητα λειτουργεί σύμφωνα με τις υποσχέσεις που δηλώνονται και τους στόχους. Τα συστατικά μέρη και οι λειτουργίες του παραμένουν ορατές και διαφανείς για τους χρήστες και τους παρόχους.

7. Σεβασμός για την Ιδιωτικότητα του χρήστη. Πάνω απ' όλα, η Privacy by Design απαιτεί αρχιτέκτονες και φορείς για να κρατήσει τα συμφέροντα του ατόμου στο ανώτερο επίπεδο, προσφέροντας μέτρα ως προεπιλογές ισχυρής ιδιωτικότητας κατάλληλα ενημερωμένα και εμπλουτισμένα με επιλογές φιλικές προς το χρήστη.

3.5.2 Privacy by design στο κύκλο ζωής των συστημάτων

Για να είναι αποτελεσματική η προσέγγιση της Privacy by Design, θα πρέπει να λαμβάνεται υπόψη ολόκληρος ο κύκλος ζωής του κάθε συστήματος ή διαδικασίας, από τα πρώτα στάδια ανάπτυξης του κύκλου, από τον καθορισμό απαιτήσεων και το σχεδιασμό τους, την παράδοση, τον έλεγχο, τη λειτουργία του, καθώς και το στάδιο απόσυρσης του συστήματος.

Αυτή η προσέγγιση σε όλη τη διάρκεια του κύκλου εξασφαλίζει ότι οι έλεγχοι για την ιδιωτικότητα είναι αποτελεσματικότεροι, απλούστεροι και συνεπώς φθηνότεροι στην εφαρμογή τους. Συνεπώς, καθίσταται πιο δύσκολη η παραβίαση της ιδιωτικότητας καθώς είναι πλήρως ενσωματωμένη στο σύστημα. Ωστόσο, ούτε οι τρέχουσες πρακτικές του σχεδιασμού στον ιδιωτικό και δημόσιο τομέα, ούτε τα υπάρχοντα εργαλεία μπορούν να υποστηρίξουν εύκολα μια τέτοια προσέγγιση. Πολλά συστήματα ή διαδικασίες εξακολουθούν να σχεδιάζονται χωρίς να δίνεται η πρέπουσα σημασία στην προστασία της ιδιωτικότητας. Σε αρκετές περιπτώσεις η προστασία της ιδιωτικότητας μπορεί να προστεθεί αργότερα. Τα τρέχοντα μέσα προστασίας της ιδιωτικότητας και οι τεχνολογίες προσαρμόζονται ανάλογα με τις

ανάγκες μιας δεδομένης στιγμής έχοντας σκοπό να ικανοποιήσουν τις συγκεκριμένες απαιτήσεις μιας επιθεώρησης [17].

3.5.3 Αρχές Privacy By Design ως Privacy By Default

Οι αρχές της Privacy by Design, οι οποίες θα μπορούσαν να θεωρηθούν Ιδιωτικότητα ως προεπιλογή (Privacy by Default), πρέπει ναι είναι ενημερωμένες από το ακόλουθο FIPs:

• Προδιαγραφές Σκοπού - τους σκοπούς για τους οποίους συλλέγονται προσωπικές πληροφορίες, χρησιμοποιούνται, διατηρούνται και αποκαλύπτονται-κοινοποιούνται στο άτομο (υποκείμενο των δεδομένων) πριν ή κατά το χρόνο που οι πληροφορίες συλλέγονται. Οι προκαθορισμένοι σκοποί θα πρέπει να είναι σαφείς, συγκεκριμένοι και σχετικοί με τις περιστάσεις.

• Περιορισμός Συλλογής - η συλλογή προσωπικών πληροφοριών πρέπει να είναι δίκαιη, νόμιμη και περιορισμένη σε αυτό που είναι απαραίτητο για τους καθορισμένους σκοπούς.

• Ελαχιστοποίηση δεδομένων - η συλλογή των προσωπικών πληροφοριών θα πρέπει να περιορίζετε στο ελάχιστο. Ο σχεδιασμός των προγραμμάτων, τεχνολογιών πληροφοριών και επικοινωνιών, καθώς και συστημάτων θα πρέπει να αρχίσει με την απόκρυψη αλληλεπιδράσεων και συναλλαγών ως προεπιλογή. Η ταυτοποίηση και παρακολούθηση των προσωπικών πληροφοριών θα πρέπει να ελαχιστοποιείται, όπου είναι δυνατόν.

• Περιορισμός χρήσης, διατήρησης, και Γνωστοποίησης - η χρήση, διατήρηση και αποκάλυψη των προσωπικών πληροφοριών πρέπει να περιορίζεται στις πληροφορίες που είναι σχετικές με τους σκοπούς που προσδιορίζονται στο άτομο και για τους οποίους το άτομο έχει συναινέσει, εκτός αν απαιτείται από το νόμο. Οι προσωπικές πληροφορίες πρέπει να διατηρούνται μόνο για όσο διάστημα είναι αναγκαίο για την εκπλήρωση των δηλωθέντων σκοπών, και στη συνέχεια να καταστρέφονται με ασφάλεια.

• Σε περίπτωση που η ανάγκη ή χρήση των προσωπικών δεδομένων δεν είναι σαφής, πρέπει να υπάρχει ένα τεκμήριο ιδιωτικότητας και θα πρέπει να εφαρμόζεται η αρχή της προφύλαξης: οι προεπιλεγμένες ρυθμίσεις είναι από τα σημαντικότερα μέτρα για την προστασία της ιδιωτικότητας.

3.6 Privacy By Default

Οι ρυθμίσεις απορρήτου είναι μια σημαντική πτυχή για την ιδιωτικότητα στο διαδίκτυο. Οι καταναλωτές περιμένουν από τις εταιρείες να δημιουργήσουν ρυθμίσεις απορρήτου που να εγγυώνται τη διαφάνεια και τον έλεγχο στους τρόπους με τους οποίους οι οργανισμοί συλλέγουν, χρησιμοποιούν και αποθηκεύουν τα προσωπικά

δεδομένα. Οι ρυθμίσεις αυτές συχνά απαιτούν σημαντική προσπάθεια προκειμένου να τεθούν σε εφαρμογή. Τέτοιες ρυθμίσεις δεν αποτελούν αξιόπιστη ένδειξη της συναίνεσης των καταναλωτών. Αυτό πρέπει να αλλάξει!

Ο κανόνας της «Ιδιωτικότητας ως προεπιλογή» είναι χρήσιμος σε περιπτώσεις αθέμιτης, αδικαιολόγητης ή απρόσμενης επεξεργασία των δεδομένων, όπως όταν τα δεδομένα χρησιμοποιούνται για διαφορετικούς σκοπούς από ότι ένα άτομο είχε δώσει αρχικά τη συγκατάθεση του ή όταν τα δεδομένα που συλλέγονται δεν είναι σχετικά με το σκοπό της επεξεργασίας. Με τους κανόνες της «Ιδιωτικότητα ως προεπιλογή» αποτρέπεται η συλλογή των δεδομένων αυτών, για παράδειγμα σε εφαρμογές λογισμικού. Η χρήση των δεδομένων για άλλους σκοπούς από αυτούς που καθορίζονται πρέπει να επιτρέπεται μόνο με τη ρητή συγκατάθεση του χρήστη ή εάν υπάρχει κάποιος άλλος λόγος για την νόμιμη επεξεργασία.

Κάποιοι ορισμοί περιλαμβάνουν μια απαίτηση ώστε οι ρυθμίσεις απορρήτου που περιορίζουν την ανταλλαγή των προσωπικών δεδομένων να είναι ενεργοποιημένες από προεπιλογή. Για παράδειγμα, μια σελίδα κοινωνικής δικτύωσης δεν θα κάνει καμία πληροφορία σχετικά με τους χρήστες της δημόσια ορατή μέχρι να λάβει από τον χρήστη τη συγκατάθεση του για να το επιτρέψει.

Εταιρείες με διαδικτυακές υπηρεσίες πρέπει να αναπτύξουν πρακτικές απορρήτου που πληρούν αυτές τις προσδοκίες. Η ιδιωτικότητα ως προεπιλογή είναι μια έννοια για σχεδιασμό λογισμικού που εξετάζεται από έναν αριθμό αρχών προστασίας δεδομένων, συμπεριλαμβανομένης και της Ευρωπαϊκής Επιτροπής.

Οι υποστηρικτές της Ιδιωτικότητας ως προεπιλογή ισχυρίζονται ότι πολλοί άνθρωποι δεν ξέρουν πώς να ενεργοποιούν τις ρυθμίσεις για την ιδιωτικότητα ή ότι η έλλειψη προεπιλεγμένων ρυθμίσεων μπορεί να οδηγήσει σε υψηλότερο κίνδυνο γα την ιδιωτικότητα των παιδιών σε υπηρεσίες όπως τα μέσα κοινωνικής δικτύωσης.

4

Κοινωνία της Πληροφορίας -Αυτορρύθμιση

4.1 Κοινωνία της Πληροφορίας

Ο όρος Κοινωνία της Πληροφορίας αναφέρεται σε μια μορφή κοινωνικής και οικονομικής ανάπτυξης όπου η απόκτηση, αποθήκευση, επεξεργασία, μεταβίβαση και διάχυση πληροφοριών οδηγεί στη δημιουργία γνώσης . Η **Κοινωνία της Πληροφορίας** είναι η σύγχρονη κοινωνία, που οργανώνεται γύρω από την πληροφορία μέσω της τεχνολογίας. Η αποδέσμευση της από τους χωροχρονικούς περιορισμούς, την καθιστούν προσπελάσιμη μέσω των δικτυωμένων Η/Υ στους ενδιαφερόμενους, οι οποίοι την αναζητούν χωρίς να απαιτείται πλέον η μετακίνηση από τον χώρο της γεωγραφικής τους εγκατάστασης προς το φυσικό ή τεχνητό σημείο αποθήκευσης της. Λειτουργεί ως οικονομικός πόρος για γνώση και για κάθε δραστηριότητα μας στην κοινωνία συμβάλλοντας στην εξέλιξη. Η ψηφιοποίηση της πληροφορίας και η διάχυση της μέσω των ηλεκτρονικών δικτύων στον τελικό χρήστη την καθιστά ως το σημαντικότερο συστατικό στοιχείο του νέου μοντέλου κοινωνικής και οικονομικής οργάνωσης[18].

