ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τίτλος Εργασίας: Γενικός Κανονισμός προστασίας δεδομένων και κοινωνικά δίκτυα

Ονοματεπώνυμο: Καλοδάνης Γεώργιος

Αθήνα 2017

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ: ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗ

ΚΑΤΕΥΘΥΝΣΗ: ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Τριμελής Εξεταστική Επιτροπή

Επιβλέπουσα Καθηγήτρια: Μήτρου Ευαγγελία

Β’ Καθηγήτρια: Νικολαΐδη Μαρία

Γ’ Καθηγήτρια: Βασιλοπούλου Κωνσταντίνα

Ο Καλοδάνης Γεώργιος

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Περίληψη

Η ιδιωτικότητα των ατόμων και ο σεβασμός των προσωπικών τους δεδομένων αποτελούν βασικά δικαιώματα των ανθρώπων σύμφωνα με διεθνείς συμβάσεις και διακηρύξεις του ΟΗΕ και του ΟΑΣΑ. Η έρευνα παρουσιάζει τους κινδύνους που ελλοχεύει το διαδίκτυο για τους χρήστες του, καθώς επίσης και τα σύγχρονα επιχειρηματικά μοντέλα που βασίζονται στη συλλογή και στην επεξεργασία μεγάλου όγκου προσωπικών δεδομένων των χρηστών στο διαδίκτυο. Επίσης, παρουσιάζονται οι κίνδυνοι που εγκυμονεί η παραβίαση της ιδιωτικότητας των ατόμων, καθώς επίσης και επιχειρήματα υπέρ και κατά της προστασίας των προσωπικών δεδομένων των ατόμων με γνώμονα την προστασία του δημοσίου συμφέροντος.

Κατόπιν, παρουσιάζονται διεθνείς προσπάθειες και νομοθετικές προτάσεις – παρεμβάσεις με σκοπό την προστασία των δικαιωμάτων των ατόμων εκ μέρους διεθνών οργανισμών και της Ευρωπαϊκής Ένωσης. Στη συνέχεια παρουσιάζονται συνοπτικά η οδηγία 95/46/ΕΚ της Ευρωπαϊκής Ένωσης και οι εθνικές διατάξεις με σκοπό την προστασία των προσωπικών δεδομένων των ατόμων, ακολουθούμενα από την παρουσίαση του καινούργιου Κανονισμού (2016/679) της Ένωσης με σκοπό την εναρμόνιση των πρακτικών διαχείρισης προσωπικών δεδομένων με τις σύγχρονες εξελίξεις στο χώρο της τεχνολογίας και την αποτελεσματικότερη προστασία των προσωπικών δεδομένων των κατοίκων της Ένωσης.

Η παρούσα μελέτη πραγματεύεται τις αλλαγές των δικαιωμάτων των κατοίκων της Ένωσης στον τομέα προστασίας των προσωπικών τους δεδομένων. Επίσης, η έρευνα εξετάζει τις αλλαγές σχετικά με τις απαιτήσεις εκ μέρους των οργανισμών που συλλέγουν και επεξεργάζονται δεδομένα στο διαδίκτυο και τις υποχρεώσεις τους απέναντι στην πολιτεία και απέναντι στα άτομα από τα οποία συλλέγονται τα δεδομένα. Επιπροσθέτως, παρουσιάζονται οι διατάξεις με σκοπό την ενοποίηση των σχετικών διαδικασιών μεταξύ των κρατών μελών και την καθιέρωση ομοιομορφίας στις διαδικασίες διαχείρισης προσωπικών δεδομένων για τους κατοίκους της Ένωσης.

Λέξεις κλειδιά: Προσωπικά δεδομένα, Ιδιωτικότητα, Ευρωπαϊκή Ένωση, 2016/679

Abstract

The privacy of individuals and respect of their personal data are fundamental rights for all persons in accordance with international conventions and declarations by UN and OECD. This study initially presents dangers internet poses to the users and modern business e-commerce models, which are based on the collection of large volume of data regarding online users and process of relevant data. Moreover, the hazards posed by the violation of the privacy of individuals are presented, as well as arguments for and against protection of personal data of individuals by reference to the public interest.

Next, international efforts and legislative proposals that aim to protect relevant rights of persons by international organizations and the European Union are presented. Then, current Directive 95/46/EU of European Union and national rules in Greece for the protection of personal data of individuals are outlined. Next, is presented the new General Regulation (2016/679) of the Union in order to harmonize practices of personal data management with current evolution in technology and to effectively protect personal data of EU residents.

Current study deals with the changes of the rights of individuals in the area of protection of their personal data. The survey also examines the changes to the requirements by organizations that collect and process personal data on the internet, their obligations towards the state and towards people from which data is collected. In addition, parts of the Regulation are presented in order to consolidate the procedures between Member States and establishing uniformity in the personal data management procedures of residents in the Union.

Keywords: Personal data, Privacy, European Union, 2016/679

ΛΙΣΤΑ ΣΧΗΜΑΤΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

Κεφάλαιο 1: Εισαγωγή

1.1 Αντικείμενο έρευνας

Το διαδίκτυο είναι διαθέσιμο στους ανθρώπους από τις αρχές της δεκαετίας του 1960 και σύντομα αποτέλεσε βασικό μέσο επικοινωνίας μεταξύ των ανθρώπων σε όλο τον κόσμο [1]. Για τους περισσότερους ανθρώπους το διαδίκτυο έχει επηρεάσει την καθημερινή ρουτίνα ζωής, τις μορφές επικοινωνίας με γνωστά ή άγνωστα πρόσωπα, την οικογενειακή ζωή και πλέον χρησιμοποιείται ως το κυρίαρχο εργαλείο αναζήτησης και επεξεργασίας δεδομένων - πληροφοριών. Το διαδίκτυο έχει απλοποιήσει την πρόσβαση σε δεδομένα - πληροφορίες και παρέχει χρήσιμα εργαλεία για την εκπαίδευση, τη βιομηχανία, την υγεία, την επικοινωνία, την ψυχαγωγία, τη μεταφορά και άλλους συναφείς τομείς [2].

Ωστόσο, η μη προσεκτική χρήση του διαδικτύου συνοδεύεται από αρκετούς κινδύνους για τους χρήστες, μεταξύ των οποίων από τους πιο σημαντικούς είναι η ιδιωτικότητα των χρηστών και η παραβίαση των προσωπικών τους δεδομένων. Επιπροσθέτως, στις μέρες μας έχουν αναπτυχτεί ειδικά επιχειρηματικά μοντέλα (μοντέλο παρακολούθησης χρηστών – surveillance model) στο διαδίκτυο, τα οποία βασίζουν το κέρδος των αντίστοιχων επιχειρήσεων στη συγκέντρωση και στην επεξεργασία των προσωπικών δεδομένων των χρηστών διαδικτύου. Όσο πιο ευρεία είναι η συλλογή και η ανάλυση των προσωπικών δεδομένων, τόσο αποτελεσματικότερη είναι η σκιαγράφηση του προφίλ των χρηστών διαδικτύου και η προβολή στοχευόμενων διαφημίσεων προς εκείνους. Επίσης, συχνά προσωπικά δεδομένα χρηστών ή τα αποτελέσματα της επεξεργασίας προσωπικών δεδομένων ομάδας χρηστών αποτελούν αντικείμενο αγοραπωλησίας μεταξύ επιχειρήσεων.

Η σχετική επιτήρηση των χρηστών στο διαδίκτυο απειλεί τα ατομικά δικαιώματα των ανθρώπων - συμπεριλαμβανομένης της προστασίας της ιδιωτικής ζωής και της ελευθερίας της έκφρασης και του συνεταιρίζεσθαι - και αναστέλλει την ελεύθερη λειτουργία μιας ζωντανής κοινωνίας πολιτών σύμφωνα με την Ναβί Πιλάι - Ύπατη Αρμοστή του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) για τα Ανθρώπινα Δικαιώματα. Επιπροσθέτως, όπως προσθέτει, "καθένας έχει το δικαίωμα προστασίας από το νόμο έναντι τέτοιων πρακτικών" και υπάρχει "διεθνής καθολική αναγνώριση της θεμελιώδους σημασίας του δικαιώματος στην ιδιωτική ζωή και την ανάγκη να διασφαλιστεί το αντίστοιχο δικαίωμα νομοθετικά και πρακτικά" [3].

Για την προστασία της προσωπικής ζωής των ατόμων έχουν ψηφιστεί κατά καιρούς διάφορες διεθνείς συμβάσεις με βασικότερες για την Ευρώπη: (i) η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (1950), (ii) το Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (1975) από τον ΟΗΕ, (iii) κατευθυντήριες αρχές (1980) εκ μέρους του ΟΑΣΑ σε θέματα επεξεργασίας προσωπικών δεδομένων και ιδιωτικότητας των ατόμων, (iv) η Σύμβαση 108 (1981) εκ μέρους του Συμβουλίου της Ευρώπης για την προστασία των φυσικών προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και (v) η υπ' αριθμόν 95/46/ΕΚ οδηγία της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη με σκοπό την προστασία των προσωπικών δεδομένων των κατοίκων της Ένωσης.

Ωστόσο, καθώς η τεχνολογία εξελίσσεται και καθώς εξελίσσονται οι πρακτικές συλλογής και επεξεργασίας προσωπικών δεδομένων υπάρχει απαίτηση ενημέρωσης της σχετικής νομοθεσίας για την αποτελεσματικότερη προάσπιση των ατόμων. Για τον σκοπό αυτό ψηφίστηκε πρόσφατα καινούργιος Κανονισμός στην Ευρωπαϊκή Ένωση που υποκαθιστά την πρότερη οδηγία 95/46/ΕΚ της Ένωσης. Ο καινούργιος Κανονισμός (2016/679) της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των προσωπικών δεδομένων των ατόμων αποτελεί το βασικό αντικείμενο της παρούσας έρευνας.

1.2 Σκοπός έρευνας

Σκοπός της εργασίας είναι η μελέτη του καινούργιου Κανονισμού της Ευρωπαϊκής Ένωσης (General Data Protection Regulation – GDPR), ο οποίος θα εφαρμοστεί αυτοδικαίως σε όλα τα κράτη μέλη της Ένωσης από τις 25 Μαΐου 2018. Πιο συγκεκριμένα σκοπός της εργασίας είναι να προσδιορίσει: (i) το πεδίο εφαρμογής του νέου Κανονισμού, (ii) τις αλλαγές που θα επιφέρει ο νέος Κανονισμός στη διαχείριση των προσωπικών δεδομένων των πολιτών της Ένωσης και (iii) στη διασυνοριακή μεταφορά τους. Επίσης, σκοπός της έρευνας είναι η σύγκριση του καινούργιου Κανονισμού με την οδηγία 95/46/ΕΚ της Ένωσης σε θέματα: (i) αποτελεσματικής προστασίας των προσωπικών δεδομένων των ατόμων και (ii) των απαιτήσεων - προϋποθέσεων που τίθενται στους οργανισμούς που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα κατοίκων της Ένωσης. Τέλος, σκοπός της έρευνας είναι να εξετάσει αν ο καινούργιος Κανονισμός ενισχύει την επιχειρηματική δραστηριότητα στο διαδίκτυο εντός της Ευρωπαϊκής Ένωσης ή αν θέτει επιπρόσθετους φραγμούς στην επιχειρηματικότητα μέσω διαδικτύου.

1.3 Δομή έρευνας

Στο παρόν (1^{ο}) κεφάλαιο παρουσιάζονται το αντικείμενο της παρούσας μελέτης, ο σκοπός της παρούσας έρευνας και η δομή της εργασίας.

Στη συνέχεια στο δεύτερο (2^{ο}) κεφάλαιο παρουσιάζονται τα οφέλη και οι κίνδυνοι από τη χρήση του διαδικτύου, καθώς επίσης και ο βαθμός διείσδυσης του διαδικτύου στις διάφορες χώρες του πλανήτη. Στο ίδιο κεφάλαιο παρουσιάζονται τα επιχειρηματικά μοντέλα που εφαρμόζονται στο χώρο του διαδικτύου, καθώς επίσης και καινούργια σχετικά επιχειρηματικά μοντέλα που απειλούν την ιδιωτικότητα των χρηστών στο διαδίκτυο.

Κατόπιν, στο τρίτο (3ο) κεφάλαιο αναλύεται η έννοια της ιδιωτικότητας των ατόμων, σχετικά προβλήματα που έχουν προκύψει από τη διάδοση του διαδικτύου και από πρακτικές εταιριών που δραστηριοποιούνται στο διαδίκτυο, καθώς επίσης και γνώμες υπέρ και κατά της υπέρμετρης προστασίας της ιδιωτικότητας των ατόμων εκ μέρους της Πολιτείας. Επίσης, στο ίδιο κεφάλαιο ορίζεται η έννοια των δεδομένων προσωπικού χαρακτήρα και των ευαίσθητων προσωπικών δεδομένων, καθώς επίσης και κινδύνων σχετικά με τη συλλογή, την επεξεργασία και τη διαχείριση ευαίσθητων δεδομένων στο διαδίκτυο.

Στη συνέχεια, στο τέταρτο (4ο) κεφάλαιο παρουσιάζονται διεθνείς συμβάσεις, αποφάσεις και συστάσεις προς τα κράτη σχετικά με την προστασία της ιδιωτικότητας των ατόμων. Επίσης, στο ίδιο κεφάλαιο παρουσιάζονται σχετικές αποφάσεις και συστάσεις της Ευρωπαϊκής Ένωσης με σκοπό την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων, καθώς και το ισχύων νομικό πλαίσιο στην Ελλάδα σχετικά με την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων.

Στο πέμπτο (5ο) κεφάλαιο παρουσιάζεται ο νέος σχετικός Κανονισμός της Ευρωπαϊκής Ένωσης που θα τεθεί σε εφαρμογή από τις 28 Μαΐου 2018 σε όλα τα κράτη μέλη της Ένωσης. Παρουσιάζεται το πεδίο εφαρμογής του νέου Κανονισμού, οι θεσμοθετούμενες βασικές αρχές επεξεργασίας προσωπικών δεδομένων, τα δικαιώματα των υποκειμένων των δεδομένων, οι υποχρεώσεις των υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία δεδομένων, θέματα σχετικά με τη διασυνοριακή μεταφορά δεδομένων καθώς και τις κυρώσεις που προβλέπονται από τον νέο Κανονισμό. Επιπροσθέτως, συγκρίνονται οι σχετικές διατάξεις του Κανονισμού 2016/679 με ότι ίσχυε μέχρι σήμερα στην Ευρωπαϊκή Ένωση, σύμφωνα με όσα ορίζονται στην οδηγία 95/46/ΕΚ.

Τέλος, στο έκτο (6ο) κεφάλαιο παρουσιάζονται τα συμπεράσματα της παρούσας μελέτης, πιθανοί περιορισμοί της έρευνας, καθώς επίσης και προτάσεις για πιθανές μελλοντικές έρευνες.

Κεφάλαιο 2: Διαδίκτυο και επιχειρηματικότητα

2.1 Το Διαδίκτυο

2.1.1 Τι είναι

Το διαδίκτυο αποτελεί ίσως το σημαντικότερο επίτευγμα - καινοτομία στον τομέα της επικοινωνίας σε ολόκληρη την ιστορία της ανθρωπότητας και αποτελεί ένα μέσο που επιτρέπει τη διασύνδεση των χρηστών σε ολόκληρο τον κόσμο. Οι άνθρωποι το χρησιμοποιούν ως μέσο για τη σύνδεση με άλλους ανθρώπους, για κοινή χρήση αρχείων, για ψυχαγωγία, για ενημέρωση και πολλές άλλες δραστηριότητες που είναι χρήσιμες και ωφέλιμες για τους χρήστες.

Στα τέλη της δεκαετίας του 1960 το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών διεξήγαγε ένα πειραματικό σχέδιο δικτύωσης ευρείας περιοχής που ονομάστηκε ARPANET (Advanced Research Projects Agency Network). Το 1969, η πρώτη εκδοχή του δικτύου ARPANET συνδέθηκε με υπολογιστή του Πανεπιστημίου της Καλιφόρνιας UCLA και μέχρι το τέλος του ίδιου έτους, άλλα τρία πανεπιστήμια είχαν συνδεθεί στο δίκτυο ARPANET. Τα σχετικά υπολογιστικά συστήματα είχαν διαφορετικά λειτουργικά συστήματα, ωστόσο ήταν σε θέση να επικοινωνούν μεταξύ τους. Με την πάροδο του χρόνου και άλλα ερευνητικά ιδρύματα, εργαστήρια και πανεπιστήμια συνδέθηκαν στο δίκτυο ARPANET [4]. Αργότερα στη δεκαετία του 1990 το δίκτυο ARPANET κατέστη διαθέσιμο στους πολίτες και δεν είχε πλέον τον έλεγχο της κυβέρνησης των Ηνωμένων Πολιτειών [5]. Η μετέπειτα μείωση των τιμών των υπολογιστών και του κόστους σύνδεσης στο διαδίκτυο οδήγησαν στην ραγδαία εξάπλωσή του.

Το διαδίκτυο αποτελεί ένα παγκόσμιο δίκτυο υπολογιστών, στο οποίο μπορεί ένας χρήστης να έχει πρόσβαση μέσω ενός υπολογιστή, κινητού τηλεφώνου, παιχνιδομηχανής ή ψηφιακής τηλεόρασης [6], ενώ αποτελεί ένα παγκόσμιο σύστημα δικτύων υπολογιστών - ένα δίκτυο πολλών δικτύων στο οποίο οι χρήστες από οποιοδήποτε υπολογιστή μπορούν, αν έχουν άδεια, να λάβουν πληροφορίες από κάθε άλλο υπολογιστή συνδεμένο στο δίκτυο των δικτύων (και μερικές φορές να μιλήσουν απευθείας με χρήστες που χρησιμοποιούν άλλους υπολογιστές).

Για τη λειτουργία του διαδικτύου δεν απαιτείται κάποιο κεντρικό κυβερνητικό σώμα, καθώς το ίδιο αποτελεί δίκτυο εθελοντικά διασυνδεδεμένων αυτόνομων δικτύων και η ιδιοκτησία του δεν ανήκει σε κανέναν.

2.1.2 Οφέλη διαδικτύου

Η **ευρεία διάθεση πληροφοριών** είναι ίσως το μεγαλύτερο πλεονέκτημα που προσφέρει το διαδίκτυο. Οποιοδήποτε είδος πληροφορίας σχετικά με οποιοδήποτε θέμα είναι διαθέσιμο μέσω του διαδικτύου. Με τη χρήση μηχανών αναζήτησης, όπως το Google ή το MSN, ο χρήστης μπορεί άμεσα και με ευκολία να εντοπίσει τα δεδομένα ή τις πληροφορίες που αναζητεί [7]. Ενδεικτικές σχετικές πληροφορίες αποτελούν ο εντοπισμός της ισχύουσας νομοθεσίας σε διάφορα θέματα, πληροφορίες για εμπορικές εκθέσεις και συνέδρια, πληροφορίες σχετικά με την αγορά, σχετικά με νέες καινοτομίες στην αγορά και σχετικής τεχνικής υποστήριξης, ακόμη και παροχή συμβουλών για την αγάπη και τις προσωπικές σχέσεις των ατόμων.

Παράλληλα με την ευρεία διάθεση πληροφοριών, το διαδίκτυο έχει διευκολύνει την επέκταση και κατάκτηση **γνώσης** εκ μέρους των ανθρώπων. Πληθώρα βιβλίων, άρθρων, πρακτικών συνεδρίων, ερευνητικές εργασίες και ακαδημαϊκές μελέτες είναι διαθέσιμες δωρεάν στους χρήστες [7].

Επιπροσθέτως, το διαδίκτυο προσφέρει μερικά από τα πιο αποτελεσματικά μέσα **επικοινωνίας** στους ανθρώπους. Τα μηνύματα ηλεκτρονικού ταχυδρομείου (email) και οι ομάδες μηνυμάτων μέσω διαδικτύου (chat) διευκολύνουν την άμεση επικοινωνία των ατόμων. Η κοινωνική δικτύωση και τα φόρουμ συζήτησης αποτελούν δημοφιλείς πλατφόρμες έκφρασης των ατόμων, ενώ άμεσα με την υποστήριξη του διαδικτύου οι άνθρωποι μπορούν να ανταλλάξουν απόψεις, να μοιραστούν πληροφορίες και να συνεργαστούν μεταξύ τους. Το διαδίκτυο έχει φέρει τους ανθρώπους πιο κοντά και έχει καταστήσει διαθέσιμες νέες μορφές επικοινωνίας σε απομακρυσμένες περιοχές [8].

Ακόμη, το διαδίκτυο αποτελεί σημαντικό εργαλείο **ψυχαγωγίας** των ανθρώπων της σύγχρονης εποχής. Ένας χρήστης μπορεί εύκολα και άμεσα μέσω του διαδικτύου να έχει πρόσβαση σε τραγούδια, ταινίες, καθώς επίσης και επεισόδια τηλεοπτικών εκπομπών [8]. Επίσης, υπάρχουν αμέτρητα ηλεκτρονικά παιχνίδια που μπορούν να εγκαταστήσουν οι χρήστες μέσω του διαδικτύου, δωρεάν ή με κάποια μικρή χρέωση.

Το διαδίκτυο έχει **διευκολύνει την καθημερινή ζωή** των ανθρώπων, παρέχοντας διάφορες υπηρεσίες στους χρήστες του. Σχετικές ενδεικτικές υπηρεσίες αποτελούν η ηλεκτρονική τράπεζα, υπηρεσίες αγοράς αεροπορικών εισιτηρίων, υπηρεσίες κράτησης δωματίων σε ξενοδοχεία, υπηρεσίες αυτοματοποιημένων μεταφράσεων κειμένου, υπηρεσίες ενημέρωσης συναλλαγματικών ισοτιμιών, υπηρεσίες μετεωρολογικών προβλέψεων και άλλες.

Μέσω του διαδικτύου οι χρήστες μπορούν να πραγματοποιήσουν αγορές προϊόντων ή υπηρεσιών **24 ώρες το 24ωρο** κάθε μέρα εύκολα από το σπίτι τους, χωρίς την ανάγκη φυσικής μετάβασής τους στα σχετικά καταστήματα. Οι αγορές μέσω διαδικτύου συνήθως (i) εξοικονομούν χρήματα για τους χρήστες, (ii) επιτρέπουν την άμεση αγορά προϊόντων από άλλα κράτη, (iii) την άμεση σύγκριση τιμών, καθώς επίσης και (iv) την πρόσβαση σε αξιολογήσεις προϊόντων από άλλους καταναλωτές, οδηγώντας σε σημαντική αύξηση της **αγοραστικής δύναμης των καταναλωτών**.

Τέλος, το διαδίκτυο προσφέρει σημαντικές **επιχειρηματικές ευκαιρίες** σε εταιρίες, επιτρέποντας την ευκολία πρόσβασης σε μεγαλύτερο αριθμό καταναλωτών, δυνατότητα διάθεσης προς πώληση προϊόντων ή υπηρεσιών απευθείας στους καταναλωτές χωρίς μεσάζοντες, δυνατότητα δημιουργίας βάσης δεδομένων με τις προτιμήσεις των πελατών με σκοπό την αύξηση της αποτελεσματικότητας μελλοντικών στρατηγικών προώθησης προϊόντων και γενικότερα τη **διασύνδεσή** της με τους καταναλωτές.

2.1.3 Κίνδυνοι διαδικτύου

Οι πληροφορίες που παρέχονται στο διαδίκτυο **δεν είναι πάντα αξιόπιστες**. Για παράδειγμα ο ιστότοπος Wikipedia χρησιμοποιείται ευρέως από τους χρήστες στο διαδίκτυο, χωρίς κατά ανάγκη οι σχετικές πληροφορίες να είναι ακριβείς ή πραγματικές. Καθένας με σχετικές γνώσεις δημοσίευσης πληροφοριών στο διαδίκτυο και κατοχή ενός διακομιστή (server) μπορεί να δημοσιεύσει οποιαδήποτε πληροφορία επιθυμεί στο διαδίκτυο, καθώς δεν υπάρχει κανένας έλεγχος εγκυρότητας - ποιότητας πριν τη δημοσίευσή τους στο διαδίκτυο.

Επίσης, το διαδίκτυο έχει κατηγορηθεί πως οδηγεί σε περιορισμό της **δημιουργικότητας** του ανθρώπου και της **κριτικής σκέψης** των ατόμων, ως αποτέλεσμα της ευκολίας πρόσβασης στην πληροφορία και ευκολίας άμεσης πρόσβασης σε προτεινόμενες λύσεις για προβλήματα ή καταστάσεις που αντιμετωπίζει κάποιος άνθρωπος. Πλέον, η εξεύρεση λύσης σε ένα πρόβλημα απαιτεί μονάχα ορισμένα κλικ στο ποντίκι του υπολογιστή, χωρίς την απαίτηση λεπτομερούς ανάλυσης των σχετικών προβλημάτων και αναζήτησης εναλλακτικών λύσεων [7].

Το διαδίκτυο δύναται επίσης να οδηγήσει τους τακτικούς του χρήστες σε απομόνωση από το υπόλοιπο κοινωνικό σύνολο και να φέρει τη **μοναξιά** στην πραγματική ζωή, παράλληλα με μια πιθανή έντονη κοινωνική παρουσία τους στο διαδικτυακό χώρο. Απόρροια της μοναξιάς που μπορεί να βιώνει ένας χρήστης που χρησιμοποιεί το

διαδίκτυο αρκετές ώρες καθημερινά είναι και η εμφάνιση άλλων **ψυχολογικών προβλημάτων** [9].

Επιπροσθέτως, το διαδίκτυο έχει αποτελέσει το μέσο εμφάνισης μιας καινούργιας μορφής εκφοβισμού, τον λεγόμενο εκφοβισμό μέσω διαδικτύου (**cyber bulling**) με ιδιαίτερα δυσάρεστες συνέπειες για τα θύματά του. Με τον όρο εκφοβισμός μέσω διαδικτύου καλείται "κάθε επιθετική πράξη ή συμπεριφορά με ηλεκτρονικά μέσα κατά μιας ορισμένης ομάδας ατόμων ή ενός μεμονωμένου άτομου κατά επανάληψη σε απευθείας σύνδεση στο διαδίκτυο" [10]. Κάθε μορφή εκφοβισμού δύναται να προκαλέσει **συναισθηματική και ψυχολογική βλάβη** στα θύματα. Ωστόσο, το φαινόμενο αυτό μεγενθύνεται με τον ψηφιακό εκφοβισμό, καθώς ο εκφοβισμός μέσω διαδικτύου προσφέρει ανωνυμία που αφαιρεί φυσικούς φραγμούς και έλεγχο του μεγέθους εκδήλωσης συμπεριφορών εκφοβισμού και του βαθμού επανάληψής τους [11]. Ενδεικτικές συνέπειες του εκφοβισμού μέσω διαδικτύου είναι η ανάπτυξη συναισθημάτων απογοήτευσης, ο θυμός και η θλίψη των θυμάτων, ενώ μπορεί να επηρεάσει άμεσα την σχολική ή ακαδημαϊκή επίδοση των θυμάτων, καθώς επίσης και τις οικογενειακές και ανθρώπινες σχέσεις συνολικά [12].

Επίσης, ένα φαινόμενο που έχει προκύψει με τη διάδοση του διαδικτύου είναι ο **εθισμός στο διαδίκτυο** (internet addiction) με δυσάρεστες επιπτώσεις για έναν εθισμένο χρήστη. Ένας χρήστης μπορεί να είναι εθισμένος σε διαφορετικές υπηρεσίες διαδικτύου: (i) διαδικτυακά ηλεκτρονικά παιχνίδια, (ii) πορνογραφικοί ιστότοποι, (iii) κοινωνικά δίκτυα, (iv) ηλεκτρονικός τζόγος και (v) υπηρεσίες διασκέδασης (παρακολούθηση ταινιών μέσω διαδικτύου). Ο εθισμός στο διαδίκτυο επηρεάζει αρνητικά τις **ανθρώπινες σχέσεις**, όπως είναι ο γάμος, οι σχέσεις γονέα – παιδιού και οι σχέσεις μεταξύ φίλων. Επίσης, ο εθισμός στο διαδίκτυο συνήθως επηρεάζει αρνητικά την απόδοση των ατόμων στην **εργασία** τους, καθώς επίσης και την ακαδημαϊκή επίδοση των νέων. Επιπροσθέτως, ο εθισμός στο διαδίκτυο βλάπτει τη σωματική και την **ψυχική υγεία** των εθισμένων χρηστών [13]. Ο λόγος που ο εθισμός στο διαδίκτυο επιφέρει τις παραπάνω συνέπειες είναι η αφαίρεση πολύτιμου χρόνου από την καθημερινή πραγματική ζωή και η χρήση του σχετικού χρόνου για άλλες δραστηριότητες στο διαδίκτυο.

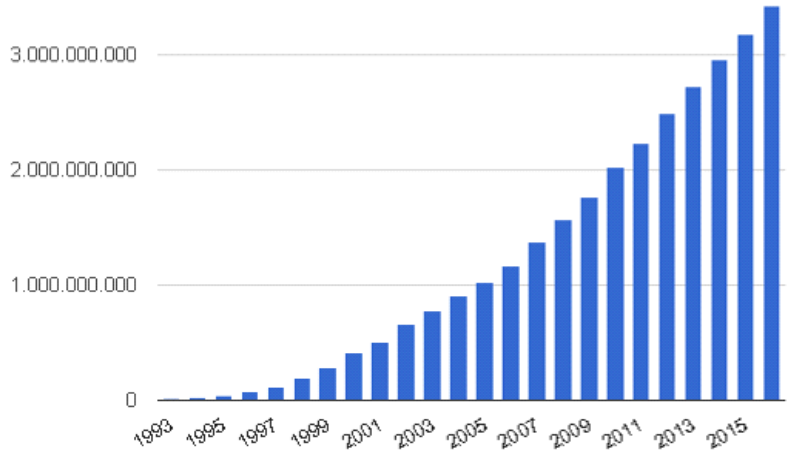
Ειδικότερα, η χρήση του διαδικτύου είναι συνδυασμένη με καθιστικό τρόπο ζωής και αυξημένο σωματικό βάρος, καθιστώντας την πολύωρη χρήση διαδικτύου αρνητικό παράγοντα για τη **σωματική υγεία** των ατόμων [14]. Επίσης, η πολύωρη χρήση του

διαδικτύου προκαλεί προβλήματα στην όραση των χρηστών, απαιτώντας τη χρήση ειδικών φακών για τον περιορισμό του προβλήματος.

Τέλος, ένα από τα πιο ενοχλητικά προβλήματα από τη χρήση του διαδικτύου είναι η ευκολία με την οποία κάποιο κακόβουλο λογισμικό μπορεί να μολύνει τους υπολογιστές των χρηστών. Οι χρήστες του διαδικτύου συχνά δέχονται επιθέσεις **ιών** που βλάπτουν τους υπολογιστές και σημαντικά αρχεία δεδομένων.

