ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΜΜΕ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Το θεσμικό πλαίσιο του διαδικτύου στην Ελλάδα

ΣΚΑΡΤΣΟΥ ΑΝΤΙΓΌΝΗ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΩΤΉΡΗΣ ΤΡΙΑΝΤΑΦΥΛΛΟΥ

ΠΥΡΓΟΣ, 2018

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω/ουμε ότι είμαι/είμαστε ο/οι συγγραφέας/εις αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα/είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία.

Επίσης, έχω/έχουμε αναφέρει τις οποίες πηγές από τις οποίες έκανα /κάναμε χρήση δεδομένων, ιδεών η λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες.

Ακόμη δηλώνω/ουμε ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα/εμάς προσωπικά και αποκλειστικά και ειδικά για την συγκεκριμένη πτυχιακή εργασία ότι θα αναλάβω/ουμε πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχτεί ότι δεν μου/μας ανήκει.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 1	ΑΡΙΘ.ΜΗΤΡΩΟΥ	ΥΠΟΓΡΑΦΗ
Σκαφτούρη Δυμήνη	2033	
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 2	ΑΡΙΘ.ΜΗΤΡΩΟΥ	ΥΠΟΓΡΑΦΗ
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ 3	ΑΡΙΘ.ΜΗΤΡΩΟΥ	ΥΠΟΓΡΑΦΗ

ΠΙΣΤΟΠΟΙΗΣΗ

Πιστοποιείται ότι η πτυχιακή εργασία με θέμα :

<< Το θεσμικό πλαίσιο του διαδικτύου στην Ελλάδα .....

.....>>

Της/Των φοιτητριας/ων του Τμήματος ΠΛΗΡΟΦΟΡΙΚΗΣ & ΜΕΣΩΝ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ	ΑΡΙΘ.ΜΗΤΡΩΟΥ
1.	Σκάρτσου Ευαγγελία	2033
2.		
3.		

Παρουσιάστηκε δημόσια και εξετάστηκε στο τμήμα ΠΛΗΡΟΦΟΡΙΚΗΣ & ΜΜΕ στις

...../...../2018

Ο ΕΠΙΒΛΕΠΩΝ

.....

Ο ΠΡΟΕΔΡΟΣ ΤΟΥ ΤΜΗΜΑΤΟΣ

Δρ. ΙΩΑΝΝΗΣ ΚΟΥΓΙΑΣ
ΚΑΘΗΓΗΤΗΣ

ΠΡΟΛΟΓΟΣ

Το διαδίκτυο αποτελεί ένα από τα πιο σημαντικά κεφάλαια της τεχνολογίας που με την δημιουργία και τη διάδοση του έφερε μια επανάσταση στη καθημερινότητα των ανθρώπων και γενικότερα στη κοινωνία. Οι άπειρες δυνατότητες που προσφέρει προσελκύει όλο και μεγαλύτερο μέρος του πληθυσμού να ανακαλύψει, να ενημερωθεί, να εξελιχθεί, να εκμεταλλευτεί όσα του προσφέρονται. Η επικοινωνία, η ψυχαγωγία, η ενημέρωση, η διάδοση των πληροφοριών και η κάλυψη καθημερινών αναγκών διευκολύνθηκαν σε μεγάλο βαθμό και άρχισαν να αποκτούν διαδραστικό χαρακτήρα σε όλους τους τομείς που αφορούν τη ζωή ενός ατόμου.

Η τεχνολογική εξέλιξη, παρόλο που αποτέλεσε ένα μεγάλο βοήθημα στη βελτίωση της ποιότητας της ζωής των ανθρώπων, επέφερε και αρνητικά αποτελέσματα λόγω των κινδύνων που παραμονεύουν σε κάθε κλικ του ποντικιού ενός χρήστη. Αυτοί οι κίνδυνοι αποτέλεσαν και το κίνητρο για να ερευνήσω τα διαφορετικά είδη απάτης που ελλοχεύουν στο διαδίκτυο και ιδιαίτερα την ασφάλεια που προσφέρουν οι νόμοι στην Ελλάδα σχετικά με τη παραβατικότητα στο διαδίκτυο.

ΠΕΡΙΛΗΨΗ

Ο σκοπός της παρούσας πτυχιακής εργασίας είναι η παρουσίαση του θεσμικού πλαισίου που υπάρχει για το διαδίκτυο στην Ελλάδα, στους τομείς των προσωπικών δεδομένων, του ηλεκτρονικού εγκλήματος και των Μέσων Μαζικής Ενημέρωσης. Για την ανάλυση του θέματος έχει πραγματοποιηθεί μια σχετική έρευνα μέσω του διαδικτύου και συγκεκριμένης βιβλιογραφίας. Επίσης, συντάχθηκε ερωτηματολόγιο σχετικό με τη χρήση του διαδικτύου, που έγινε από μια γκάμα ατόμων διαφόρων ηλικιών.