Μερικοί από τους ορισμούς που έχουν δοθεί είναι:

• Μια κοινωνία που αυτο-οργανώνεται γύρω από την έννοια της γνώσης προς όφελος του κοινωνικού ελέγχου και της διαχείρισης της καινοτομίας και της αλλαγής... (Daniel Bell)

• Ένας νέος τύπος κοινωνίας, στην οποία η κατοχή πληροφορίας (σε αντιδιαστολή με τα υλικά πλούτη) είναι η κινητήρια δύναμη που βρίσκεται πίσω από την εξέλιξη και ανάπτυξή της. (Yoneji Masuda)

• Μια κοινωνία, όπου η πληροφορία χρησιμοποιείται ως οικονομικός πόρος, η κοινότητα τη δαμάζει και την εκμεταλλεύεται και πίσω από όλα αυτά υπάρχει μια ολόκληρη βιομηχανία, η οποία παράγει αυτή την αναγκαία πληροφορία. (Nick Moore)

4.1.1 Δίκαιο στη κοινωνία της Πληροφορίας

Το δίκαιο της Κοινωνίας της Πληροφορίας περιλαμβάνει ερωτήματα προσβασιμότητας, δικαιώματα πνευματικής ιδιοκτησίας, προστασία προσωπικών δεδομένων, ελευθερία της έκφρασης, ηλεκτρονικό εμπόριο, νόμο έντυπου υλικού, συγκεκριμένους τύπους εγκλημάτων μέσω υπολογιστών, ηλεκτρονικές υπογραφές όπως επίσης και θέματα δικαιοδοσίας του διεθνούς δικαίου. Θα μπορούμε να πούμε ότι εκτός από τους κανόνες που δημιουργούνται και θεσπίζονται από τα νομοθετικά σώματα, ο αυτό-κανονισμός της αγοράς και των παραγόντων που συμμετέχουν σε αυτή είναι επίσης σημαντικός και ότι όλοι οι νόμοι, οι δικαστικές αποφάσεις, η αυτο-ρύθμιση και οι κοινωνικές φόρμες αποτελούν μέρος του νομικού υλικού της Κοινωνίας της Πληροφορίας.

4.2Αυτορύθμιση

Με τον όρο αυτορρύθμιση, εννοούμε τα ανεξάρτητα συστήματα κανόνων των διαφόρων τομέων της επιχειρηματικής ζωής, όπως π.χ. τα εμπορικά και βιομηχανικά επιμελητήρια, όσον αφορά στο θεσμικό τους ρόλο. Όταν μιλάμε για τα σύστημα αρχών και αξιών που διέπουν την Κοινωνία της Πληροφορίας, δεν μπορούμε να αγνοήσουμε το γεγονός ότι η κοινωνία μεταβάλλεται με ταχείς ρυθμούς. Το σύστημα των κανόνων που δημιουργείται από τους παράγοντες της αγοράς μπορεί και προσαρμόζεται πιο ευέλικτα στις ταχείες μεταβολές της Κοινωνίας της Πληροφορίας. Αυτοί οι μηχανισμοί αυτό-κανονισμού μπορούν να χρησιμεύσουν ως ενδείξεις στον νομοθέτη. Οποτεδήποτε η αγορά είναι σε θέση να αυτορυθμιστεί, τότε δεν υπάρχει ανάγκη νομοθετικής και κρατικής παρεμβολής.

Ένας πολύ γενικός ορισμός για την αυτο-ρύθμιση έχει δοθεί από τους Efklides, Niemivirta, και Yamauchi (2002), σύμφωνα με τον οποίο ως αυτο-ρύθμιση ορίζεται «η ικανότητα εκείνη που επιτρέπει στο άτομο να παρακολουθεί και να ελέγχει τη συμπεριφορά του, το γιγνώσκειν και το θυμικό του, καθώς και το περιβάλλον, προκειμένου να πετύχει έναν στόχο». Κατά τον Koops το 2006, «η αυτορρύθμιση θα μπορούσε να περιγραφεί ως η ρύθμιση και ο συντονισμός της συμπεριφοράς ατόμων ή ομάδων μέσω κανόνων των κοινωνικών οργανώσεων ή μέσω της εφαρμογής, του ελέγχου συμμόρφωσης και της επιβολής των κανόνων αυτών. Μπορεί να υπάρχει ή να μην υπάρχει συγκεκριμένη νομική βάση για τους κανόνες αυτούς.»

Η ιδέα της αυτό-ρύθμισης ξεκίνησε από τη θεωρία της Κυβερνητικής (Weiner, 1948-1961) για τα προσαρμοζόμενα συστήματα. Ένα προσαρμοζόμενο σύστημα περιλαμβάνει τα ακόλουθα συστατικά στοιχεία:

- την ύπαρξη μιας επιθυμητής τελικής κατάστασης, που μπορεί να ταυτίζεται με τον επιδιωκόμενο στόχο
- όργανα ή μέσα παρακολούθησης της τρέχουσας (πραγματικής) κατάστασης του συστήματος
- ένα μηχανισμό σύγκρισης της επιθυμητής με την πραγματική κατάσταση
- ένα μηχανισμό λειτουργίας, ο οποίος προσδιορίζει το αποτέλεσμα της δράσης του
- ένα μηχανισμό επανατροφοδότησης του αποτελέσματος της λειτουργίας στο ίδιο το σύστημα.

Το κανονιστικό τοπίο της αυτορρύθμισης κυριαρχείται από εναλλακτικές κανονιστικές προσεγγίσεις και μία ποικιλία (πιθανών) συμμετεχόντων. Τρεις προσεγγίσεις είναι οι πλέον επιφανείς: η ρητή (explicit) αυτορρύθμιση, η σιωπηρή τεκμαιρόμενη (implicit) ρύθμιση μέσω του τεχνικού κώδικα και η αυτο-βοήθεια /αυτοπροστασία του χρήστη [19].

4.2 Πλεονεκτήματα –Μειονεκτήματα Αυτορρύθμισης

4.2.1 Πλεονεκτήματα

Στα πλεονεκτήματα της αυτορρύθμισης είναι η αποδοτικότητα και η ευελιξία. Επιτρέπει την εύκολη προσαρμογή σε μεταβαλλόμενες συνθήκες, νέα τεχνογνωσία και εκ νέου αλλαγή των αξιών, των επιλογών παρακολούθησης και των μηχανισμών επιβολής. Η σύνταξη των κανόνων στηρίζετε στην εμπειρία των εμπλεκομένων φορέων, και είναι λιγότερο χρονοβόρα. Επιπλέον οι κανόνες συνήθως εξελίσσονται σταδιακά και δεν υπάρχει η έντονη άσκηση πίεσης, όπως συμβαίνει με την ανάπτυξη της νομοθεσίας και των διεθνών κανόνων.

Ακόμη ένα πλεονέκτημα είναι ότι οι κανόνες συντάσσονται από τα ίδια τα μέρη ή από τους εκπροσώπους τους και η υιοθέτηση αυτο-καθορισμένων προδιαγραφών

αυξάνει την ευαισθητοποίηση μεταξύ των εταίρων. Επίσης οι κανόνες που θεσπίζονται από την ίδια την ομάδα μπορεί να είναι πιο συγκεκριμένοι από τους νόμους που εκδίδονται από τις εθνικές ή διεθνείς κυβερνήσεις.

Η αυτορρύθμιση οδηγεί σε κόστος για τα εμπλεκόμενα μέρη για να συμμορφωθούν με τους κανόνες τους. Η κυβέρνηση μπορεί να επιβλέπει την απόδοση της αυτορρύθμισης, αλλά αυτό το κόστος σε γενικές γραμμές θα είναι πολύ χαμηλότερο από το κόστος για τη ρύθμιση της αγοράς.

4.2.2 Μειονεκτήματα

Η ευελιξία που προαναφέρθηκε μπορεί επίσης να αποτελέσει και μειονέκτημα της αυτορρύθμισης καθώς οι κανόνες μπορούν να αναθεωρηθούν κατά βούληση, και αυτό δεν αποτελεί εγγύηση. Στην αυτορρύθμιση, σε αντίθεση με τη θέσπιση νομοθεσίας, όπου υπάρχουν διαδικασίες για τη δημοσίευση των νόμων, υπάρχει έλλειψη διαφάνειας. Το γεγονός ότι οι κανόνες βασίζονται σε εσωτερικευμένες αξίες μπορεί επίσης να είναι ένα μειονέκτημα γιατί οι αξίες μπορεί να αποδειχθεί ότι είναι επιλεκτικές .

Επιπλέον υπάρχει έλλειψη δημοκρατικού ελέγχου και μπορεί η δύναμη του ισχυρότερου ή καλύτερα οργανωμένου συμμετέχοντα να αυξηθεί. Επομένως θα πρέπει να οριστούν κανόνες για τη διαχείριση του μηχανισμού της αυτορρύθμισης και αυτοί οι κανόνες πρέπει να δημοσιοποιούνται.

Το σημαντικότερο μειονέκτημα του μηχανισμού είναι η ανυπαρξία των κυρώσεων. Η αυτορρύθμιση αποδίδει μόνο αν υπάρχουν κυρώσεις για την παράβαση της. Σε αυτή τη περίπτωση παύει να γίνετε λόγος για αυτορρύθμιση και επιστρέφουμε στο μοντέλο της ρύθμισης [20].