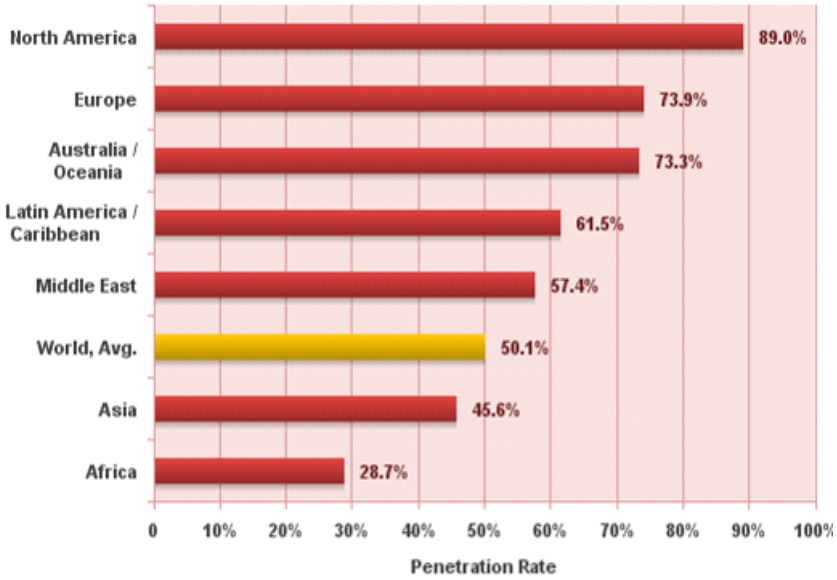
2.1.4 Διείσδυση διαδικτύου

Ο αριθμός των ενεργών χρηστών διαδικτύου πλησιάζει το 50% του παγκόσμιου πληθυσμού (46.8%), με εκτιμώμενο αριθμό χρηστών σε παγκόσμιο επίπεδο ίσο με 3,424,971,237 χρήστες. Το παρακάτω διάγραμμα απεικονίζει την πορεία αύξησης του αριθμού χρηστών του διαδικτύου την τελευταία εικοσαετία:



Σχήμα 1: Αριθμός χρηστών διαδικτύου σε παγκόσμιο επίπεδο 1993 – 2016 [6]

Για τα αναπτυγμένα κράτη το σχετικό ποσοστό διείσδυσης είναι αρκετά μεγαλύτερο. Οι τρεις ήπειροι με τα μεγαλύτερα ποσοστά διείσδυσης του διαδικτύου είναι: (i) η Βόρεια Αμερική (89%), (ii) η Ευρώπη (73.9%) και (iii) η Ωκεανία (73.3%). Το παρακάτω σχήμα απεικονίζει το σχετικό ποσοστό διείσδυσης του διαδικτύου στις ηπείρους του πλανήτη [15]:



Σχήμα 2: Ποσοστό διείσδυσης διαδικτύου για τις ηπείρους του πλανήτη [15]

Για την Ελλάδα ο αριθμός χρηστών (2016) διαδικτύου εκτιμάται πως βρίσκεται στο επίπεδο του 64.8% του συνολικού πληθυσμού με συνολικό αριθμό ενεργών χρηστών διαδικτύου ίσο με 7,072,534 χρήστες. Συγκριτικά με τα υπόλοιπα κράτη μέλη της Ευρωπαϊκής Ένωσης η Ελλάδα συγκαταλέγεται μεταξύ των κρατών – μελών με τα μικρότερα ποσοστά διείσδυσης. Το μεγαλύτερο ποσοστό διείσδυσης του διαδικτύου σε παγκόσμιο επίπεδο παρατηρείται στην Ισλανδία (100%), τα νησιά Φερόες (98.5%) και τη Νορβηγία (98%). Στην Ευρωπαϊκή Ένωση τα κράτη μέλη με τα μεγαλύτερα ποσοστά διείσδυσης παρουσιάζουν η Δανία (96.3%), το Λουξεμβούργο (95.2%) και η Ολλανδία (93.7%) [16].

Ειδικότερα σχετικά με τη χρήση του διαδικτύου στην Ελλάδα, σύμφωνα με έρευνα της Ελληνικής Στατιστικής Υπηρεσίας (ΕΛΣΤΑΤ), οι Έλληνες χρήστες διαδικτύου, χρησιμοποιούν κατά κύριο λόγο το διαδίκτυο για: (i) ενημερωτικούς λόγους (85.3%), (ii) αναζήτηση συνοδευτικών στοιχειών σχετικά με προϊόντα ή υπηρεσίες (81.9%), (iii) επικοινωνία (74.7%), (iv) κοινωνικά δίκτυα (67.5%), (v) παρακολούθηση βίντεο στο διαδίκτυο (59.9%) και (vi) αναζήτηση πληροφοριών σχετικά με θέματα υγείας (58.8%) [17].

2.2 Επιχειρηματικά μοντέλα στο διαδίκτυο

Η επιχειρηματική ιδέα και ο τρόπος που μια εταιρία πραγματοποιεί κέρδη στο διαδίκτυο ονομάζεται ηλεκτρονικό επιχειρηματικό μοντέλο (e-commerce business model). Τα σχετικά μοντέλα αναφέρονται στον τρόπο που μια εταιρία έχει εμπορική παρουσία στο διαδίκτυο και δημιουργεί αξία για τους χρήστες – πελάτες της. Ένα

επιχειρηματικό μοντέλο καθορίζει "από πού πληρώνεται μια εταιρία προκειμένου να αποκομίσει κέρδη" [18].

2.2.1 Παραδοσιακά επιχειρηματικά μοντέλα

Από την εμφάνιση του διαδικτύου μέχρι σήμερα έχουν εμφανιστεί διάφορα επιχειρηματικά μοντέλα ηλεκτρονικού εμπορίου που μια εταιρία μπορεί να αποφασίσει να χρησιμοποιήσει στο διαδίκτυο [19].

Ένα από τα πιο κοινά επιχειρηματικά μοντέλα ηλεκτρονικού εμπορίου είναι το μοντέλο του Χρηματιστή (**Brokerage model**). Στο σχετικό μοντέλο ο ιστότοπος λειτουργεί ως μεσίτης, παρέχοντας την πλατφόρμα για αγοραπωλησία αγαθών ή προϊόντων μεταξύ των χρηστών του ιστότοπου. Τα κέρδη για την εταιρία προκύπτουν από τη λήψη αμοιβής ή προμήθειας για κάθε συναλλαγή (π.χ. το eBay, Amazon) [19].

Ένα άλλο κοινό επιχειρηματικό μοντέλο ηλεκτρονικού εμπορίου είναι το μοντέλο του διαφημιστή (**Advertising model**). Στο σχετικό μοντέλο ο ιστότοπος παρέχει δωρεάν περιεχόμενο ή υπηρεσίες στους χρήστες σε συνδυασμό με την προβολή διαφημιστικών μηνυμάτων στους χρήστες. Τα έσοδα για τους σχετικούς δικτυακούς τόπους βασίζονται στις διαφημίσεις που εμφανίζονται στην ιστοσελίδα κατά την περιήγηση των χρηστών του (π.χ. Google) [19].

Επίσης, κοινό επιχειρηματικό μοντέλο είναι το κοινοτικό μοντέλο (**Community model**), το οποίο αναφέρεται σε διαδικτυακές κοινότητες όπως το Facebook και το Twitter. Οι κύριες πηγές εσόδων για αυτές τις ιστοσελίδες είναι οι διαφημίσεις οι οποίες εμφανίζονται κατά τη χρήση του ιστότοπου στους χρήστες [19].

Επιπλέον, υπάρχουν πολλές ιστοσελίδες που εφαρμόζουν το λεγόμενο εμπορικό επιχειρηματικό μοντέλο (**Merchant model**), αποτελώντας ιστότοπους όπου οι χρήστες μπορούν άμεσα να αγοράσουν προϊόντα ή υπηρεσίες (π.χ. Marks & Spenser) [19].

Μια άλλη επιλογή επιχειρηματικής δράσης για ένα δικτυακό τόπο είναι η κατεύθυνση των χρηστών προς την αγορά προϊόντων ή υπηρεσιών από άλλους συνεργαζόμενους ιστότοπους. Αν ο χρήστης αγοράσει προϊόντα από τον ηλεκτρονικό συνεργάτη του ιστότοπου, η συνεργαζόμενη επιχείρηση πληρώνει ένα ποσοστό των πωλήσεων στην σχετική ιστοσελίδα (π.χ. Groupon). Το σχετικό επιχειρηματικό μοντέλο ονομάζεται **Affiliate model** [19].

Ένα άλλο κοινό επιχειρηματικό μοντέλο είναι το μοντέλο συνδρομής (**Subscription model**), στο οποίο μοντέλο μια ιστοσελίδα παρέχει δωρεάν ένα υποσύνολο των

διαθέσιμων υπηρεσιών ή περιεχομένου ενός ιστότοπου και οι χρήστες πρέπει να καταβάλλουν ένα τέλος - συνδρομή για πιο εξειδικευμένο περιεχόμενο. (π.χ. Netfelix) [19].

Τέλος υπάρχουν ιστοσελίδες που αναλύουν τα δεδομένα των πελατών και τις καταναλωτικές τους συνήθειες και μεταπωλούν τα αποτελέσματα της σχετικής ανάλυσης σε διαφημιστικές εταιρίες με σκοπό την προβολή στοχευμένων διαφημίσεων. Επιπλέον, οι σχετικές ιστοσελίδες ενεργούν αρκετές φορές ως ενδιάμεσοι υποστηρικτές στους αγοραστές για την πρόταση περί αγοράς προϊόντων σύμφωνα με τις ανάγκες τους (π.χ. DoubleClick). Το σχετικό επιχειρηματικό μοντέλο καλείται **Infomediary model** [19].

Σε πολλά επιχειρηματικά μοντέλα (διαφήμιση, κοινότητα) που περιγράφονται παραπάνω, οι διαφημίσεις αποτελούν την κύρια πηγή εσόδων. Στα σχετικά επιχειρηματικά μοντέλα, το επίπεδο των εσόδων από διαφημίσεις εξαρτάται κυρίως από το επίπεδο της επισκεψιμότητας σε μια ιστοσελίδα. Κατά το έτος 2015 εκτιμάται ότι τα συνολικά έσοδα σε όλο τον κόσμο από τη διαδικτυακή διαφήμιση ήταν περίπου $150 δις και ο σχετικός αριθμός εκτιμάται πως θα φθάσει τα $260 δις το 2020 [20].

2.2.2 Καινούργια επιχειρηματικά μοντέλα

Καθώς η επιχειρηματική δραστηριότητα στο διαδίκτυο εξαρτάται σε σημαντικό βαθμό από τα έσοδα από τις διαδικτυακές διαφημίσεις, σήμερα έχουν κυριαρχήσει στην αγορά επιχειρηματικά μοντέλα που αποβλέπουν στην αύξηση της αποτελεσματικότητας προβολής στοχευμένων διαφημίσεων προς του χρήστες.

2.2.2.1 Μοντέλο παρακολούθησης χρηστών (surveillance model)

2.2.2.1.1 Τι είναι

Το μοντέλο επιτήρησης (**surveillance model**) αποτελεί ένα καινούργιο επιχειρηματικό μοντέλο στο διαδίκτυο, κατά το οποίο οι ιστότοποι προσφέρουν δωρεάν υπηρεσίες στους χρήστες και ταυτόχρονα παρακολουθούν όλες τις ενέργειες του χρήστη στο διαδίκτυο. Οι ιστότοποι που εφαρμόζουν το σχετικό επιχειρηματικό μοντέλο δημιουργούν - διατηρούν αναλυτικά στοιχεία σχετικά με τους χρήστες τους, έτσι ώστε να είναι σε θέση να δημιουργήσουν το προφίλ του καθενός, τα οποία επιτρέπουν στις σχετικές ιστοσελίδες να είναι σε θέση να προβλέψουν τι μπορεί να ενδιαφέρει τον καθέναν από τους χρήστες και να προβάλλουν στοχευμένες

διαφημίσεις για τον καθένα ξεχωριστά. Αυτές οι διαφημίσεις αντικατοπτρίζουν την κύρια πηγή εσόδων για πάρα πολλές ιστοσελίδες [21].

Ο όρος επιτήρηση των δεδομένων αναφέρεται στη "συστηματική χρήση των συστημάτων πληροφορικής με σκοπό την ανάλυση – έρευνα ή την παρακολούθηση των ενεργειών ή των επικοινωνιών ενός ή περισσότερων ατόμων" [22]. Αυτό αποτελεί το αντικείμενο επιχειρηματικής δράσης εταιριών όπως η Google, το Yahoo και το Facebook, οι οποίες προκειμένου να αυξήσουν τα κέρδη τους, παρακολουθούν τις ενέργειες των χρηστών τους με σκοπό να κατανοήσουν καλύτερα τις προτιμήσεις τους και να είναι σε θέση να προβάλλουν σε αυτούς στοχευμένες διαφημίσεις.

Πρακτικά, οι επιχειρήσεις που εφαρμόζουν το μοντέλο επιτήρησης δεν έχουν ως πελάτες τους χρήστες των σχετικών ιστότοπων, αλλά τις διαφημιστικές εταιρίες που πληρώνουν για την εμφάνιση στοχευμένων διαφημίσεων σε συγκεκριμένες ομάδες χρηστών. Όπως αναφέρει σχετικά ο Rushkoff, το προϊόν στους σχετικούς ιστότοπους δεν είναι το περιεχόμενο των ιστοσελίδων, αλλά οι ίδιοι οι χρήστες των ιστότοπων ("The product online in not the content, the product online is you!") [23].

Το 2013 η Google είχε έσοδα ύψους $15 δις και τα κέρδη του οργανισμού ήταν $3 δις. Η διαφορά μεταξύ των εσόδων και των κερδών αντικατοπτρίζει το κόστος των δωρεάν υπηρεσιών που προσφέρονται από την Google, και αποτελούν το προϊόν διάθεσης – πώλησης του οργανισμού στις διαφημιστικές εταιρίες [24].

2.2.2.1.2 Πως λειτουργεί

Οι κύριοι λόγοι που οι επιχειρήσεις εφαρμόζουν το επιχειρηματικό μοντέλο επιτήρησης και το σχετικό μοντέλο τείνει να κυριαρχήσει στους ιστότοπους είναι οι εξής: (i) οι άνθρωποι επιθυμούν να λαμβάνουν δωρεάν υπηρεσίες στο διαδίκτυο και (ii) το σχετικό μοντέλο εκτιμάται ως "βολικό (convenient)" μοντέλο στην εφαρμογή του. Εκτιμάται πως αυτό το επιχειρηματικό μοντέλο θα κυριαρχήσει στο διαδίκτυο για αρκετά χρόνια στο μέλλον [25].

Για να ενισχυθεί το μοντέλο επιτήρησης, οι ιστοσελίδες προσφέρουν υπηρεσίες υψηλής ζήτησης δωρεάν, προκειμένου να κυριαρχήσουν στην αγορά και να επιβληθούν σε κάθε εταιρία που χρησιμοποιεί άλλα επιχειρηματικά μοντέλα, όπως την πληρωμή για την παροχή εξειδικευμένων υπηρεσιών στο διαδίκτυο. Με την προσφορά δωρεάν εργαλείων αναζήτησης στο διαδίκτυο, η Google έχει καταστρέψει τη σχετική αγορά μηχανών αναζήτησης, ενώ αντίστοιχα με την προσφορά δωρεάν χαρτών στο διαδίκτυο, έχει καταστρέψει την αγορά χρήσης χαρτών επι πληρωμή.

Ομοίως, με την προσφορά δωρεάν βίντεο σε απευθείας σύνδεση, το You Tube έχει καταστρέψει την αγορά βίντεο στο διαδίκτυο [26].

Καταστρέφοντας λοιπόν αυτές τις αγορές, η Google και το YouTube έχουν εκατομμύρια χρήστες που χρησιμοποιούν τις σχετικές υπηρεσίες δωρεάν. Αυτοί οι χρήστες αποτελούν τα προϊόντα των αγορών που έχουν καθιερωθεί από τη Google, το Facebook και το YouTube και έχουν ως πελάτες τους, τις εταιρίες που θέλουν να διαφημίσουν τα προϊόντα ή τις υπηρεσίες τους σε συγκεκριμένες ομάδες - στόχους.

2.2.2.3 Πως εφαρμόζεται η παρακολούθηση

Οι περισσότερες ιστοσελίδες αποθηκεύουν πληροφορίες σχετικά με τους χρήστες τους και τις επισκέψεις τους στον δικτυακό τόπο σε αρχεία κειμένου που ονομάζονται cookies. Σ' αυτά αποθηκεύονται πληροφορίες όπως το όνομα και η θέση του υπολογιστή του χρήστη, η δραστηριότητά του στον ιστότοπο, απαντήσεις σε πιθανές δημοσκοπήσεις και γενικά οι προτιμήσεις του κατά την περιήγησή του εντός ενός δικτυακού τόπου. Οι σχετικές πληροφορίες συνήθως χρησιμοποιούνται από τις ιστοσελίδες για να προτείνουν στους χρήστες προϊόντα ή αντικείμενα σύμφωνα με τις προτιμήσεις τους ή για την προβολή στοχευμένων διαφημίσεων [27]. Παρ'όλ'αυτά, δεν μπορεί κανείς να εγγυηθεί πως οι πληροφορίες αυτές δεν θα πουληθούν σε διαφημιστικές εταιρίες ή πως δε θα χρησιμοποιηθούν για κάποιο άλλο σκοπό.

Το Facebook μπορεί εύκολα να παρακολουθεί τις προτιμήσεις των χρηστών με το κουμπί Like που βρίσκεται στις περισσότερες ιστοσελίδες στο διαδίκτυο. Με τον ίδιο ακριβώς τρόπο η Google μπορεί να παρακολουθεί τις προτιμήσεις των χρηστών με το κουμπί δήλωσης προτίμησης Google+, που βρίσκεται στις περισσότερες ιστοσελίδες σε παγκόσμιο επίπεδο [25].

Κάθε αναζήτηση ενός χρήστη σε μια μηχανή αναζήτησης για πληροφορίες σχετικά με τα φάρμακα, σχετικά με θέματας υγείας, με την υγιεινή διατροφή, με το πώς να αντιμετωπίσουν προβλήματα κατά τη διάρκεια της εφηβείας των παιδιών τους ή σχετικά με θέματα για το σεξ - επιτρέπει στον πάροχο σχετικών υπηρεσιών να δημιουργήσει μια λεπτομερή βάση δεδομένων για σχεδόν κάθε πτυχή του χαρακτήρα των χρηστών, τις προσωπικές τους προτιμήσεις, τις θρησκευτικές πεποιθήσεις, πιθανά ιατρικά προβλήματα, σεξουαλικές προτιμήσεις, προβλήματα με την ανατροφή των παιδιών, τις πολιτικές πεποιθήσεις τους και ούτω καθεξής.

Ακόμη και αν η ιστοσελίδα δεν ξέρει το όνομα των χρηστών, μπορεί να διακρίνει τον καθένα από τη διεύθυνση IP, η οποία είναι μοναδική για την τρέχουσα θέση του

χρήστη ή του υπολογιστή που χρησιμοποιείται. Στη συνέχεια, καθώς οι χρήστες χρησιμοποιούν διαθέσιμες ηλεκτρονικές υπηρεσίες, η εταιρία μπορεί να βρει τελικά τα ονόματά τους, τη διεύθυνσή τους και τον αριθμό τηλεφώνου. Όταν χρησιμοποιείται η μηχανή αναζήτησης ή οποιοδήποτε άλλο προϊόν της Google, η Google εγκαθιστά απευθείας στον υπολογιστή που χρησιμοποιείται ένα αναγνωριστικό αρχείο cookie, το οποίο επιτρέπει την παρακολούθηση των ενεργειών των χρηστών σε απευθείας σύνδεση.

Χαρακτηριστικά, η Google ξέρει ποιοι είμαστε, ποιοι είναι οι φίλοι μας, τι τρώμε και ποια είναι τα συμφέροντά μας. Κάθε κλικ στο διαδίκτυο καταγράφεται, αποθηκεύεται και μπορεί να ανακτηθεί από μια βάση δεδομένων, ώστε να αναλυθεί από τον πάροχο σχετικών υπηρεσιών. Όπως έχει αναφερθεί, στην εφημερίδα The Wall Street Journal (2010) από τον κ Eric Schmidt, πρόεδρο και διευθύνοντα σύμβουλο της Google, "γνωρίζουμε σε γενικές γραμμές τα πάντα για εσάς, ποιά τα ενδιαφέροντά σας και ποιοι είναι οι φίλοι σας" [28].

2.2.2.4 Τρόποι προστασίας

Παρά το γεγονός ότι ορισμένες ιστοσελίδες επιτρέπουν την περιήγηση στον ιστότοπο μόνο αν είναι ενεργοποιημένα τα cookies, οι χρήστες θα πρέπει να είναι ιδιαίτερα προσεκτικοί πριν την εκχώρηση δικαιωμάτων σε μια ιστοσελίδα. Όλα τα προγράμματα περιήγησης στο διαδίκτυο επιτρέπουν την απενεργοποίηση των cookies και ορισμένα προγράμματα περιήγησης στο διαδίκτυο περιλαμβάνουν κουμπί ενεργοποίησης "ιδιωτικής περιήγησης", η οποία εμποδίζει τα cookies να αποθηκευτούν στον δίσκο του υπολογιστή [29].

Επίσης, υπάρχουν διαθέσιμα εργαλεία στο διαδίκτυο για την απόκρυψη της πραγματικής διεύθυνσης IP του χρήστη ή τη συνεχή εναλλαγή της. Η χρήση σχετικών εφαρμογών από τους χρήστες, δυσκολεύουν την ταυτοποίηση των επισκέψεών τους σε έναν ιστότοπο [29].

Επίσης, συστήνεται η χρήση διαφορετικών λογαριασμών ηλεκτρονικού ταχυδρομείου και η χρήση ενός κύριου λογαριασμού με τα πραγματικά στοιχεία χρήστη μόνο από άτομα που γνωρίζει ο χρήστης. Ακόμη, για πιθανή συμμετοχή του χρήστη σε ομάδες ειδήσεων ή άλλα δημόσια φόρουμ ή κοινωνικά δίκτυα συστήνεται η χρήση ενός δευτερεύοντα λογαριασμού ηλεκτρονικού ταχυδρομείου με ψευδώνυμο [29].

Τέλος, συστήνεται η χρήση μηχανών αναζήτησης που δεν συλλέγουν προσωπικά δεδομένα χρηστών, όπως είναι η μηχανή αναζήτησης Start Page [29].

Ωστόσο, όσον αφορά την προστασία των χρηστών από σχετικές πρακτικές επιτήρησης των ενεργειών τους που εφαρμόζονται από τη Google, το Facebook ή άλλες ιστοσελίδες, ο χρήστης δεν έχει πολλές επιλογές για να προστατεύσει τον εαυτό του από την επιτήρηση. Αν και υπάρχουν διαθέσιμα εργαλεία που επιτρέπουν την απόκρυψη της διεύθυνσης IP του χρήστη, όταν ένας χρήστης συνδέεται σε μια ιστοσελίδα, η ιστοσελίδα ξέρει ποιος είναι ο αυτός, χωρίς να χρειάζεται να γνωρίζει την πραγματική διεύθυνση IP του χρήστη ή άλλες σχετικές πληροφορίες. Καθώς ένας πιστοποιημένος χρήστης περιηγείται σε μια ιστοσελίδα, όλες οι ενέργειές του μπορούν εύκολα να αποθηκευτούν σε μια βάση δεδομένων και μπορούν να αναλυθούν από τους ιδιοκτήτες του ιστότοπου, προκειμένου να δημιουργηθεί το προφίλ του και να χρησιμοποιηθεί για την πώληση σε διαφημιστικές εταιρίες που στοχεύουν σε σχετικές ομάδες χρηστών [30].

2.3 Web 2.0

Το διαδίκτυο στην αρχική του μορφή περιλάμβανε επικοινωνία μιας κατεύθυνσης, επιτρέποντας σε μεγάλο αριθμό χρηστών να προσπελάζουν τα περιεχόμενα ενός συγκριτικά μικρού αριθμού ιστότοπων. Η καινούργια τάση στο χώρο του διαδικτύου, αποκαλούμενη, ως Web 2.0, αποτελεί μια αμφίδρομη συνεργασία στην οποία οι χρήστες είναι σε θέση να αλληλεπιδρούν με τους ιστότοπους και να προσθέτουν οι ίδιοι περιεχόμενο στους διάφορους δικτυακούς τόπους, το οποίο στη συνέχεια είναι άμεσα διαθέσιμο σε όλους τους χρήστες [31].

Η ηλεκτρονική εγκυκλοπαίδεια Wikipedia αποτελεί παράδειγμα ιστότοπου Web 2.0. Στην ηλεκτρονική εγκυκλοπαίδεια Wikipedia οι χρήστες είναι σε θέση να ενημερώνουν τα περιεχόμενα της εγκυκλοπαίδειας, η οποία διοικείται από μια σχετικά μικρή ομάδα διαχειριστών [32].

Το Web 2.0 δεν είναι απλώς μια νέα έκδοση μιας πρότερης έκδοσης διαδικτύου, αλλά αποτελεί μια διαφορετική φιλοσοφία σχεδίασης ιστοσελίδων. Το Web 2.0 μεταξύ άλλων [33]:

- διευκολύνει την ευέλικτη σχεδίαση διαδικτύου και την επαναχρησιμοποίηση της σχεδίασης ενός ιστότοπου
- παρέχει μια πλούσια και ανταποκρινόμενη διεπαφή χρήστη
- διευκολύνει τη συνεργατική δημιουργία περιεχομένου και τροποποίησης περιεχομένου

- επιτρέπει τη δημιουργία νέων εφαρμογών συνδυάζοντας διαφορετικές εφαρμογές διαδικτύου ή συνδυάζοντας δεδομένα και πληροφορίες από διαφορετικές πηγές

- επιτρέπει τη δημιουργία δικτυακών ομάδων ανθρώπων με κοινά ενδιαφέροντα

- υποστηρίζει τη συνεργασία και βοηθά την συγκέντρωση συλλογικής νοημοσύνης μεταξύ των χρηστών

Βασικά εργαλεία του Web 2.0 είναι τα παρακάτω:

- **Κοινωνικά δίκτυα**: ένα κοινωνικό δίκτυο αποτελεί ιστοσελίδα, στην οποία οι χρήστες έχουν τη δυνατότητα να επικοινωνούν άμεσα μεταξύ τους, να μοιράζονται τις σκέψεις και τις γνώμες τους, να συζητούν περί θεμάτων που τους απασχολούν και γενικότερα να σχολιάζουν περί οποιουδήποτε θέματος τους ενδιαφέρει. Η επικοινωνία σε ένα κοινωνικό δίκτυο μπορεί να είναι σύγχρονη ή ασύγχρονη. Γενικότερα, ένα κοινωνικό δίκτυο επιτρέπει τη δημιουργία εικονικών κοινοτήτων ατόμων που μοιράζονται κοινά ενδιαφέροντα, κοινές πεποιθήσεις ή κοινό τρόπο ζωής [34].

- **Wiki**: αποτελεί συλλογή ιστοσελίδων ειδικά σχεδιασμένων για να επιτρέπουν σε οποιονδήποτε έχει πρόσβαση, να προσθέσει νέο περιεχόμενο ή να τροποποιήσει το υπάρχον περιεχόμενο των ιστοσελίδων. Τα wikis χρησιμοποιούνται συχνά για τη δημιουργία συνεργατικών εκπαιδευτικών ιστοσελίδων. Μία από τις πιο γνωστές σελίδες wikis είναι η ηλεκτρονική εγκυκλοπαίδεια Wikipedia [35].

- **Blogs**: ένα blog αποτελεί εργαλείο αμφίδρομης επικοινωνίας μέσω διαδικτύου. Ένα blog είναι μια ιστοσελίδα όπου οι άνθρωποι μπορούν να εκφράσουν ελεύθερα τις σκέψεις τους, τις ιδέες τους, τις προτάσεις τους και να διατυπώσουν σχόλια επί διαφόρων θεμάτων. Τα σχετικά μηνύματα σε ένα blog παρουσιάζονται με τη μορφή εγγράφων, στο ύφος ενός περιοδικού και συνήθως εμφανίζονται με αντίστροφη χρονολογική σειρά εγγραφής στο σύστημα. Ένα blog μπορεί να περιλαμβάνει κείμενο, εικόνες, ή συνδέσμους για άλλα blogs και ιστοσελίδες. Τα περισσότερα blogs περιλαμβάνουν κυρίως κείμενο, ωστόσο υπάρχουν κατηγορίες blog που εστιάζουν σε φωτογραφίες

(photoblog ή photolog), αρχεία βίντεο (videoblog ή videolog) ή αρχεία ήχου (podcast) [33].

- **Εικονικοί κόσμοι (virtual words)**: αποτελεί προσομοιωμένο εικονικό περιβάλλον που επιτρέπει στους χρήστες να αλληλεπιδρούν μεταξύ τους χωρίς γεωγραφικά όρια. Κάθε χρήστης αντιπροσωπεύεται από ένα avatar. Το avatar αποτελεί την αντιπροσώπευση του χρήστη στον εικονικό κόσμο και μπορεί να προσαρμοστεί η εμφάνισή τους ανάλογα με τις προτιμήσεις του χρήστη. Οι εικονικοί κόσμοι είναι διαθέσιμοι στους χρήστες 24 ώρες το 24ωρο και στους οποίους οι χρήστες μπορούν να εξερευνήσουν, να κοινωνικοποιηθούν και να επιλύσουν συνεργατικές προκλήσεις. Το εικονικό περιβάλλον Second Life της Linden Lab αποτελεί τον μεγαλύτερο και δημοφιλέστερο εικονικό κόσμο στο διαδίκτυο [34].

Στο σημείο αυτό αξίζει να αναφερθεί πως η αποκλειστική πηγή εσόδων των ιστότοπων που συγκαταλέγονται στην κατηγορία ιστοτόπων Web 2.0 είναι οι στοχευμένες διαφημίσεις. Ο παρακάτω πίνακας αναφέρεται στους περισσότερο δημοφιλείς ιστότοπους Web 2.0 και τη βασική τους πηγή εσόδων:

Πίνακας 1: Οικονομικός προσανατολισμός και πηγή εσόδων βασικών ιστότοπων Web 2.0 [36]

Α/Α	**Ιστότοπος**	**Οικονομικός προσανατολισμός**	**Προβολή διαφημίσεων**
1	Facebook	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
2	You Tube	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
3	Wikipedia	Μη κερδοσκοπικός οργανισμός	Χωρίς διαφημίσεις
4	MySpace	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
5	BlogSpot	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
6	WordPress	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
7	Photo bucket	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
8	Twitter	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις
9	eHow	Κερδοσκοπικός οργανισμός με πηγή εσόδων τις διαφημίσεις	Στοχευμένες διαφημίσεις

Όπως διαπιστώνεται από τον παραπάνω πίνακα, η κύρια πηγή εσόδων των πλέον δημοφιλών ιστότοπων που ανήκουν στην κατηγορία ιστότοπων Web 2.0 είναι οι διαφημίσεις. Οι συγκεκριμένες εταιρίες με σκοπό τη μεγιστοποίηση των κερδών τους και την αποτελεσματική επιλογή – προβολή διαφημίσεων προς τους χρήστες εφαρμόζουν το επιχειρηματικό μοντέλο παρακολούθησης (surveillance model), θίγοντας την ιδιωτικότητα των χρηστών τους [36].

Κεφάλαιο 3: Προσωπικά δεδομένα και ιδιωτικότητα στο διαδίκτυο

3.1 Προσωπικά δεδομένα

3.1.1 Τι είναι

Στον όρο προσωπικά δεδομένα περιλαμβάνεται κάθε πληροφορία η οποία χαρακτηρίζει ένα άτομο. Σύμφωνα με το άρθρο 2 του Νόμου 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) τα προσωπικά δεδομένα διακρίνονται σε δυο κατηγορίες:

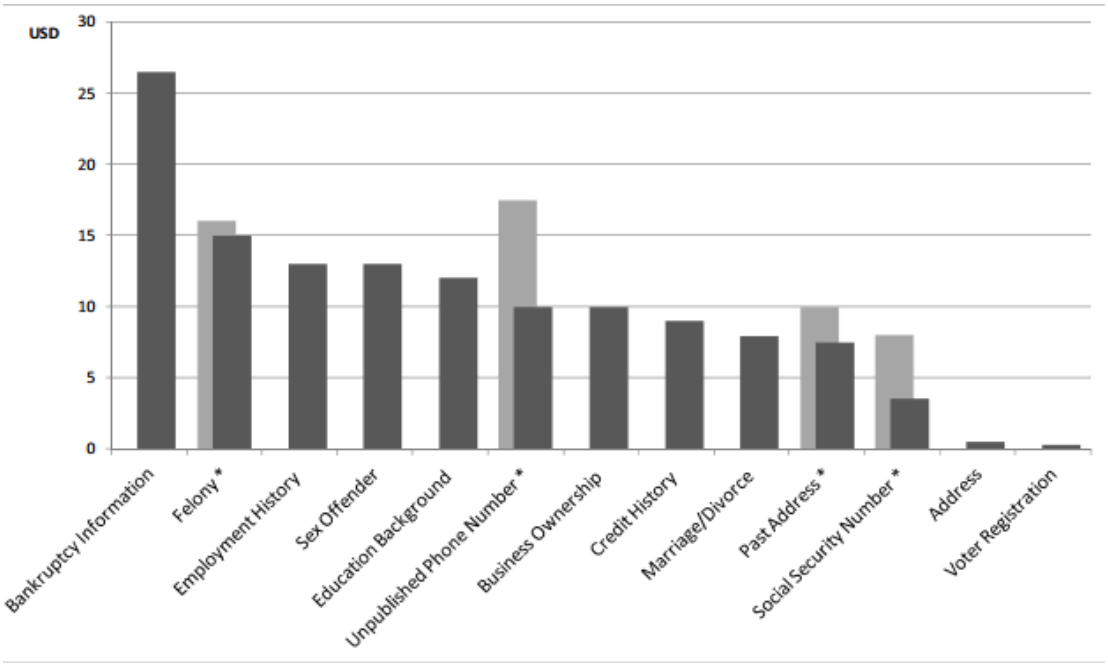
- **Δεδομένα προσωπικού χαρακτήρα**: " κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Δε λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων". Παραδείγματα δεδομένων προσωπικού χαρακτήρα είναι το ονοματεπώνυμο ενός ατόμου, η διεύθυνση κατοικίας του, η διεύθυνση εργασίας του, η διεύθυνση ηλεκτρονικού ταχυδρομείου (email), το τηλέφωνό του, τα ενδιαφέροντα και το επάγγελμά του.