Αρχικά, έγινε μια ανασκόπηση της ιστορίας του Διαδικτύου που δείχνει πως δημιουργήθηκε, ποιες λειτουργίες πρόσφερε τότε και πως εξελίχθηκε σε αυτό που είναι σήμερα. Επίσης, αναλύονται τα μέσα κοινωνικής δικτύωσης που έχουν εισέλθει δυναμικά στη καθημερινότητα των ανθρώπων με θετικά και αρνητικά αποτελέσματα. Παράλληλα, έγινε λόγος για το νέο ψηφιακό τοπίο που εκσυγχρόνισε όλα τα εργαλεία που χρησιμοποιούνταν από τον άνθρωπο.

Στη συνέχεια, γίνεται αναφορά στα προσωπικά δεδομένα και την ακαταλόγιστη χρήση τους στο διαδίκτυο που επιφέρει ανησυχίες σχετικά με τη προστασία και καταλήγει, αν γίνει κακή χρήση αυτών, στη παραβίαση της προσωπικής ζωής του χρήστη. Για αυτό και στο τέλος του κεφαλαίου γίνετε λόγος για το νομικό πλαίσιο της προστασίας των προσωπικών δεδομένων στην Ελλάδα που θα πρέπει κάθε χρήστης να είναι ενήμερος.

Στο επόμενο κεφάλαιο, παρουσιάζονται τα είδη του ηλεκτρονικού εγκλήματος που παραμονεύουν στο διαδίκτυο, στους γνώστες της τεχνολογίας που τη χρησιμοποιούν ως «όπλο» τους για να προβούν σε άνομες ενέργειες και στις μεθόδους πρόληψης, νομική-ποινική αντιμετώπιση του εν λόγο εγκλήματος, για την αποφυγή των απειλών.

Επιπλέον, αναλύονται οι λόγοι που το διαδίκτυο έχει πάρει τη πρωτοκαθεδρία της ενημέρωσης των πολιτών στην Ελλάδα από τα παραδοσιακά μέσα και γίνεται μια σύγκριση των δυνατοτήτων που προσφέρει το κάθε μέσο ενημέρωσης. Παράλληλα, γίνεται λόγος για την ελευθερία έκφρασης που προσφέρει το διαδικτύου αλλά και για τη αρνητική πλευρά που θέλει τους πολίτες ως παθητικούς θεατές και πιόνα στη διάδοση της παραπληροφόρησης. Ιδιαίτερα, τονίζεται ο ρόλος των ΜΜΕ στη ζωή των εφήβων και ο διαδικτυακός εθισμός που δεσπόζει στη σημερινή εποχή και οδηγεί το κράτος στη νομιμοποίηση των ΜΜΕ με πρόσθετο μέλος το διαδίκτυο.

Τέλος, εμφανίζονται τα αποτελέσματα του ερωτηματολογίου που έγινε σε μια γκάμα ανθρώπων για να γνωστοποιηθεί η χρήση του διαδικτύου, από ποιόν γίνεται, πως γίνεται, τι προτιμάται και πόσοι είναι γνώστες των δικαιωμάτων τους. Επίσης, αποτυπώνονται οι απαντήσεις από μια συνέντευξη με ένα έννομο όργανο του κράτους για μια πιο επιστημονική άποψη σχετικά με το θεσμικό πλαίσιο στο διαδίκτυο που επικρατεί στην Ελλάδα.

EXECUTIVE SUMMARY

The purpose of this dissertation is to present the institutional framework for the Internet in Greece, in the areas of personal data, electronic crime and media. In order this topic to be analyzed, has been conducted a relevant research through internet and specific bibliography. Also, a questionnaire was drawn up, on the use of the internet, by a range of people of different ages.

Initially, there has been a review in the history of Internet that shows how it was created, what were the functions offered then and how evolved into what it is today. It also analyzes the social media that have entered dynamically in the everyday life of people with positive and negative results. At the same time, we talked about the new digital landscape that has modernized all the tools used by humans.

Then, reference is made to personal data and their incomprehensible (unreasonable) use on the Internet that gives rise to concerns about protection and misuses which could ended up in violating the privacy of the user. For this reason, at the end of the chapter we are talking about the legal framework on the protection of personal data in Greece that should be kept up to date by every user.

In the next chapter are presented the types of online crimes that are lurking on the internet, technology “specialists” who use it as "weapon" for their illegal actions and prevention methods to avoid threats and criminal treatment of the crime.

In addition, they are analyzed the reasons why the internet has taken the lead of informing citizens in Greece by traditional media and comparing the abilities offered by each type of media. At the same time, there is a talk about the freedom of expression offered by internet, but also the negative side which want citizens as passive viewers to the proliferation of misinformation. Particularly, it emphasizes the role of media in the life of adolescents and the online addiction that prevails in the current era and leads the state to legalize media including internet among them.