4.3 Η ανάγκη ύπαρξης Ρυθμίσεων

Η μεγαλύτερη πρόκληση για τη ρύθμιση είναι οι ραγδαίες αλλαγές στο χώρο των τεχνολογιών πληροφορικής και επικοινωνιών. Αυτός ο ρυθμός εξέλιξης κάνει δύσκολη την ύπαρξη ρυθμίσεων, όμως η αυτορρύθμιση δεν μπορεί να οργανώσει το διαδίκτυο χωρίς την ύπαρξη κάποιων νομοθετικών διατάξεων και συνεπώς κάποιον κυρώσεων που θα υπάρχουν από τη μη τήρηση τους. Για να μπορέσει να υπάρξει σωστή

ρύθμιση του διαδικτύου θα πρέπει να υπάρχει «συνεργασία» νομικών κανονισμών, κάτι που σημαίνει εφαρμογή των κατάλληλων κανονιστικών συστημάτων και του ρυθμιστικού μηχανισμού της αγοράς. Μερικοί λόγοι που καθιστούν την κρατική παρέμβαση αναγκαία είναι η αδυναμία της αγοράς να επιλύσει κάποια προβλήματα και να ρυθμιστή από μόνη της , το Δημόσιο συμφέρον και το ιδιωτικό συμφέρων.

5

Νομοθετικό πλαίσιο

Τις τελευταίες δεκαετίες έχει παρατηρηθεί ταχεία ανάπτυξη στις Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ), οι οποίες σταδιακά επέφεραν αλλαγές στον κοινωνικό βίο, στις ώρες εργασίας και στις διαπροσωπικές σχέσεις. Αυτό έγινε λόγω της ριζικής αλλαγής στον τρόπο συλλογής, πρόσβασης, χρήσης και διαβίβασης των δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, το Διαδίκτυο και το Web 2.0, είναι τα νέα πρότυπα της δημόσιας επικοινωνιακής διαδικασίας δημιουργώντας μια νέα κατάσταση όπου οι επικοινωνίες δεν έχουν κάποια ιεραρχία και μπορούν να πραγματοποιηθούν ανώνυμα.

Αυτή η νέα κατάσταση των πραγμάτων θα πρέπει να ελεγχθεί από το νόμο και να δοθούν απαντήσεις σε τρέχοντα ζητήματα που προκύπτουν από την παγκόσμια αρχιτεκτονική του δικτύου. Επιπλέον υπάρχουν πολλά θέματα για τα οποία ο νόμος πρέπει να δώσει απαντήσεις, όπως το νομικό πλαίσιο για την ελευθερία του λόγου στο Διαδίκτυο, τους κίνδυνους της αποπλαισιοποίησης των δημοσιευμένων πληροφοριών, τα όρια της ανωνυμίας στο δίκτυο κ.α.

Όλα αυτά τα θέματα θα πρέπει να μελετηθούν και τα περισσότερα από αυτά να ενταχθούν σε μια νέα ολοκληρωμένη προσέγγιση για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση, η οποία θα ολοκληρωθεί με μια σημαντική μεταρρύθμιση της ευρωπαϊκής οδηγίας 95/46/ΕΚ σχετικά με την προστασία δεδομένων.

5.1 Διεθνές νομοθετικό πλαίσιο

Από τις πρώτες συμβάσεις που έγιναν για την προστασία προσωπικών δεδομένων και της ιδιωτικότητας ήταν η Σύμβαση της Ρώμης (1950) για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών και η Σύμβαση 108/28.1.1981 για την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, η οποία κωδικοποίησε τις

θεμελιώδεις αρχές που αποτελούσαν τον «σκληρό πυρήνα» της προστασίας δεδομένων προσωπικού χαρακτήρα. Η Σύμβαση αυτή αποτέλεσε το έναυσμα για αρκετές χώρες να προβούν στη ψήφιση ειδικών νόμων, ενώ άλλες να τροποποιήσουν τη νομοθεσίας τους προκειμένου να θεσπίσουν ένα ολοκληρωμένο και κατάλληλο νομοθετικό πλαίσιο προστασίας του ανθρώπου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα [21].

Η εξέλιξη προηγμένων ψηφιακών τεχνολογιών στα δημόσια τηλεπικοινωνιακά δίκτυα απαιτούσε ειδικές ρυθμίσεις για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτική ζωή των συνδρομητών και των χρηστών. Για να καλυφθούν οι απαιτήσεις αυτές, το κοινοτικό κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων συμπληρώθηκε από την Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997, για την προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα. Η οδηγία αυτή είχε σκοπό την εναρμόνιση των διατάξεων των κρατών μελών οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, καθώς και στην ελεύθερη κυκλοφορία των δεδομένων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα [22].

Επίσης περιλάμβανε ζητήματα ασφάλειας των δεδομένων, του απόρρητου των επικοινωνιών, των δεδομένων κίνησης και χρέωσης, της αναλυτικής χρέωσης, της αναγραφής της ταυτότητας της καλούσας ή συνδεδεμένης γραμμής, της αυτόματης προώθησης κλήσεων, των τηλεφωνικών καταλόγων των συνδρομητών καθώς και το πρόβλημα των αυτόματων συστημάτων κλήσης για εμπορικούς σκοπούς.
Η Οδηγία 97/66/ΕΚ στη συνέχεια αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[23].

5.1.1 Οδηγία 95/46/ΕΚ

Η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [24]. Η οδηγία αυτή αποτελεί το κείμενο αναφοράς, σε ευρωπαϊκό επίπεδο, στα θέματα προστασίας των δεδομένων προσωπικού χαρακτήρα. Θεσπίζει ένα κανονιστικό πλαίσιο που αποσκοπεί στην εγκαθίδρυση μιας ισορροπίας μεταξύ ενός υψηλού επιπέδου προστασίας της ιδιωτικής ζωής των προσώπων και της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα ανά την Ευρωπαϊκή Ένωση (ΕΕ). Προς το σκοπό αυτό, η οδηγία ορίζει τα όρια για τη συλλογή και τη χρησιμοποίηση των δεδομένων προσωπικού χαρακτήρα και ζητά τη δημιουργία, σε κάθε κράτος μέλος, ενός ανεξάρτητου εθνικού οργανισμού επιφορτισμένου με την προστασία των δεδομένων αυτών.

Έτσι λοιπόν το άρθρο 1 της Οδηγίας, αναφέρεται στην προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής και θεσπίζει την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών, εφόσον εξασφαλίζονται τα προηγούμενα.

Στο Άρθρο 6 της Οδηγίας, καταγράφονται οι βασικές αρχές της ιδιωτικότητας και της προστασίας προσωπικών δεδομένων. Τα κράτη μέλη προβλέπουν ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει:

- να υφίστανται σύννομη και θεμιτή επεξεργασία (όπως ορίζετε στο άρθρο 7).
- να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς
- να είναι συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται και υφίστανται επεξεργασία
- να είναι ακριβή και, εφόσον χρειάζεται, να ενημερώνονται,
- να διατηρούνται με μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των προσώπων στα οποία αναφέρονται μόνο κατά τη διάρκεια περιόδου που δεν υπερβαίνει την απαιτούμενη για την επίτευξη των σκοπών για τους οποίους έχουν συλλεγεί.

Στο άρθρο 7 της οδηγίας οριοθετείται η νομιμότητα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Χαρακτηριστικά στο άρθρο 7 της Οδηγίας, ορίζονται οι περιπτώσεις στις οποίες η επεξεργασία προσωπικών δεδομένων είναι θεμιτή. Όπως αναφέρετε στο άρθρο, η επεξεργασία προσωπικών δεδομένων επιτρέπεται όταν:

- το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει τη ρητή συγκατάθεση του
- η επεξεργασία των δεδομένων είναι απαραίτητη για την εκτέλεση σύμβασης, της οποίας το ενδιαφερόμενο πρόσωπο είναι συμβαλλόμενο μέρος ή για την εκτέλεση προσυμβατικών μέτρων που έχουν ληφθεί μετά από αίτηση του προσώπου
- είναι απαραίτητη για την τήρηση εκ του νόμου υποχρεώσεως του υπευθύνου της επεξεργασίας
- είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται τα δεδομένα
- είναι απαραίτητη για την εκπλήρωση έργου δημοσίου συμφέροντος
- είναι απαραίτητη για την ικανοποίηση ενός έννομου συμφέροντος του υπεύθυνου επεξεργασίας εφόσον δεν προέχει το συμφέρον του υποκειμένου των δεδομένων.

Στο άρθρο 8 της οδηγίας οριοθετείται η νομιμότητα για την επεξεργασία ειδικών κατηγοριών δεδομένων. Σε αυτές τις κατηγορίες ορίζονται τα δεδομένα που παρέχουν πληροφορίες σχετικά με τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία και τη σεξουαλική ζωή. Επίσης σαν ειδικές κατηγορίες δεδομένων θεωρούνται οι πληροφορίες που αφορούν ποινικά αδικήματα, καθώς και τον εθνικό αναγνωριστικό αριθμό ταυτότητας.

Βάση του άρθρου τα κράτη μέλη απαγορεύουν την επεξεργασία δεδομένων που παρέχουν τέτοιου είδους πληροφορίες εκτός και αν:

- το πρόσωπο στο οποίο αναφέρονται τα δεδομένα έχει δώσει ρητά τη συγκατάθεση του για την επεξεργασία.

- η επεξεργασία είναι απαραίτητη προκειμένου να εκπληρωθούν οι υποχρεώσεις και τα ειδικά δικαιώματα του υπευθύνου της επεξεργασίας στον τομέα του εργατικού δικαίου
- η επεξεργασία δεδομένων είναι αναγκαία για τη διασφάλιση του ζωτικού συμφέροντος του προσώπου στο οποίο αναφέρονται
- η επεξεργασία διεξάγετε από διάφορους μη κερδοσκοπικούς φορείς, η οποία λαμβάνει χώρα μόνο για τα μέλη αυτών και τα δεδομένα ανακοινώνονται σε τρίτους μόνον με τη συγκατάθεση των προσώπων στα οποία αναφέρονται
- η επεξεργασία αφορά δεδομένα τα οποία προδήλως δημοσιοποιούνται από το πρόσωπο στο οποίο αναφέρονται
- η επεξεργασία δεδομένων που αφορά ιατρική πρόληψη ή διάγνωση, την παροχή ιατροφαρμακευτικής αγωγής ή τη διαχείριση των ιατροφαρμακευτικών υπηρεσιών.
- αφορούν την προώθηση του δημόσιου συμφέροντος.