- **Ευαίσθητα προσωπικά δεδομένα**: "τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων". Παραδείγματα ευαίσθητων προσωπικών δεδομένων αποτελούν οι πολιτικές πεποιθήσεις ενός ατόμου, το ποινικό του μητρώο, η ερωτική του ζωή, οι θρησκευτικές του πεποιθήσεις, η φυλή που ανήκει και το ιατρικό του ιστορικό.

Τα προσωπικά δεδομένα μπορεί να βρίσκονται αποθηκευμένα σε αρχεία υπολογιστή (π.χ. σε βάσεις δεδομένων, σε διακομιστές στο διαδίκτυο ή άλλα κλειστά δίκτυα υπολογιστών) ή σε έντυπα αρχεία. Η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα για τα άτομα και προστατεύεται από την εθνική νομοθεσία της Ελλάδας, αλλά και από το ευρωπαϊκό δίκαιο.

Για την κατανόηση της αξίας των προσωπικών δεδομένων των ατόμων, αρκεί η εξέταση της τιμής πώλησης τους μεταξύ των επιχειρήσεων. Η τιμή για τα προσωπικά δεδομένα στην αγορά προσδιορίζεται με βάση την προσφορά και τη ζήτηση προσωπικών δεδομένων χρηστών διαδικτύου. Το παρακάτω διάγραμμα απεικονίζει

την τιμή πώλησης δεδομένων χρηστών μεταξύ των επιχειρήσεων ανά χρήστη, σύμφωνα με σχετική έρευνα του ΟΑΣΑ το 2013 [37]:



Σχήμα 3: Τιμή πώλησης προσωπικών δεδομένων στην αγορά ανά κατηγορία δεδομένων [37]

Από το παραπάνω διάγραμμα διαπιστώνεται πως υπάρχει μεγαλύτερη ζήτηση για προσωπικά δεδομένα σχετικά με υποθέσεις χρεοκοπίας, ποινικό μητρώο, εργασιακό ιστορικό ατόμων , σεξουαλικές προτιμήσεις και εκπαιδευτικό υπόβαθρο.

Επίσης, λαμβάνοντας υπόψη πως τα προσωπικά δεδομένα μπορούν να πωληθούν σε πολλές επιχειρήσεις συγχρόνως, η πραγματική χρηματική αξία των προσωπικών δεδομένων των χρηστών στο διαδίκτυο είναι ακόμα μεγαλύτερη από τις τιμές που παρουσιάζονται στο παραπάνω διάγραμμα.

3.1.2 Προσωπικά δεδομένα και κοινωνικά δίκτυα

Μεγάλη απειλή για τα προσωπικά δεδομένα των χρηστών αποτελούν τα κοινωνικά δίκτυα. Ένα θέμα σχετικά με τα προσωπικά δεδομένα και την ιδιωτική ζωή στο Facebook αποτελεί η αδυναμία του χρήστη να διαγράψει άμεσα το λογαριασμό του στο Facebook. Εάν ένα μέλος επιλέξει να διαγράψει το λογαριασμό του, σύμφωνα με τους Όρους Χρήσης του Facebook "το περιεχόμενο που αφαιρείται μπορεί να παραμείνει σε αντίγραφα ασφαλείας του Facebook για ένα εύλογο χρονικό διάστημα" [38]. Ορισμένοι χρήστες διαμαρτύρονται για τους Όρους Χρήσης του Facebook, παρομοιάζοντάς τους με τους στίχους του τραγουδιού Hotel California "Μπορείτε να μπείτε μέσα οποιαδήποτε στιγμή θέλετε, αλλά δεν μπορείτε να φύγετε ποτέ" [39].

Με σκοπό τον προσδιορισμό πιθανών απειλών για την ιδιωτική ζωή των χρηστών οι Krasnova et al. (2009) πραγματοποίησαν σχετική έρευνα σε φοιτητές στο Βερολίνο. Από την αντίστοιχη έρευνα διαπιστώθηκε πως η θεωρούμενη ως μεγαλύτερη απειλή των χρηστών ιστοσελίδων κοινωνικής δικτύωσης ήταν η ανεπιθύμητη πρόσβαση σε στοιχεία του προσωπικού προφίλ των χρηστών από μελλοντικούς εργοδότες, από τους καθηγητές του Πανεπιστημίου, από μέλη της οικογένειας, από συμφοιτητές και γνωστά άτομα. Επίσης, οι συμμετέχοντες στην αντίστοιχη έρευνα θεώρησαν ως απειλή για την ελευθερία τους, πιθανή συλλογή και χρήση προσωπικών τους δεδομένων από του υπευθύνους των ιστοσελίδων κοινωνικής δικτύωσης ή άλλες τρίτες επιχειρήσεις που συνεργάζονται με τις ιστοσελίδες κοινωνικής δικτύωσης. Τέλος, ένα ζήτημα που όπως διαφάνηκε από την έρευνα απασχολούσε τους χρήστες κοινωνικών δικτύων ήταν ο κίνδυνος παρενόχλησης μέσω των κοινωνικών δικτύων και η γενικότερη έλλειψη μεθόδων ελέγχου – αντιμετώπισης του αντίστοιχου κινδύνου [40].

Επίσης, σε ανάλογη έρευνα των Johnson et al. (2012) διαπιστώθηκε πως για την πλειοψηφία των συμμετεχόντων στην έρευνα υπήρχε ιδιαίτερη ανησυχία των χρηστών ιστοσελίδων κοινωνικής δικτύωσης σχετικά με: (i) τη χρήση προσωπικών δεδομένων των χρηστών από ληστές για τη διευκόλυνση πραγματοποίησης μιας κλοπής (ii) πιθανή χρήση προσωπικών δεδομένων των ατόμων από εργοδότες είτε για την αξιολόγησή τους σχετικά με την καταλληλότητά τους για συγκεκριμένη θέση εργασίας, είτε για μια γενικότερη άποψη των εργοδοτών σχετικά με το προσωπικό τους και (iii) τη χρήση προσωπικών δεδομένων διαθέσιμων στις ιστοσελίδες κοινωνικής δικτύωσης από άτομα για τον εντοπισμό ευαίσθητων ατόμων, τη σύναψη φιλίας με εκείνους με σκοπό τη σεξουαλική εκμετάλλευση – κακοποίησή τους [41].

Επιπροσθέτως, οι ιστοσελίδες κοινωνικής δικτύωσης ανήκουν σε ιδιωτικές επιχειρήσεις, οι οποίες αποκομίζουν κέρδη από τη συλλογή και επεξεργασία δεδομένων σχετικά με τους χρήστες και τη μεταπώληση σχετικών δεδομένων σε τρίτους και ιδιαίτερα σε διαφημιστικές εταιρίες. Όταν ένας χρήστης εισέρχεται σε μια ιστοσελίδα κοινωνικής δικτύωσης, εισέρχεται σε ένα ιδιωτικό δίκτυο με συγκεκριμένους ιδιοκτήτες. Οι όποιες διαθέσιμες ρυθμίσεις ασφαλείας - απορρήτου αποβλέπουν στην προστασία των προσωπικών δεδομένων των χρηστών από τα υπόλοιπα μέλη του κοινωνικού δικτύου. Ωστόσο, οι σχετικές ρυθμίσεις ασφαλείας δεν προστατεύουν τα προσωπικά δεδομένα των χρηστών από τους ιδιοκτήτες των ιστοσελίδων κοινωνικής δικτύωσης.

3.1.3 Τρόποι προστασίας χρηστών

Οι χρήστες δε θα πρέπει να βασίζονται αποκλειστικά στην παρέμβαση της πολιτείας με τη θέσπιση σχετικής νομοθεσίας για την προστασία των προσωπικών τους δεδομένων. Οφείλουν και οι ίδιοι να είναι ιδιαίτερα προσεκτικοί κατά τη χρήση του διαδικτύου και να υιοθετήσουν ορισμένες απλές πρακτικές κατά την περιήγησή τους στο διαδίκτυο [42] [43]:

- Αποφυγή πλήρους καταγραφής των στοιχείων προφίλ στα κοινωνικά δίκτυα
- Ρύθμιση του προφίλ χρήστη στα κοινωνικά δίκτυα σε ιδιωτικό επίπεδο ασφάλειας
- Χρήση ειδικών λογισμικών (password vault) παραγωγής ισχυρών κωδικών σύνδεσης στις διάφορες ιστοσελίδες και αποθήκευσης των κωδικών στο σχετικό λογισμικό
- Χρήση κωδικού σύνδεσης στον προσωπικό υπολογιστή των χρηστών
- Χρήση διπλής επιβεβαίωσης χρήστη (two factor authentication) με λήψη κωδικού σύνδεσης μέσω μηνύματος στο κινητό τηλέφωνο, για όσους παρόχους υπηρεσιών στο διαδίκτυο (Facebook, Microsoft, Google) προσφέρουν σχετικές υπηρεσίες σύνδεσης
- Ορισμός ιδιωτικής περιήγησης στον φυλλομετρητή (browser)
- Ρύθμιση λήψης ειδοποιήσεων από το Google για κάθε καινούργια σελίδα που δημοσιεύεται και περιλαμβάνει το όνομα ή το λογαριασμό ηλεκτρονικού ταχυδρομείου του χρήστη
- Αποφυγή δήλωσης του ταχυδρομικού κώδικα και της διεύθυνσης του χρήστη, όταν η συμπλήρωση των σχετικών πεδίων δεν είναι υποχρεωτική κατά τη χρήση υπηρεσιών στο διαδίκτυο
- Δήλωση ψευδών στοιχείων στις ερωτήσεις ασφαλείας ξεκλειδώματος λογαριασμών
- Απενεργοποίηση του GPS στο κινητό τηλέφωνο όταν δε απαιτείται η χρήση του
- Απενεργοποίηση σύνδεσης σε ασύρματο δίκτυο (WiFi) στο κινητό τηλέφωνο όταν δε απαιτείται η χρήση του

- Χρήση σύνδεσης με κρυπτογράφηση σε όσους ιστότοπους (Facebook, Gmail, Twitter) παρέχουν σχετική δυνατότητα
- Αποφυγή χρήσης του υπολογιστή στην εργασία ή δημόσιου ασύρματου δικτύου για την αποστολή προσωπικών μηνυμάτων και γενικότερα τη διατήρηση των προσωπικών δεδομένων μονάχα σε προσωπικό υπολογιστή
- Χρήση τείχους προστασίας (firewall) και ενημερωμένων προγραμμάτων προστασίας από υιούς
- Κρυπτογράφηση κλήσεων μέσω διαδικτύου

3.2 Ιδιωτικότητα

3.2.1 Τι είναι

Από την αρχική διατύπωση περί ιδιωτικότητας εκ μέρους των Warren & Brandeis (1890) ως "το δικαίωμα να μένει κανείς ήσυχος - right to be let alone" [44], η έννοια της ιδιωτικότητας έχει αναπροσαρμοστεί ακολουθώντας τις εξελίξεις στο χώρο της τεχνολογίας και της επιχειρηματικότητας. Την περίοδο του πρώτου ορισμού περί ιδιωτικότητας (το 1890), η κύρια απειλή παραβίασης προσωπικών δεδομένων ήταν οι εφημερίδες που χωρίς τη συγκατάθεση των ατόμων δημοσίευαν φωτογραφίες ή δηλώσεις ατόμων. Σήμερα, η προστασία της ιδιωτικής ζωής είναι συνώνυμη με τα προσωπικά στοιχεία και ο μεγαλύτερος κίνδυνος γι'αυτά θεωρείται η τεχνολογία πληροφορικής [45].

Ο Tavani (2008) προτείνει τέσσερα διαφορετικά είδη προστασίας της ιδιωτικότητας, το καθένα εκ των οποίων επικεντρώνεται σε διαφορετικό σημείο ιδιωτικότητας [46]:

- **προστασία προσβασιμότητας (accessibility privacy)**: καλείται επίσης και φυσική προστασία της ιδιωτικής ζωής και αναφέρεται στο δικαίωμα αποτροπής εισβολής ξένων ατόμων στο ατομικό φυσικό περιβάλλον (πχ οικία) ενός ανθρώπου
- **προστασία επίδρασης (decisional privacy)**: αναφέρεται στην ελευθερία του ατόμου από επιδράσεις – παρεμβολές κατά τη λήψη αποφάσεων σχετικά με την ιδιωτική του ζωή

- **προστασία ψυχολογική (psychological privacy)**: γνωστή ως ψυχική προστασία της ιδιωτικής ζωής, αναφέρεται στην ελευθερία απομόνωσης και προστασίας των σκέψεων ενός ατόμου και της προσωπικής ταυτότητας του χαρακτήρα

- **προστασία πληροφοριών (informational privacy)**: αναφέρεται στο δικαίωμα ελέγχου και περιορισμού της πρόσβασης σε προσωπικές πληροφορίες ενός ατόμου

Η ιδιωτικότητα συχνά ορίζεται σε συνάφεια με τον έλεγχο πρόσβασης και χρήσης πληροφοριών. Για παράδειγμα, ο Fried (1984) αναφέρει πως "η ιδωτικότητα δεν αναφέρεται απλά στην έλλειψη πρόσβασης σε πληροφορίες που μας αφορούν, αλλά περισσότερο στον έλεγχο σχετικά με το ποιές πληροφορίες που μας αφορούν είναι διαθέσιμες σε άλλους ανθρώπους" [47]. Αντίστοιχα, ο Westin (1967) ορίζει την ιδιωτικότητα ως την "απαίτηση των ατόμων, ομάδων ατόμων ή ιδρυμάτων να καθορίζουν εκείνοι: πότε, πώς και σε ποιο βαθμό πληροφορίες που σχετίζονται με εκείνους δύναται να κοινοποιούνται σε άλλους" [48]. Ομοίως η Beardsley (1971) αναφέρεται στην ιδιωτικότητα ως η επιλογή - απόφαση σχετικά με το πότε και σε ποιόν βαθμό πληροφορίες που αφορούν κάποια άτομα, δύναται να αποκαλυφθούν σε άλλους [49].

Η τέταρτη διάσταση περί ιδιωτικότητας που αναφέρει ο Tavani (2008) και διατυπώθηκε παραπάνω είναι όμοια – σε συμφωνία με τους ορισμούς περί ιδιωτικότητας που αναφέρθηκαν (Westin, 1967; Beardsley, 1971; Fried, 1984). Η σχετική ανάγκη προστασίας της, προέκυψε από την εξέλιξη της τεχνολογίας και την εισβολή της στην καθημερινή ζωή των ατόμων μέσω της διάδοσης του διαδικτύου.

3.2.2 Παραβίαση ιδιωτικότητας

Οι διαθέσιμες ηλεκτρονικές υπηρεσίες από διάφορους οργανισμούς, τις περισσότερες φορές περιλαμβάνουν συλλογή και επεξεργασία προσωπικών δεδομένων από τους οργανισμούς που παρέχουν τις υπηρεσίες αυτές. Για παράδειγμα, τα νοσοκομεία τηρούν αρχεία για την υγεία των ασθενών τους, οι επιχειρήσεις διατηρούν αρχεία αγορών των πελατών τους, οι εργοδότες τηρούν αρχεία σχετικά με τους υπαλλήλους τους και οι φορολογικές αρχές κάθε κράτους τηρούν φορολογικά μητρώα για τους πολίτες της χώρας. Σε αυτό το πλαίσιο, οι παραβιάσεις της ιδιωτικής ζωής συχνά σχετίζονται με την αποκάλυψη σχετικών πληροφοριών σε άλλα άτομα ή οργανώσεις ή στο ευρύτερο κοινό. Ενδεικτικά παραδείγματα περιλαμβάνουν [50]:

- ανάρτηση περιεχομένου από χρήστες σε κοινωνικά δίκτυα και στη συνέχεια διαθεσιμότητα του σχετικού περιεχομένου σε άτομα για τα οποία δεν προορίζονταν το αντίστοιχο περιεχόμενο. Για παράδειγμα, ένας πιθανός εργοδότης μπορεί να έχει πρόσβαση σε φωτογραφίες της προσωπικής ζωής ενός ατόμου, ορισμένες από τις οποίες μπορεί να είναι σε κατάσταση μέθης

- παραβιάσεις των πληροφοριακών συστημάτων των οργανισμών από κακόβουλους χρήστες με σκοπό είτε την πρόσβαση σε προσωπικά στοιχεία χρηστών (αριθμοί πιστωτικών καρτών) για ιδία χρήση είτε την αποκάλυψη πληροφοριών υποκλοπής στο ευρύτερο κοινό

- μεταπώληση των προσωπικών στοιχείων των ατόμων σε άλλους οργανισμούς για διάφορους λόγους (στοχευόμενες διαφημίσεις) χωρίς τη συγκατάθεση των ατόμων

- παραβίαση της πολιτικής πρόσβασης σε εμπιστευτικές πληροφορίες από το προσωπικό του οργανισμού για ιδίους λόγους. Για παράδειγμα, υπάλληλος ενός νοσοκομείου πουλάει σε περιοδικά πληροφορίες για την υγεία διασημοτήτων

- χρήση των δεδομένων για άλλους σκοπούς χωρίς τη συγκατάθεση του χρήστη, όπως παράνομη διάκριση μεταξύ των ατόμων με βάση τη θρησκεία, τη φυλή ή άλλον παράγοντα

3.2.3 Κίνδυνοι παραβίασης ιδιωτικότητας

Υπάρχει μεγάλη μερίδα πληθυσμού που αναφέρει πως οι κίνδυνοι παραβίασης της ιδιωτικότητας των ατόμων στο διαδίκτυο είναι μηδαμινοί, καθότι δεν έχουν κάτι κακό να κρύψουν. Ωστόσο, όπως έχει αναφέρει σχετικά ο Σνόουντεν (2015), ο οποίος αποκάλυψε προγράμματα ηλεκτρονικής παρακολούθησης των πολιτών σε όλα τα μέρη του κόσμου από τις μυστικές υπηρεσίες των Ηνωμένων Πολιτειών: "το επιχείρημα ορισμένων πως δεν τους ενδιαφέρει το δικαίωμα στην ιδιωτική ζωή, καθώς δεν έχουν κάτι να κρύψουν, δε διαφέρει ιδιαίτερα από την άποψη πως δεν ενδιαφέρει κάποιον το δικαίωμα της ελευθερίας του λόγου, επειδή δεν έχει κάτι να πεί" [51].

Γενικότερα, διακρίνονται δυο κατηγορίες συνεπειών στα άτομα που παραβιάζεται η ιδιωτικότητάς τους: (i) υποκειμενικές συνέπειες και οι (ii) αντικειμενικές συνέπειες [52].

Οι υποκειμενικές συνέπειες παραβίασης της ιδιωτικότητας των ατόμων περιλαμβάνει καταστάσεις βίωσης άγχους ή αμηχανίας, ως απόρροια της γνώσης περί παραβίασης των προσωπικών τους δεδομένων. Ωστόσο, για την πρόκληση ψυχολογικών ή ψυχικών συμπτωμάτων από την παραβίαση της ιδιωτικότητας δεν απαιτείται να λάβει χώρα η σχετική παραβίαση, αρκεί η πεποίθηση περί υπαρκτού κινδύνου παραβίασης της ιδιωτικότητας των ανθρώπων. Οι σχετικές υποκειμενικές συνέπειες μπορεί να κυμαίνονται σε σοβαρότητα, από μιας μορφής ήπιας δυσφορίας έως ενός μεγάλου ψυχικού πόνου και αγωνίας πολύ μεγαλύτερης από τον πόνο που θα μπορούσε να είχε προκαλέσει μια σωματική επίθεση [52].

Οι αντικειμενικές συνέπειες δεν καθορίζονται από το άτομο του οποίου τα προσωπικά δεδομένα παραβιάστηκαν. Συνδέονται με τη μη αναμενόμενη χρήση των προσωπικών δεδομένων ενός ατόμου εναντίον του ίδιου. Ενδεικτικές συνέπειες αποτελούν, η χρήση προσωπικών δεδομένων σε κοινωνικούς ιστότοπους που μπορούν να επηρεάσουν αρνητικά την πρόσληψη ενός ατόμου σε μια εργασία εκ μέρους του εργοδότη ή τη διαμόρφωση αρνητικής εικόνας ενός ατόμου σε μια τοπική κοινωνία με βάση τις αναρτήσεις του στα κοινωνικά δίκτυα. [52].

Συνεπώς, η παραβίαση της ιδιωτικότητας ενός ατόμου δύναται να αποφέρει αρνητικές οικονομικές συνέπειες, κοινωνικές συνέπειες και ψυχολογικές ή ψυχικές συνέπειες στα άτομα.

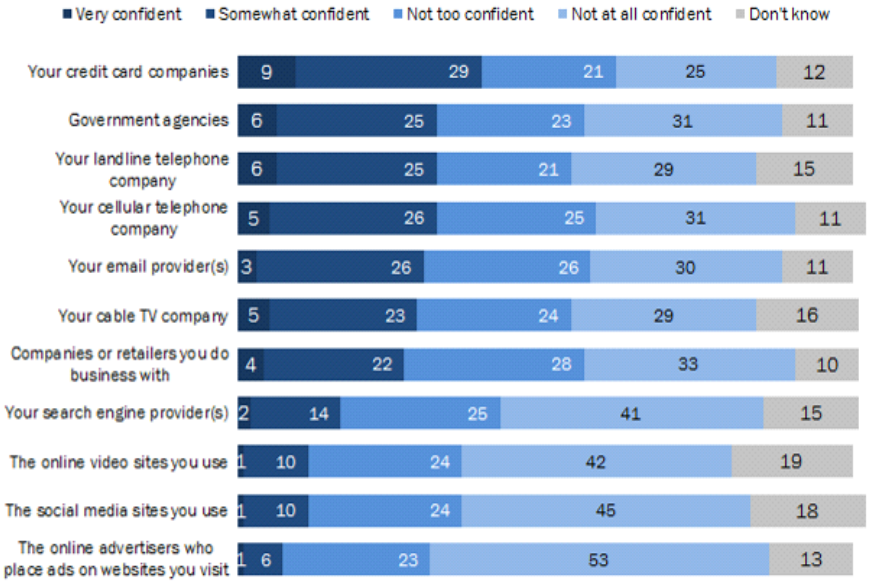
3.2.4 Η άποψη των χρηστών διαδικτύου

Σε παγκόσμια κλίμακα το 64% των χρηστών έχει ανησυχία για την τύχη των προσωπικών του δεδομένων κατά τη σύνδεσή του στο διαδίκτυο. Επιπροσθέτως, το 68% των χρηστών διαδικτύου σε παγκόσμια κλίμακα θεωρεί πως η υφιστάμενη νομοθεσία δεν προστατεύει επαρκώς την ιδιωτικότητά τους. [53].

Σε σχετική έρευνα του οργανισμού Pew Research Center (2014) σχετικά με την εμπιστοσύνη των χρηστών διαδικτύου σε κατηγορίες φορέων ή παρεχόμενων υπηρεσιών στο διαδίκτυο, διαπιστώθηκε πως οι χρήστες είναι περισσότερο δύσπιστοι όσον αφορά την εμπιστευτικότητα των προσωπικών τους δεδομένων απέναντι [54]:

- στις διαφημιστικές εταιρίες στο διαδίκτυο (53%)
- στους ιστότοπους κοινωνικής δικτύωσης (45%)
- στους ιστότοπους προβολής βίντεο (42%)
- στις μηχανές αναζήτησης (41%)

Στο παρακάτω σχήμα παρουσιάζονται τα σχετικά ποσοστά εμπιστοσύνης – δυσπιστίας για τις διάφορες κατηγορίες εταιριών στο διαδίκτυο που διατηρούν προσωπικά δεδομένα χρηστών:



Σχήμα 4: Επίπεδο εμπιστοσύνης χρηστών διαδικτύου στις ΗΠΑ σχετικά με την ιδιωτικότητα και την ασφάλεια των προσωπικών τους δεδομένων από διάφορες κατηγορίες δικτυακών τόπων [54]

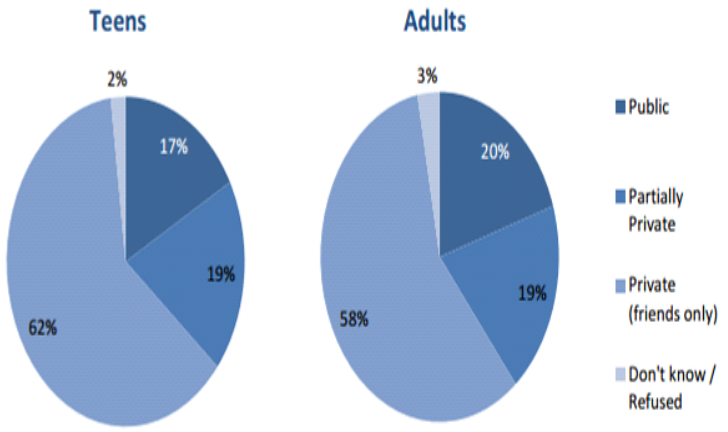
Σύμφωνα με την ίδια έρευνα το 74% των συμμετεχόντων θεωρεί πολύ σημαντικό να διατηρεί τον έλεγχο του ποιος μπορεί να λάβει ενημέρωση για πληροφορίες σχετικά με τους ίδιους και το 65% θεωρεί πολύ σημαντικό να έχει τη δυνατότητα ελέγχου του τι πληροφορίες συλλέγονται για τους ίδιους από τους διάφορους ιστότοπους στο διαδίκτυο [54].

Μια κοινωνική πλατφόρμα διαθέτει γνώση για ένα τεράστιο όγκο προσωπικών δεδομένων των χρηστών τους, όπως τα προσωπικά στοιχεία τους (όνομα, επίθετο, κινητό, ηλεκτρονικό ταχυδρομείο, επάγγελμα, διεύθυνση), ποιοι είναι οι φίλοι του κάθε χρήστη, τι κάνει στην πραγματικότητα στη ζωή του (με σχετική ανάρτηση γίνεται από έναν χρήστη), τα συμφέροντα ενός προσώπου κ.λπ.

Οι περισσότεροι χρήστες σε οποιαδήποτε κοινωνική πλατφόρμα ανησυχούν για την ανάλυση των προσωπικών τους στοιχείων με τεχνικές εξόρυξης δεδομένων από τις πλατφόρμες κοινωνικής δικτύωσης ή από οποιαδήποτε δευτερεύουσα επιχείρηση που έχει πρόσβαση στις εν λόγω πληροφορίες [55].

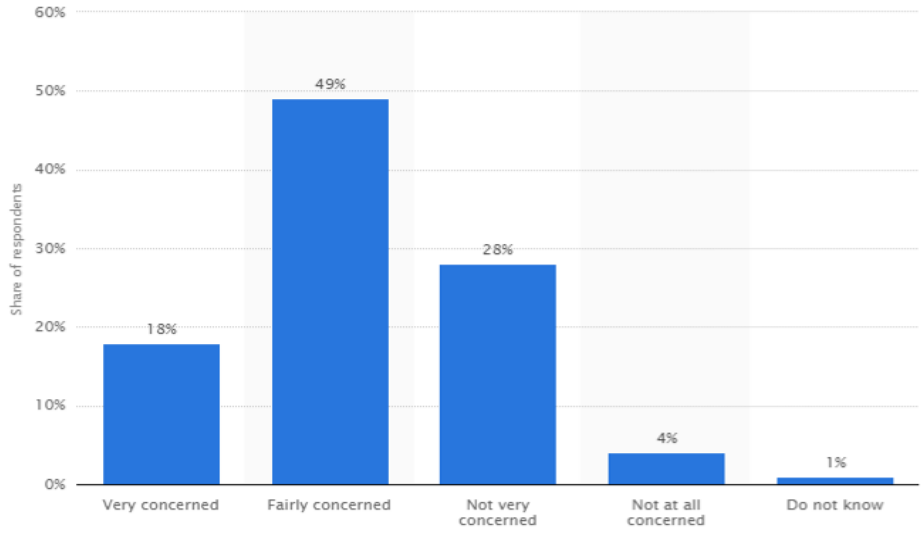
Περισσότεροι από τους μισούς χρήστες του Facebook έχουν το προφίλ τους ρυθμισμένο σε ιδιωτικό επίπεδο ασφάλειας (ορατό μόνο για φίλους), προκειμένου να

μην επιτρέπουν σε αγνώστους να δημοσιεύσουν κάτι στο προφίλ τους ή να έχουν πρόσβαση σε αναρτήσεις τους στο Facebook [50]:



Σχήμα 5: Ρυθμίσεις επιπέδου ασφαλείας χρηστών στο Facebook [56]

Ομοίως, σε αντίστοιχη έρευνα που πραγματοποιήθηκε στην Ευρωπαϊκή Ένωση διαπιστώθηκε αντίστοιχα πως οι περισσότεροι από τους Ευρωπαίους πολίτες είναι ανήσυχοι σχετικά με την τύχη των δεδομένων που καταχωρούν στο διαδίκτυο [57]:



Σχήμα 6: Ενδιαφέρον πολιτών της Ευρωπαϊκής Ένωσης σχετικά με την τύχη των προσωπικών δεδομένων που καταχωρούν στο διαδίκτυο [57]

3.2.5 Αντίθετη άποψη περί ιδιωτικότητας

Σε γνωμοδότηση περί της δυνατότητας λήψης εξετάσεων DNA χωρίς τη συγκατάθεση των κατηγορούμενων ο αντιεισαγγελέας του Αρείου Πάγου κ. Κονταξής είχε αναφέρει σε απάντησή του προς το Υπουργείο Προστασίας του Πολίτη πως "Οι ατομικές ελευθερίες δεν είναι, ούτε μπορεί να είναι απεριόριστες. Όποιος ζητάει κάτι τέτοιο είναι εκτός πραγματικότητας" [58].

Η σχετική εισήγηση του αντιεισαγγελέα του Αρείου Πάγου επισημαίνει την ανάγκη προστασίας του δημόσιου συμφέροντος παράλληλα με την προστασία της ιδιωτικότητας των ατόμων. Επίσης, εκτός από την ανάγκη προστασίας του δημόσιου συμφέροντος, μια πολιτεία υποχρεούται να προστατεύσει τους πολίτες της από διάφορους κινδύνους.

Το διαδίκτυο αποτελεί έναν υπαρκτό κίνδυνο για αρκετούς πολίτες. Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο το διαδίκτυο αποτελεί συχνά το μέσο για την εξεύρεση θυμάτων σεξουαλικής αποπλάνησης - κακοποίησης, για τον εκφοβισμό ατόμων μέσω διαδικτύου, για τη διάδοση της παιδικής πορνογραφίας και παράνομων ηλεκτρονικών παιχνιδιών. Για την αύξηση της αποτελεσματικότητας της προστασίας των πολιτών από σχετικούς κινδύνους, υπάρχει ανάγκη πρόσβασης σε προσωπικά δεδομένα χρηστών από υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος, με αποτέλεσμα την παραβίαση της ιδιωτικότητας των χρηστών από όργανα της Πολιτείας.

Ωστόσο, οι απόψεις διίστανται σχετικά με την ανάγκη παραβίασης της ιδιωτικότητας των πολιτών με σκοπό την προστασία του δημόσιου συμφέροντος. Οι υποστηρικτές της ανάγκης παραβίασης της ιδιωτικότητας αναφέρουν πως η απώλειά της είναι αναπόφευκτη και απαραίτητη, για την προστασία του δημόσιου συμφέροντος και ενδεικτικά για την προστασία από τρομοκρατικές επιθέσεις. Οι υποστηρικτές της αντίθετης άποψης υποστηρίζουν πως η προστασία της ιδιωτικότητας των πολιτών αποτελεί θεμέλιο της δημοκρατίας και πως δε μπορεί να διαβρώνονται τα θεμέλια της δημοκρατίας με σκοπό την προστασία της [59].

Όπως προτείνουν οι Mullikin & Rahman (2010) η ενδεδειγμένη λύση βρίσκεται κάπου στη μέση. Η Πολιτεία έχει την ευθύνη της προστασίας των πολιτών και ως εκ τούτου θα πρέπει να έχει και τη δυνατότητα να προστατεύσει τους πολίτες της αποτελεσματικά, μέσω της παρακολούθησης των ατόμων με σκοπό την έγκαιρη αντιμετώπιση πιθανών κινδύνων. Ωστόσο, κατά τη λήψη δράσεων για την προστασία των πολιτών, η Πολιτεία θα πρέπει να λαμβάνει σοβαρά υπόψη της τα δικαιώματα των πολιτών που προστατεύει [59].