Το άρθρο 10 της οδηγίας καθορίζει της πληροφορίες που πρέπει να γνωστοποιούνται στο άτομο του οποίου συλλέγονται τα δεδομένα. Αυτές οι πληροφορίες είναι η ταυτότητα του υπευθύνου της επεξεργασίας, οι σκοποί της επεξεργασίας, τους αποδέκτες των δεδομένων, την ύπαρξη δικαιώματος πρόσβασης στα συγκεκριμένα δεδομένα και του δικαιώματος διόρθωσής τους.

Η οδηγία στο άρθρο 12 ρυθμίζει το δικαίωμα πρόσβασης το δικαίωμα του ατόμου να λαμβάνει από τον υπεύθυνο επεξεργασίας:

- την επιβεβαίωση για την ύπαρξη ή όχι της επεξεργασίας, το σκοπό της, τις κατηγορίες των δεδομένων υπό επεξεργασία και τους αποδέκτες των δεδομένων
- γνωστοποίηση των δεδομένων και των διαθέσιμων πληροφοριών καθώς και την προέλευση τους
- ενημέρωση για τη λογική της αυτοματοποιημένης επεξεργασίας.

Επίσης στα δικαιώματα συμπληρώνεται το δικαίωμα της διόρθωσης, διαγραφής ή κλειδώματος των δεδομένων των οποίων η επεξεργασία δεν είναι σύμφωνη και την

κοινοποίηση των μεταβολών αυτών στους τρίτους που υπήρξαν αποδέκτες των δεδομένων αυτών.

Σύμφωνα με το άρθρο 13, τα δικαιώματα πρόσβασης στα δεδομένα περιορίζονται όταν πρόκειται για:

- την ασφάλεια του κράτους
- την άμυνα
- τη δημόσια ασφάλεια,
- την πρόληψη, διερεύνηση, διαπίστωση και δίωξη παραβάσεων του ποινικού νόμου
- τα οικονομικά και χρηματοοικονομικά συμφέροντα του κράτους μέλους ή της Ευρωπαϊκής Ένωσης.
- τον έλεγχο, την επιθεώρηση και τα ρυθμιστικά καθήκοντα που συνδέονται με την άσκηση δημόσιας εξουσίας
- την προστασία των δικαιωμάτων του προσώπου στο οποίο ανήκουν τα δεδομένα.

Στα άρθρα 16 και 17 της οδηγίας γίνετε αναφορά στο απόρρητο και την ασφάλεια της επεξεργασίας [25].

Χαρακτηριστικά στο άρθρο 16 ορίζεται ότι κάθε πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου της επεξεργασίας ή του εκτελούντος την επεξεργασία, περιλαμβανομένου του ιδίου του εκτελούντος την επεξεργασία και έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, μπορεί να τα επεξεργασθεί μόνο κατ' εντολή του υπευθύνου της επεξεργασίας, εκτός και αν είναι υποχρεωμένος για αυτό από το νόμο.

Τα Άρθρο 17 αναφέρεται στην Ασφάλεια της επεξεργασίας και προβλέπει τα εξής:

1. ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως εάν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσων δικτύου.

Τα μέτρα αυτά πρέπει να λαμβάνουν υπόψη τις τεχνολογικές εξελίξεις και το κόστος εφαρμογής τους, το επίπεδο ασφαλείας να είναι ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και τη φύση των δεδομένων.

2. ο υπεύθυνος της επεξεργασίας οφείλει, σε περίπτωση επεξεργασίας για λογαριασμό του, να επιλέγει προς εκτέλεση της επεξεργασίας πρόσωπο το οποίο παρέχει επαρκείς εγγυήσεις όσον αφορά τα μέτρα τεχνικής ασφάλειας και οργάνωσης της επεξεργασίας και να εξασφαλίζει την τήρηση των μέτρων αυτών.

3. Η εκτέλεση επεξεργασίας μέσω άλλου προσώπου πρέπει να διέπεται από σύμβαση ή δικαιοπραξία που συνδέει τον εκτελούντα με τον υπεύθυνο της επεξεργασίας.

4. Για αποδεικτικούς λόγους, τα τμήματα της σύμβασης ή δικαιοπραξίας που αφορούν την προστασία των δεδομένων και τις απαιτήσεις σχετικά με τα μέτρα καταρτίζονται εγγράφως ή σε άλλη ανάλογη μορφή.

5.2 Νομοθετικές Διατάξεις στην Ελλάδα

Στις 10 Απριλίου το 1997 ψηφίστηκε ο νόμος **2472/1997** για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νόμος 2472/97 μεταφέρει τις ρυθμίσεις της κοινοτικής Οδηγίας 95/46/ΕΚ για την προστασία δεδομένων προσωπικού χαρακτήρα στην εσωτερική έννομη τάξη. Ο παρόν νόμος θεσπίζει προϋποθέσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα [26].

Ο νόμος 2472/1997 τροποποιήθηκε το 2000 (2819/2000) και το 2001 (2915/2001). Τελική τροποποίηση του νόμου ήταν ο νόμος **3471/2006** για την Προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Η τροποποίηση αυτή αποτελεί πράξη προσαρμογής της ελληνικής νομοθεσίας στην κοινοτική Οδηγία 2002/58/ΕΚ. Σκοπός του παρόντος νόμου ήταν η προστασία των θεμελιωδών δικαιωμάτων των ατόμων, της ιδιωτικής ζωής, η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών[27].

Το 2011 έγινε τροποποίηση του νόμου 3471/2006 στο Νόμο 3917/2011 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με

τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις [28]. Τέλος το 2012 κάποια από τα άρθρα του νόμου 3471 αντικαταστάθηκαν από το άρθρο 171 του νόμου 4070.

5.2.1 Νόμος 2472/97

Ο νόμος 2472/1997 είναι στην πράξη η εναρμόνιση του ελληνικού δικαίου με την Οδηγία 95/46/ΕΚ. Αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής. Ο έλληνας νομοθέτης δε διαφοροποιεί τις ρυθμίσεις ανάμεσα σε ιδιωτικό και δημόσιο τομέα αλλά εισαγάγει ενιαία ρύθμιση.

Με τον νόμο αυτό καθορίσθηκε τι αποτελεί προσωπικό δεδομένο και πώς επιτρέπεται η συλλογή και επεξεργασία του καθώς και τα δικαιώματα του υποκειμένου των πληροφοριών απέναντι στον κάτοχο των πληροφοριών. Επίσης καθιερώθηκε ο δημόσιος έλεγχος της τήρησης των προσωπικών δεδομένων

Στο άρθρο 4 θεσπίζονται οι περιέχονται οι γενικές αρχές που αποτελούν βασική προϋπόθεση για την διαφύλαξη της νομιμότητας της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα οι αρχές αυτές αναφέρονται αποκλειστικά στο υπολογιστικό περιβάλλον, με εξαίρεση τις αρχές της νόμιμης και θεμιτής συλλογής και επεξεργασίας που πράγματι προστατεύουν και την ιδιωτικότητα. Επιπλέον, καθιερώνονται τέσσερις βασικές αρχές: του σκοπού, της αναλογίας σκοπού και δεδομένων, της ακρίβειας και της ενημέρωσης και της χρονικά πεπερασμένης διατήρησης.

Στα άρθρο 5 ορίζονται οι προϋποθέσεις για την εκτέλεση επεξεργασίας. Συγκεκριμένα ορίζεται ότι η επεξεργασία είναι νόμιμη και κατά συνέπεια επιτρεπτή μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του.

Επίσης στο άρθρο αναφέρονται οι περιπτώσεις υπό τις οποίες μπορεί να πραγματοποιηθεί επεξεργασία χωρίς τη συγκατάθεση του υποκειμένου. Αυτές οι περιπτώσεις είναι:

- για την εκτέλεση σύμβασης, στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος, ή για τη λήψη μέτρων κατόπιν αιτήσεως του

υποκειμένου κατά το προσυμβατικό στάδιο. Πρόκειται για περιπτώσεις τραπεζικών δανείων, ασφαλιστηρίων συμβολαίων, εργασιακών σχέσεων, ιατρού εργασίας κλπ.

- για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.
- για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.
- για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου.
- την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας.

Με τις εξαιρέσεις που μόλις είδαμε διαπιστώνεται ότι η εξουσία του ατόμου στα προσωπικά του δεδομένα δεν είναι απεριόριστη και ότι το άτομο πρέπει να δεχτεί κάποιους περιορισμούς στο δικαίωμα του πληροφοριακού ανακαθορισμού για εκτέλεση έργου δημόσιου συμφέροντος

Βάση του άρθρου 6, ο υπεύθυνος επεξεργασίας υποχρεούται να γνωστοποιήσει εγγράφως στην Αρχή, τη σύσταση και λειτουργία αρχείου ή την έναρξη της επεξεργασίας.

Στο άρθρο 7 γίνετε απαγόρευση της επεξεργασίας ευαίσθητων δεδομένων έκτος και αν συντρέχουν κάποιοι από τους λόγους που είδαμε και στο άρθρο 8 της οδηγίας 95/46.