Κεφάλαιο 4: Νομοθετικό πλαίσιο

4.1 Διεθνές Δίκαιο

Το δικαίωμα στην προστασία της ιδιωτικής ζωής ενός ατόμου από τους άλλους και κυρίως από το κράτος, καθορίστηκε σε διεθνές νομικό μέσο για πρώτη φορά στο άρθρο 12 της Οικουμενικής Διακήρυξης των Ηνωμένων Εθνών (**ΟΗΕ**) για τα Ανθρώπινα Δικαιώματα το 1948 σχετικά με το σεβασμό της ιδιωτικής και της οικογενειακής ζωής [60]. Στο σχετικό άρθρο αναφέρεται: "κανείς δε θα πρέπει να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε να δεχθεί προσβολές της τιμής και της υπόληψής του. Όλοι οι άνθρωποι έχουν το δικαίωμα στην προστασία του νόμου εναντίων σχετικών παρεμβολών ή επιθέσεων" [61].

Ακολούθησε το Διεθνές Σύμφωνο για τα Ατομικά και τα Πολιτικά Δικαιώματα, το οποίο αποτελεί μια πολυμερή Συνθήκη που εγκρίθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών στις 16 Δεκεμβρίου 1966, και τέθηκε σε ισχύ από τις 23 Μαρτίου 1976. Το σχετικό Σύμφωνο δεσμεύει τα συμβαλλόμενα μέρη να σέβονται τα ατομικά και τα πολιτικά δικαιώματα των ατόμων, συμπεριλαμβανομένων του δικαιώματος στη ζωή, της ελευθερίας της θρησκείας, της ελευθερίας του λόγου, της ελευθερίας του συνέρχεσθαι, των εκλογικών δικαιωμάτων και του δικαιώματος σε δίκαιη δίκη για όλους [62]. Ειδικότερα το άρθρο 17 παράγραφος 1 του Συμφώνου αναφέρεται στην προστασία της ιδιωτικότητας των ατόμων [61].

Κατόπιν, ο Οργανισμός Ηνωμένων Εθνών (ΟΗΕ) κατά τη διάρκεια διεθνούς διάσκεψης το 1968 για τα ανθρώπινα δικαιώματα αναγνώρισε πως η ιδιωτικότητα των ατόμων και τα σχετικά ανθρώπινα δικαιώματα επηρεάζονται άμεσα από τις τεχνολογικές εξελίξεις. Κατά τη διάρκεια της ίδιας διάσκεψης αναγνωρίστηκε η ανάγκη λήψης επιπρόσθετων μέτρων στον τομέα προστασίας της ιδιωτικότητας των ατόμων με σκοπό την προσαρμογή των μέτρων προστασίας στις σύγχρονες τεχνολογικές εξελίξεις [63].

Επίσης, το 1980 ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (**ΟΟΣΑ)** δημοσίευσε κατευθυντήριες αρχές που συστήνεται να ακολουθούνται από τα κράτη σε θέματα επεξεργασίας προσωπικών δεδομένων και στην ιδιωτικότητα των ατόμων. Ο ΟΟΣΑ αποτελεί ένα φόρουμ όπου οι κυβερνήσεις συνεργάζονται για την

αντιμετώπιση των οικονομικών, των κοινωνικών και των περιβαλλοντικών προκλήσεων της παγκοσμιοποίησης.

Οι βασικές κατευθυντήριες αρχές που δημοσιεύτηκαν το 1980 είναι οι εξής [64]:

- **Αρχή περιορισμένης συλλογής**: θα πρέπει να υπάρχουν όρια στη συλλογή των δεδομένων προσωπικού χαρακτήρα και τα δεδομένα αυτά θα πρέπει να λαμβάνονται με νόμιμα και δίκαια μέσα και ενδεχομένως, με τη γνώση ή τη συγκατάθεση του ατόμου.

- **Αρχή ποιότητας δεδομένων**: τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή με τους σκοπούς για τους οποίους συλλέγονται και θα πρέπει να είναι ακριβή, πλήρη και να διατηρούνται ενημερωμένα.

- **Αρχή προσδιορισμού σκοπού**: οι λόγοι για τους οποίους τα προσωπικά δεδομένα συλλέγονται θα πρέπει να είναι καθορισμένοι πριν τη διαδικασία συλλογής τους. Η επακόλουθη χρήση των δεδομένων περιορίζεται στην εκπλήρωση των λόγων για τους οποίους συλλέχτηκαν τα δεδομένα.

- **Αρχή περιοριστικής χρήσης**: τα προσωπικά δεδομένα δε θα πρέπει να αποκαλύπτονται ή να διατίθενται σε άλλους οργανισμούς ή άτομα χωρίς την συγκατάθεση του ατόμου.

- **Αρχή διασφάλισης ασφάλειας**: τα προσωπικά δεδομένα πρέπει να προστατεύονται από λογικές εγγυήσεις ασφάλειας έναντι κινδύνων, όπως απώλεια ή μη εξουσιοδοτημένη πρόσβαση, καταστροφή, τροποποίηση ή δημοσιοποίηση των δεδομένων.

- **Αρχή διαφάνειας**: Θα πρέπει να υπάρχει μια γενική πολιτική διαφάνειας σχετικά με τις πρακτικές και τις πολιτικές που ακολουθούνται σε σχέση με τα προσωπικά δεδομένα, η οποία θα πρέπει να είναι διαθέσιμη προς ενημέρωση στο κοινό.

- **Αρχή ατομικής συμμετοχής**: ένα άτομο θα πρέπει να έχει το δικαίωμα: α) να λαμβάνει από τον υπεύθυνο επεξεργασίας δεδομένων ενημέρωση, αν διαθέτει στοιχεία σχετικά με εκείνον, β) να ζητήσει πρόσβαση στα σχετικά δεδομένα, με πιθανή χρέωση, σε μορφή κατανοητή από τα περισσότερα άτομα γ) ένα άτομο θα πρέπει να λαμβάνει αιτιολόγηση για πιθανή άρνηση εξυπηρέτησής του σε σχετικά αιτήματα, όπως αναφέρθηκαν παραπάνω και δ) να μπορεί να αμφισβητήσει τα

δεδομένα που τον αφορούν και να μπορεί να ζητήσει πιθανή τροποποίηση ή διαγραφή τους.

- **Αρχή λογοδοσίας**: ένας διαχειριστής - ελεγκτής δεδομένων είναι υπεύθυνος για τη συμμόρφωσή του με μέτρα που σχετίζονται με τις παραπάνω κατευθυντήριες αρχές.

Οι παραπάνω αρχές δεν είναι δεσμευτικές για τα κράτη, αλλά αποτελούν συστάσεις για την προστασία της ιδιωτικότητας των ατόμων προς τα κράτη [64].

Το Συμβούλιο της Ευρώπης ιδρύθηκε μετά τον Β' Παγκόσμιο Πόλεμο για να φέρει τα κράτη της Ευρώπης πιο κοντά με σκοπό την προώθηση του κράτους δικαίου, της δημοκρατίας, των ανθρωπίνων δικαιωμάτων και να οδηγήσει στην κοινωνική ανάπτυξη την Ευρώπη. Για αυτό το σκοπό, το Συμβούλιο της Ευρώπης ενέκρινε την **Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου** (ΕΣΔΑ) το 1950, η οποία τέθηκε σε ισχύ το 1953. Τα κράτη μέλη του Συμβουλίου της Ευρώπης έχουν την υποχρέωση της συμμόρφωσης με την ΕΣΔΑ, η οποία απαιτεί από τα κράτη μέλη να ενεργούν σύμφωνα με τις διατάξεις της Σύμβασης [60].

Για να διασφαλιστεί πως όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης τηρούν τις υποχρεώσεις τους, που απορρέουν από την ΕΣΔΑ, συστήθηκε στο Στρασβούργο το 1959 το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων (ΕΔΑΔ). Το ΕΔΑΔ διασφαλίζει ότι τα κράτη τηρούν τις υποχρεώσεις τους, που απορρέουν από τη Σύμβαση και αναλαμβάνει την εξέταση πιθανών σχετικών καταγγελιών από άτομα, ομάδες ατόμων, ΜΚΟ ή νομικά πρόσωπα. Το 2013, το Συμβούλιο της Ευρώπης περιελάμβανε 47 κράτη μέλη, 28 από τα οποία είναι επίσης κράτη μέλη της Ευρωπαϊκής Ένωσης (ΕΕ) [60].

Το δικαίωμα προστασίας των προσωπικών δεδομένων των ατόμων αποτελεί μέρος των δικαιωμάτων που προστατεύονται από το άρθρο 8 της ΕΣΔΑ, το οποίο εγγυάται το δικαίωμα στο σεβασμό της ιδιωτικής και της οικογενειακής ζωής, της κατοικίας, καθώς επίσης και της αλληλογραφίας και ορίζει τις προϋποθέσεις υπό τις οποίες δύναται τα σχετικά δικαιώματα των ατόμων να μην τηρηθούν [60].

Το 1981, το Συμβούλιο της Ευρώπης επικύρωσε τη σύμβαση για την προστασία των φυσικών προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα (**Σύμβαση 108**). Η σχετική Σύμβαση αποτέλεσε και παραμένει μέχρι σήμερα, νομικά δεσμευτικό διεθνές όργανο στον τομέα της

προστασίας των δεδομένων έναντι της αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων από διάφορους οργανισμούς [60].

Η Σύμβαση 108 βρίσκει εφαρμογή σε κάθε επεξεργασία δεδομένων που πραγματοποιείται από ιδιωτικούς και δημόσιους φορείς, όπως η επεξεργασία δεδομένων από τις δικαστικές και τις διωκτικές αρχές ενός κράτους. Η σχετική Σύμβαση προστατεύει το άτομο από καταχρήσεις κατά την επεξεργασία δεδομένων, η οποία μπορεί να αφορά τη συλλογή και την επεξεργασία δεδομένων προσωπικού χαρακτήρα και επιδιώκει ταυτόχρονα να ρυθμίσει τη διασυνοριακή ροή δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα που συλλέγουν οι διάφοροι οργανισμοί αποθηκεύονται για συγκεκριμένους νόμιμους σκοπούς και όχι για χρήση που δεν συμβιβάζεται με τους σκοπούς συλλογής τους, ούτε διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό, τι είναι απαραίτητο. Επίσης, η σχετική Σύμβαση ορίζει την απαίτηση συλλογής δεδομένων με τρόπο κατάλληλο, ακριβή, συναφή και όχι υπερβολικό σε σχέση με το σκοπό συλλογής τους. Η σύμβαση κατοχυρώνει επίσης το δικαίωμα του ατόμου να γνωρίζει ότι κάποιος οργανισμός κατέχει πληροφορίες σχετικά με εκείνον και εάν είναι απαραίτητο να ζητήσει τη διόρθωσή τους. Όλα τα κράτη μέλη της ΕΕ έχουν επικυρώσει τη Σύμβαση 108 [60].

4.2 Δίκαιο Ευρωπαϊκής Ένωσης

Η πρώτη απόφαση της Ευρωπαϊκής Ένωσης σχετικά με την προστασία της ιδιωτικότητας των ατόμων είναι η υπ' αριθμόν 95/46/EC σύσταση προς τα κράτη μέλη της Ένωσης, που απαιτούσε από τα κράτη μέλη την υιοθέτηση των σχετικών αποφάσεων εντός τριών ετών. Σκοπός της σχετικής οδηγίας είναι η εφαρμογή ανάλογης νομοθεσίας σε όλα τα κράτη μέλη σχετικά με την προστασία της ιδιωτικότητας των πολιτών της Ένωσης [65].

Η οδηγία 95/46/ΕΚ ορίζει το ευρωπαϊκό κοινό πλαίσιο για την προστασία των προσωπικών δεδομένων μέσα από μια γενική και ολοκληρωμένη θεώρηση για κάθε τομέα (ιδιωτικό ή δημόσιο) και σκοπό (εμπορικό ή μη) χρήσης των δεδομένων. Η οδηγία ήταν εμπνευσμένη όχι μόνο από την πρόθεση της άρσης των εμποδίων στην διασυνοριακή μεταφορά δεδομένων προσωπικού χαρακτήρα, προκειμένου να διευκολυνθούν οι οικονομικές δραστηριότητες εντός της Ένωσης, αλλά και από το στόχο να προσφερθεί ένα υψηλό επίπεδο προστασίας των ατομικών δικαιωμάτων των κατοίκων της Ένωσης. Η συγκεκριμένη προσέγγιση διέφερε από αυτές που έχουν υιοθετηθεί σε άλλες χώρες του πλανήτη, όπως στην περίπτωση των Ηνωμένων

Πολιτειών της Αμερικής, όπου υπάρχουν διαφορετικές ρυθμίσεις που λαμβάνουν υπόψη μόνο κάποιες συγκεκριμένες πτυχές της προστασίας των προσωπικών δεδομένων και δεν υπάρχει καμία γενική και ολοκληρωμένη διάταξη - ρύθμιση. Επιπροσθέτως, σε αρκετές σχετικές νομοθετικές ρυθμίσεις στις Ηνωμένες Πολιτείες, οι σχετικές ρυθμίσεις είναι προσανατολισμένες προς μια οικονομική και επιχειρηματική προοπτική και όχι εμπνευσμένες από την ανάγκη προστασίας των προσωπικών δικαιωμάτων [66].

Η οδηγία 95/46/ΕC, περιλαμβάνει όλα τα βασικά στοιχεία από το άρθρο 8 της Ευρωπαϊκής Σύμβασης για τα Ανθρώπινα Δικαιώματα, η οποία αποβλέπει στο σεβασμό των δικαιωμάτων της ιδιωτικής, της προσωπικής και της οικογενειακής ζωής των ατόμων, καθώς επίσης και στην προστασία του ασύλου της οικίας και της προσωπικής αλληλογραφίας. Η σχετική οδηγία βασίζεται στις κατευθυντήριες αρχές περί προστασίας της ιδιωτικότητας των ατόμων που εξέδωσε ο ΟΟΣΑ το 1980. Πιο συγκεκριμένα η οδηγία 95/46/ΕC επικεντρώνεται στις εξής βασικές αρχές [66]:

- **Ενημέρωση**: υποχρέωση των οργανισμών περί ενημέρωσης των ατόμων κατά τη συλλογή και την αποθήκευση προσωπικών δεδομένων τους
- **Σκοπός**: τα δεδομένα που συλλέγονται θα πρέπει να χρησιμοποιούνται αποκλειστικά για δηλωμένο σκοπό (ους) και για κανέναν άλλον λόγο
- **Συγκατάθεση**: τα προσωπικά δεδομένα ενός ατόμου δε θα πρέπει να γνωστοποιούνται ή να μοιραστούν σε τρίτους χωρίς τη συγκατάθεση του ατόμου
- **Ασφάλεια**: μετά τη συλλογή των προσωπικών δεδομένων, εκείνα θα πρέπει να διατηρούνται ασφαλή από πιθανή κατάχρηση, κλοπή ή απώλεια τους
- **Αποκάλυψη**: άτομα των οποίων τα προσωπικά δεδομένα συλλέγονται θα πρέπει να ενημερώνονται από τους οργανισμούς που συλλέγουν – διατηρούν προσωπικά τους δεδομένα
- **Πρόσβαση**: τα άτομα θα πρέπει να έχουν πρόσβαση στα προσωπικά τους δεδομένα που διατηρούνται από διάφορους οργανισμούς και τη δυνατότητα να διορθώσουν τυχόν ανακρίβειες
- **Λογοδοσία**: οι οργανισμοί που συλλέγουν προσωπικά δεδομένα είναι υπεύθυνοι για την τήρηση των αρχών της σχετικής οδηγίας

Επιπροσθέτως, οι θεμελιώδεις αρχές της αντίστοιχης οδηγίας προς τα κράτη μέλη είναι: (i) ο καθορισμός της ποιότητας των δεδομένων και των προϋποθέσεων νομιμοποίησης της επεξεργασίας τους (άρθρα 6 και 7 της οδηγίας), (ii) το δικαίωμα της πρόσβασης σε δεδομένα (άρθρο 12 της οδηγίας), (iii) η απαίτηση της συγκατάθεσης από το υποκείμενο των δεδομένων (άρθρο 7 της οδηγίας) με βάση τις πληροφορίες σχετικά με την αντίστοιχη επεξεργασία των δεδομένων (άρθρο 10 της οδηγίας) και (iv) η εμπιστευτικότητα και η ασφάλεια της επεξεργασίας των δεδομένων (άρθρα 16 και 17 της οδηγίας). Όσον αφορά τις διάφορες πτυχές της εσωτερικής οργάνωσης των διαδικασιών επεξεργασίας δεδομένων, η Ευρωπαϊκή Ένωση έχει υιοθετήσει ένα συγκεκριμένο μοντέλο, προκειμένου να εγγυάται την ορθή ταυτοποίηση του προσώπου που είναι υπεύθυνο για την προστασία των δεδομένων και την ορθή ταυτοποίηση των υποκειμένων των δεδομένων. Το αντίστοιχο μοντέλο θα πρέπει να διατηρείται ακόμα και όταν μια εταιρία χρησιμοποιεί υπηρεσίες τρίτων και ιδιαίτερα όταν αυτές παρέχονται με τη χρήση υποδομών εκτός της Ευρωπαϊκής Ένωσης, σε χώρες με χαμηλό επίπεδο προστασίας των προσωπικών δεδομένων [67].

Επίσης, ο Κανονισμός 45/2001/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών, αποβλέπει στην προστασία των προσωπικών δεδομένων των κατοίκων της Ένωσης κατά την επεξεργασία τους από όργανα ή φορείς της Ευρωπαϊκής Ένωσης. Επίσης, με τον αντίστοιχο Κανονισμό ιδρύεται ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, με σκοπό την επίβλεψη της εφαρμογής των διατάξεων του Κανονισμού.

Ωστόσο, όπως και με την οδηγία 95/46/ΕΚ, οι διατάξεις της οδηγίας 45/2001/ΕΚ δεν εφαρμόζονται για οργανισμούς και όργανα πλήρως εγκατεστημένα εκτός των ορίων της Ευρωπαϊκής Ένωσης.

Κατόπιν, η οδηγία 58/2002/ΕΚ – "για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες" θεσπίζει κανόνες για την προστασία του δικαιώματος της ιδιωτικής ζωής σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών και προβλέπει κανόνες για την ελεύθερη κυκλοφορία των δεδομένων στην κοινότητα της ΕΕ.

Η αντίστοιχη οδηγία προέκυψε ως αποτέλεσμα της εξέλιξης των τεχνολογιών πληροφορικής όπως αναφέρεται στην αιτιολογική σκέψη 5. Τα κακόβουλα λογισμικά

(spyware), υιοί υπολογιστών, κρυφά αναγνωριστικά υπολογιστών, αποτελούν παραδείγματα νέων τεχνολογιών που καθιστούν ευκολότερη την πρόσβαση στα προσωπικά δεδομένα των χρηστών διαδικτύου. Επιπλέον, οι δυνατότητες των κινητών τηλεφωνικών συσκευών λήψης πληροφοριών τοποθεσίας του χρήστη, δημιουργούν νέους κινδύνους για την προστασία των δεδομένων που θα έπρεπε να ρυθμιστούν σε ευρωπαϊκό επίπεδο [67].

Σκοπός της οδηγίας 58/2002/ΕΚ είναι να καθορίσει τα χαρακτηριστικά των νέων τεχνολογιών προκειμένου να μη γίνεται κατάχρηση των δυνατοτήτων τους με σκοπό την πρόσβαση σε προσωπικά δεδομένα χρηστών. Ενδεικτικά ορίστηκε, τα δεδομένα περί τοποθεσίας χρήστη να μην διατηρούνται αποθηκευμένα περισσότερο από όσο χρειάζεται για τη μετάδοση μιας επικοινωνίας (άρθρο 5) και να υποβάλλονται σε επεξεργασία μόνο ανώνυμα (άρθρο 9), χωρίς διασύνδεση με συγκεκριμένους χρήστες [67].

Η οδηγία 58/2002/ΕΚ, σε αντίθεση με τις οδηγίες 95/46/ΕΚ και 45/2001/ΕΚ έχει εφαρμογή σε παρόχους που έχουν την έδρα των δραστηριοτήτων τους εντός ή εκτός των ορίων της Ένωσης.

Τέλος, η οδηγία 136/2009/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αποτελεί τροποποίηση της οδηγίας 58/2002/ΕΚ, η οποία αφορά την προστασία των δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο. Το πιο σημαντικό σημείο στην οδηγία 136/2009/ΕΚ, αναφέρεται στους κανονισμούς που αφορούν στην αποθήκευση cookies από τους διάφορους ιστότοπους.

Η σχετική οδηγία απαιτεί από τις ιστοσελίδες την πρότερη ενημέρωση και τη λήψη της συναίνεσης των επισκεπτών πριν την αποθήκευση πληροφοριών με τη μορφή cookies σε έναν υπολογιστή ή οποιαδήποτε συσκευή συνδεδεμένη στο διαδίκτυο. Τα cookies, όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, αποτελούν εργαλείο που δύναται να χρησιμοποιηθούν για την παρακολούθηση των προτιμήσεων των επισκεπτών ενός ιστότοπου.

Η προηγούμενη οδηγία της Ευρωπαϊκής Ένωσης απαιτούσε από τις ιστοσελίδες να ενημερώνουν τους χρήστες για τον τρόπο διαγραφής ή απενεργοποίησης των cookies σε έναν φυλλομετρητή. Ωστόσο, η σχετική πληροφορία στους περισσότερους ιστότοπους ήταν διαθέσιμη στους χρήστες ως μέρος των Όρων Χρήσης ενός ιστότοπου, την οποία ως επί το πλείστον οι χρήστες δεν μελετάνε με ιδιαίτερη λεπτομέρεια. Με την οδηγία της 136/2009/ΕΚ απαιτείται η συγκατάθεση του χρήστη πριν οι επισκέπτες δώσουν τη συγκατάθεσή τους για τη χρήση τους.

4.3 Εθνικό δίκαιο

Σύμφωνα με το Σύνταγμα της Ελλάδας η ιδιωτικότητα των πολιτών προστατεύεται από το **Σύνταγμα**. Πιο συγκεκριμένα στο άρθρο 2 (Πρωταρχικές υποχρεώσεις της πολιτείας) του Συντάγματος παράγραφος 1 ορίζεται η υποχρέωση της Πολιτείας περί "σεβασμού και η προστασία της αξίας του ανθρώπου". Μέρος της αξίας του ανθρώπου αποτελεί η ελευθερία. Η καταγραφή προσωπικών δεδομένων των ατόμων χωρίς τη συγκατάθεσή τους, παραβιάζει την ελευθερία των ατόμων.

Επιπροσθέτως, στο άρθρο 5 (Ελεύθερη ανάπτυξη της προσωπικότητας, προσωπική ελευθερία) παράγραφος 1 του Συντάγματος, ορίζεται πως "Καθένας έχει δικαίωμα να αναπτύσσει ελεύθερα την προσωπικότητά του και να συμμετέχει στην κοινωνική, οικονομική και πολιτική ζωή της Χώρας, εφόσον δεν προσβάλλει τα δικαιώματα των άλλων και δεν παραβιάζει το Σύνταγμα ή τα χρηστά ήθη". Σύμφωνα με το συγκεκριμένο άρθρο ένα άτομο έχει δικαίωμα να αυτοκαθορίζεται, επιλέγοντας ποιες πληροφορίες της ιδιωτικής του ζωής θα είναι διαθέσιμες στο ευρύ κοινό.

Επίσης, στο ίδιο άρθρο, παράγραφος 2, δηλώνεται πως: "Όλοι όσοι βρίσκονται στην Ελληνική Επικράτεια απολαμβάνουν την απόλυτη προστασία της ζωής, της τιμής και της ελευθερίας τους, χωρίς διάκριση εθνικότητας, φυλής, γλώσσας και θρησκευτικών ή πολιτικών πεποιθήσεων". Επιπροσθέτως, στο ίδιο άρθρο (5§3) δηλώνεται η υποχρέωση της πολιτείας για την προστασία της προσωπικής ελευθερίας ("Η προσωπική ελευθερία είναι απαραβίαστη. Κανένας δεν καταδιώκεται ούτε συλλαμβάνεται ούτε φυλακίζεται ούτε με οποιονδήποτε άλλο τρόπο περιορίζεται, παρά μόνο όταν και όπως ορίζει ο νόμος"). Τέλος, στο ίδιο άρθρο (5§5) δηλώνεται η υποχρέωση της πολιτείας για την προστασία "της υγείας και της γενετικής ταυτότητας" των πολιτών.

Ακόμα, στο άρθρο 9 του Συντάγματος θεσπίζεται το άσυλο της κατοικίας των πολιτών. "Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη. Καμία έρευνα δεν γίνεται σε κατοικία, παρά μόνο όταν και όπως ορίζει ο νόμος και πάντοτε με την παρουσία εκπροσώπων της δικαστικής εξουσίας."

Επίσης, το άρθρο 14 (Ελευθερία του Τύπου) παράγραφος 5 προστατεύει τα άτομα από ψευδείς ή ανακριβείς αναρτήσεις στον Τύπο και ορίζει τη δυνατότητα του ατόμου να απαντήσει σε δημοσιεύματα του Τύπου, που είναι με τη σειρά του υποχρεωμένος για την άμεση δημοσίευση της σχετικής απάντησης.

Ανάλογα, το άρθρο 15 (Κινηματογράφος, φωνογραφία, ραδιοφωνία, τηλεόραση) παράγραφος 2 προστατεύει τα άτομα από ψευδείς ή ανακριβείς μεταδόσεις στο ραδιόφωνο και την τηλεόραση.

Επιπροσθέτως, στο άρθρο 19 του Συντάγματος θεσπίζεται "το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστα", όταν δεν συντρέχουν λόγοι εθνικής ασφάλειας ή έρευνα για σοβαρά εγκλήματα.

Επίσης, με την αναθεώρηση του Συντάγματος το 2011 προστέθηκε το άρθρο 9Α που ορίζει πως "Καθένας έχει δικαίωμα προστασίας από την συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει".

Τέλος, το άρθρο 5Α (Δικαίωμα στην πληροφόρηση) ορίζει την υποχρέωση της πολιτείας περί διευκόλυνσης χρήσης νέων τεχνολογιών διαδικτύου εκ μέρους των πολιτών και πρόσβασής της σε σχετικές πληροφορίες, πάντα στο πλαίσιο περιορισμών που ορίζουν τα άρθρα 5, 9, 9Α και 19 του Συντάγματος.

Επιπροσθέτως, ο **Ν. 2472/ 1997** - "Για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα", αποτελεί την ενσωμάτωση στην Ελληνική νομοθεσία της ευρωπαϊκής οδηγίας 95/46/ΕC σχετικά με την προστασία της ιδιωτικότητας των ατόμων [69]. Αντικείμενο του σχετικού νόμου είναι "η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για την προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής" (άρθρο 1).

Στον ίδιο νόμο ορίζεται ως επεξεργασία δεδομένων "η συλλογή, η καταχώρηση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή" των δεδομένων (άρθρο 2). Επιπροσθέτως, για να θεωρηθεί μια σχετική επεξεργασία δεδομένων ως νόμιμη θα πρέπει τα δεδομένα να συλλέγονται με "θεμιτό και νόμιμο τρόπο, για σαφείς και νόμιμους σκοπούς και να υφίσταται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών" (άρθρο 4). Επιπροσθέτως, για τη νομιμοποίησή της απαιτείται η συγκατάθεση του υποκειμένου των δεδομένων (άρθρο 5).

Με τον ίδιο Νόμο (2472/1997) συστήνεται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (άρθρο 15) και καθορίζονται οι αρμοδιότητες(άρθρο 19), τα

πρόστιμα παραβίασης των προσωπικών δεδομένων (άρθρα 21 - 23) καθώς και τα δικαιώματα του υποκειμένου των δεδομένων (άρθρα 11 - 14):

- Δικαίωμα ενημέρωσης
- Δικαίωμα πρόσβασης
- Δικαίωμα αντίρρησης
- Δικαίωμα προσωρινής δικαστικής προστασίας

Στη συνέχεια ακολούθησε η έκδοση του **Ν. 3471/2006** – "Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997", που αποτέλεσε την ενσωμάτωση στο Ελληνικό δίκαιο της οδηγίας 2002/58/ΕΚ. Σκοπός του αντίστοιχου νόμου είναι "η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών" (άρθρο 1).

Με τον Ν. 3471/2006 διασφαλίζεται το απόρρητο της ηλεκτρονικής επικοινωνίας των ατόμων (άρθρο 4). Επίσης, κάθε επεξεργασία δεδομένων θα πρέπει να περιορίζεται στη συλλογή και στη χρήση των αποκλειστικά απαραίτητων δεδομένων για την επίτευξη του σκοπού για τον οποίο γίνεται η σχετική επεξεργασία (άρθρο 5). Τέλος, στον ίδιο νόμο καθορίζονται οι κυρώσεις για τους οργανισμούς που θα παραβιάσουν τις διατάξεις του, (υψηλά πρόστιμα) (άρθρα 14 - 15) καθώς και ο σχετικός ρόλος – αρμοδιότητες της Ανεξάρτητης Αρχής Προστασίας προσωπικών δεδομένων (άρθρα 12 – 13).

Κατόπιν, εκδόθηκε ο **Ν. 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", για την ενσωμάτωση στην Ελληνική έννομη τάξη της κοινοτικής οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου.

Σύμφωνα με τον αντίστοιχο Νόμο είναι υποχρεωτική η διατήρηση εκ μέρους των παρόχων υπηρεσιών ηλεκτρονικής επικοινωνίας στοιχείων σχετικά με (άρθρο 5):

- την ανίχνευση της πηγής μιας επικοινωνίας

- τον προορισμό μιας επικοινωνίας
- τη χρονική στιγμή έναρξης και λήξης μιας επικοινωνίας
- το είδος της επικοινωνίας
- τον εξοπλισμό επικοινωνίας
- τη γεωγραφική θέση του εξοπλισμού κινητής τηλεφωνίας

Το διάστημα που αποθηκεύονται τα σχετικά δεδομένα από τους παρόχους υπηρεσιών ηλεκτρονικής επικοινωνίας είναι 12 μήνες (άρθρο 6), και οι πάροχοι θα πρέπει να τα διατηρούν αποθηκευμένα εντός της Ελληνικής επικράτειας. Σκοπός του Ν. 3917/2011 είναι η προστασία από την τρομοκρατία και το οργανωμένο έγκλημα.

Συνοψίζοντας, η Ελλάδα διαθέτει ένα ολοκληρωμένο νομοθετικό πλαίσιο σχετικά με την προστασία των προσωπικών δεδομένων, το οποίο είναι εναρμονισμένο με τη νομοθεσία - οδηγίες της Ευρωπαϊκής Ένωσης περί προστασίας προσωπικών δεδομένων. Οι σχετικές διατάξεις καθορίζουν τους όρους και τις προϋποθέσεις υπό τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να πραγματοποιηθεί, έτσι ώστε να προστατεύονται παράλληλα τα θεμελιώδη δικαιώματα και οι ελευθερίες των φυσικών προσώπων στη χώρα, με ιδιαίτερη μέριμνα υπέρ του δικαιώματος στην ιδιωτική ζωή [70].

Κεφάλαιο 5: Κανονισμός (ΕΕ) 2016/679

5.1 Ιστορική αναδρομή

Το 2009, η Ευρωπαϊκή Επιτροπή ξεκίνησε να εξετάζει εκ νέου το υπάρχον νομικό πλαίσιο για την προστασία των δεδομένων στην Ευρωπαϊκή Ένωση, οργανώνοντας μια σειρά συνεδρίων και στοχευόμενες διαβουλεύσεις με τους ενδιαφερόμενους. Το Νοέμβριο του 2010, ο Ευρωπαίος Επίτροπος για τη Δικαιοσύνη, τα Θεμελιώδη Δικαιώματα και την Ιθαγένεια, Viviane Reding προσδιόρισε τη νέα στρατηγική για την ενίσχυση των κανόνων προστασίας προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης σε συνέντευξη Τύπου που παραχώρησε στις Βρυξέλλες: "Η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα ... για να μπορεί η Ευρωπαϊκή Ένωση να εγγυηθεί αυτό το δικαίωμα, χρειαζόμαστε σαφείς και συνεκτικούς κανόνες προστασίας των δεδομένων. Επίσης, απαιτείται η συμμόρφωση της ισχύουσας νομοθεσίας με τις τρέχουσες εξελίξεις στις νέες τεχνολογίες και την παγκοσμιοποίηση" [71].

Κατόπιν, ακολούθησε σχετική δημόσια διαβούλευση μέχρι τις 15 Ιανουαρίου 2011. Η Ευρωπαϊκή Επιτροπή έλαβε συνολικά 288 προτάσεις - διαβουλεύσεις από διάφορους δημόσιους και ιδιωτικούς οργανισμούς, ακόμα και από ιδιώτες. Η πλειονότητα των συμμετεχόντων στη διαβούλευση συμφώνησαν στην ανάγκη ενημέρωσης – προσαρμογής της ισχύουσας νομοθεσίας για την προστασία των προσωπικών δεδομένων των κατοίκων της Ευρωπαϊκής Ένωσης, προκειμένου να ανταποκρίνεται στη σύγχρονη τεχνολογική ανάπτυξη και την παγκοσμιοποίηση. Ειδικότερα, οι ιδιωτικοί οργανισμοί ζήτησαν την εναρμόνιση των υφιστάμενων κανονισμών, για να αποφευχθεί η διαφορετική αντιμετώπιση μεταξύ των κρατών μελών της Ένωσης σε θέματα προστασίας προσωπικών δεδομένων [72]. Όπως αναφέρει σχετικά η κα. Χρονοπούλου, σύμβουλος προστασίας δεδομένων παράταξης στο Ευρωπαϊκό Κοινοβούλιο: "είχαμε 27 διαφορετικές νομοθεσίες, σε ολόκληρη την ΕΕ. Ήταν ένα χάος, ανάλογες περιπτώσεις αντιμετωπίζονταν διαφορετικά σε δικαστήρια από διαφορετικά κράτη μέλη. Η κρίση των δικαστηρίων σε ανάλογες περιπτώσεις μπορούσε να είναι διαφορετική, συνεπώς υπήρχε ανάγκη πλήρης εναρμόνισης της νομοθεσίας προστασίας προσωπικών δεδομένων για όλα τα κράτη μέλη της Ένωσης" [73].

Ακολούθησαν σχετικές διαπραγματεύσεις μεταξύ των κρατών μελών και των αντίστοιχων φορέων της Ευρωπαϊκής Ένωσης για τέσσερα χρόνια, μέχρι την οριστικοποίηση του τελικού κειμένου του καινούργιου Κανονισμού και την έγκρισή του από το Ευρωπαϊκό Κοινοβούλιο.

Ο λόγος της μεγάλης καθυστέρησης οριστικοποίησης του τελικού κειμένου του Κανονισμού, οφείλονταν στις διαφορετικές απόψεις των πολιτικών παρατάξεων στο Ευρωπαϊκό Κοινοβούλιο για ορισμένες ειδικές διατάξεις του Κανονισμού. Ωστόσο, ο βασικός λόγος που λειτούργησε θετικά για την αμεσότερη οριστικοποίηση του τελικού κειμένου του Κανονισμού, ήταν οι αποκαλύψεις του Edward Snowden, που είχαν ως αποτέλεσμα τη μεγαλύτερη ευαισθητοποίηση των πολιτών και την απαίτηση από τους πολιτικά ιθύνοντες να λάβουν άμεσα μέτρα προστασίας για τους πολίτες της Ένωσης [73].

5.2 Αντικείμενο Κανονισμού

Στις 27 Απριλίου 2016 ψηφίστηκε ο νέος Ευρωπαϊκός Κανονισμός (General Data Protection Regulation - GDPR) για την προστασία των προσωπικών δεδομένων, ο οποίος από 25 Μαΐου 2018 αποκτά υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης χωρίς την ανάγκη της ψήφισης σχετικής νομοθεσίας από το κάθε κράτος μέλος, όπως ίσχυε με προηγούμενες αποφάσεις – συστάσεις της Ένωσης.

Αντικείμενο του νέου Κανονισμού είναι η προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από οργανισμούς, καθώς επίσης και οι αρχές της ελεύθερης κυκλοφορίας των δεδομένων αυτών. Ο νέος κανονισμός αντικαθιστά όσα ορίζονται στην οδηγία 95/46/EC, η οποία καταργείται. Σκοπός του νέου Κανονισμού είναι η προστασία όλων των πολιτών της ΕΕ από παραβιάσεις της ιδιωτικής τους ζωής και των προσωπικών τους δεδομένων. Η ισχύουσα σήμερα οδηγία (95/46/EC) ψηφίστηκε πριν από μια δεκαετία, οπότε το ποσοστό ενεργών χρηστών στο διαδίκτυο ήταν ιδιαίτερα περιορισμένο σε σχέση με σήμερα και δεν είχε καθιερωθεί ακόμα η εφαρμογή του επιχειρηματικού μοντέλου Επιτήρησης εκ μέρους των επιχειρήσεων στο διαδίκτυο. Συνεπώς, σκοπός του νέου Κανονισμού είναι η πληρέστερη προστασία των πολιτών. Ωστόσο, ο νέος Κανονισμός και η εφαρμογή ενιαίων κανόνων - νομοθεσίας εντός των κρατών μελών της ΕΕ, διευκολύνει την επιχειρηματικότητα στο διαδίκτυο, μειώνοντας τη

γραφειοκρατία και την ανάγκη προσαρμογής των παρεχόμενων υπηρεσιών ανά χώρα δραστηριοποίησης των επιχειρήσεων [74].

Ο καινούργιος Κανονισμός θα εφαρμόζεται στην περίπτωση που ο υπεύθυνος επεξεργασίας ή ο επεξεργαστής (οργανισμός) ή το υποκείμενο των δεδομένων (πρόσωπο) βρίσκεται εντός της επικράτειας της ΕΕ. Επιπλέον (και σε αντίθεση με την οδηγία 95/46/ΕC) ο νέος Κανονισμός θα εφαρμόζεται σε οργανισμούς που εδρεύουν εκτός της Ευρωπαϊκής Ένωσης, εφόσον η επεξεργασία των προσωπικών δεδομένων αφορά κατοίκους της ΕΕ. Τέλος, ο Κανονισμός δε θα εφαρμόζεται κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την εθνική ασφάλεια ενός κράτους ή την διευκόλυνση επιβολής του νόμου.

5.3 Λόγοι θέσπισης καινούργιου Κανονισμού

Όπως αναφέρεται στο προοίμιο, βασικοί παράγοντες που συντέλεσαν στην θέσπιση του καινούργιου Κανονισμού και ελήφθησαν υπόψη κατά τη σύνταξή του είναι:

Άρθρα του **Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης** και της **Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης** (ΣΛΕΕ) που αναφέρονται στην απαίτηση προστασίας από την επεξεργασία των προσωπικών δεδομένων των ατόμων. (1)

Επίσης, η προστασία των πολιτών δεν θα πρέπει να εξαρτάται από την **ιθαγένεια** ή τον **τόπο κατοικίας** των ατόμων. Ιδιαίτερη βαρύτητα δίνεται σε αυτό από τον Κανονισμό. (2)

Η προστασία των προσωπικών δεδομένων είναι σημαντική σε μια Πολιτεία, αλλά δε θα πρέπει αυτή να παρεμποδίζει την εκτέλεση βασικών υποχρεώσεων μιας Πολιτείας απέναντι στους πολίτες της, ενώ ο βαθμός προστασίας τους θα πρέπει να υλοποιείται με βάση την **αρχή της αναλογικότητας** σε σχέση με τα δικαιώματα άλλων πολιτών της Πολιτείας ή του ίδιου του ατόμου σε σχέση με τα προσωπικά τους δεδομένα. (4)

Η **ολοκλήρωση της οικονομίας** και η **ελεύθερη διακίνηση των ατόμων** εντός της Ένωσης έχουν ως αποτέλεσμα την αύξηση των ροών προσωπικών δεδομένων μεταξύ των κρατών μελών. Επιπροσθέτως, ανάλογη αύξηση υπάρχει και στις ανταλλαγές σχετικών δεδομένων μεταξύ δημοσίων και ιδιωτικών οργανισμών ή επιχειρήσεων εντός της Ένωσης. Σύμφωνα με το ισχύον νομικό πλαίσιο λειτουργίας της Ένωσης, τα κράτη μέλη είναι υποχρεωμένα να συνεργάζονται με σκοπό την αποτελεσματικότερη εκτέλεση των υποχρεώσεών τους απέναντι στους πολίτες ή για τη σχετική διευκόλυνση άλλων κρατών μελών. (5)

Η **εξέλιξη της τεχνολογίας** και η **παγκοσμιοποίηση** έχουν συμβάλει στην αύξηση της συλλογής δεδομένων προσωπικού χαρακτήρα από δημόσιους ή ιδιωτικούς φορείς. Ως συνέπεια, έχουν αυξηθεί σημαντικά οι ανάγκες ανταλλαγής σχετικών δεδομένων μεταξύ διαφόρων φορέων, καθιστώντας απαραίτητη τη διασφάλιση της ασφαλούς μεταφοράς των δεδομένων προσωπικού χαρακτήρα εντός της ΕΕ ή με άλλα κράτη εκτός της ΕΕ. (6)

Επιπροσθέτως, η ισχύουσα οδηγία 95/46/ΕΚ είχε ως αποτέλεσμα τη διαφοροποίηση της εφαρμογής προστασίας προσωπικών δεδομένων στα διάφορα κράτη μέλη της Ένωσης. Οι σχετικές **αποκλίσεις μεταξύ των κρατών μελών** επηρέασαν (i) τον **ελεύθερο ανταγωνισμό**, (ii) την **ελευθερία διακίνησης πληροφοριών**, καθώς επίσης και (iii) τις Αρχές στα διάφορα κράτη μέλη από την αποτελεσματική εκτέλεση των υποχρεώσεών τους. (9) Για αυτόν τον λόγο είναι απαραίτητη η **θέσπιση ενιαίων κανονισμών** προστασίας των προσωπικών δεδομένων από όλα τα κράτη μέλη της Ένωσης. (10) Για τον ίδιο λόγο απαιτείται η **θέσπιση ενιαίων προστίμων** ή ποινών κατά την παραβίαση του καινούργιου Κανονισμού σε όλα τα κράτη μέλη. (13)

5.4 Πεδίο εφαρμογής

Ο Κανονισμός 2016/679 ισχύει και για τους υπεύθυνους επεξεργασίας των δεδομένων και τους εκτελούντες την επεξεργασία τους. Οι ορισμοί περί υπευθύνων και εκτελούντων την επεξεργασία είναι ανάλογοι του σχετικού ορισμού στην οδηγία 95/46/ΕΚ - δηλαδή ο υπεύθυνος επεξεργασίας τεκμηριώνει πώς και γιατί γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο εκτελών την επεξεργασία ενεργεί για λογαριασμό του υπευθύνου επεξεργασίας..

Ο παρών Κανονισμός διευρύνει το εδαφικό πεδίο εφαρμογής των κανόνων προστασίας των δεδομένων, λαμβάνοντας υπόψη τόσο τον τόπο εγκατάστασης του υπευθύνου της επεξεργασίας δεδομένων, όσο τον τόπο κατοικίας του υποκειμένου των δεδομένων. Η σχετική νομοθεσία για την προστασία των προσωπικών δεδομένων εφαρμόζεται στις ακόλουθες περιπτώσεις (Άρθρο 3):

- όταν ο υπεύθυνος επεξεργασίας δεδομένων ή ο εκτελών της υλοποιεί την επεξεργασία για κάποιο πρόσωπο ή οργανισμό εντός της Ένωσης, ανεξαρτήτως την τοποθεσία - κράτος που λαμβάνει χώρα η σχετική επεξεργασία δεδομένων

- όταν ο υπεύθυνος επεξεργασίας δεδομένων ή ο εκτελών επεξεργασίας τους δεν έχει την έδρα του εντός της Ένωσης, αλλά προσφέρει προϊόντα ή υπηρεσίες σε κατοίκους της ΕΕ και / ή επεξεργάζεται προσωπικά δεδομένα με σκοπό την κατανόηση της συμπεριφοράς των ατόμων αυτών

- όταν ο υπεύθυνος επεξεργασίας δεδομένων ή ο εκτελών επεξεργασίας δεδομένων δεν έχει την έδρα του εντός της Ένωσης, αλλά σε περιοχή όπου εφαρμόζεται το δίκαιο κράτους μέλους που πρόκειται να συμπεριληφθεί στη δημόσια διεθνή νομοθεσία

Όπως διαπιστώνεται από τα παραπάνω ο Κανονισμός εφαρμόζεται όταν η επεξεργασία πραγματοποιείται από οργανισμούς που λειτουργούν εντός της ΕΕ, καθώς επίσης και σε οργανισμούς εκτός ΕΕ που προσφέρουν αγαθά ή υπηρεσίες σε ιδιώτες στην ΕΕ.

Ο Κανονισμός δεν εφαρμόζεται σε ορισμένες δραστηριότητες, συμπεριλαμβανομένης της επεξεργασίας που καλύπτεται από την οδηγία για την επιβολή του νόμου της Ένωσης (2016/680), όπως στην επεξεργασία για λόγους εθνικής ασφάλειας και σε αυτή που διενεργείται από ιδιώτες αποκλειστικά για παροχή προσωπικών υπηρεσιών ή υπηρεσιών σε νοικοκυριά.

Τέλος, ο Κανονισμός αφορά επεξεργασία (i) προσωπικών δεδομένων και (ii) ευαίσθητων προσωπικών δεδομένων κατοίκων της ΕΕ. Όπως διαπιστώνεται στην επόμενη ενότητα οι ορισμοί των κατηγοριών δεδομένων που εντάσσονται στις σχετικές κατηγορίες δεδομένων είναι διευρυμένες σε σχέση με την πρότερη οδηγία 95/46/ΕΚ της Ένωσης.

5.5 Νέος Κανονισμός και εθνική νομοθεσία

Όπως ορίζεται στο άρθρο 2 του Κανονισμού κατά την επεξεργασία προσωπικών δεδομένων "στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης" δεν εφαρμόζεται ο Κανονισμός 2016/679 αλλά εθνικές διατάξεις στα κράτη μέλη της Ένωσης.

Επίσης, όπως ορίζεται στο άρθρο 85 του Κανονισμού τα κράτη μέλη δύναται να θεσπίσουν εθνικές διατάξεις που θα καθορίζουν τα όρια του νέου Κανονισμού, με σκοπό την προάσπιση των δικαιωμάτων της πληροφόρησης και της έκφρασης. Στις σχετικές διατάξεις συγκαταλέγονται και εξαιρέσεις με εθνικές διατάξεις επεξεργασίας δεδομένων για ακαδημαϊκούς ή δημοσιογραφικούς σκοπούς.

Επιπροσθέτως, σύμφωνα με το άρθρο 86 του Κανονισμού πιθανή απόφαση πρόσβασης σε έγγραφα που είναι διαθέσιμα σε δημόσιους ή ιδιωτικούς φορείς για την υποστήριξη του δημοσίου, θα λαμβάνεται από εθνική νομοθεσία με γνώμονα την παράλληλη προστασία των προσωπικών δεδομένων σύμφωνα με τον καινούργιο Κανονισμό της Ένωσης.

Επίσης, όπως ορίζεται στο άρθρο 87 του Κανονισμού ο προσδιορισμός των προϋποθέσεων επεξεργασίας του αριθμού ταυτότητας των υποκειμένων των δεδομένων ή άλλου δεδομένου που χρησιμοποιείται ως αναγνωριστικό των ατόμων (πχ ΑΦΜ), μπορεί να πραγματοποιηθεί μόνο εφόσον ικανοποιεί τις προϋποθέσεις που θέτονται από την εθνική νομοθεσία των κρατών μελών.

Ακόμα, σύμφωνα με το άρθρο 88 το κάθε κράτος μέλος δύναται με εθνικές διατάξεις να προσδιορίσει τους κανόνες – προϋποθέσεις πρόσβασης και επεξεργασίας προσωπικών δεδομένων που σχετίζονται με την απασχόληση των ατόμων και την εργατική νομοθεσία κάθε κράτους μέλους. Με το άρθρο 88 το κάθε κράτος μέλος μπορεί να καθορίσει ξεχωριστά το επίπεδο προστασίας της ιδιωτικότητας των υπαλλήλων από τον οργανισμό που εργάζονται.

Επίσης, όπως ορίζεται στο άρθρο 89 του Κανονισμού το κάθε κράτος μέλος μπορεί να νομοθετήσει παρεκκλίσεις από τις διατάξεις του Κανονισμού, όταν η επεξεργασία δεδομένων πραγματοποιείται για επιστημονικούς σκοπούς, για στατιστικούς σκοπούς, για σκοπούς ιστορικής έρευνας ή για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον. Τέλος, αντίστοιχες προβλέψεις ψήφισης εθνικών διατάξεων για θέματα που άπτονται του απορρήτου της συλλογής και της επεξεργασίας δεδομένων σε σχέση με τις εξουσίες των ελεγκτικών αρχών (άρθρο 90) και του θρησκευτικού απορρήτου (άρθρο 91) είναι σε ισχύ σύμφωνα με τον καινούργιο Κανονισμό.

Ανάλογες προβλέψεις δυνατότητας ψήφισης εθνικών διατάξεων που θα ρυθμίζουν ανάλογα θέματα με όσα αναφέρθηκαν παραπάνω, ίσχυαν και στην πρότερη οδηγία 95/46/ΕΚ της Ένωσης.

5.6 Ορισμός προσωπικών δεδομένων

Σύμφωνα με το άρθρο 2 του Κανονισμού ως προσωπικά δεδομένα θεωρούνται "κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε

δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου".

Ο παραπάνω ορισμός περί προσωπικών δεδομένων δε μεταβάλλει σε ιδιαίτερο βαθμό τον ορισμό περί προσωπικών δεδομένων άλλων αποφάσεων ή οδηγιών της Ένωσης, διατηρώντας ουσιαστικά αμετάβλητο το πλαίσιο συμπερίληψης δεδομένων στην κατηγορία δεδομένων προσωπικού χαρακτήρα. Ωστόσο, η συμπερίληψη στον ορισμό της έννοιας δεδομένα θέσης (location data) θα απαιτήσει πρόσθετες υποχρεώσεις συμμόρφωσης σε διάφορες επιχειρήσεις – οργανισμούς (π.χ. επιχειρήσεις με αντικείμενο την προβολή διαδικτυακών διαφημίσεων, οι οποίες χρησιμοποιούν αρχεία cookies που επιτρέπουν την αναγνώριση της τοποθεσίας ενός χρήστη).

Σχετικά με την κατηγορία ευαίσθητων προσωπικών δεδομένων σύμφωνα με το άρθρο 9 του Κανονισμού εκείνα περιλαμβάνουν "δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό".

Ο παραπάνω ορισμός περί ευαίσθητων προσωπικών δεδομένων δε μεταβάλλει σε ιδιαίτερο βαθμό τον ορισμό περί ευαίσθητων προσωπικών δεδομένων άλλων αποφάσεων ή οδηγιών της Ένωσης, διατηρώντας ουσιαστικά αμετάβλητο το πλαίσιο συμπερίληψης δεδομένων στη σχετική κατηγορία δεδομένων. Ωστόσο, η συμπερίληψη στον ορισμό των γενετικών δεδομένων θα απαιτήσει πρόσθετες υποχρεώσεις συμμόρφωσης σε διάφορες επιχειρήσεις – οργανισμούς που διατηρούν ή επεξεργάζονται σχετικά δεδομένα.

Ο ορισμός περί προσωπικών δεδομένων είναι σημαντικός, καθώς ο καινούργιος Κανονισμός της ΕΕ ισχύει μόνο για τα προσωπικά δεδομένα. Δεδομένα ή πληροφορίες που δεν εμπίπτουν στον ορισμό των δεδομένων προσωπικού χαρακτήρα δεν υπόκειται στη νομοθετική προστασία που ορίζει ο Κανονισμός 2016/679 της ΕΕ. Επίσης, ο ορισμός περί ευαίσθητων προσωπικών δεδομένων καθορίζει τα δεδομένα προσωπικού χαρακτήρα για τα οποία έχουν εφαρμογή οι σχετικές διατάξεις περί επεξεργασίας και προστασίας ευαίσθητων προσωπικών δεδομένων του Κανονισμού.

5.7 Αρχές επεξεργασίας προσωπικών δεδομένων

Σύμφωνα με το Άρθρο 5 του Κανονισμού η επεξεργασία των προσωπικών δεδομένων θα πρέπει απαραιτήτως να διέπεται από τις εξής αρχές:

- **Νομιμότητα, αντικειμενικότητα και διαφάνεια**: η επεξεργασία των προσωπικών δεδομένων θα πρέπει να είναι σε συμφωνία με την ισχύουσα νομοθεσία, να υπάρχει αμεροληψία κατά την επεξεργασία τους και να γίνεται με τρόπο διαφανή προς το άτομο του οποίου γίνεται η επεξεργασία των προσωπικών του δεδομένων. Στην πρότερη αντίστοιχη αρχή επεξεργασίας προσωπικών δεδομένων σε οδηγία της ΕΕ (95/46/ΕΚ) γινόταν αναφορά σε θεμιτή και σύννομη επεξεργασία προσωπικών δεδομένων. Πλέον, ουσιαστικά ο νέος Κανονισμός αναφέρεται στην πρόσθετη φροντίδα συμμόρφωσης για τους οργανισμούς κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

- **Περιορισμός του σκοπού**: τα δεδομένα θα πρέπει να συλλέγονται αποκλειστικά για τον σκοπό που προορίζονται. Οποιαδήποτε περαιτέρω επεξεργασία τους για άλλους σκοπούς θεωρείται παράνομη δραστηριότητα. Η σχετική αρχή δε διαφοροποιείται σημαντικά σε σχέση με την αντίστοιχη αρχή που ορίζονταν στην οδηγία 95/46/ΕΚ, με τη μόνη διαφοροποίηση να σχετίζεται με τις εξαιρέσεις επεξεργασίας προσωπικών δεδομένων για περαιτέρω σκοπούς όπως ορίζονται στο άρθρο 89 του Κανονισμού.

- **Ελαχιστοποίηση των δεδομένων**: τα δεδομένα που συλλέγονται είναι τα απολύτως απαραίτητα για την επίτευξη του σκοπού συλλογής τους, χωρίς τη συμπερίληψη μη σχετικών προσωπικών δεδομένων. Η μόνη διαφοροποίηση της σχετικής αρχής σε σχέση με την οδηγία 95/46/ΕΚ, έγκειται στην αλλαγή του όρου "υπερβολικά δεδομένα" (excessive) με "μη σχετικά δεδομένα" (what is necessary) προσωπικού χαρακτήρα, η οποία θα απαιτήσει μια εν μέρει επανεξέταση των προσωπικών δεδομένων που αποθηκεύονται από τους διάφορους οργανισμούς.

- **Ακρίβεια δεδομένων**: μη ακριβή δεδομένα θα πρέπει να διαγράφονται ή να τροποποιούνται άμεσα. Επίσης, θα πρέπει να υπάρχει η δυνατότητα τροποποίησης των δεδομένων ανά πάσα στιγμή προκειμένου να είναι ακριβή. Η σχετική αρχή δε διαφοροποιείται σε σχέση με την οδηγία 95/46/ΕΚ, απλά

προστίθεται ο όρος "χωρίς καθυστέρηση" σχετικά με τις ενέργειες ενημέρωσης δεδομένων χωρίς ακρίβεια από έναν οργανισμό.

- **Περιορισμός της περιόδου αποθήκευσης**: τα προσωπικά δεδομένα διατηρούνται μονάχα για το χρονικό διάστημα που καθορίζεται από τον σκοπό σύστασής τους και όχι για περισσότερο. Διαφοροποίηση της σχετικής αρχής σε σχέση με την οδηγία 95/46/ΕΚ, υπάρχει σε συνδυασμό με το άρθρο 9 του Κανονισμού, που επιτρέπει σε άτομα να ζητήσουν τη διαγραφή προσωπικών τους δεδομένων, πριν το πέρας του αρχικά προσδιοριζόμενου χρόνου αποθήκευσής τους.

- **Ακεραιότητα και εμπιστευτικότητα**: τα προσωπικά δεδομένα προστατεύονται επαρκώς κατά την επεξεργασία και την αποθήκευσή τους από πιθανά αθέμιτη τροποποίησή τους, από καταστροφή ή φθορά. Επίσης, η σχετική αρχή επεξεργασίας προσωπικών δεδομένων δε διαφοροποιείται σημαντικά σε σχέση με την οδηγία 95/46/ΕΚ.

Επιπροσθέτως, για να θεωρηθεί μια επεξεργασία προσωπικών δεδομένων νόμιμη θα πρέπει (άρθρο 6):

- να υπάρχει η συγκατάθεση του υποκειμένου των δεδομένων

- να υπάρχει νόμιμη βάση για την πραγματοποίηση της επεξεργασίας δεδομένων

- η επεξεργασία των δεδομένων να είναι προϋπόθεση για την εκτέλεση σύμβασης που το υποκείμενο δεδομένων είναι συμβαλλόμενο μέλος ή αποτελούν αίτημα του υποκειμένου πριν τη σχετική σύναψη συμφωνίας

- να έχει ήδη πραγματοποιηθεί η επεξεργασία προσωπικών δεδομένων για να συμβεί εκπλήρωση νομικών υποχρεώσεων του υπεύθυνου επεξεργασίας των δεδομένων

- η επεξεργασία των δεδομένων να είναι απαραίτητη για την προστασία ζωτικού συμφέροντος είτε για τον υπεύθυνο επεξεργασίας ή άλλο πρόσωπο

- η επεξεργασία των προσωπικών δεδομένων να αποτελεί προυπόθεση για την προάσπιση του δημοσίου συμφέροντος

5.8 Συγκατάθεση του υποκειμένου των δεδομένων

Σύμφωνα με το Άρθρο 6 (1) του Κανονισμού προκειμένου μια επεξεργασία δεδομένων να είναι σύννομη απαιτείται η σχετική συγκατάθεση του υποκειμένου των δεδομένων. Ο σχετικός παράγοντας δε διαφοροποιείται σε σχέση με την οδηγία 95/46/ΕΚ, ωστόσο τίθενται αυστηρότερες προϋποθέσεις στην υπόθεση πως κάποιος οργανισμός έχει λάβει τη σχετική συγκατάθεση του υποκειμένου των δεδομένων ή στην περίπτωση νομιμοποίησης της επεξεργασίας των δεδομένων χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων.

Σύμφωνα με το άρθρο 4 (11) η συγκατάθεση του υποκειμένου των δεδομένων ορίζεται ως "κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν".

Επιπροσθέτως, στο Άρθρο 7 του Κανονισμού δηλώνεται πως ο υπεύθυνος της επεξεργασίας δεδομένων θα πρέπει να μπορεί να αποδείξει ότι έχει λάβει τη συγκατάθεση του υποκειμένου των δεδομένων. Επίσης, η περιγραφή της δήλωσης συγκατάθεσης θα πρέπει να είναι διατυπωμένη σε απλή γλώσσα και να ορίζει με σαφήνεια τα θέματα για τα οποία δίνεται η συγκατάθεση.

Το υποκείμενο των δεδομένων διατηρεί το δικαίωμα ανάκλησης της συγκατάθεσης που έχει δώσει στον υπεύθυνο επεξεργασίας των δεδομένων σε δεύτερο χρόνο στο μέλλον. Η σχετική διαδικασία θα πρέπει να είναι εξίσου απλή, όσο και η διαδικασία παροχής της αρχικής συγκατάθεσης επεξεργασίας των προσωπικών του δεδομένων.

Επίσης, ο Κανονισμός απαιτεί η συγκατάθεση να δίνεται ελεύθερα και να μην συνδέεται άμεσα με την παροχή υπηρεσιών από έναν οργανισμό, με την προϋπόθεση της συγκατάθεσης των προσωπικών δεδομένων του υποκειμένου ειδικά όταν η εν λόγω υπηρεσία δεν σχετίζεται άμεσα με τα συμφέροντα του υποκειμένου.

Επιπροσθέτως, σύμφωνα με τον καινούργιο Κανονισμό, η μη δήλωση συγκατάθεσης του χρήστη σε επεξεργασία προσωπικών δεδομένων, δεν συνεπάγεται αυτόματα τη σιωπηλή συγκατάθεση του χρήστη. Πιο συγκεκριμένα δηλώνεται με σαφήνεια στην παράγραφο 32 του σκεπτικού σύνταξης του Κανονισμού ότι "η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δε θα πρέπει να εκλαμβάνονται ως συγκατάθεση". Όσον αφορά τη σιωπηλή συγκατάθεση του υποκειμένου των δεδομένων η πρότερη οδηγία (95/46/ΕΚ) της Ένωσης δε περιλάμβανε κάποια σχετική δήλωση – διευκρίνηση.

Επιπλέον, ο καινούργιος Κανονισμός στο Άρθρο 49 με σαφήνεια δηλώνει πως η συγκατάθεση του χρήστη δεν απαιτείται μονάχα για την επεξεργασία των δεδομένων, αλλά και για πιθανή μεταφορά τους σε κράτη εκτός της Ένωσης, έχοντας προηγουμένως ενημερώσει τα σχετικά πρόσωπα για πιθανούς κινδύνους που ελλοχεύουν.

Τέλος, όπως δηλώνεται στο Άρθρο 171, υπεύθυνοι επεξεργασίας δεδομένων που διατηρούν ήδη αποθηκευμένα δεδομένα κατόπιν εξασφάλισης της συγκατάθεσης του χρήστη δεν απαιτείται να λάβουν εκ νέου νέα συγκατάθεσή του για χρήση τους στο μέλλον. Ωστόσο, οι υπεύθυνοι επεξεργασίας προσωπικών δεδομένων θα πρέπει να είναι σε θέση να αποδείξουν πως η συγκατάθεση του χρήστη που ήδη διαθέτουν έχει ληφθεί σύμφωνα με όσα ορίζονται στον Κανονισμό. Πρακτικά, το σχετικό άρθρο θα απαιτήσει από αρκετούς υπεύθυνους επεξεργασίας δεδομένων να αναζητήσουν εκ νέου τη συγκατάθεση των υποκειμένων των δεδομένων, καθώς δε θα μπορούν να αποδείξουν πως η συγκατάθεση του χρήστη που ήδη διαθέτουν έχει προέρθει σύμφωνα με όσα ορίζονται στον καινούργιο Κανονισμό.

5.9 Δικαιώματα του υποκειμένου των δεδομένων

Σύμφωνα με τον Κανονισμό το υποκείμενο των δεδομένων διαθέτει τα εξής δικαιώματα :

Δικαίωμα πρόσβασης (Άρθρο 15): να λάβει γνώση από τον υπεύθυνο επεξεργασίας αν υφίστανται την όποια επεξεργασία τα προσωπικά του δεδομένα. Στην περίπτωση που υφίστανται σχετική επεξεργασία, το υποκείμενο των δεδομένων διατηρεί το δικαίωμα ενημέρωσης περί:

- του σκοπού της επεξεργασίας
- των κατηγοριών των προσωπικών δεδομένων που αποτελούν αντικείμενο της επεξεργασίας
- των ατόμων ή των οργανισμών στους οποίους κοινοποιούνται τα αποτελέσματα της επεξεργασίας
- της διάρκειας αποθήκευσης των δεδομένων προσωπικού χαρακτήρα του υποκειμένου ή των παραγόντων που καθορίζουν τη σχετική χρονική διάρκεια

- της δυνατότητας υποβολής αιτήματος προς τον υπεύθυνο επεξεργασίας για την τροποποίηση των δεδομένων, τη διαγραφή τους ή την απαίτηση διακοπής της επεξεργασίας δεδομένων από τον υπεύθυνο επεξεργασίας

- της δυνατότητας καταγγελίας σε εποπτικές αρχές

- της προέλευσης των δεδομένων, όταν τα δεδομένα δεν έχουν συλλεχθεί από τον υπεύθυνο επεξεργασίας

- των πληροφοριών σχετικά με την αιτιολογία κάθε αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που έχει σημαντική επίδραση στο υποκείμενο των δεδομένων.

Συγκρίνοντας το δικαίωμα της πρόσβασης όπως ορίζεται στον καινούργιο Κανονισμό με το αντίστοιχο δικαίωμα, όπως εκείνο ορίζονταν στην οδηγία 95/46/ΕΚ, διαπιστώνεται διεύρυνση των κατηγοριών των πληροφοριών πρόσβασης για το υποκείμενο των δεδομένων. Το γεγονός αυτό αναμένεται να επιφέρει απαιτήσεις εκ μέρους των οργανισμών ή επιχειρήσεων για επιπρόσθετη εργασία για την ικανοποίηση πιθανών σχετικών αιτημάτων των ατόμων.