Στο άρθρο 9 του νόμου καθορίζετε η διασυνοριακή ροή των δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα στο άρθρο ορίζετε ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη για χώρες-μέλη της Ευρωπαϊκής Ένωσης και προς χώρες που δεν είναι μέλη της Ευρωπαϊκής Ένωσης, μετά από άδεια της Αρχής που παρέχεται εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Επιπλέον, η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή ένωση, η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ' εξαίρεση, με άδεια της Αρχής, εάν υπάρχει κάποιος από του παρακάτω λόγους: α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, β) Η διαβίβαση είναι απαραίτητη, γ) Η

διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη δημόσιου συμφέροντος, δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου, ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, στ) Ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων και την άσκηση των σχετικών δικαιωμάτων τους.

Το άρθρο 10 του νόμου αναφέρεται στο απόρρητο και την ασφάλεια της επεξεργασίας. Συγκεκριμένα στο άρθρο ορίζεται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απόρρητη και διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνον κατ' εντολή του. Επίσης για τη διεξαγωγή της ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Με την επιφύλαξη άλλων διατάξεων, η Αρχή παρέχει οδηγίες ή εκδίδει κανονιστικές πράξεις σύμφωνα με το άρθρο 19 παρ. 1 ι' για τη ρύθμιση θεμάτων σχετικά με τον βαθμό ασφαλείας των δεδομένων και των υπολογιστικών και επικοινωνιακών υποδομών, τα μέτρα ασφάλειας που είναι αναγκαίο να λαμβάνονται για κάθε κατηγορία και επεξεργασία δεδομένων, καθώς και για τη χρήση τεχνολογιών ενίσχυσης της ιδιωτικότητας.

Τέλος αν η επεξεργασία διεξάγεται για λογαριασμό του υπεύθυνου από πρόσωπο μη εξαρτώμενο από αυτόν, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Η ανάθεση προβλέπει υποχρεωτικά ότι ο ενεργών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπεύθυνου και ότι οι λοιπές υποχρεώσεις του παρόντος άρθρου βαρύνουν αναλόγως και αυτόν.

Στα άρθρα 11, 12, 13, 14 ορίζεται η κατοχύρωση των δικαιωμάτων των υποκειμένων στο δικαίωμα ενημέρωσης, το δικαίωμα πρόσβασης στα αρχεία, το δικαίωμα αντίρρησης και το δικαίωμα προσωρινής δικαστικής προστασίας.

5.2.2 Νόμος 3471/06

Όπως προαναφέρθηκε ο νόμος 3471/06 ήταν η τελική τροποποίηση του νόμου 2472/97 για την Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών[29].

Στο άρθρο 5 του νόμου το οποίο αντικαταστάθηκε από το άρθρο 171 παρ. 1 του νόμου 4071/2012 αναφέρονται οι κανόνες επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Στη παρ.1 του άρθρου ορίζετε ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, περιλαμβανομένων των δεδομένων κίνησης και θέσης, πρέπει να περιορίζεται στο απολύτως αναγκαίο μέτρο για την εξυπηρέτηση των σκοπών της.

Εν συνεχεία στη παρ. 2 ορίζονται οι προϋποθέσεις που πρέπει να ισχύουν για να είναι επιτρεπτή η επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Στη παρ. 3 ορίζετε ότι όπου ο νόμος απαιτεί τη συγκατάθεση του συνδρομητή ή χρήστη, η σχετική δήλωση δίδεται εγγράφως ή με ηλεκτρονικά μέσα. Στην τελευταία περίπτωση, ο υπεύθυνος επεξεργασίας εξασφαλίζει ότι ο συνδρομητής ενεργεί με την πλήρη επίγνωση των συνεπειών που έχει η δήλωσή του η οποία καταγράφεται με ασφαλή τρόπο, είναι ανά πάσα στιγμή προσβάσιμη στον συνδρομητή και μπορεί οποτεδήποτε να ανακληθεί.

Στη παρ. 4 του άρθρου καθορίζετε ότι ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα.

Περισσότερο θα μας απασχολήσει η παράγραφος 4 του άρθρου στην οποία θα μπορούσε να θεωρηθεί ότι ο νομοθέτης δίνει κατευθυντήριες γραμμές για το Privacy by Design και οι οποίες θα αναλυθούν στη συνέχεια.

5.3 Πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία δεδομένων.

Στις 25 Ιανουαρίου 2012 η Ευρωπαϊκή Επιτροπή πρότεινε την αναμόρφωση της νομοθεσίας που αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Σκοπός της πρότασης είναι οι Ευρωπαίοι πολίτες να έχουν μεγαλύτερο έλεγχο στα δεδομένα τους. Οι κανόνες αποσκοπούν στην αναμόρφωση της υφιστάμενης νομοθεσίας για την προστασία προσωπικών δεδομένων, που δεν μπορούσε να συμβαδίσει με τις εξελίξεις στο Διαδίκτυο, όπως για παράδειγμα τα μέσα κοινωνικής δικτύωσης. Με την έγκριση της αναμένεται να ενισχυθούν τα δικαιώματα των πολιτών και θα μπορούσε να έχει εκτεταμένη επίδραση στον τρόπο που συλλέγονται και επεξεργάζονται τα προσωπικά δεδομένα στο διαδίκτυο

Το προτεινόμενο νομικό πλαίσιο αποτελείται από δύο νομοθετικές προτάσεις:

- μια πρόταση κανονισμού για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (γενικός κανονισμός για την προστασία δεδομένων)
- μια πρόταση οδηγία για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τον σκοπό της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Μερικές από τις αλλαγές, προσθήκες που προτάθηκαν σε σχέση με την οδηγία 95/46 ΕΚ είναι:

Στο άρθρο 14 (άρθρο 11 95/46ΕΚ) έχουν εισαχθεί πρόσθετες πληροφορίες τις οποίες πρέπει να γνωρίζει το πρόσωπο στο οποίο αναφέρονται τα δεδομένα όπως:

- το χρονικό διάστημα για το οποίο θα αποθηκευθούν τα δεδομένα προσωπικού χαρακτήρα.

- το δικαίωμα υποβολής καταγγελίας στην αρχή ελέγχου και τα στοιχεία επικοινωνίας με την αρχή ελέγχου.
- όπου συντρέχει περίπτωση, ότι ο υπεύθυνος επεξεργασίας προτίθεται να διαβιβάσει τα δεδομένα σε τρίτη χώρα ή διεθνή οργανισμό και το επίπεδο προστασίας που παρέχει η εν λόγω τρίτη χώρα ή ο διεθνής οργανισμός διά παραπομπής σε απόφαση περί επάρκειας της Επιτροπής.
- κάθε περαιτέρω απαραίτητη πληροφορία προκειμένου να διασφαλίζεται θεμιτή επεξεργασία έναντι του προσώπου που αφορούν τα δεδομένα, λαμβάνοντας υπόψη τις ειδικές συνθήκες υπό τις οποίες συλλέγονται τα δεδομένα προσωπικού χαρακτήρα.

Σημαντική προσθήκη στην πρόταση της Ευρωπαϊκής Επιτροπής είναι το άρθρο 17 το οποίο προβλέπει το δικαίωμα του προσώπου στο οποίο αναφέρονται τα δεδομένα «να λησμονηθεί» και το δικαίωμα διαγραφής των δεδομένων του. Επίσης συμπεριλαμβάνει και την υποχρέωση του υπευθύνου επεξεργασίας ο οποίος δημοσιοποίησε τα δεδομένα να ενημερώνει τους τρίτους για το αίτημα του προσώπου στο οποίο αναφέρονται τα δεδομένα για διαγραφή τυχόν συνδέσμων ή αντιγράφων ή αναπαραγωγής των εν λόγω δεδομένων προσωπικού χαρακτήρα.

Η διαγραφή δεν πραγματοποιείται εάν η διατήρηση των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη:

- για την άσκηση του δικαιώματος ελευθερίας της έκφρασης
- για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας
- για ιστορικούς και στατιστικούς σκοπούς ή για σκοπούς ιστορικής έρευνας
- για την τήρηση εκ του νόμου υποχρεώσεως διατήρησης των δεδομένων προσωπικού χαρακτήρα την οποία υπέχει ο υπεύθυνος επεξεργασίας από το δίκαιο της Ένωσης ή από τη νομοθεσία κράτους μέλους στην οποία υπάγεται.

Το άρθρο 18 το οποίο θεσπίζει το δικαίωμα του προσώπου στο οποίο αναφέρονται τα δεδομένα στη φορητότητα των δεδομένων, δηλαδή στη μεταφορά δεδομένων από ένα ηλεκτρονικό σύστημα επεξεργασίας σε ένα άλλο, χωρίς να εμποδίζεται από τον υπεύθυνο επεξεργασίας να πράξει κάτι τέτοιο[30].

Ακόμη μία σημαντική προσθήκη στην πρόταση της Ευρωπαϊκής Επιτροπής είναι το άρθρο 23 για τη προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού το οποίο θα αναλύσουμε στη συνέχεια.

5.4Νομοθετικές Διατάξεις και Privacy by Design

Η προστασία της Ιδιωτικότητας είναι ζήτημα που πρέπει να επιλυθεί με τεχνολογικά μέσα. Συγκεκριμένα να γίνετε η σχεδίαση και η εφαρμογή τεχνολογικών προϊόντων και υπηρεσιών με τρόπο ώστε να προωθείται και να γίνεται σεβαστή η ιδιωτικότητα. Η επιλογή των ρυθμιστικών απαιτήσεων που θα μετουσιωθούν σε τεχνολογία δεν είναι τεχνοκρατικό αλλά θεσμικό ζήτημα.

Οι υπεύθυνοι της Προστασίας Προσωπικών Δεδομένων στην Ευρώπη και τις ΗΠΑ υποστηρίζουν τη προστασία της ιδιωτικότητας από τον σχεδιασμό (PbD) όπως ποτέ άλλοτε. Αυτή είναι η ιδέα, ότι κατά τον σχεδιασμό τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ), πρέπει να γίνετε ενσωμάτωση της ιδιωτικότητας από την αρχή, επιτυγχάνοντας καλύτερα αποτελέσματα από το όταν προσθέτονται στο τέλος. Η οδηγία της Ευρωπαϊκής Ένωσης για τη προστασίας δεδομένων πάντα περιλάμβανε διατάξεις που απαιτούσαν από τους υπευθύνους επεξεργασίας δεδομένων να εφαρμόζουν τεχνικά και οργανωτικά μέτρα στο σχεδιασμό και τη λειτουργία των ΤΠΕ. Αυτό αποδείχθηκε ανεπαρκές και στη νέα πρόκληση για ιδιωτικότητα από τον σχεδιασμό (Privacy by Design), η Ευρωπαϊκή Επιτροπή (EC) ζητά οι αρχές προστασίας δεδομένων να λαμβάνονται υπόψη κατά την έναρξη του σχεδιασμού, την κατασκευή και τη λειτουργία των συστημάτων ΤΠΕ. Ειδικότερα, ενθαρρύνουν τη χρήση των Τεχνολογιών προστασία της ιδιωτικότητας (PETs) καθώς επίσης και τη χρήση των προεπιλεγμένων ρυθμίσεων που ευνοούν την ιδιωτικότητα.

Στις ΗΠΑ, μια πολύ πρόσφατη έκθεση της Ομοσπονδιακής Επιτροπής Εμπορίου (FTC) περιγράφει ένα προτεινόμενο πλαίσιο με τρεις βασικούς άξονες: ιδιωτικότητα από τον σχεδιασμό, απλουστευμένες επιλογές των καταναλωτών και αύξηση της διαφάνειας των πρακτικών των δεδομένων.

Σύμφωνα με μια έκθεση [31], οι εταιρείες συμμετέχουν στην ιδιωτικότητα από τον σχεδιασμό, όταν προωθούν την ιδιωτικότητα των καταναλωτών σε όλη τη οργάνωση τους και σε κάθε στάδιο της ανάπτυξης των προϊόντων και των υπηρεσιών τους. Πιο

συγκεκριμένα, η ιδιωτικότητα τον σχεδιασμό (PbD) διαθέτει δύο βασικά στοιχεία: πρώτον, την ενσωμάτωση ουσιαστικής προστασία της ιδιωτικότητας σε πρακτικές μιας επιχείρησης και δεύτερο, την τήρηση ολοκληρωμένων διαδικασιών διαχείρισης δεδομένων καθ 'όλη τη διάρκεια του κύκλου ζωής των προϊόντων και των υπηρεσιών τους. Η έκθεση αναφέρει επίσης τη χρήση των PETs, όπως τη διαχείριση ταυτότητας, τα εργαλεία σήμανσης δεδομένων, κρυπτογραφημένη μεταφορά, και τα εργαλεία για έλεγχο και προσαρμογή των προεπιλεγμένων ρυθμίσεων. Εν ολίγοις, οι ρυθμιστικές αρχές και στις δύο πλευρές του Ατλαντικού συμφωνούν ως προς την ανάγκη για ένα νέο νομικό πλαίσιο για την προστασία της ιδιωτικότητας στο διαδίκτυο (online) στον 21ο αιώνα και ότι μία από τις σημαντικές πτυχές του θα πρέπει να είναι η ιδιωτικότητα από το σχεδιασμό(PbD).

Παρά τον ενθουσιασμό των ρυθμιστικών αρχών, οι PETs δεν είναι ευρέως αποδεκτές στην αγορά και σχετικά λίγες επιχειρήσεις έχουν υιοθετήσει προστασία στην ιδιωτικότητα από τον σχεδιασμό. Αυτό οφείλεται σε διάφορους παράγοντες, όπως η σύγχυση γύρω από βασικούς ορισμούς, το πώς η ιδιωτικότητα από τον σχεδιασμό σχετίζεται με συγκεκριμένες τεχνολογίες ή οργανωτικά μέτρα και στην αβεβαιότητα ως προς το τι πραγματικά είχαν οι ρυθμιστικές αρχές στο μυαλό όταν παρότρυναν τις επιχειρήσεις να «επενδύσουν» στην ιδιωτικότητα.

Τα οικονομικά παίζουν επίσης σημαντικό ρόλο στον καθορισμό του ρυθμού υιοθέτησης των PETs και των πρακτικών σχεδιασμού της ιδιωτικότητας. Από την πλευρά των καταναλωτών, μερικές τεχνολογίες ενίσχυσης της ιδιωτικότητας (PETs) έχουν αποδειχθεί δημοφιλείς και η ζήτηση για τα προϊόντα και τις υπηρεσίες με ισχυρή προστασία της ιδιωτικότητας φαίνεται αρκετά περιορισμένη. Μερικοί από τους λόγους είναι η έλλειψη γνώσεων των καταναλωτών σχετικά με τους κινδύνους για την ιδιωτικότητα, που συνδέονται με την περιήγηση στο διαδίκτυο, τις αναζητήσεις, τα κοινωνικά δίκτυα, το ηλεκτρονικό εμπόριο και άλλες καθημερινές δραστηριότητες στο Διαδίκτυο καθώς και την περιορισμένη κατανόηση του πώς οι PETs ή η ιδιωτικότητα από το σχεδιασμό (PbD) μπορεί να βοηθήσουν στη μείωση των κινδύνων αυτών. Από την πλευρά των επιχειρήσεων, λόγω της μειωμένης ζήτησης των καταναλωτών, αποθαρρύνονται οι δαπάνες για την τεχνολογία των πληροφοριών(IT). Επιπλέον, λαμβάνοντας υπόψη τα τεράστια κέρδη που αποκομίζουν πολλές επιχειρήσεις από την ηλεκτρονική διαφήμιση, είναι απρόθυμοι να εφαρμόσουν εθελοντικά οποιεσδήποτε PETs ή πρακτικές σχεδιασμού που θα

περιόριζαν τη δυνατότητά τους να συλλέγουν, αναλύουν ή να μοιραστούν τα δεδομένα των καταναλωτών.

Παρά το γεγονός ότι η Ευρωπαϊκή Επιτροπή χρηματοδότησε μια μελέτη για το οικονομικό κόστος και τα οφέλη των PETs και το Ηνωμένο Βασίλειο εξετάζει πώς μπορεί να βελτιωθεί το επιχειρηματικό ενδιαφέρον και την επένδυση στην ιδιωτικότητα από το σχεδιασμό (PbD), υπάρχουν λιγοστές ενδείξεις ότι η τεχνολογία της ιδιωτικότητας από μόνης της δίνει ανταγωνιστικό πλεονέκτημα στις επιχειρήσεις που θα την υιοθετήσουν. Πράγματι, τα οικονομικά ή ρυθμιστικά κίνητρα για την υιοθέτηση της ιδιωτικότητας από το σχεδιασμό (PbD) χρειάζονται περισσότερη προσοχή στην Ευρώπη και απουσιάζουν σε μεγάλο βαθμό από τις εκθέσεις της FTC.

5.4.1 Privacy by design στο Διεθνές Νομοθετικό πλαίσιο.

Το νομοθετικό πλαίσιο όπως προαναφέρθηκε στα άρθρα 16 και 17 της οδηγίας 95/46 ΕΚ και αντιστοίχως το άρθρο 10 του νόμου 2472/97 αναφέρετε στο απόρρητο και την ασφάλεια της επεξεργασίας. Στα συγκεκριμένα άρθρα παρατηρείται η νομική υποχρέωση του υπεύθυνου επεξεργασίας να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των δεδομένων καθώς επίσης και ότι τα μέτρα αυτά πρέπει να λαμβάνουν υπόψη τις τεχνολογικές εξελίξεις.

Οι προϋποθέσεις που τίθενται από το νόμο μπορούν να εξασφαλιστούν από τις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας καθώς όπως είδαμε προηγουμένως περιορίζουν τη συλλογή προσωπικών δεδομένων και εμποδίζουν τη μη αναγκαία ή ανεπιθύμητη επεξεργασία. Επιπλέον, θα μπορούσε να γίνει χρήση της PbD. Έτσι τα συστήματα θα είχαν ενσωματωμένα όλα αυτά τα χαρακτηριστικά από την αρχή της δημιουργίας τους με αποτέλεσμα από το πρώτο δεδομένο που θα καταχωρούταν να υπήρχε ασφάλεια και προστασία.

Επίσης, όπως προαναφέρθηκε στην πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και συμβουλίου στο άρθρο 23, καθορίζετε η προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού. Σύμφωνα με την παράγραφο 1 του άρθρου 23, ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα και διαδικασίες τόσο κατά τον καθορισμό των μέσων επεξεργασίας όσο και κατά την ίδια την επεξεργασία κατά τρόπο ώστε η

επεξεργασία να πληροί τις απαιτήσεις του κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του προσώπου στο οποίο αναφέρονται τα δεδομένα. Όπως διαπιστώνεται, το Σχέδιο Κανονισμού εισάγει περισσότερες απαιτήσεις για την λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων, αφού απαιτείται τα μέτρα να λαμβάνονται από τον καθορισμό των μέσων επεξεργασίας, συνεπώς από τον σχεδιασμό.

Επιπλέον στη παράγραφο 2 του άρθρου 23 επιβάλετε ο υπεύθυνος επεξεργασίας εφαρμόζει μηχανισμούς ώστε να διασφαλίζεται ότι, εξ ορισμού, υποβάλλονται σε επεξεργασία μόνον εκείνα τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι αναγκαία για κάθε συγκεκριμένο σκοπό επεξεργασίας και ότι τα εν λόγω δεδομένα δεν συλλέγονται ούτε διατηρούνται πέραν του ελάχιστου απαραίτητου ορίου για τους σκοπούς αυτούς, από την άποψη τόσο της ποσότητας των δεδομένων όσο και του χρόνου της αποθήκευσής τους. Ειδικότερα, οι εν λόγω μηχανισμοί διασφαλίζουν ότι, εξ ορισμού, δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσπελάσιμα σε αόριστο αριθμό φυσικών προσώπων. Σε αυτή τη παράγραφο γίνετε εισαγωγή της αρχής του Privacy by Default.