Δικαίωμα διόρθωσης (Άρθρο 16): το υποκείμενο των δεδομένων, όπως προβλέπονταν και από την οδηγία 95/46/ΕΚ, διατηρεί το δικαίωμα απαίτησης διόρθωσης ή διαγραφής ανακριβών ή ελλιπών στοιχείων που αφορούν τα προσωπικά του δεδομένα.

Δικαίωμα διαγραφής (δικαίωμα στη λήθη) (Άρθρο 17): υπάρχει η δυνατότητα υποβολής προς τον υπεύθυνο επεξεργασίας αιτήματος διαγραφής προσωπικών δεδομένων όταν:

- δεν απαιτούνται πλέον τα δεδομένα αυτά για την εκπλήρωση του αρχικού σκοπού συλλογής τους

- το υποκείμενο των δεδομένων ανακαλεί την άδεια επεξεργασίας που έχει παραχωρήσει στον υπεύθυνο επεξεργασίας

- το υποκείμενο των δεδομένων ασκεί το δικαίωμα αντίρρησης επί της επεξεργασίας των προσωπικών του δεδομένων (σύμφωνα με όσα ορίζονται στο Άρθρο 21), όταν ο ελεγκτής δεν έχει επιτακτικούς λόγους για τη συνέχιση της επεξεργασίας

- η επεξεργασία των δεδομένων δεν είναι σύννομη
- η διαγραφή των δεδομένων είναι απαραίτητη σύμφωνα με τους νόμους της ΕΕ ή τη νομοθεσία του αντίστοιχου κράτους μέλους

Συγκρίνοντας το δικαίωμα της διαγραφής όπως ορίζεται στον καινούργιο Κανονισμό με το αντίστοιχο δικαίωμα, όπως εκείνο ορίζονταν στην οδηγία 95/46/ΕΚ, διαπιστώνεται διεύρυνση των περιπτώσεων που μπορεί το υποκείμενο των δεδομένων να απαιτήσει τη διαγραφή τους. Το γεγονός αυτό αναμένεται να επιφέρει απαιτήσεις εκ μέρους των οργανισμών ή επιχειρήσεων για επιπρόσθετη εργασία για την ικανοποίηση πιθανών σχετικών αιτημάτων των ατόμων.

Δικαίωμα περιορισμού της επεξεργασίας (Άρθρο 18): το υποκείμενο των δεδομένων διατηρεί το δικαίωμα να ζητήσει τον περιορισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, πράγμα που σημαίνει ότι τα δεδομένα μπορούν να διατηρούνται αποθηκευμένα μονάχα από τον ελεγκτή και επιτρέπεται περιορισμένη επεξεργασία τους. Ο περιορισμός της επεξεργασίας προσωπικών δεδομένων μπορεί να ζητηθεί από το υποκείμενο δεδομένων όταν:

- αμφισβητείται από το υποκείμενο των δεδομένων η ακρίβειά τους, για το χρονικό διάστημα που απαιτείται μέχρι την επαλήθευση της ακρίβειας
- η επεξεργασία των δεδομένων είναι παράνομη και το υποκείμενο των δεδομένων ζητάει αντί της διαγραφής τους, τον περιορισμό των σκοπών επεξεργασίας τους
- δεν είναι πλέον απαραίτητη η επεξεργασία των δεδομένων για τον αρχικό σκοπό συλλογής τους. Ωστόσο, το υποκείμενο δεδομένων μπορεί να απαιτήσει τη διατήρηση των δεδομένων για τη διεκδίκηση νομικών απαιτήσεων από τον υπεύθυνο επεξεργασίας των δεδομένων ή άλλα πρόσωπα – οργανισμούς.
- Εκκρεμεί η επαλήθευση αιτήματος του υποκειμένου, σύμφωνα με όσα ορίζονται στο Άρθρο 21 περί διακοπής της επεξεργασίας των δεδομένων, όταν συντρέχουν λόγοι που απαιτούν την άμεση διακοπή της επεξεργασίας τους ή τη συνέχιση επεξεργασίας τους σύμφωνα με τη σχετική τεκμηρίωση του υπεύθυνου επεξεργασίας των δεδομένων

Εφόσον εξασφαλιστεί ο περιορισμός της επεξεργασίας των δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει το υποκείμενο των δεδομένων σε περίπτωση άρσης του περιορισμού, για λόγους δημοσίου συμφέροντος ή για την διεκδίκηση νομικών απαιτήσεων.

Το δικαίωμα περιορισμού της επεξεργασίας, όπως ορίζεται στο Άρθρο 18 προσθέτει επιπρόσθετες εργασίες για τους φορείς – οργανισμούς που επεξεργάζονται προσωπικά δεδομένα σε σχέση με όσα ορίζονταν στην οδηγία 95/46/ΕΚ.

Υποχρεωτική γνωστοποίηση διαφοροποίησης κατάστασης προσωπικών δεδομένων (Άρθρο 19): ο υπεύθυνος επεξεργασίας των δεδομένων υποχρεούται να ενημερώσει κάθε τρίτο πρόσωπο ή οργανισμό στον οποίο έχουν γνωστοποιηθεί τα προσωπικά δεδομένα που έχουν τροποποιηθεί, διαγραφεί ή βρίσκονται σε κατάσταση περιορισμού επεξεργασίας σύμφωνα με τα άρθρα 16, 17 και 18. Ο υπεύθυνος επεξεργασίας διατηρεί το δικαίωμα να μην προχωρήσει σε σχετική γνωστοποίηση αν κάτι τέτοιο κρίνεται μη εφικτό ή συνεπάγεται δυσανάλογη προσπάθεια. Επιπροσθέτως, το υποκείμενο δεδομένων διατηρεί το δικαίωμα ενημέρωσης σχετικών τρίτων προσώπων ή οργανισμών, εφόσον υπάρξει αίτημά τους προς τον υπεύθυνο επεξεργασίας των δεδομένων. Η σχετική υποχρέωση του υπευθύνου συλλογής και επεξεργασίας των δεδομένων προσθέτει επιπλέον εργασίες ανάπτυξης και διατήρησης συστήματος αυτοματοποιημένης ενημέρωσης των τρίτων προσώπων ή φορέων στους οποίους γνωστοποιούνται προσωπικά στοιχεία που έχουν συλλεχθεί από τον υπεύθυνο επεξεργασίας.

Δικαίωμα στη φορητότητα των δεδομένων (Άρθρο 20): το υποκείμενο των δεδομένων διατηρεί το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας δεδομένων να λάβει αντίγραφό τους σε μορφή αναγνώσιμη από μηχανή με σκοπό τη μεταφορά τους σε άλλον υπεύθυνο επεξεργασίας δεδομένων ή την αυτοματοποιημένη μεταφορά τους σε άλλον υπεύθυνο επεξεργασίας δεδομένων.

Ομοίως, με άλλα δικαιώματα του υποκειμένου που αναφέρθηκαν παραπάνω, το δικαίωμα στη φορητότητα δεδομένων απαιτεί επιπρόσθετες επενδύσεις εκ μέρους των υπευθύνων επεξεργασίας των δεδομένων σε σχέση με την οδηγία 95/46/ΕΚ, καθώς επίσης και επιπρόσθετες εργασίες εκ μέρους τους.

Ωστόσο, το συγκεκριμένο δικαίωμα του υποκειμένου των δεδομένων αναμένεται να λειτουργήσει θετικά υπέρ του ανταγωνισμού και συμβάλει στον περιορισμό εμποδίων αλλαγής παρόχου λήψης υπηρεσιών στο διαδίκτυο.

Δικαίωμα εναντίωσης (Άρθρο 21): το υποκείμενο των δεδομένων διατηρεί το δικαίωμα ανά πάσα στιγμή να ζητήσει από τον υπεύθυνο επεξεργασίας τη διακοπή της επεξεργασίας προσωπικών του δεδομένων. Σε αυτή την περίπτωση, αν ο υπεύθυνος επεξεργασίας δε μπορεί να αποδείξει πως θα πρέπει να συνεχιστεί η δυνατότητα επεξεργασίας των σχετικών δεδομένων για ιδιαίτερα σοβαρούς λόγους για την επιχείρηση ή ότι συντρέχουν νομικοί λόγοι υπέρ της συνέχισης επεξεργασίας των δεδομένων, τότε θα πρέπει να διακοπεί άμεσα οποιαδήποτε επεξεργασία των δεδομένων του υποκειμένου.

Η αναγνώριση του συγκεκριμένου δικαιώματος για το υποκείμενο των δεδομένων, θα δημιουργήσει προβλήματα σε αρκετούς υπεύθυνους επεξεργασίας προσωπικών δεδομένων σχετικά με την τεκμηρίωση της δυνατότητας συνέχισης πιθανής επεξεργασίας των υποκειμένων, αν ζητήσει το αντίθετο το υποκείμενο δεδομένων. Όσον αφορά την οδηγία 95/46/ΕΚ, υπήρχε μεγαλύτερη ευκολία των υπευθύνων επεξεργασίας των δεδομένων να συνεχίσουν την επεξεργασία δεδομένων, παρά την εναντίωση του υποκειμένου δεδομένων επικαλούμενοι έννομα συμφέροντα του υπεύθυνου επεξεργασίας.

Επιπροσθέτως, με τον νέο Κανονισμό δηλώνεται η υποχρέωση του υπεύθυνου επεξεργασίας, για τη σχετική ενημέρωση του υποκειμένου σχετικά με το δικαίωμα εναντίωσης της επεξεργασίας προσωπικών του δεδομένων.

5.10 Υποχρεώσεις υπεύθυνου επεξεργασίας δεδομένων

Σύμφωνα με τον Κανονισμό, υπεύθυνος επεξεργασίας των δεδομένων θεωρείται "το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους". Ο σχετικός ορισμός είναι σε συμφωνία με τον πρότερο σχετικό ορισμό στην οδηγία 95/46/ΕΚ.

Η βασική υποχρέωση του υπεύθυνου επεξεργασίας δεδομένων είναι η τήρηση όσων αναφέρονται στον Κανονισμό περί προστασίας προσωπικών δεδομένων της Ένωσης. Επιπροσθέτως, σε σχέση με την οδηγία 95/46/ΕΚ, ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τον καινούργιο Κανονισμό της Ένωσης (Άρθρο 5). Επίσης, στο άρθρο 24 γίνεται αναφορά σε

τρόπους που δύναται να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας δεδομένων, προκειμένου να αποδείξει τη συμμόρφωσή του με όσα αναφέρονται στον καινούργιο σχετικό Κανονισμό της ΕΕ.

Επιπροσθέτως, το Άρθρο 25 του Κανονισμού απαιτεί από τους υπευθύνους επεξεργασίας των δεδομένων τη σχεδίαση των διαδικασιών συλλογής και επεξεργασίας δεδομένων με βάση τις Αρχές προστασίας προσωπικών δεδομένων που αναφέρθηκαν παραπάνω (Ενότητα 5.4). Δηλαδή, ο Κανονισμός απαιτεί από τους υπεύθυνους επεξεργασίας όχι μόνο τη συμμόρφωσή τους στις Αρχές του Κανονισμού κατά τη συλλογή ή την επεξεργασία των δεδομένων, αλλά και την εξ αρχής σχεδίαση (design by default) των διαδικασιών με γνώμονα τη συμμόρφωσή τους προς τις σχετικές Αρχές προστασίας.

Το Άρθρο 30 του Κανονισμού υποχρεώνει τον υπεύθυνο επεξεργασίας περί της διατήρησης αρχείων σχετικά με:

- τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας δεδομένων
- τους σκοπούς της σχετικής επεξεργασίας δεδομένων
- τις κατηγορίες των υποκειμένων δεδομένων
- τις κατηγορίες των δεδομένων που αποτελούν αντικείμενο επεξεργασίας
- τις προβλεπόμενες προθεσμίες διαγραφής των δεδομένων, εφόσον μπορούν να εκτιμηθούν
- τα πρόσωπα – οργανισμούς στους οποίους τα αποτελέσματα της σχετικής επεξεργασίας δεδομένων θα κοινοποιηθούν
- τις εγγυήσεις που πάρθηκαν περί πιθανών σχετικών κοινοποιήσεων σε πρόσωπα – οργανισμούς εκτός της Ένωσης
- την περιγραφή σχετικών μέτρων προστασίας των δεδομένων

Η υποχρέωση διατήρησης σχετικού αρχείου εκ μέρους του υπεύθυνου επεξεργασίας και η διαθεσιμότητά του προς διαβίβαση στην αρμόδια εποπτική αρχή, δεν επιβαρύνει επιπρόσθετα τους οργανισμούς, καθώς με την οδηγία 95/46/ΕΚ οι υπεύθυνοι επεξεργασίας δεδομένων ήταν υποχρεωμένοι να καταθέσουν σχετικά αρχεία στην εποπτική αρχή πριν την έναρξη επεξεργασίας των δεδομένων.

Επιπροσθέτως, η σχετική υποχρέωση δεν είναι απαραίτητη για οργανισμούς – υπεύθυνους επεξεργασίας που απασχολούν λιγότερους από 250 υπαλλήλους, εκτός και αν:

- υπάρχει κίνδυνος των ελευθεριών ή των δικαιωμάτων των υποκειμένων των δεδομένων από την αντίστοιχη επεξεργασία
- η σχετική επεξεργασία δεδομένων δεν είναι περιστασιακή
- η επεξεργασία περιλαμβάνει ευαίσθητα προσωπικά δεδομένα
- η επεξεργασία αναφέρεται σε ποινικά αδικήματα

Επίσης, σύμφωνα με το Άρθρο 31 ο υπεύθυνος επεξεργασίας δεδομένων είναι υποχρεωμένος να συνεργάζεται με την εθνική εποπτική αρχή για την εκπλήρωση των υποχρεώσεών του. Η σχετική πρόβλεψη δε δηλώνονταν με σαφήνεια στην οδηγία 95/46/ΕΚ. Ωστόσο, υπήρχε σχετική νομική πρόβλεψη στα περισσότερα κράτη – μέλη της Ένωσης.

Επιπροσθέτως, το άρθρο 32 ορίζει δυνατούς τρόπους που δύναται να εφαρμόσει ο υπεύθυνος επεξεργασίας δεδομένων για τη διασφάλιση της ασφάλειας των δεδομένων, κάτι που δεν αναφέρονταν με αντίστοιχη σαφήνεια στην οδηγία 95/46/ΕΚ. Σχετικοί τρόποι – μέθοδοι προστασίας των δεδομένων μπορούν να αποτελούν:

- η κρυπτογράφηση δεδομένων
- η διατήρηση αντιγράφων ασφαλείας και ανάκτησης δεδομένων
- η τακτική αναθεώρηση των τεχνικών - πολιτικών ασφαλείας
- η απαίτηση διασφάλισης της ακεραιότητας, του απόρρητου επικοινωνίας και της διαθεσιμότητας των δεδομένων

Επίσης, σύμφωνα με το Άρθρο 33 ο υπεύθυνος επεξεργασίας των δεδομένων είναι υποχρεωμένος αν υποπέσει στην αντίληψή του πιθανή παραβίαση της ασφάλειας προσωπικών δεδομένων των υποκειμένων, να ενημερώσει σχετικά την αρμόδια εποπτική αρχή εντός 72 ωρών, εκτός αν κρίνεται πως η εν λόγω παραβίαση δεν επηρεάζει κάποια ελευθερία ή δικαιώματα του υποκειμένου. Η ενημέρωση προς την εποπτική αρχή θα πρέπει να περιλαμβάνει πληροφορίες σχετικά με τις συνέπειες της παραβίασης των δεδομένων και τους τρόπους αύξησης της προστασίας των σχετικών πληροφοριών. Σύμφωνα με το ίδιο άρθρο αν δεν ενημερώσει εντός 72 ωρών την

αρμόδια εποπτική αρχή θα πρέπει παράλληλα να αιτιολογήσει την καθυστέρηση αυτή της ενημέρωσης. Το σχετικό άρθρο αυξάνει ιδιαίτερα τις απαιτήσεις προστασίας εκ μέρους των υπευθύνων επεξεργασίας, οι οποίοι καλούνται σε 72 ώρες να εντοπίσουν, να τεκμηριώσουν και εγγράφως να ενημερώσουν σχετικά την εποπτική αρχή. Η πρότερη οδηγία 95/46/ΕΚ της Ένωσης δεν περιλάμβανε σχετική υποχρέωση των υπευθύνων επεξεργασίας των δεδομένων και τον σχετικό χρονικό περιορισμό ενημέρωσης. Ωστόσο, ορισμένα κράτη μέλη είχαν συμπεριλάβει στην εθνική νομοθεσία τους σχετικές υποχρεώσεις για τους υπεύθυνους επεξεργασίας των δεδομένων.

Ακόμα, σύμφωνα με το Άρθρο 34 ο υπεύθυνος επεξεργασίας των δεδομένων, είναι υποχρεωμένος, αν κρίνεται πως μια παραβίαση προσωπικών δεδομένων δύναται να επιφέρει υψηλό κίνδυνο στο υποκείμενο των δεδομένων, να ενημερώσει άμεσα το υποκείμενο των δεδομένων. Η σχετική ενημέρωση θα πρέπει να περιγράφει με σαφήνεια τη φύση της παραβίασης και να περιλαμβάνει τις πληροφορίες που έχει κοινοποιήσει ο υπεύθυνος επεξεργασίας στην εποπτική αρχή, όπως περιγράφονται στο Άρθρο 33. Ωστόσο, ο υπεύθυνος επεξεργασίας δεν είναι υποχρεωμένος να ενημερώσει το υποκείμενο των δεδομένων όταν:

- δεν είναι δυνατή η χρήση των δεδομένων που υποκλάπηκαν, λόγω μέτρων ασφαλείας που εφαρμόζει στα αποθηκευμένα δεδομένα ο υπεύθυνος επεξεργασίας (πχ κρυπτογράφηση)

- έλαβε μέτρα εκ των υστέρων που δεν καθιστούν τη σχετική παραβίαση υψηλού κινδύνου για το υποκείμενο των δεδομένων

- η σχετική ενημέρωση περιλαμβάνει δυσανάλογες προσπάθειες εκ μέρους του υπεύθυνου επεξεργασίας

Η σχετική υποχρέωση για τους υπευθύνους επεξεργασίας των δεδομένων, τους επιβαρύνει με επιπλέον εργασίες και επιπροσθέτως υπάρχει ο κίνδυνος να επηρεαστεί αρνητικά η επωνυμία του υπεύθυνου επεξεργασίας από την κοινοποίηση σχετικών παραβιάσεων δεδομένων.

Ένας νέος όρος που εισάγεται με τον καινούργιο Κανονισμό, αφορά τους από κοινού υπεύθυνους επεξεργασίας, όταν στον καθορισμό των σκοπών και των μέσων επεξεργασίας των δεδομένων συμμετέχουν δυο ή περισσότεροι υπεύθυνοι επεξεργασίας. Σε αυτή την περίπτωση θα πρέπει να είναι καθορισμένες με σαφήνεια

οι αρμοδιότητες και οι ευθύνες του κάθε υπεύθυνου επεξεργασίας που συμμετέχει σε μια από κοινού επεξεργασία δεδομένων. Ένα υποκείμενο δεδομένων σε περίπτωση παραβίασης των διατάξεων του νέου Κανονισμού, μπορεί να προσφύγει ενάντια και σε μεμονωμένο υπεύθυνο επεξεργασίας δεδομένων.

Επίσης, όπως ορίζεται στο άρθρο 27 του Κανονισμού όταν ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων κατοίκων της Ευρωπαϊκής Ένωσης έχει την έδρα του εκτός της Ένωσης είναι υποχρεωμένος να ορίσει εκπρόσωπό του εντός της εδαφικής επικράτειας της Ένωσης. Ενώ με την οδηγία 95/46/ΕΚ ο σχετικός εκπρόσωπος δεν είχε κάποια ευθύνη για τυχόν παραβιάσεις όσων ορίζονταν στην οδηγία από τον υπεύθυνο επεξεργασίας, η σχετική έλλειψη ευθύνης δεν ισχύει για παραβιάσεις των διατάξεων του καινούργιου Κανονισμού. Η σχετική ευθύνη των οργανισμών εντός της Ένωσης που λειτουργούν ως αντιπρόσωποι υπευθύνων επεξεργασίας με έδρα σε χώρες εκτός της Ένωσης, θα έχει ως αποτέλεσμα εκείνοι οι οργανισμοί να είναι ιδιαίτερα προσεκτικοί κατά την ανάληψη σχετικών υποχρεώσεων και την απαίτηση δέσμευσής τους με ρήτρες περί τήρησης των διατάξεων του νέου Κανονισμού.

Τέλος, όπως ορίζεται στον καινούργιο Κανονισμό και πιο συγκεκριμένα στο άρθρο 35 πριν την έναρξη μιας επεξεργασίας δεδομένων είναι απαραίτητη η υποβολή προς την αντίστοιχη εποπτική αρχή εκτίμησης των επιπτώσεων από την επεξεργασία δεδομένων. Η ανάγκη περί αρχικών εκτιμήσεων των επιπτώσεων επεξεργασίας δεδομένων θα επιτρέπει στους υπεύθυνους επεξεργασίας καλύτερη εκτίμηση των κινδύνων που σχετίζονται με μια αντίστοιχη επεξεργασία δεδομένων, καθώς επίσης και τη συμμόρφωση των σχετικών διαδικασιών με τις διατάξεις του καινούργιου Κανονισμού.

5.11 Υποχρεώσεις εκτελούντος την επεξεργασία

Σύμφωνα με τον Κανονισμό, ο εκτελών την επεξεργασία δεδομένων θεωρείται "το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας". Ο σχετικός ορισμός είναι σε συμφωνία με τον πρότερο σχετικό ορισμό στην οδηγία 95/46/ΕΚ.

Καταρχάς, σύμφωνα με το άρθρο 28, ο εκτελών την επεξεργασία δεδομένων αν διαπιστώσει πως οι οδηγίες επεξεργασίας των δεδομένων που έχει λάβει από τον υπεύθυνο επεξεργασίας έρχονται σε αντίθεση με τον παρόντα Κανονισμό ή άλλες εθνικές νομικές διατάξεις, οφείλει να ενημερώσει σχετικά τον υπεύθυνο επεξεργασίας

δεδομένων. Στο σημείο αυτό αξίζει να αναφερθεί πως η πρότερη οδηγία της Ένωσης δεν περιλάμβανε πρόβλεψη για σχετικά σενάρια επεξεργασίας δεδομένων. Ωστόσο, ο καινούργιος Κανονισμός δεν προσδιορίζει ποια θα πρέπει να είναι η στάση του εκτελούντος την επεξεργασία δεδομένων, αν οι οδηγίες που λάβει κατόπιν σχετικής ενημέρωσης του υπεύθυνου επεξεργασίας, δεν είναι σύμφωνες με τον καινούργιο Κανονισμό της Ένωσης.

Στο σημείο αυτό αξίζει να αναφερθεί πως στην οδηγία 95/46/ΕΚ δεν προβλέπονταν ιδιαίτερες κυρώσεις ενάντια του εκτελούντος την επεξεργασία, αλλά η οδηγία κυρίως αναφέρονταν σε υποχρεώσεις και ευθύνες του υπεύθυνου επεξεργασίας δεδομένων. Ωστόσο, ο νέος κανονισμός (άρθρο 3) κάνει λόγο για ευθύνες και υποχρεώσεις τόσο των υπευθύνων επεξεργασίας, όσο και των εκτελούντων την επεξεργασία δεδομένων.

Οι υποχρεώσεις τήρησης αρχείου σχετικά με κάθε επεξεργασία του υπευθύνου επεξεργασίας δεδομένων που ορίζεται στο Άρθρο 30 του Κανονισμού, ισχύει και για τον εκτελών την επεξεργασία. Οι πληροφορίες που περιλαμβάνει το σχετικό αρχείο είναι ανάλογες του αντίστοιχου αρχείου που διατηρεί ο υπεύθυνος επεξεργασίας (όπως περιγράφηκε στην προηγούμενη ενότητα) και θα πρέπει να είναι διαθέσιμο στην εποπτική αρχή όταν και εφόσον ζητηθεί από την αρχή.

Σύμφωνα με το Άρθρο 31 ο εκτελών την επεξεργασία είναι υποχρεωμένος να συνεργάζεται με την εθνική εποπτική αρχή για την εκπλήρωση των υποχρεώσεών του. Η σχετική πρόβλεψη δε δηλώνονταν με σαφήνεια στην οδηγία 95/46/ΕΚ. Ωστόσο, υπήρχε σχετική νομική πρόβλεψη στα περισσότερα κράτη – μέλη της Ένωσης.

Σχετικά με υποχρεώσεις διασφάλισης της προστασίας προσωπικών δεδομένων όπως ορίζονται στο άρθρο 32 του Κανονισμού και αναφέρθηκαν στην προηγούμενη ενότητα για τις σχετικές υποχρεώσεις – συστάσεις των υπευθύνων επεξεργασίας δεδομένων, ισχύουν ανάλογες υποχρεώσεις – συστάσεις και προς τους εκτελούντες την επεξεργασία των δεδομένων.

Ο εκτελών την επεξεργασία είναι υποχρεωμένος (Άρθρο 33) μόλις υποπέσει στην αντίληψή του οποιαδήποτε παραβίαση της ασφάλειας προσωπικών δεδομένων που διαχειρίζεται, να ενημερώσει σχετικά τον υπεύθυνο επεξεργασίας δεδομένων. Η ενημέρωση θα πρέπει να περιλαμβάνει πληροφορίες σχετικά με:

- τη φύση της παραβίασης δεδομένων
- τις κατηγορίες των πληροφοριών που παραβιάστηκε η ασφάλεια

- τον αριθμό των υποκειμένων (εκτίμηση) των οποίων τα δεδομένα παραβιάστηκαν
- τα στοιχεία επικοινωνίας με τον υπεύθυνο ασφαλείας των σχετικών πληροφοριών
- τις πιθανές συνέπειες της παραβίασης των δεδομένων
- τους ενδεδειγμένους τρόπους αύξησης μελλοντικής προστασίας των σχετικών δεδομένων
- τους ενδεδειγμένους πιθανούς τρόπους άμβλυνσης των πιθανών συνεπειών από τη σχετική παραβίαση των δεδομένων

Αν η παροχή των σχετικών πληροφοριών δε μπορεί να πραγματοποιηθεί άμεσα, υπάρχει η δυνατότητα σταδιακής παροχής των σχετικών πληροφοριών εκ μέρους του εκτελούντος την επεξεργασία δεδομένων.
Βασική αλλαγή που επιφέρει ο νέος Κανονισμός και σχετίζεται με τους εκτελούντες την επεξεργασία δεδομένων είναι η ευθύνη που εκείνοι έχουν για την ασφάλεια της επεξεργασίας δεδομένων. Πλέον, ένα υποκείμενο δεδομένων μπορεί να καταφύγει δικαστικά εναντίον ενός εκτελούντος την επεξεργασία δεδομένων και όχι του υπεύθυνου επεξεργασίας των δεδομένων. Η σχετική δικαστική προσφυγή μπορεί να υπάρξει αν ο εκτελών την επεξεργασία ενήργησε αντίθετα με όσα προβλέπονται για τον ίδιο από τον Κανονισμό ή αν δεν συμμορφώθηκε με τις υποδείξεις του υπεύθυνου επεξεργασίας που ήταν εντός του πλαισίου νομιμότητας του Κανονισμού. Η σχετική ευθύνη του εκτελούντος την επεξεργασία δεδομένων επιβαρύνει τις εργασίες – λειτουργία των σχετικών ατόμων – οργανισμών, αλλά ωστόσο απαλλάσσει παράλληλα από αντίστοιχες ευθύνες – υποχρεώσεις τους υπεύθυνους επεξεργασίας δεδομένων.

5.12 Υπεύθυνος προστασίας δεδομένων

Σύμφωνα με το άρθρο 37 του Κανονισμού ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία δεδομένων είναι υποχρεωμένοι να ορίζουν ένα φυσικό πρόσωπο ως υπεύθυνο προστασίας των δεδομένων όταν:

- πρόκειται για συστηματική και τακτική επεξεργασία των δεδομένων των υποκειμένων σε ευρεία κλίμακα

- πρόκειται για ευρείας κλίμακας επεξεργασία ευαίσθητων προσωπικών δεδομένων

- η επεξεργασία δεδομένων διενεργείται από δημόσια αρχή

Η σχετική απαίτηση προσθέτει για μικρούς σε κλίμακα οργανισμούς επιπλέον εργασία, δαπάνες και απαιτήσεις σε ανθρώπινο δυναμικό. Επίσης, σύμφωνα με το άρθρο 38 θα πρέπει να αποτελεί μέριμνα του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία δεδομένων η παροχή των απαραίτητων πόρων στον υπεύθυνο προστασίας δεδομένων για την εκτέλεση του έργου του, καθώς επίσης και για τη σχετική επιμόρφωσή του και διατήρηση της τεχνογνωσίας που θα πρέπει να διαθέτει.

Επίσης, σύμφωνα με το άρθρο 38 δεν είναι δυνατή η παρέμβαση στην εκτέλεση του έργου του υπεύθυνου προστασίας δεδομένων από τον υπεύθυνο επεξεργασίας ή από τον εκτελούντα την επεξεργασία δεδομένων. Επιπροσθέτως, δεν είναι δυνατή η απόλυση ενός ορισμένου υπεύθυνου προστασίας δεδομένων από έναν οργανισμό. Οι σχετικοί περιορισμοί αφενός εγγυώνται σε ορισμένο βαθμό την αμεροληψία του υπεύθυνου προστασίας δεδομένων, αλλά αφετέρου θέτουν φραγμούς στην λειτουργία ενός οργανισμού που επεξεργάζεται δεδομένα υποκειμένων και είναι υποχρεωμένος εκ του νόμου να ορίσει υπεύθυνο προστασίας δεδομένων και να κοινοποιήσει το όνομά του στην αντίστοιχη εποπτική αρχή (άρθρο 37).

Ειδικότερα, στο άρθρο 39 ορίζονται τα καθήκοντα του υπεύθυνου προστασίας των δεδομένων που είναι:

- συνεργασία με όλους τους υπεύθυνους επεξεργασίας και τον εκτελούντα την επεξεργασία δεδομένων με σκοπό τη συμμόρφωση στις διατάξεις του Κανονισμού 2016/679 ή άλλες εθνικές διατάξεις σχετικά με την προστασία των δεδομένων

- διαρκής παρακολούθηση της συμμόρφωσης των πρακτικών και των διαδικασιών του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία δεδομένων με την ισχύουσα νομοθεσία προστασίας προσωπικών δεδομένων

- υποστήριξη με σχετική κατάρτιση του προσωπικού που εμπλέκεται με την επεξεργασία δεδομένων

- να παρέχει συμβουλές και εκτιμήσεις στους υπεύθυνους επεξεργασίας κατά τη σύνταξη έκθεσης εκτίμησης κινδύνων από μια καινούργια διαδικασία επεξεργασίας δεδομένων

- συνεργασία με την αντίστοιχη εποπτική αρχή

Σύμφωνα με την οδηγία 95/46/ΕΚ, δεν απαιτούνταν ο ορισμός υπεύθυνου προστασίας δεδομένων από τους υπεύθυνους επεξεργασίας και τον εκτελούντα την επεξεργασία δεδομένων. Επίσης, η οδηγία δεν περιλάμβανε ειδική μέριμνα προστασίας του υπεύθυνου επεξεργασίας δεδομένων και λεπτομερή καταγραφή των καθηκόντων του. Ωστόσο, η σχετική πρόβλεψη διευκολύνει τη συμμόρφωση στα καθήκοντά τους, τόσο των υπευθύνων επεξεργασίας όσο και του εκτελούντος την επεξεργασία δεδομένων, σύμφωνα με τις διατάξεις του καινούργιου Κανονισμού.

5.13 Διασυνοριακές μεταφορές δεδομένων

Οι βασικές αρχές σχετικά με τη μεταφορά δεδομένων από τα κράτη μέλη της ΕΕ σε τρίτες χώρες (συμπεριλαμβανομένων και των Ηνωμένων Πολιτειών) παραμένουν σε ισχύ, συμπεριλαμβανομένης της απαίτησης, οι σχετικές μεταφορές δεδομένων να μπορούν να πραγματοποιηθούν μόνο εάν παρέχεται επαρκές επίπεδο προστασίας στις αντίστοιχες τρίτες χώρες προορισμού των δεδομένων.

Το άρθρο 45 ορίζει μια σειρά από κριτήρια τα οποία λαμβάνει υπόψη της η Επιτροπή πριν τη λήψη της απόφασης περί επαρκών απαιτήσεων προστασίας προσωπικών δεδομένων από ένα τρίτο κράτος ή οργανισμό εκτός των ορίων της Ένωσης, όπως είναι τα εξής:

- η εθνική νομοθεσία και νομολογία

- η προστασία των ανθρωπίνων δικαιωμάτων

- η εθνική ασφάλεια

- η λειτουργία ή μη εποπτικής αρχής προστασίας προσωπικών δεδομένων στο τρίτο κράτος

- πιθανές διεθνείς συμβάσεις που έχει υπογράψει και εφαρμόζει το τρίτο κράτος

- και άλλοι συναφείς παράγοντες

Ο αριθμός των παραγόντων που λαμβάνει η Επιτροπή για την έκδοση σχετικών αποφάσεων περί δυνατότητας ή μη διαβίβασης προσωπικών δεδομένων σε τρίτα κράτη είναι περισσότερο ευρύς σε σχέση με την οδηγία 95/46/ΕΚ. Ωστόσο, δεν προσδιορίζεται στον Κανονισμό αν οι ισχύουσες άδειες για δυνατότητα μεταφοράς δεδομένων θα εξακολουθούν να ισχύουν με την έναρξη εφαρμογής του καινούργιου Κανονισμού ή αν θα απαιτηθεί καινούργια αντίστοιχη έγκριση από την Επιτροπή.

Επιπροσθέτως, στο ίδιο άρθρο (45) ορίζεται η απαίτηση της τακτικής αναθεώρησης της σχετικής άδειας ανά τέσσερα χρόνια. Σχετική πρόβλεψη δεν ορίζονταν στην οδηγία 95/46/ΕΚ. Επίσης, στο άρθρο 46 προβλέπεται η δυνατότητα διασυνοριακής μεταφοράς δεδομένων, η οποία βασίζεται σε σχετική συμφωνία μεταξύ δημόσιων φορέων ενός κράτους μέλους και ενός τρίτου κράτους, η οποία διασφαλίζει τη συμμόρφωση με τον Κανονισμό 2016/679, χωρίς ειδική εξουσιοδότηση διασυνοριακής μεταφοράς δεδομένων από εποπτική αρχή. Σχετική πρόβλεψη δεν υπήρχε στη οδηγία 95/46/ΕΚ και πιθανότατα η σχετική πρόβλεψη του καινούργιου Κανονισμού να διευκολύνει τη μεταφορά δεδομένων των οργανισμών με διεθνή δράση.

Σε περίπτωση απουσίας επαρκούς ασφάλειας των δεδομένων, μπορεί υπό συγκεκριμένες προϋποθέσεις να πραγματοποιηθεί μια διασυνοριακή μεταφορά δεδομένων. Σύμφωνα με τον καινούργιο Κανονισμό (άρθρο 49), πριν τη διασυνοριακή μεταφορά δεδομένων χωρίς την ύπαρξη επαρκούς ασφάλειας, απαιτείται η ενημέρωση του υποκειμένου των δεδομένων για τους πιθανούς κινδύνους που συνεπάγεται μια διασυνοριακή μεταφορά δεδομένων, καθώς επίσης και η συγκατάθεση του υποκειμένου πριν τη μεταφορά των δεδομένων εκτός της Ευρωπαϊκής Ένωσης. Ωστόσο, στην πράξη ίσως να υπάρχει δυσκολία απόδειξης πως το υποκείμενο δεδομένων έλαβε τη σχετική ενημέρωση και συγκατέθεσε για τη διασυνοριακή μεταφορά των προσωπικών του δεδομένων.

Επιπροσθέτως, αν ισχύει μια από τις ακόλουθες προϋποθέσεις είναι επιτρεπτή η διασυνοριακή μεταφορά δεδομένων προς άλλο προορισμό χωρίς την ύπαρξη επαρκούς ασφάλειας (άρθρο 49):

- για λόγους δημοσίου συμφέροντος
- για την υποστήριξη νομικής αξίωσης

- για την εκτέλεση σύμβασης, κατόπιν αιτήματος του υποκειμένου των δεδομένων
- για την εκτέλεση σύμβασης, προς όφελος του υποκειμένου των δεδομένων
- εφόσον το υποκείμενο των δεδομένων δε δύναται να δώσει τη συγκατάθεσή του, αλλά η σχετική μεταφορά δεδομένων είναι απαραίτητη για ζωτικής σημασίας συμφέρον του υποκειμένου των δεδομένων

Τέλος, ένας περιορισμός που τίθεται από τον καινούργιο Κανονισμό (άρθρο 49), είναι πως κατά τη διασυνοριακή μεταφορά δεδομένων χωρίς την ύπαρξη επαρκούς ασφάλειας, δίνεται το δικαίωμα στα κράτη μέλη, να μπορούν για λόγους δημοσίου συμφέροντος να καθορίσουν συγκεκριμένες κατηγορίες δεδομένων που δε δύναται να συμμετέχουν σε διασυνοριακή μεταφορά δεδομένων προς προορισμούς, χωρίς την ασφάλεια των δεδομένων. Το αντίστοιχο άρθρο πιθανόν να αποτελέσει εμπόδιο στην ομοιομορφία διαχείρισης των προσωπικών δεδομένων εκ μέρους των υπευθύνων επεξεργασίας στα διάφορα κράτη μέλη, σε αντίθεση με την προσπάθεια του καινούργιου Κανονισμού για καθιέρωση ενιαίων διαδικασιών διαχείρισης προσωπικών δεδομένων εντός των ορίων της Ευρωπαϊκής Ένωσης.

5.14 Προσφυγές, ευθύνες, κυρώσεις

5.14.1 Δικαίωμα προσφυγής

Σύμφωνα με το άρθρο 77 του Κανονισμού κάθε υποκείμενο δεδομένων διατηρεί το δικαίωμα να υποβάλλει καταγγελία στην εποπτική εργασία του κράτους μέλους, όπου εργάζεται ή κατοικεί ή εικάζεται πως έλαβε χώρα η σχετική παραβίαση των διατάξεων του καινούργιου Κανονισμού της Ένωσης. Η εποπτική αρχή στην οποία υποβάλλει την αίτησή του το υποκείμενο των δεδομένων, είναι υποχρεωμένη να ενημερώνει το υποκείμενο των δεδομένων για την έκβαση της αίτησής του και τυχόν δυνατότητά του για σχετική δικαστική προσφυγή. Συγκρίνοντας τις σχετικές διατάξεις με την οδηγία 95/46/ΕΚ, ο καινούργιος Κανονισμός με μεγαλύτερη σαφήνεια προσδιορίζει τις εποπτικές αρχές στις οποίες μπορεί να υποβάλλει την καταγγελία του ένα υποκείμενο δεδομένων.

Επιπροσθέτως, σύμφωνα με το άρθρο 78 το υποκείμενο των δεδομένων έχει το δικαίωμα να προσφύγει στην δικαιοσύνη κατά της εποπτικής αρχής, εάν εκείνη δεν εξετάσει την καταγγελία του ή αν δεν ενημερώσει το υποκείμενο των δεδομένων για

την έκβαση της καταγγελίας του εντός τριών (3) μηνών. Οι σχετικές δικαστικές καταγγελίες κρίνονται από τα δικαστήρια του κράτους μέλους που υπάγεται η σχετική εποπτική αρχή. Συγκρίνοντας τις σχετικές διατάξεις με την οδηγία 95/46/ΕΚ, ο καινούργιος Κανονισμός με μεγαλύτερη σαφήνεια προσδιορίζει τους όρους της δικαστικής προσφυγής κατά των εποπτικών αρχών.

Σύμφωνα με το άρθρο 79§2 οποιαδήποτε προσφυγή κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία δεδομένων, μπορεί να κριθεί από τα δικαστήρια της χώρας που εδρεύουν οι σχετικοί οργανισμοί ή από τα δικαστήρια της χώρας όπου κατοικεί το υποκείμενο των δεδομένων. Το σχετικό άρθρο εγκυμονεί για τους οργανισμούς τον κίνδυνο δικαστικών διαμαχών σε άλλα κράτη μέλη εκτός της έδρας τους και με διαφοροποιήσεις στην εθνική τους νομοθεσία.

Επίσης, με τον καινούργιο Κανονισμό προβλέπεται το ενδεχόμενο ένας υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεδομένων να βρίσκεται συγχρόνως σε δικαστική διαμάχη σε διάφορα κράτη μέλη της Ένωσης, με αντικείμενο την ίδια κατηγορία της παραβίασης δεδομένων. Σε αυτήν την περίπτωση, σύμφωνα με το άρθρο 81 του Κανονισμού, δύναται το δικαστήριο ενός κράτους μέλους αφού επιβεβαιώσει την εκκρεμότητα της σχετικής δίκης σε εξέλιξη, σε άλλο κράτος μέλος, να αναστείλει τις διαδικασίες εκδίκασης της υπόθεσης. Η σχετική πρόβλεψη στον καινούργιο Κανονισμό πρακτικά μειώνει τις παράλληλες δικαστικές διαμάχες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία δεδομένων σε διάφορα κράτη μέλη με το ίδιο αντικείμενο. Επίσης, η εκδίκαση της πρώτης υπόθεσης σε δικαστήριο ενός κράτους μέλους, πιθανόν να επηρεάσει – καθορίσει μελλοντικά ανάλογες δικαστικές διαμάχες σε άλλα κράτη μέλη για τις ίδιες παραβιάσεις των διατάξεων του Κανονισμού.

5.14.2 Δικαίωμα αποζημίωσης

Σύμφωνα με το άρθρο 82 του Κανονισμού, κάθε υποκείμενο δεδομένων του οποίου έχει υπάρξει παραβίαση των δεδομένων από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία δεδομένων, δικαιούται σχετική αποζημίωση. Σύμφωνα με το ίδιο άρθρο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεδομένων, δύναται να απαλλαγεί από την υποχρέωση καταβολής αποζημίωσης, εάν αποδειχθεί πως "δεν φέρει καμία ευθύνη για το γενεσιουργό γεγονός της ζημίας". Για το ύψος της πιθανής αποζημίωσης αποφαίνονται τα δικαστήρια του κράτους μέλους όπου κατοικεί το υποκείμενο των δεδομένων ή βρίσκεται η έδρα του οργανισμού. Όπως

αναφέρθηκε και παραπάνω, με τον καινούργιο Κανονισμό, υπάρχει μεγάλη πιθανότητα για τους οργανισμούς να διατρέχουν τον κίνδυνο δικαστικών διαμαχών σε άλλα κράτη μέλη εκτός της έδρας τους και με διαφοροποιήσεις στην εθνική τους νομοθεσία.

Επίσης, σύμφωνα με το ίδιο άρθρο (82) σε περίπτωση από κοινού επεξεργασίας δεδομένων, κάθε υπεύθυνος επεξεργασίας των δεδομένων φέρει ευθύνη για τη συνολική ζημιά που προκλήθηκε στο υποκείμενο των δεδομένων. Αν ωστόσο, κάποιος εκ των υπευθύνων επεξεργασίας δεν φέρει ευθύνη για την παραβίαση των δεδομένων, μετά τη καταβολή της αποζημίωσης στο υποκείμενο των δεδομένων μπορεί να ζητήσει την καταβολή σχετικής αποζημίωσης από λοιπούς υπεύθυνους επεξεργασίας για τη ζημιά που υπέστη.

5.14.3 Πρόστιμα παραβίασης Κανονισμού

Ο νέος Κανονισμός καθορίζει το μέγιστο ποσό των διοικητικών προστίμων που δύναται να επιβληθούν σε έναν οργανισμό αν διαπιστωθεί παραβίαση των διατάξεων του καινούργιου Κανονισμού προστασίας προσωπικών δεδομένων της ΕΕ. Σύμφωνα με το Άρθρο 83 του Κανονισμού οι εποπτικές αρχές των κρατών μελών είναι υπεύθυνες για την καταβολή προστίμων σε περίπτωση παραβίασης του Κανονισμού 2016/679. Ειδικότερα σύμφωνα με το ίδιο άρθρο οι εποπτικές αρχές θα πρέπει να διασφαλίζουν την "αποτελεσματική, αναλογική και αποτρεπτική" επιβολή των προστίμων σε κάθε περίπτωση παραβίασης του Κανονισμού. Σύμφωνα με το ίδιο άρθρο, κατά την επιβολή των προστίμων η εποπτική αρχή λαμβάνει υπόψη:

- το σκοπό της παραβίασης
- τον αριθμό των υποκειμένων που επηρεάστηκαν
- τη διάρκεια της παραβίασης
- αν η παραβίαση οφείλεται σε δόλο ή αμέλεια
- το πιθανό ιστορικό παραβιάσεων από τον ίδιο τον υπεύθυνο επεξεργασίας ή από τον εκτελούντα την επεξεργασία, άτομο – οργανισμό
- τις προσπάθειες επανόρθωσης της ζημιάς που προκλήθηκε
- τις κατηγορίες των δεδομένων που αφορά η παραβίαση

- τον τρόπο σχετικής ενημέρωσης της εποπτικής αρχής, με ή χωρίς τη συνδρομή του κατηγορούμενου ατόμου – οργανισμού

- τα πιθανά οικονομικά οφέλη ή την οικονομική ζημιά, που προέκυψαν από την εν λόγω παραβίαση για τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, άτομο – οργανισμό

Ο καινούργιος Κανονισμός σε αντίθεση με την προηγούμενη οδηγία της Ένωσης, ορίζει με σαφήνεια το μέγιστο δυνατό πρόστιμο ανάλογα με την περίπτωση. Τα σχετικά διοικητικά πρόστιμα είναι ιδιαίτερα αυξημένα σε σχέση με τα σχετικά πρόστιμα που καταλογίζονται σήμερα και αλλάζουν τις οικονομικές συνέπειες των οργανισμών σε περιπτώσεις παραβιάσεων του καινούργιου Κανονισμού της Ένωσης. Ειδικότερα, ως ανώτατο ύψος των σχετικών προστίμων ορίζεται το μέγιστο ποσό μεταξύ των € 10 εκατομμυρίων και του 4% του ετήσιου κύκλου των εργασιών του προηγούμενου οικονομικού έτους, σε περιπτώσεις παραβιάσεων:

- των υποχρεώσεων του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία δεδομένων (άρθρα 8, 11, 25-39, 42, 43)

- των υποχρεώσεων του φορέα πιστοποίησης (άρθρα 41, 42)

- των υποχρεώσεων του φορέα παρακολούθησης (άρθρο 41§4)

Επίσης, ως ανώτατο ύψος των σχετικών προστίμων ορίζεται το μέγιστο ποσό μεταξύ των € 20 εκατομμυρίων και το 4% του ετήσιου κύκλου των εργασιών του προηγούμενου οικονομικού έτους, αν η διαπιστωμένη παραβίαση αφορά:

- τα δικαιώματα των υποκειμένων των δεδομένων (άρθρα 12 έως 22)

- τις αρχές επεξεργασίας δεδομένων και τη διαδικασία λήψης-έγκρισης δεδομένων (άρθρα 6, 7, 9)

- τη διασυνοριακή μεταφορά δεδομένων σε τρίτες χώρες (άρθρα 44-49)

- τη μη συμμόρφωση με τη σύσταση της εποπτικής αρχής, σύμφωνα με όσα ορίζονται στο άρθρο 58

Στο σημείο αυτό αξίζει να αναφερθεί πως η οδηγία 95/46/ΕΚ δεν προσδιόριζε τους παράγοντες που θα πρέπει να λάβουν υπόψη τους οι εποπτικές αρχές των κρατών μελών, δίνοντας πρακτικά στους οργανισμούς τη δυνατότητα υπολογισμού του

πιθανού προστίμου που θα τους καταβληθεί σε περίπτωση παραβίασης των διατάξεων του Κανονισμού.

Όσον αφορά την επιβολή κυρώσεων μη διοικητικών προστίμων για παραβιάσεις του Κανονισμού (όπως περιγράφονται στο άρθρο 83), τα κράτη μέλη ορίζουν τους σχετικούς κανόνες σύμφωνα με το άρθρο 84, φροντίζοντας οι εν λόγω πιθανές κυρώσεις να είναι "αποτελεσματικές, αναλογικές και αποτρεπτικές". Η σχετική δυνατότητα διαφοροποίησης των πιθανών ποινικών κυρώσεων σε περιπτώσεις παραβιάσεων των διατάξεων του Κανονισμού 2016/679, πιθανόν να έχει ως αποτέλεσμα την διαφοροποίηση μεταξύ των ποινικών κυρώσεων για συναφείς παραβιάσεις του Κανονισμού από οργανισμούς με έδρα σε διαφορετικά κράτη μέλη της Ένωσης.

5.15 Κώδικες δεοντολογίας - Πιστοποιήσεις

Σύμφωνα με το άρθρο 40 του Κανονισμού τα κράτη μέλη της Ένωσης, οι κρατικές εποπτικές αρχές και η Επιτροπή ενθαρρύνονται υπέρ της εκπόνησης Κωδικών δεοντολογίας, με σκοπό τη διευκόλυνση της εφαρμογής των διατάξεων του καινούργιου Κανονισμού. Η εκπόνηση σχετικών Κωδικών δεοντολογίας οφείλει να λαμβάνει υπόψη την ειδική περίπτωση της εφαρμογής επεξεργασίας δεδομένων ανά περίπτωση και τις πιθανές ανάγκες για τις μικρές και τις μεσαίες επιχειρήσεις.

Προς την ίδια κατεύθυνση ενθαρρύνονται να κινηθούν φορείς ή άτομα που αντιπροσωπεύουν υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία δεδομένων. Ειδικότερα, ένας Κώδικας δεοντολογίας συστήνεται σύμφωνα με το άρθρο 40 να περιλαμβάνει προτάσεις σχετικά με:

- τη διαφάνεια της επεξεργασίας δεδομένων
- τη συλλογή ευαίσθητων προσωπικών δεδομένων
- την κωδικοποίηση των δεδομένων
- τα πιθανά έννομα συμφέροντα των υπευθύνων επεξεργασίας ανά κατηγορία επεξεργασίας δεδομένων
- τη σχετική ενημέρωση των υποκειμένων των δεδομένων και του ευρύτερου κοινού
- την υπεράσπιση των δικαιωμάτων των υποκειμένων των δεδομένων

- την ειδική μέριμνα προστασίας των παιδιών
- τα προτεινόμενα μέσα – τεχνικές προστασίας των δεδομένων
- τη διασυνοριακή μεταφορά δεδομένων
- την ενημέρωση του υποκειμένου των δεδομένων και των αντίστοιχων εποπτικών αρχών κατά τη διαπίστωση παραβίασης δεδομένων
- τις εξωδικαστικές διαδικασίες επίλυσης διαφορών με τα υποκείμενα δεδομένων

Με την οδηγία 95/46/ΕΚ η σχετική αρμοδιότητα ασκούνταν από τις εποπτικές αρχές των κρατών μελών. Με τον καινούργιο Κανονισμό διευρύνεται το εύρος των φορέων – οργανισμών που μπορούν να συμμετέχουν στην εκπόνηση Κωδικών δεοντολογίας και πιθανώς ο συγκεκριμένος παράγοντας να λειτουργήσει θετικά στην εκπόνηση πρακτικών και αποτελεσματικών στην εφαρμογή τους Κωδικών δεοντολογίας.
Επίσης, σύμφωνα με το άρθρο 41, για την παρακολούθηση της εφαρμογής των Κωδικών δεοντολογίας υπάρχει η δυνατότητα ορισμού ενός υπεύθυνου φορέα που να διαθέτει τις αντίστοιχες γνώσεις και να έχει πιστοποιηθεί σχετικά από την αντίστοιχη εποπτική αρχή.
Πέραν, της πιστοποίησης των φορέων για την παρακολούθηση της ενδελεχούς εφαρμογής ενός Κώδικα δεοντολογίας, οι εποπτικές αρχές των κρατών μελών και οι σχετικοί πιστοποιημένοι φορείς σύμφωνα με το άρθρο 42 του Κανονισμού, θα μπορούν να πιστοποιήσουν και τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων. Με τον νέο Κανονισμό εισάγεται η Ευρωπαϊκή Σφραγίδα Προστασίας των Δεδομένων, η οποία θα χορηγείται σε υπεύθυνους επεξεργασίας ή στον εκτελούντα την επεξεργασία δεδομένων, όταν εκείνοι συμμορφώνονται με τον Κώδικα δεοντολογίας που έχει εγκριθεί από το Συμβούλιο Προστασίας Δεδομένων. Η σχετική σφραγίδα θα πιστοποιεί στα υποκείμενα των δεδομένων την υιοθέτηση υψηλών πρακτικών προστασίας των δεδομένων τους.
Η λήψη της σχετικής πιστοποίησης θα είναι προαιρετική και θα απαιτεί ανανέωση ανά τρία χρόνια. Επίσης, αν διαπιστωθεί πως κάποιος υπεύθυνος επεξεργασίας ή κάποιος εκτελών την επεξεργασία δεδομένων δεν εφαρμόζει απόλυτα έναν Κώδικα δεοντολογίας, θα αφαιρείται άμεσα η σχετική πιστοποίηση, μέχρι την πλήρη συμμόρφωσή του στον αντίστοιχο Κώδικα δεοντολογίας.

Στην οδηγία 95/46/ΕΚ δεν υπήρχε σχετική πρόβλεψη με την παροχή πιστοποιήσεων σε υπεύθυνους επεξεργασίας ή σε εκτελούντες την επεξεργασία δεδομένων, ούτε πρόβλεψη περί Ευρωπαϊκής Σφραγίδας Προστασίας των Δεδομένων. Οι σχετικές ρυθμίσεις μπορούν να λειτουργήσουν προς όφελος των υποκειμένων των δεδομένων, καθώς θα τους διασφαλίζουν την προστασία των δεδομένων τους σύμφωνα με όσα θα προβλέπονται στον αντίστοιχο Κώδικα δεοντολογίας. Επιπροσθέτως, οι σχετικές πιστοποιήσεις θα παρέχουν οδηγίες προς τους υπεύθυνους και τους εκτελούντες την επεξεργασία δεδομένων, προκειμένου να διευκολύνουν τη συμμόρφωσή τους προς τις διατάξεις του καινούργιου Κανονισμού της Ένωσης.

5.16 Εποπτικές αρχές

Σύμφωνα με το άρθρο 51 του Κανονισμού, σε κάθε κράτος μέλος θα πρέπει να υφίσταται μια εποπτική αρχή για την προστασία των δικαιωμάτων των κατοίκων της Ένωσης. Η δικαιοδοσία της κάθε εποπτικής αρχής περιορίζεται εντός των ορίων του κράτους μέλλους που υφίσταται σύμφωνα με το άρθρο 55 του Κανονισμού. Η σχετική παράμετρος πιθανόν να δημιουργεί δυσκολίες σε επιχειρήσεις που δραστηριοποιούνται σε πολλά κράτη. Αντίθετα, αν μια επιχείρηση δραστηριοποιείται μόνο σε ένα κράτος μέλος και επεξεργάζεται τα προσωπικά δεδομένα μόνο των πολιτών του ίδιου κράτους μέλους δεν επηρεάζεται από το σχετικό γεγονός.

Ο Κανονισμός στο άρθρο 52 επισημαίνει την ανάγκη της ανεξαρτησίας των σχετικών εποπτικών αρχών, στο άρθρο 53 καθορίζει τις προϋποθέσεις επιλογής των μελών των εποπτικών αρχών, στο άρθρο 54 καθορίζει τις διαδικασίες σύστασης των εποπτικών αρχών και στα άρθρα 55 και 57 τις αρμοδιότητες - καθήκοντα των εποπτικών αρχών. Οι σχετικοί προσδιορισμοί του Κανονισμού δε διαφέρουν σημαντικά από την οδηγία 95/46/ΕΚ, η μόνη διαφοροποίηση αφορά τον εμπλουτισμό των αρμοδιοτήτων των εποπτικών αρχών. Ωστόσο, πρακτικά οι σχετικές διαφοροποιήσεις δε θα επιφέρουν κάποια αλλαγή στον τρόπο λειτουργίας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία δεδομένων.

Ενδεικτικές αρμοδιότητες που προστίθενται στις εποπτικές αρχές των κρατών μελών είναι οι εξής:

- να προωθούν τη σχετική ευαισθητοποίηση του κοινού, ιδιαίτερα σε θέματα προστασίας προσωπικών δεδομένων των παιδιών
- να συμβουλεύουν τη νομοθετική εξουσία για τη θέσπιση της σχετικής απαιτούμενης νομοθεσίας

- να προωθούν τη σχετική ευαισθητοποίηση των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία σε θέματα συμμόρφωσής τους με τον νέο Κανονισμό
- να διατηρούν αρχείο των παραβιάσεων που έχουν διαπιστωθεί και των μέτρων που λήφθηκαν αλλά και των ποινών που επιβλήθηκαν
- να ενθαρρύνουν στην κατάρτιση σχετικών κωδικών δεοντολογίας

Μια καινούργια υπηρεσία-δυνατότητα που παρέχεται από τον Κανονισμό στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων είναι η λεγόμενη υπηρεσία μιας στάσης (one stop shop), που τους επιτρέπει τη διαπραγμάτευση – συνδιάλεξη μιας και μόνο εποπτικής αρχής (της έδρας τους) για την επεξεργασία δεδομένων που αφορούν πολλαπλά κράτη μέλη της Ένωσης. Η συγκεκριμένη δυνατότητα θα επιτρέπει την ομοιόμορφη αντιμετώπιση ζητημάτων σχετικά με την επεξεργασία δεδομένων των κατοίκων διαφορετικών κρατών μελών της Ένωσης. Ωστόσο, στην πράξη μετά της 28 Μαΐου του 2018, θα αποδειχθεί αν είναι εφικτή η συνδιάλεξη με μια μόνο εποπτική αρχή, ή αν οι σχετικές αποφάσεις της εποπτικής αρχής (έδρα υπευθύνου ή εκτελούντος την επεξεργασία) θα έρχονται σε αντίθεση με άλλες εθνικές διατάξεις στα λοιπά κράτη μέλη της Ένωσης. Σχετική πρόβλεψη – δυνατότητα δεν παρέχονταν από την πρότερη οδηγία 95/46/ΕΚ της Ένωσης.

Τέλος, στο άρθρο 61 ορίζεται η απαίτηση συνεργασίας και ανταλλαγής πληροφοριών μεταξύ των εποπτικών αρχών διαφόρων κρατών μελών της Ένωσης, κάτι που έρχεται σε συμφωνία με όσα ορίζονταν και στην οδηγία 95/46/ΕΚ. Μια διαφοροποίηση του νέου Κανονισμού σε σχέση με την οδηγία 95/46/ΕΚ είναι η πρόβλεψη κοινών εργασιών και κοινών μέτρων επιβολής (άρθρο 62) για την αντιμετώπιση παραβιάσεων των διατάξεων του Κανονισμού που παρατηρούνται σε αρκετά κράτη μέλη της Ένωσης. Η σχετική πρόβλεψη μπορεί να διευκολύνει την εξέταση από τις εποπτικές αρχές αντίστοιχων παραβιάσεων των διατάξεων του Κανονισμού από υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία δεδομένων.

5.17 Επίδραση πρότερων αποφάσεων της Ένωσης

Όπως ορίζεται στο άρθρο 94 του Κανονισμού από 28 Μαΐου του 2018 καταργείται η οδηγία 95/46/ΕΚ. Επίσης, ο νέος Κανονισμός δεν επηρεάζει τις υποχρεώσεις των παρόχων τηλεπικοινωνιακών υπηρεσιών, οι οποίοι επεξεργάζονται δεδομένα

προσωπικού χαρακτήρα σύμφωνα με την οδηγία 2002/58/ΕΚ. Ωστόσο, η παράλληλη ισχύ της οδηγίας 2002/58/ΕΚ και του καινούργιου Κανονισμού πιθανόν να δημιουργήσει αβεβαιότητα στο μέλλον, σε θέματα επεξεργασίας δεδομένων εκ μέρους των παρόχων υπηρεσιών τηλεφωνίας ή σε ό,τι αφορά τη διασυνοριακή μεταφορά σχετικών δεδομένων.

Τέλος, όποιες διεθνείς συμφωνίες έχουν ήδη υπογράψει τα κράτη με άλλα κράτη ή διεθνείς οργανισμούς πριν τις 24 Μαΐου 2016, παραμένουν σε ισχύ μέχρι την πιθανή μελλοντική αναθεώρησή τους σύμφωνα με τον νέο Κανονισμό. Ωστόσο, για το συγκεκριμένο ζήτημα πιθανόν να υπάρξει αβεβαιότητα στο μέλλον σχετικά με τα θέματα επεξεργασίας προσωπικών δεδομένων ή τη διασυνοριακή μεταφορά τους.

5.18 Νέος κανονισμός και κοινωνικά δίκτυα

Ένας από τους στόχους του νέου Κανονισμού είναι να δώσει στους ανθρώπους μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα που διατηρούν στα κοινωνικά δίκτυα. Το δικαίωμα στη λήθη που προβλέπει ο νέος Κανονισμός, απαιτεί τη δυνατότητα των ατόμων να απαιτήσουν την άμεση διαγραφή των δεδομένων προσωπικού χαρακτήρα, που συλλέγονται ή δημοσιεύονται σε διάφορα κοινωνικά δίκτυα. Εάν κατά τη διάρκεια της επεξεργασίας δεδομένων ένα κοινωνικό δίκτυο υποχρεώνεται να δημοσιοποιήσει τα δεδομένα σε άλλους φορείς ή επιχειρήσεις, θα είναι πλέον υποχρεωμένο να θεσπίσει τα απαραίτητα μέτρα, όχι μόνο οργανωτικά αλλά και τεχνικά, προκειμένου να διασφαλίζει την άμεση ενημέρωση τρίτων σχετικά με το αίτημα ματαίωσης από την πλευρά του υποκειμένου των δεδομένων για τη διαγραφή αυτών [75].

Επίσης, το δικαίωμα στη φορητότητα απαιτεί τη διευκόλυνση της διαβίβασης - μεταφοράς δεδομένων προσωπικού χαρακτήρα από ένα κοινωνικό δίκτυο σε ένα άλλο, σε μια δομημένη, ευρέως χρησιμοποιούμενη μορφή, αναγνωρίσιμη από μια μηχανή - υπολογιστή. Το γεγονός αυτό αναμένεται να αυξήσει τα δικαιώματα προστασίας δεδομένων και να ενισχύσει τον ανταγωνισμό μεταξύ των παρόχων υπηρεσιών κοινωνικής δικτύωσης [75].

Ειδικότερα, ο νέος Κανονισμός πραγματεύεται την προστασία της ιδιωτικής ζωής των μαθητών και την προστασία τους από κινδύνους που ελλοχεύει λόγω της ελευθερίας πρόσβασης σε προσωπικές πληροφορίες μικρών παιδιών στο διαδίκτυο. Πιο συγκεκριμένα στο άρθρο 8 προβλέπεται πως για τη γενικότερη παροχή υπηρεσιών της κοινωνίας της πληροφορίας προς παιδιά κάτω των 16 ετών (ή 13 ετών, εάν τα

κράτη μέλη αποφασίσουν σχετικά), απαιτείται η γονική συναίνεση και η σχετική επαλήθευση εκ μέρους του υπεύθυνου επεξεργασίας δεδομένων ενός οργανισμού πριν τη διάθεση σχετικών υπηρεσιών σε ανήλικους (κάτω των 16 ή 13 ετών).

Επίσης, στο άρθρο 12 απαιτείται η διαφάνεια της επικοινωνίας σε "συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά". Συνεπώς, σύμφωνα με τον Κανονισμό τα παιδιά που χρησιμοποιούν κοινωνικά δίκτυα θα πρέπει να γνωρίζουν επ' ακριβώς περί της χρήσης των προσωπικών τους δεδομένων από αυτά. Επιπροσθέτως, όπως αναφέρεται στο άρθρο 57 "προωθείται η ευαισθητοποίηση του κοινού και η κατανόηση των κινδύνων, των κανόνων, των εγγυήσεων και των δικαιωμάτων που σχετίζονται με την επεξεργασία. Ειδική προσοχή αποδίδεται σε δραστηριότητες που απευθύνονται ειδικά σε παιδιά".

Ακόμα στην αιτιολογική σκέψη 71 αναφέρεται πως δε θα πρέπει προσωπικά δεδομένα παιδιών να συλλέγονται (και δεν θα συλλέγονται) για εμπορικούς σκοπούς, προσθέτοντας ένα ακόμα φράγμα προστασίας υπέρ των παιδιών. Ωστόσο, στην πράξη ίσως παρουσιαστούν προβλήματα στην εφαρμογή των αντίστοιχων διατάξεων και της προστασίας που θα μπορέσει να προσφέρει στα παιδιά ο καινούργιος Κανονισμός. Ενδεικτικά, δεν υπάρχει σαφήνεια όσον αφορά έναν αξιόπιστο τρόπο διάκρισης των δεδομένων που αφορούν τα παιδιά και τα υπόλοιπα δεδομένα που διατηρεί ένα κοινωνικό δίκτυο.