Επίσης οι παράγραφοι 3 και 4 του άρθρου 23 αναφέρουν ότι η Επιτροπή εξουσιοδοτείται να εκδίδει κατ' εξουσιοδότηση πράξεις για τον προσδιορισμό τυχόν περαιτέρω κριτηρίων και απαιτήσεων σχετικά με τα κατάλληλα μέτρα και τους μηχανισμούς που αναφέρονται στις παραγράφους 1 και 2, ιδίως για τις απαιτήσεις προστασίας των δεδομένων ήδη από τον σχεδιασμό οι οποίες εφαρμόζονται σε όλους τους τομείς, τα προϊόντα και τις υπηρεσίες. Ακόμη, η Επιτροπή μπορεί να θεσπίσει τεχνικά πρότυπα για τις απαιτήσεις που προβλέπονται στις παραγράφους 1 και 2 [30].

Σύμφωνα με την άποψη της Ομάδας 29 το Φεβρουάριο του 2012, η υποχρέωση του υπεύθυνου επεξεργασίας είναι αρκετά σαφής, καθώς του θέτει την ευθύνη για την εφαρμογή κατάλληλων μέτρων. Στη γνωμοδότηση της η ομάδα 29 λέει ότι φαίνεται σχεδόν αδύνατο να καλύπτονται όλες οι περιπτώσεις του παρόντος κανονισμού, δεδομένου ότι μπορεί να εκτιμηθεί μόνο για κάθε περίπτωση ξεχωριστά αν ο υπεύθυνος επεξεργασίας έχει λάβει τα κατάλληλα μέτρα και διαδικασίες ή όχι, έχοντας υπόψη το επίπεδο τεχνικής (state of art) και το κόστος εφαρμογής. Επίσης, καταλήγει στο συμπέρασμα ότι δεν κρίνεται απαραίτητη περαιτέρω νομοθεσία ή

καθοδήγηση. Ωστόσο οδηγίες που εκδίδονται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) μπορεί να είναι χρήσιμες [32].

5.4.2 Privacy by design στο Ελληνικό δίκαιο

Όπως αναφέραμε και πιο πάνω στο Ελληνικό δίκαιο υπάρχει το άρθρο 10 του νόμου 2472/97 στο οποίο απαιτείται η λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων καθώς και το να λαμβάνονται υπόψη οι τεχνολογικές εξελίξεις.

Επιπλέον ο νόμος 3471/2006 στο άρθρο 5 στις παραγράφους 6 και 7 παραπέμπει στην αρχή της Privacy by design και στις Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας αντίστοιχα. Η παράγραφος 6 αναφέρει ότι «ο σχεδιασμός και η επιλογή των τεχνικών μέσων και των πληροφοριακών συστημάτων, καθώς και ο εξοπλισμός για την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, πρέπει να γίνονται με βασικό κριτήριο την επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα»[33]. Όπως παρατηρείται πρέπει να λαμβάνεται υπόψη η επεξεργασία όσο το δυνατόν λιγότερων δεδομένων από το σχεδιασμό των συστημάτων. Δηλαδή θα πρέπει να ληφθεί υπόψη η ιδιωτικότητα στο σχεδιασμό, γεγονός που μας παραπέμπει στην αρχή της Privacy by Design.

Επίσης σύμφωνα με τη παράγραφο 7 «φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει στο βαθμό που αυτό είναι τεχνικώς εφικτό, να καθιστά δυνατή τη χρήση και πληρωμή των υπηρεσιών αυτών ανωνύμως ή με ψευδώνυμο».

Ακόμη σύμφωνα με το νόμο 3979/2011 άρθρο 7 παράγραφο 3 «ο σχεδιασμός, η διαμόρφωση και η προμήθεια πληροφοριακών συστημάτων και υπηρεσιών ηλεκτρονικής διακυβέρνησης πρέπει να γίνεται, λαμβάνοντας υπόψη το δικαίωμα προστασίας των προσωπικών δεδομένων και την ανάγκη διαμόρφωσης των συστημάτων και υπηρεσιών κατά τρόπο ώστε να διασφαλίζεται η επεξεργασία όσο το δυνατόν λιγότερων δεδομένων προσωπικού χαρακτήρα» [34].Ο νόμος και εδώ επιβάλει τη λήψη μέτρων για τη προστασία των προσωπικών δεδομένων κατά των σχεδιασμό και τη διαμόρφωση των συστημάτων.

Εν κατακλείδι, το νομοθετικό πλαίσιο με τις παρούσες νομοθετικές διατάξεις, δεν επιβάλει τη χρήση των τεχνολογιών ενίσχυσης της ιδιωτικότητας ούτε της Privacy by Design στο σχεδιασμό και τη διαμόρφωση των συστημάτων. Παρ' όλα αυτά, οι απαιτήσεις που υπάρχουν καλύπτονται επαρκώς από την λογική και τις αρχές των προαναφερθέντων.

5.5 Δικαίωμα στη λήθη

Σε αυτή τη κοινωνία με ένα ευρύ φάσμα από νέες απειλές για των άνθρωπο, ξεχωρίζει και πρέπει να δοθεί έμφαση στο ζήτημα της διατήρησης των πληροφοριών στο διαδίκτυο, το οποίο αποτελεί συνδυασμό μιας τεράστιας ικανότητας αποθήκευσης, με εργαλεία όπως μηχανές αναζήτησης, προκειμένου να διευκολυνθεί η αναζήτηση και εύρεση πληροφοριών.

Το διαδίκτυο καταγράφει τα πάντα (έγγραφα, φωτογραφίες, εικόνες κ.α) και δεν ξεχνά τίποτα. Σε αυτά τα νέα περιβάλλοντα όλα τα αρχεία/εγγραφές είναι διαθέσιμα για μετάδοση, αναπροσαρμογή, ανάλυση, αποθήκευση, ανάκτηση και απεικόνιση. Κάθε ενημέρωση κατάστασης (status update), φωτογραφία στο διαδίκτυο, ακόμη και οποιαδήποτε ανάρτηση από εμάς ή για εμάς μπορεί να αποθηκευτεί για πάντα. Επίσης, κάτι πιο σημαντικό από αυτό, είναι το να διεξαχθεί αναζήτηση με συγκεκριμένο όνομα και επώνυμο στις μηχανές αναζήτησης, όπου μπορούν με ευκολία να βρουν πολλές προσωπικές πληροφορίες σχετικά με το παρελθόν αυτού του ατόμου. Τα δεδομένα μας καταγράφονται στο δίκτυο και μας «ακολουθούν» για πάντα.

Η διατήρηση του παρελθόντος, η υπενθύμιση του καθώς και ολόκληρη η διατήρηση των πληροφοριών του, μπορεί να είναι το τέλος της λήθης, καθώς επηρεάζει το παρόν και μπορεί να δημιουργήσει προβλήματα στο μέλλον. Είναι στη φύση του ανθρώπου να διαπράττει λάθη. Οι άνθρωποι αλλάζουν, εξελίσσονται, ωριμάζουν, ακόμη και αντιφάσκουν μεταξύ τους κατά την πορείας της ζωής τους. Συνεπώς, σε σύγκριση με τις τεράστιες δυνατότητες των ΤΠΕ και της ψηφιακής μνήμης, το δικαίωμα στη λήθη προσπαθεί να διασφαλίσει την ιδιωτικότητα και την υπόληψη των ατόμων, αποφεύγοντας τη συνεχή καταδίωξη τους από το παρελθόν.

Αυτή η νέα πραγματικότητα ενός κόσμου που θυμάται τα πάντα και τίποτα δεν μπορεί να ξεχαστεί, έρχεται σε δυσαρμονία με την «ασταθή» ανθρώπινη μνήμη. Για το λόγο αυτό έχει προκύψει στο ευρωπαϊκό κοινό μια συζήτηση σχετικά με την ανάγκη για ρύθμιση του «δικαιώματος στη λήθη», το οποίο θα βασίζεται στα δικαιώματα της προσωπικότητας και θα περιλαμβάνει διάφορα στοιχεία όπως τα δικαιώματα στην ιδιωτική ζωή, την προστασία των δεδομένων, την ιδιωτικότητα και την αξιοπρέπεια [35].

Όπως είδαμε νωρίτερα, η Ευρωπαϊκή Επιτροπή πρότεινε την αναμόρφωση της νομοθεσίας που αφορά στην προστασία των προσωπικών δεδομένων των πολιτών στην Ευρωπαϊκή Ένωση. Η πρόταση της Ευρωπαϊκής Επιτροπής περιλάμβανε τη δημιουργία ένας νέου κανόνα Ιδιωτικότητας, το «δικαίωμα στη λήθη».

Το άρθρο 17 στην «πρόταση για Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» προβλέπει το δικαίωμα του υποκειμένου των δεδομένων στη λήθη και τη διαγραφή.

Κάθε πρόσωπο πρέπει να έχει το δικαίωμα να έχει τα δεδομένα προσωπικού χαρακτήρα διορθωμένα, ενημερωμένα και να έχει και το «δικαίωμα στη λήθη» σε όποια περίπτωση η διατήρηση των δεδομένων αυτών δεν είναι σύμφωνη με τον παρόντα κανονισμό. Ειδικότερα, τα υποκείμενα των δεδομένων θα πρέπει να έχουν το δικαίωμα τα προσωπικά τους δεδομένα να διαγράφονται και να μην είναι πλέον υπό επεξεργασία, σε περιπτώσεις που τα δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχτηκαν. Επίσης, αν τα υποκείμενα των δεδομένων έχουν αποσύρει τη συγκατάθεσή τους για επεξεργασία, αν υπάρχουν αντιρρήσεις για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που τους αφορούν ή αν η επεξεργασία των προσωπικών τους δεδομένων με άλλο τρόπο δεν συμμορφώνεται με τον κανονισμό, πρέπει να έχουν το δικαίωμα διαγραφής των δεδομένων αυτών.