Επιπροσθέτως, η αιτιολογική σκέψη 65, ορίζει το δικαίωμα των ενηλίκων να ζητήσουν τη διαγραφή πληροφοριών (δικαίωμα στη λήθη) που είχαν αναρτήσει σε κοινωνικά δίκτυα όντας ανήλικοι και πλέον θεωρούν πως δεν τους εκφράζουν ή θέτουν εμπόδια στη ζωής τους. Πρακτικά, η εφαρμογή της εν λόγω διάταξης θα αντιμετωπίσει δυσκολίες για τη θέσπιση μηχανισμών υποβολής αιτημάτων διαγραφής υλικού αναρτημένου σε κοινωνικά δίκτυα.

Ένα ζητούμενο στην προστασία χρήσης των κοινωνικών δικτύων από παιδιά στη σύγχρονη ψηφιακή εποχή, είναι πώς θα πρέπει να επιτευχθεί η ισορροπία μεταξύ των δικαιωμάτων των παιδιών για ενημέρωση και συμμετοχή στην κοινωνία της πληροφορίας και των δικαιωμάτων τους στην προστασία της ιδιωτικής τους ζωής. Ποιος μπορεί καλύτερα να αποφασίσει σχετικά και να δώσει τη συγκατάθεσή του περί πρόσβασης παιδιών σε κοινωνικά δίκτυα: (i) οι επιχειρήσεις – κοινωνικά δίκτυα, (ii) οι κυβερνήσεις, (iii) οι γονείς ή (iv) τα ίδια τα παιδιά;

Με βάση το νέο Κανονισμό για τα κοινωνικά δίκτυα και γενικότερα για όλους τους ιστότοπους που διατηρούν προσωπικά δεδομένα χρηστών, δεν επιτρέπεται η εφαρμογή μεθόδων εξόρυξης δεδομένων σε προσωπικά δεδομένα παιδιών ή κατηγοριοποίηση των προφίλ χρηστών (παιδιών) με σκοπό την προβολή στοχευμένων διαφημίσεων σε εκείνα. Για τη συλλογή και την επεξεργασία των προσωπικών δεδομένων των παιδιών θα απαιτείται πλέον η συγκατάθεση των γονέων. Πιθανές σχετικές μέθοδοι μπορεί να αποτελέσουν: η επιβεβαίωση του γονέα μέσω του ηλεκτρονικού ταχυδρομείου, η επιβεβαίωση δήλωσης της πιστωτικής κάρτας του γονέα, η καταχώρηση των προσωπικών δεδομένων των παιδιών εκ μέρους των γονέων ή άλλοι συναφείς τρόποι.

Για το λόγο αυτό τα κοινωνικά δίκτυα θα πρέπει: (i) εξ αρχής να διατυπώσουν τους όρους χρήσης των ιστότοπων με βάση την ηλικία του κάθε χρήστη, (ii) να προσδιορίσουν τις υπηρεσίες που απαιτούν συγκατάθεση γονέα και του σταδίου δήλωσης της σχετικής συγκατάθεσης, (iii) να αφαιρέσουν τις τεχνολογίες συλλογής δεδομένων στις ιστοσελίδες κοινωνικής δικτύωσης, που δε συμμορφώνονται με τις αρχές του νέου Κανονισμού και (iv) να υιοθετήσουν τεχνολογίες για τη λήψη της συγκατάθεσης του γονέα, όταν εκείνη θα απαιτείται.

Σύμφωνα με το νέο Κανονισμό τα κοινωνικά δίκτυα και οι επιχειρήσεις που συλλέγουν μεγάλο όγκο προσωπικών δεδομένων στο διαδίκτυο θα πρέπει να διορίσουν υπεύθυνο προστασίας δεδομένων. Δε θα είναι σε θέση να μεταφέρουν δεδομένα προσωπικού χαρακτήρα σε τρίτους χωρίς τη ρητή συγκατάθεση του χρήστη όταν τα δεδομένα χρησιμοποιούνται για άλλους σκοπούς από όσους αναφέρονταν στους όρους χρήσης του κοινωνικού δικτύου. Λαμβάνοντας υπόψη πως οι πρακτικές που εφαρμόζουν τα κοινωνικά δίκτυα σήμερα είναι οι ίδιες για τους ανήλικους και τους ενήλικες, όπως ενδεικτικά γίνεται τόσο με την παρακολούθηση της τοποθεσίας του χρήστη όταν χρησιμοποιεί το κινητό του τηλέφωνο όσο και με την ανάλυση της προσωπικότητας των χρηστών, θα απαιτηθούν αλλαγές των πρακτικών των κοινωνικών δικτύων και επομένως θα προσφερθεί μεγαλύτερη προστασία στους ανήλικους.

Ωστόσο, σύμφωνα με αρκετούς, ο νέος Κανονισμός πιθανότατα να αφαιρέσει από τους Ευρωπαίους νέους το δικαίωμα πρόσβασης σε κοινωνικά δίκτυα, καθώς θα απαιτείται η συγκατάθεση των γονέων για τη χρήση τους από άτομα κάτω των 16 ετών. Έμμεσα, υπάρχει ο κίνδυνος ο νέος Κανονισμός να στερήσει από τους νέους το δικαίωμα επικοινωνίας με συνομηλίκους, με εκπαιδευτικούς και τη συμμετοχή τους

σε δημόσιο διάλογο. Παράλληλα με την τοποθέτηση φραγμών στη χρήση του διαδικτύου και των κινδύνων που εκείνο ελλοχεύει για τα παιδιά, πόση διασκέδαση, πόση έκφραση επικοινωνίας, δημιουργικότητας, συμμετοχής και μάθησης περιορίζονται από τον νέο Κανονισμό με σκοπό την προστασία των παιδιών; Μπορούν οι έφηβοι να επιστρέψουν πραγματικά στις προ-ψηφιακές εποχές; [76]

Δεν είναι σαφές από τον Κανονισμό με ποια κριτήρια και με ποιες διαδικασίες τα διάφορα κράτη μέλη θα αποφασίσουν σε ποια ηλικία (13 ή 16) θα απαιτείται η γονική συναίνεση για τη χρήση υπηρεσιών στο διαδίκτυο. Επιπροσθέτως, αν δεν υιοθετήσουν όλα τα κράτη μέλη της Ένωσης ένα ενιαίο όριο ηλικίας, δημιουργείται άμεσα ένα εμπόδιο στην επιχειρηματική δράση, καθώς θα πρέπει εκείνη να προσαρμόζεται ανάλογα με το όριο ηλικίας που θα έχει ορίσει το κάθε κράτος μέλος.

Μέχρι σήμερα μια πληροφορία που αναρτάται σε ένα κοινωνικό δίκτυο δεν είναι απολύτως ιδιωτική, καθώς έχουν πρόσβαση σε εκείνη όλοι οι φίλοι του χρήστη στο αντίστοιχο δίκτυο, αλλά επίσης και δυνητικά όλοι οι χρήστες σε παγκόσμιο επίπεδο του κοινωνικού δικτύου, αν ο εν λόγω χρήστης δεν έχει ορίσει ως ιδιωτικό το προφίλ του. Επιπροσθέτως, αρκετές πληροφορίες σχετικά με τη δράση του χρήστη στα κοινωνικά δίκτυα είναι διαθέσιμες σε ιδιωτικές εταιρίες, με σκοπό τη σκιαγράφηση του προφίλ του χρήστη και την προβολή στοχευμένων διαφημίσεων σε εκείνον.

Με το νέο Κανονισμό κανένα κοινωνικό δίκτυο δε θα μπορεί να διαθέσει προσωπικές πληροφορίες ή πληροφορίες σχετικά με τις προτιμήσεις του χρήστη, σε άλλους οργανισμούς, χωρίς την πρότερη συγκατάθεσή του. Επίσης, με το νέο Κανονισμό ο χρήστης θα μπορεί να διαγράψει άμεσα συγκεκριμένες πληροφορίες (δικαίωμα στη λήθη) που τον αφορούν και βρίσκονται αναρτημένες σε κοινωνικά δίκτυα, γεγονός που δε μπορούσε να πραγματοποιήσει νωρίτερα. Όσες αναρτήσεις κρίνει πως δεν τον αντιπροσωπεύουν πια ή μπορεί να τον βλάψουν άμεσα ή έμμεσα στην προσωπική, οικογενειακή ή επαγγελματική ζωή, ο χρήστης θα μπορεί να ζητήσει την οριστική διαγραφή τους από το αντίστοιχο κοινωνικό δίκτυο και τους τρίτους στους οποίους τυχόν έχει κοινοποιηθεί. Επιπροσθέτως, θα μπορεί άμεσα να κλείσει κάποιον λογαριασμό σε ένα κοινωνικό δίκτυο και να μεταφέρει τις σχετικές πληροφορίες σε ένα άλλο κοινωνικό δίκτυο (δικαίωμα στη φορητότητα).

Τέλος, σύμφωνα με το νέο Κανονισμό, για την καλύτερη λειτουργία των κοινωνικών δικτύων θα πρέπει οι χρήστες αυτών να δηλώνουν τους λογαριασμούς – προφίλ που δημιουργούν σε ένα επίπεδο με τη μεγαλύτερη δυνατή προστασία (privacy by design)

και μόνο με δικές τους ενέργειες να μπορεί να οριστεί το προφίλ τους ως δημόσια διαθέσιμο προς όλους.

Συνοψίζοντας, τα κοινωνικά δίκτυα και οι εταιρίες στόχευσης μάρκετινγκ και παρακολούθησης που τυχόν συνεργάζονται, θα χρειάζονται πλέον να λαμβάνουν τη συγκατάθεση του χρήστη με κάποιο τρόπο προκειμένου να χρησιμοποιήσουν τα προσωπικά του δεδομένα. Όλες οι πληροφορίες που ακολουθούν "αόρατα" έναν χρήστη στο διαδίκτυο και στα κοινωνικά δίκτυα, θα πρέπει από το Μάιο του 2018, να προσδιοριστούν με σαφήνεια, να ενημερωθούν σχετικά οι χρήστες και να ληφθεί η ρητή συγκατάθεσή τους για τη συνέχιση χρήσης και επεξεργασίας των αντίστοιχων δεδομένων.

Συνεπώς, ο νέος Κανονισμός προστατεύει παράλληλα (i) τα προσωπικά δεδομένα των χρηστών απο τα κοινωνικά δίκτυα και από διαφημιστικές εταιρίες που συνεργάζονται, αλλά και (ii) την πρόσβαση σε πληροφορίες που αναρτούν οι ίδιοι οι χρήστες στα κοινωνικά δίκτυα από άτομα που δεν επιθυμούν. Η σχετική προστασία δεν απαιτεί ειδικές γνώσεις από το χρήστη προκειμένου να τεθεί σε εφαρμογή, αλλά θα εφαρμόζεται αυτόματα για όλους τους χρήστες των κοινωνικών δικτύων. Επιπροσθέτως, ο χρήστης θα μπορεί κάθε στιγμή να αναιρέσει την πιθανή συγκατάθεση που έχει παραχωρήσει σε κοινωνικά δίκτυα ή τις πιθανές δράσεις του σε αυτά απαιτώντας την άμεση αφαίρεσή τους από τα κοινωνικά δίκτυα.

Κεφάλαιο 6: Συμπεράσματα

6.1 Συμπεράσματα έρευνας

Η παραβίαση της ιδιωτικής ζωής στο διαδίκτυο περιλαμβάνει τη μη εξουσιοδοτημένη συλλογή, αποκάλυψη ή άλλη χρήση των προσωπικών δεδομένων των χρηστών στο διαδίκτυο [75]. Καθώς το ηλεκτρονικό εμπόριο εξαπλώνεται και καθώς τα κέρδη των εταιριών που δραστηριοποιούνται στο διαδίκτυο εξαρτώνται άμεσα από την παραβίαση της ιδιωτικότητας των χρηστών, τα προσωπικά δεδομένα που συλλέγουν οι εταιρίες που δραστηριοποιούνται στο διαδίκτυο αυξάνονται σημαντικά. Επιπροσθέτως, η αποτελεσματικότητα και η αποδοτικότητα των στρατηγικών μάρκετινγκ των διαφόρων επιχειρήσεων εξαρτάται άμεσα από τη συλλογή και την επεξεργασία προσωπικών δεδομένων των πελατών τους και του καταναλωτικού κοινού γενικότερα. Συνεπώς, είναι πλέον σχεδόν αδύνατη η χρήση υπηρεσιών στο διαδίκτυο, χωρίς την αποκάλυψη προσωπικών πληροφοριών εκ μέρους των χρηστών [76].

Για τη σχετική προστασία των ατόμων διάφοροι διεθνείς οργανισμοί έχουν δημοσιεύσει κατά καιρούς οδηγίες – συστάσεις όσον αφορά τη διαδικασία συλλογής, αποθήκευσης και επεξεργασίας των σχετικών δεδομένων. Στον τομέα της προστασίας των προσωπικών δεδομένων η Ευρωπαϊκή Ένωση εδώ και μια δεκαετία έχει δημοσιεύσει μια σχετική οδηγία προς τα κράτη μέλη. Ωστόσο, καθώς η τεχνολογία εξελίσσεται και έχοντας αυξηθεί σημαντικά, από το χρόνο έκδοσης της σχετικής οδηγίας, ο όγκος των δεδομένων που συλλέγονται και επεξεργάζονται, πρόσφατα η Ευρωπαϊκή Ένωση εξέδωσε καινούργιο Κανονισμό για την αποτελεσματικότερη προστασία των δικαιωμάτων και των ελευθεριών των κατοίκων της Ένωσης, με τη διορθώνοντας την ισχύουσα οδηγία της Ένωσης (95/46/ΕΚ).

Οι βασικότερες αλλαγές που εισάγει ο νέος Κανονισμός της Ένωσης για την προστασία των προσωπικών δεδομένων των κατοίκων της ΕΕ, αφορούν τη διεύρυνση των δεδομένων που εντάσσονται στις κατηγορίες των προσωπικών δεδομένων και των ευαίσθητων προσωπικών δεδομένων, έχοντας ως αποτέλεσμα τη νομική προστασία τους από την Ένωση.

Εκτός της διεύρυνσης των κατηγοριών των δεδομένων που προστατεύονται από τον καινούργιο Κανονισμό, αυξάνονται οι απαιτήσεις για τη λήψη έγκυρης συγκατάθεσης

του υποκειμένου των δεδομένων για την επεξεργασία των δεδομένων, προσφέροντας επιπλέον προστασία στους κατοίκους της Ένωσης.

Επίσης, ο νέος Κανονισμός διευρύνει το γεωγραφικό πεδίο εφαρμογής της καινούργιας νομοθεσίας, περιλαμβάνοντας οργανισμούς με έδρα εκτός της ΕΕ ή οργανισμούς που εκτελούν την επεξεργασία των δεδομένων εκτός της ΕΕ, όταν τα δεδομένα αφορούν κατοίκους της Ένωσης.

Επιπροσθέτως, οι κυρώσεις παραβίασης του Κανονισμού γίνονται σημαντικά αυστηρότερες και δύναται να οδηγήσουν σε διοικητικό πρόστιμο μέχρι € 20.000.000 ή όταν η παραβίαση του Κανονισμού πραγματοποιείται από μια επιχείρηση, έως 4% του συνολικού ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους.

Επίσης, σημαντική προσθήκη στον καινούργιο Κανονισμό αποτελεί το "δικαίωμα της λήθης (right to be forgotten)" των ατόμων, δηλαδή όταν ένα άτομο δεν επιθυμεί πλέον την επεξεργασία των προσωπικών του δεδομένων και υπό την προϋπόθεση ότι δεν συντρέχουν νόμιμοι λόγοι για τη διατήρηση των δεδομένων, εκείνα θα πρέπει να διαγραφούν άμεσα.

Επιπροσθέτως, με τον νέο Κανονισμό οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία δεδομένων θα έχουν περισσότερες ευθύνες και υποχρεώσεις σε σχέσξ με ότι ίσχυε μέχρι σήμερα (οδηγία 95/46/ΕΚ). Πλέον, οι εκτελούντες την επεξεργασία θα είναι υπόλογοι για πιθανές παραβιάσεις των διατάξεων του Κανονισμού και αντιμέτωποι με βαριά πρόστιμα.

Τέλος, όπως διαφάνηκε από την παρουσίαση του Κανονισμού στο προηγούμενο κεφάλαιο, βασικός στόχος του καινούργιου Κανονισμού είναι η ομοιομορφία της σχετικής νομοθεσίας στα κράτη μέλη της Ένωσης και η καθιέρωση υπηρεσιών μιας στάσης (one-stop-shop) για όλη την Ευρωπαϊκή Ένωση, εξαλείφοντας την ανάγκη παράλληλης επικοινωνίας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία δεδομένων με τις εποπτικές αρχές διαφόρων κρατών μελών για το ίδιο ζήτημα πιθανής παραβίασης δεδομένων των υποκειμένων ή της ορθής εφαρμογής των διατάξεων του νέου Κανονισμού. Η σχετική διευκόλυνση αναμένεται να λειτουργήσει θετικά για την επιχειρηματική δράση στο διαδίκτυο και την αμεσότερη επίλυση πιθανών ζητημάτων που σχετίζονται με τον καινούργιο Κανονισμό.

6.2 Περιορισμοί έρευνας

Βασικός περιορισμός της παρούσας μελέτης αποτελεί η έλλειψη επικοινωνίας του ερευνητή με τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία

δεδομένων με σκοπό να διαπιστωθεί άμεσα και από έγκυρη πηγή ο όγκος των αλλαγών που προκαλούνται στη λειτουργία των σχετικών οργανισμών από την εφαρμογή του καινούργιου Κανονισμού. Μια σχετική έρευνα θα επέτρεπε την αποτίμηση πιθανών οικονομικών δυσκολιών για τους αντίστοιχους οργανισμούς που προκαλεί ο καινούργιος Κανονισμός ή πρακτικών δυσκολιών στην αποτελεσματική και έγκαιρη εφαρμογή του από τις 28 Μαΐου 2018.

Επίσης, η παρούσα μελέτη δεν περιλαμβάνει στοιχεία έρευνας με τα υποκείμενα των δεδομένων, προκειμένου να διαπιστωθεί ποιες είναι οι απαιτήσεις τους από έναν καινούργιο Κανονισμό στην Ένωση, με σκοπό την προάσπιση των προσωπικών τους δεδομένων.

Η συμπερίληψη μιας σχετικής έρευνας θα επέτρεπε την αποτελεσματικότερη αποτίμηση των οφελών και των περιορισμών του καινούργιου Κανονισμού της Ένωσης.

6.3 Προτάσεις για μελλοντικές έρευνες

Από την παρουσίαση του καινούργιου Κανονισμού της Ένωσης σχετικά με την προστασία των προσωπικών δεδομένων των κατοίκων της Ένωσης, διαφαίνονται σημαντικές αλλαγές στις υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία δεδομένων. Επίσης, υπάρχει διαφοροποίηση στα δικαιώματα των υποκειμένων των δεδομένων και της διαδικασίας αντιμετώπισης σχετικών παραβιάσεων των δεδομένων. Επιπροσθέτως, οι κυρώσεις (διοικητικά πρόστιμα) για τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων αυξάνονται σημαντικά, αποτελώντας έναν ορατό κίνδυνο για τους αντίστοιχους οργανισμούς.

Με σκοπό την προσαρμογή των σχετικών οργανισμών στα νέα δεδομένα θα ήταν χρήσιμη η υλοποίηση έρευνας σχετικά με τα βήματα – οδηγό εφαρμογής που θα πρέπει να ακολουθήσει ένας οργανισμός που ήδη εφαρμόζει επεξεργασία δεδομένων εντός της Ένωσης ή επεξεργασία δεδομένων κατοίκων της Ένωσης εκτός των γεωγραφικών ορίων της Ευρωπαϊκής Ένωσης, προκειμένου να διασφαλιστεί η συμμόρφωση των σχετικών οργανισμών προς τις απαιτήσεις του νέου Κανονισμού.

Βιβλιογραφία

[1] Moschovitis, C. J. P., Polle, H., Schuyler, T., & Senft, T. M. (1843). From Sputnik to the ARPAnet: 1957-1969. History of the Internet: A Chronological, 33-62.

[2] Khazaal, Y., Chatton, A., Atwi, K., Zullino, D., Khan, R. and Billieux, J., (2011). Arabic validation of the compulsive Internet use scale (CIUS). Substance abuse treatment, prevention, and policy, 6(1), p.1.

[3] United Nations High Commissioner for Human Rights - OHCHR, (2014). Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age, 24 February 2014, Room XXI, Palais des Nations, Geneva. Λήψη από: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E#sthash.zj49BZlJ.dpuf

[4] Chen, T. C. (2002). ISPRS and Internet: history, presence, and future. Journal of Photogrammetry and Remote Sensing, 7(0), 77-87.

[5] Castells, Manuel (2013). The Impact of the Internet on Society: A Global Perspective. In BBVA. Ch@nge, Bilbao: BBVA Bilbao, 127–149.

[6] Internet Live Stats, (2016). Internet Users. Λήψη από: http://www.internetlivestats.com/internet-users/

[7] Weyers, B. (2013). The Internet's Impact on Our Thinking. AP Literature. nd. Online. Λήψη από: https://www.nshss.org/media/1497/weyers.pdf

[8] Oak, M. (2016). Positive Effects of the Internet That Have Been Very Profitable. Λήψη από: http://www.buzzle.com/articles/positive-effects-of-internet.html

[9] Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukophadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being?. American psychologist, 53(9), 1017-1031.

[10] Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. Research Brief No. RBX03-06. London: DfES.

[11] Atkinson, R. (2008). Societal effects of cyberbullying: The dark side of building bridges with technology. South Atlantic Philosophy of Education Society Yearbook, 32-41.

[12] Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard a preliminary look at cyberbullying. Youth violence and juvenile justice, 4(2), 148-169.

[13] Young, K. S. (1999). Internet addiction: symptoms, evaluation and treatment.Innovations in clinical practice: A source book, 17, 19-31.

[14] Harvey- Berino, J., Pintauro, S., Buzzell, P., & Gold, E. C. (2004). Effect of internet support on the long- term maintenance of weight loss. Obesity research, 12(2), 320-329.

[15] Internet World Stats, (2016). INTERNET USAGE STATISTICS. Λήψη από: http://www.internetworldstats.com/stats.htm

[16] Internet Live Stats, (2016). Internet Users by Country (2016). Λήψη από: http://www.internetlivestats.com/internet-users-by-country/

[17] CNN Greece, (2016). ΕΛΣΤΑΤ: 6 στους 10 Έλληνες μπαίνουν στο internet

μέσω τηλεφώνου. Λήψη από: http://www.cnn.gr/money/story/54139/elstat-6-stoys-10-ellines-mpainoyn-sto-internet-meso-tilefonoy
[18] Drucker, P.F., (1994). The theory of the business. Harvard business review, 72(5), 95-104.
[19] Rappa, M., (2001). Managing the digital enterprise-Business models on the Web. North Carolina State University. Λήψη από: http://digitalenterprise.org/models/models.html
[20] Statista, (2016). Global internet advertising revenue in 2015 and 2020 (in billion U.S. dollars). Λήψη από: https://www.statista.com/statistics/237800/global-internet-advertising-revenue
[21] Doctorow, C., (2015). The shrinking of the big data promise. The Guardian. Λήψη από: https://www.theguardian.com/world/2015/jun/30/the-shrinking-of-the-big-data-promise
[22] Clarke, R. (1994). The digital persona and its application to data surveillance. The information society, 10(2), 77-92.
[23] Fuchs, C. (2010). Remarks on the BBC documentary "Virtual Revolution: The Cost of Free". Λήψη από: http://fuchs.uti.at/326/
[24] Schneier, B., (2013). 'Stalker economy' here to stay. CNN. Λήψη από: http://edition.cnn.com/2013/11/20/opinion/schneier-stalker-economy/
[25] Schneier, B., (2015). How we sold our souls – and more – to the internet giants. The Guardian. Λήψη από: https://www.theguardian.com/technology/2015/may/17/sold-our-souls-and-more-to-internet-giants-privacy-surveillance-bruce-schneier
[26] Newman, N., (2011). You're Not Google's Customer — You're the Product: Antitrust in a Web 2.0 World. Λήψη από: http://www.huffingtonpost.com/nathan-newman/youre-not-googles-custome_b_841599.html
[27] Saxe, R.S., (2008). Website personalization using data mining and active database techniques. In 20th Computer Science Seminar (pp. 1-5).
[28] The Wall Street Journal, (2010). The Big Interview with Eric Schmidt [video file]. Λήψη από: http://www.wsj.com/video/the-big-interview-with-eric-schmidt/635487A7-CE86-462E-8783-F1AF61BC988A.html
[29] The New Transparency Project, (2014). Protecting your Online Privacy: FAQs. Λήψη από: http://www.surveillanceincanada.org/resources
[30] Goodson, S., (2012). If You're Not Paying For It, You Become The Product. Forbes. Λήψη από: http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product
[31] Goodchild, M. F. (2007). Citizens as voluntary sensors: spatial data infrastructure in the world of Web 2.0. IJSDIR 2: 24–32.
[32] Dee, J. (2007). All the news that's fit to print out. New York Times Magazine, July 1.
[33] Murugesan, S. (2007). Understanding Web 2.0. IT professional, 9(4), 34-41.
[34] Bolotaeva, V., & Cata, T. (2010). Marketing opportunities with social networks.Journal of Internet Social Networking and Virtual Communities, 2010, 1-8.
[35] Harris, A. L., & Rea, A. (2009). Web 2.0 and virtual world technologies: A growing impact on IS education. Journal of Information Systems Education, 20(2), 137 – 144.
[36] Allmer, T. (2010). The Internet & Surveillance-Research Paper Series 2011. Λήψη από: http://www.sns3.uti.at/wp-content/uploads/2010/09/The-Internet-

Surveillance-Research-Paper-Series-11-Thomas-Allmer-Toward-a-Critical-Theory-of-Surveillance-Studies.pdf
[37] OECD (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220
[38] Gorgone, K. (2016). 4 Ways to Protect Your Online Privacy. Λήψη από: http://m.ragan.com/Main/Articles/50465.aspx
[39] Aspan, M. (2008). How Sticky Is Membership on Facebook? Just Try Breaking Free. The New York Times. Λήψη από: http://www.nytimes.com/2008/02/11/technology/11facebook.html?_r=0
[40] Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. Identity in the Information Society, 2(1), 39-63.
[41] Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: it's complicated. In Proceedings of the eighth symposium on usable privacy and security (p. 9). ACM.
[42] DesMarais, C. (2013). 11 Simple Ways to Protect Your Privacy. The Time. Λήψη από: http://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy
[43] Lawrence, J. & Rintel, S. (2013). Eight ways to protect your privacy online. The Guardian. Λήψη από: https://www.theguardian.com/commentisfree/2013/dec/03/eight-ways-to-protect-your-privacy-online
[44] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.
[45] Pelteret, M. (2015). Information Privacy and Its Importance to Consumers and Organisations. University of Cape Town.
[46] Tavani, Herman T. (2008). Informational Privacy: Concepts, Theories, and Controversies, pp. 131-164 in Himma, Kenneth E. & Tavani, Herman T. (eds.) The Handbook of Information and Computer Ethics. Hoboken, NJ: Wiley.
[47] Fried, C. (1984). Privacy. In F. D. Schoeman (Ed.), Philosophical dimensions of privacy (pp.203-22). New York: Cambridge University Press.
[48] Westin, A. (1967), Privacy and Freedom, Altheneum, New York, NY
[49] Beardsley, E. (1971). Privacy: Autonomy and selective disclosure. In J. R. Pennock & J. W. Chapman (Eds.), Nomos XZZZ: Privacy (pp. 56-70). New York: Atherton Press
[50] Diaz, C., & Gürses, S. (2012). Understanding the landscape of privacy technologies. Extended abstract of invited talk in proceedings of the Information Security Summit, 58-63.
[51] Kleeman, S. (2015). In One Quote, Snowden Just Destroyed the Biggest Myth About Privacy. Λήψη από: https://mic.com/articles/119602/in-one-quote-edward-snowden-summed-up-why-our-privacy-is-worth-fighting-for#.yqSglVNx6
[52] Calo, R. (2010). The boundaries of privacy harm. Indiana Law Journal. 86(3). 1130-1162.
[53] Go Globe, (2016). The state of online privacy - Statistics and Trends. Λήψη από: http://www.go-globe.hk/blog/online-privacy
[54] Rainie, L. (2016). The state of privacy in post-Snowden America. Λήψη από: http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/

[55] Kietzmann, J., & Angell, I. (2010). Panopticon revisited. Communications of the ACM, 53(6), 135-138.
[56] Madden, (2012). Privacy management on social media sites. Λήψη από: http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/
[57] Statistica, (2015). Level of concern about the control over personal information provided online in the European Union (EU-28) as of March 2015. Λήψη από: https://www.statista.com/statistics/533874/level-of-concern-about-the-control-over-personal-data-shared-online-in-the-eu
[58] Εισαγγελέας του Αρείου Πάγου (2011), Εξετάσεις DNA. Λήψη από: http://www.eisap.gr/sites/default/files/consulations/gnom2011_0015.pdf
[59] Mullikin, A., & Rahman, S. (2010). The Ethical Dilemma of the USA Government Wiretapping. International Journal of Managing Information Technology (IJMIT), 2(4). ISSN : 0975-5586
[60] Boillat, P., & Kjaerum, M. (2014). Handbook on European data protection law. Luxembourg: Publications Office of the European Union.
[61] De Hert, P., & Papakonstantinou, V. (2013). Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?. I/S: A Journal of Law and Policy for the Information Society. 9(3). 272–324
[62] Rule, J. B., & Greenleaf, G. W. (Eds.). (2010). Global privacy protection: the first generation. Edward Elgar Publishing.
[63] Fuster, G. G. (2014). The Emergence of Personal data Protection as a Fundamental Right of the EU (Vol. 16). Springer Science & Business.
[64] Kobsa, A. (2002). Personalized hypermedia and international privacy. Communications of the ACM, 45(5), 64-67.
[65] Ακριβοπούλου, Χ. (2011). Η προστασία της ιδιωτικότητας στην ΕΕ: μια ανάλυση του νομοθετικού πλαισίου και της νομολογίας του δεκ. Διάλεξη στο πλαίσιο επιστημονικων εκδηλωσεων ΕΙΔΑΔ. Λήψη από:http://www.hiifl.gr/wp-content/uploads/Akrivopoulou-Final.pdf
[66] Mantelero, A. (2012). Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution. European Journal of Law and Technology, 3(2). Λήψη από:http://ejlt.org//article/view/96
[67] Nickenig, J. (2011). The challenges of European data protection policy: an analysis of supranational decision-making processes (Bachelor's thesis, University of Twente).
[68] TechTarget, (2010). EU Data Protection Directive (Directive 95/46/EK). Λήψη από: http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC
[69] Μερίδου, Ε. (2002). Το νομικό πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα στο Ελληνικό Δίκαιο. Λήψη από: http://www.sofos.com.gr/news2.html
[70] Fulbright, N. R. (2013). Global Data Privacy Directory. Λήψη από: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf
[71] Ευρωπαϊκή Επιτροπή, (2010). European Commission sets out strategy to strengthen EU data protection rules (Βρυξέλλες, 4 Νοεμβρίου 2010). Λήψη από: http://www.europa.eu/rapid/press-release_IP-10-1462_en.htm
[72] Ευρωπαϊκή Επιτροπή, (2012).Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs f

or businesses, (Βρυξέλλες, 25 Φεβρουαρίου 2012). Λήψη από: http://europa.eu/rapid/press-release_IP-12-46_en.htm
[73] Berg-Larsen, E. (2015). The Issue of Privacy in the European Union-Controversies of the General Data Protection Regulation (Master's thesis).
[74 Ευρωπαϊκή Επιτροπή, (2012). Μεγαλύτερη προστασία του δικαιώματος ιδιωτικότητας στο Διαδίκτυο - 25/01/2012. Λήψη από: http://ec.europa.eu/news/business/120125_el.htm
[75] Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: awareness, attitudes and actions. Information Management & Computer Security, 19(1), 53-73.
[76] Bandyopadhyay, S. (2012). Consumers' online privacy concerns: causes and effects. Innovative Marketing, 8(3), 32-39.