Οι Ευρωπαϊκές ρυθμιστικές αρχές θεωρούν ότι οι πολίτες αντιμετωπίζουν τη δυσκολία διαφυγής από το παρελθόν τους τώρα που το διαδίκτυο καταγράφει τα πάντα και τίποτα δεν διαγράφεται. Το «δικαίωμα στη λήθη» έρχεται να αντιμετωπίσει αυτό το σημαντικό πρόβλημα της ψηφιακής εποχής, τη στιγμή που

οποιαδήποτε πληροφορία καταγράφεται και αποθηκεύεται για πάντα στο νέφος (cloud) [36].

Σύμφωνα με «το δικαίωμα στη λήθη», όταν δεν επιθυμείται πλέον από κάποιον η επεξεργασία των δεδομένων του και εφόσον δεν συντρέχουν νομικοί λόγοι για τη διατήρησή τους, τα δεδομένα πρέπει να διαγράφονται. Οι κανόνες έχουν ως στόχο την ενίσχυση των δικαιωμάτων των ατόμων και όχι τη διαγραφή γεγονότων του παρελθόντος ή τον περιορισμό της ελευθερίας του Τύπου [37].

6

Επίλογος

Σε μια παγκόσμια δικτυωμένη κοινωνία όπου υπάρχουν συνεχείς τεχνολογικές εξελίξεις, το πρόβλημα της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας γίνεται ολοένα και πιο έντονο. Οι ηλεκτρονικές επικοινωνίες, από μια οπτική γωνία βελτιώνουν τη ζωή μας με την παροχή ενός μεγάλου εύρους υπηρεσιών και από μια άλλη οπτική θέτουν σε κίνδυνο τη προσωπική ζωή των χρηστών, αποκαλύπτοντας λεπτομέρειες που σχετίζονται με τα δεδομένα τους.

Σε αυτό το νέο περιβάλλον πληροφορίας, η τεχνολογία που το δημιουργεί μπορεί να συμβάλει καθοριστικά και στην παράλληλη προστασία και ασφάλεια της ιδιωτικότητας. Ένα πρόβλημα το οποίο δεν μπορεί να επιλυθεί με τεχνολογικά μέσα είναι η προστασία του χρήστη από πιθανή κατάχρηση των δεδομένων του αφού αυτά φτάσουν στη κατοχή κάποιου τρίτου. Έτσι λοιπόν, αν και η τεχνολογία ελαχιστοποιεί ή πολλές φορές αποφεύγει την αποκάλυψη δεδομένων, δεν μπορεί να τα προστατέψει από τη στιγμή που αυτά θα αποκαλυφθούν σε άλλους και κατ' επέκταση να αποθηκευτούν στη βάση δεδομένων τους.

Με την αναγνώριση της αξίας της πληροφορίας και της γνώσης που μπορεί να αντληθεί από την επεξεργασία της, είναι βασικό ζητούμενο η προστασία των προσωπικών δεδομένων από τη συλλογή και την επεξεργασία. Για να επιτευχθεί η προστασία των δεδομένων απαιτείται εναρμονισμένη προσπάθεια από τις εποπτικές αρχές, την εκπαίδευση, την έρευνα, τη βιομηχανία ανάπτυξης προϊόντων και υπηρεσιών, τους οργανισμούς τυποποίησης, τους υπευθύνους επεξεργασίας αλλά και τα άτομα στα οποία αφορούν τα δεδομένα.

Στα πλαίσια της παρούσας διπλωματικής εργασίας αναπτύχθηκε η έννοια της Privacy by design και η προσπάθεια εισαγωγής της στο Διεθνές νομοθετικό πλαίσιο, στην Πρόταση του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία δεδομένων. Επίσης, έγινε αναφορά στις τροποποιήσεις που έγιναν στις οδηγίες της Ευρωπαϊκής Ένωσης αλλά και των Ελληνικών νομοθετικών διατάξεων για να μπορέσουν να καλυφτούν οι νέες απατήσεις που θέτει η τεχνολογία. Όμως,

και πάλι δημιουργούνται κάποια ερωτήματα στα οποία δε δίνεται ικανοποιητική απάντηση. Τελικά το νομοθετικό πλαίσιο μπορεί να συμβαδίζει με τις τεχνολογικές εξελίξεις ή απλά προσαρμόζετε σε αυτές; Ποιές είναι οι αρχές που πρέπει να ενσωματωθούν στην τεχνολογία και κατά πόσο αυτές θα είναι αποτελεσματικές; Θα μπορέσει η Privacy by Design να εξασφαλίσει την προστασία που χρειάζεται ένα σύστημα; Και αν ναι, για πόσο;

Το πρόβλημα της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων με την πάροδο του χρόνου θα αρχίσει να γίνετε όλο και πιο έντονο, με τη συνεχή αύξηση των ευφυών συσκευών, των συσκευών παρακολούθησης κ.α. Για αυτό το λόγο, τα νομικά και τεχνικά μέσα θα πρέπει να τυγχάνουν συνεχούς ενημέρωσης προκειμένου να επιτευχθεί η διαφύλαξη της ιδιωτικότητας και η προστασία των δεδομένων προσωπικού χαρακτήρα.

Βιβλιογραφία

[1] https://security.berkeley.edu/fipps?destination=node/324

[2] "Bridging the gap Between PRIVACY AND DESIGN", *Deirdre K. Mulligan*

[3] "The Right to Privacy", Warren and Brandeis, 15 December 1890

http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[4] "Science, Privacy, and Freedom: Issues and Proposals", Alan Westin, Columbia University, June 1966

[5] "Privacy", Ruth Gavison, 89 YALE L.J.

[6] "Individual & Group Privacy", Edward J. Bloustein,1978

[7] «PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice», GLOBAL INTERNET LIBERTY CAMPAIGN

http://gilc.org/privacy/survey/intro.html

[8] "Ενότητα V: Προστασία Προσωπικών Δεδομένων", Λ. Μήτρου

[9]http://el.wikipedia.org/wiki/%CE%A0%CF%81%CE%BF%CF%83%CF%89%CF%80%CE%B9%CE%BA%CE%AC_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1#.CE.A5.CF.80.CE.BF.CE.BA.CE.B5.CE.AF.CE.BC.CE.B5.CE.BD.CE.BF_.CF.84.CF.89.CE.BD_.CE.B4.CE.B5.CE.B4.CE.BF.CE.BC.CE.AD.CE.BD.CF.89.CE.BD

[10] http://www.greeklaws.com/pubs/uploads/596.pdf

[11] "Προστασία Προσωπικών Δεδομένων σε «Έξυπνα» Περιβάλλοντα", Ιάκωβος Στ. Βενιέρης, Ιούλιος 2007

[12] Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection, Ann Cavoukian, 2011

[13] "Privacy by design: delivering the promises", Peter Hustinx, January 2010

[14]http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/pdb_report_html/PBD_PETS_PAPER.ashx

[15] http://el.wikipedia.org/wiki/Tor

[16] www.privacybydesign.ca

[17] "Privacy by design", Information Commissioner's Office

[18]http://el.wikipedia.org/wiki/%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%AF%CE%B1_%CF%84%CE%B7%CF%82_%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%AF%CE%B1%CF%82]

[19] (ΑΥΤΟΡ)ΡΥΘΜΙΣΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ, ΛΙΛΙΑΝ ΜΗΤΡΟΥ ,Αθήνα 2005

[20] "Self Regulation in Cyberspace", Emily M. Weitzenböck, February 2012

[21] "Δίκαιο της Πληροφορίας – 2 Προστασία Προσωπικών Δεδομένων", Λ. Μήτρου

[22] Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα.

http://eur-law.eu/EL/Odegia-97-66-EK-Europaikou-Koinobouliou-Sumbouliou-tes,322993,d

[23] Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF

[24] Οδηγία 95/46/ΕΚ Ευρωπαϊκού Κοινοβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

[25]http://europa.eu/legislation_summaries/information_society/data_protection/l14012_el.htm

[26] Νόμος 2472 του 1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

http://www.nis.gr/npimages/docs/2472-1997.pdf

[27] Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

http://www.elinyae.gr/el/lib_file_upload/133a_06.1152699607927.pdf

[28] Νομός 3917/2011 Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις

http://www.elinyae.gr/el/item_details.jsp?item_id=8862&cat_id=179

[29] ΝΟΜΟΣ 3471/2006 (ΦΕΚ 133/Α'/28.6.2006). Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/%CE%9DOMOTHESIA%20PROSOPIKA%20DEDOMENA_GREEK/3471_06_MAY2012 FINAL.PDF

[30]http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_el.pdf

[31] "Protecting Consumer Privacy in an Era of Rapid Change",FTC Staff Report, December 2010

http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[32] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

[33] **ΝΟΜΟΣ 3471/2006 - ΦΕΚ 133/Α'/28.6.2006** Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

http://www.dsanet.gr/Epikairothta/Nomothesia/n3471_06.htm

[34] ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3979Για την ηλεκτρονική διακυβέρνησηκαι λοιπές διατάξεις.

http://www.ydmed.gov.gr/wp-content/uploads/20110616_FekA138_3979_2011.pdf

[35] "The right to be forgotten under European Law: a Constitutional debate", Pere Simón Castellano, Winter 2012

[36] http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

[37]http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_el.pdf

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΕΚ Ευρωπαϊκό Κοινοβούλιο

ΤΠΕ Τεχνολογίες της Πληροφορικής και Επικοινωνιών

EDPB European Data Protection Board

FTC Federal Trade Commission

FIPPs Fair Information Practice Principles

FIPS Federal Information Processing Standard

HTTP HyperText Transfer Protocol

IT Information technology

PbD Privacy by Design

PETs Privacy Enhancing Technologies

SSL Secure Sockets Layer