Finally, the results of the questionnaire made in a range of people are presented to make the use of internet known, by who they are, how they do, what they prefer, and how many are aware of their rights. Also the replies, from an interview with a legal body of the state for a more scientific view on the institutional framework on the internet prevailing in Greece, are reflected.

Πίνακας περιεχομένων

ΠΡΟΛΟΓΟΣ 3
ΠΕΡΙΛΗΨΗ 5
ΕΙΣΑΓΩΓΗ 10
ΚΕΦΑΛΑΙΟ 1ο – ΔΙΑΔΙΚΤΥΟ 11
1.1 Ιστορική εξέλιξη διαδικτύου 11
1.1.1 Παγκόσμιος Ιστός (WWW) 12
1.2 Το διαδίκτυο σήμερα 14
1.2.1 Ψηφιακή Ανισότητα 14
1.3 Νέα Μέσα & Μέσα κοινωνικής δικτύωσης 15
1.3.1 Πλεονεκτήματα και μειονεκτήματα των μέσων κοινωνικών δικτύων 17
1.3.2 Η αντικειμενικότητα και τα νέα μέσα 19
1.4 Νέο ψηφιακό τοπίο & Ψηφιακή επανάσταση 21
1.4.1 Το τοπίο της ψηφιακής ενημέρωσης στην Ελλάδα και τον κόσμο. 23
ΚΕΦΑΛΑΙΟ 2ο - ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ 28
2.1 Ορισμός των προσωπικών δεδομένων 28
2.1.1 Χρήση προσωπικών δεδομένων στο Διαδίκτυο 29
2.1.2. Προστασία των προσωπικών δεδομένων 30
2.2 Η ιδιωτικότητα στο Διαδίκτυο 31
2.2.1 Η διαδικτυακή ιδιωτικότητα 31
2.2.2 Δεδομένα προσωπικής και μη προσωπικής ταυτοποίησης του χρήστη 32
2.2.3 Ανησυχίες για την ιδιωτικότητα 33
2.2.4 Παραβίαση Ιδιωτικής Ζωής 33
2.2.5 Facebook και ιδιωτικότητα 34
2.2.6 Συνέπειες παραβίασης προσωπικών δεδομένων 36
2.3 Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων στην Ελλάδα 36
2.3.1 Τρόποι προστασίας προσωπικών δεδομένων 41
2.3.2 Τεχνολογίες προστασίας των χρηστών του διαδικτύου 41
ΚΕΦΑΛΑΙΟ 3^{ο} - ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ 42
3.1 Ορισμός ηλεκτρονικού εγκλήματος 42
3.2 Κυβερνοέγκλημα 43
3.3 Ηλεκτρονικοί εγκληματίες 44
3.3.1 Εξωτερικές απειλές-hackers 44
3.3.2 Εσωτερικές απειλές 46

3.4 Μορφές ηλεκτρονικού εγκλήματος....46
3.4.1 Γνήσια ηλεκτρονικά εγκλήματα....47
3.4.2 Εγκλήματα με τη χρήση υπολογιστή....49
3.5 Η απάτη στο διαδίκτυο....49
3.6 Ασφάλεια στο διαδίκτυο και ηλεκτρονικό έγκλημα....51
3.6.1 Ηλεκτρονικό έγκλημα και πρόληψη....52
3.6.2 Αντιμετώπιση καταστροφών....54
3.7 Η νομοθεσία στο ηλεκτρονικό έγκλημα....57
3.7.1 Ειδικότερες διατάξεις που έχουν σχέση με το ηλεκτρονικό έγκλημα....64
3.7.2 Το πρόβλημα δικαιοδοσίας στο διαδίκτυο....65
ΚΕΦΑΛΑΙΟ 4^{ο} - ΜΕΣΑ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ....66
4.1 Η αλλαγή του τοπίου της Ενημέρωσης από τα Νέα Μέσα....66
4.1.1 Μέσα κοινωνικής δικτύωσης....69
4.2 ΔΙΑΔΙΚΤΥΑΚΗ ΕΝΗΜΕΡΩΣΗ....70
4.2.1 Παθητικοί θεατές....72
4.3 Η ελευθερία της έκφρασης στο διαδίκτυο....73
4.3.1 Σύγκριση ενημέρωσης διαδικτύου από τα παραδοσιακά μέσα....75
4.3.2 Παραπληροφόρηση....76
4.4 Ο ρόλος των ΜΜΕ στη ζωή των εφήβων....77
4.4.1 Mobile journalism....79
4.4.2 Διαδικτυακός εθισμός....80
4.5 Νομιμοποίηση των ΜΜΕ....81
ΚΕΦΑΛΑΙΟ 5ο- Έρευνα μέσω ερωτηματολογίου - Αποτελέσματα....83
5.1. Θέμα και σκοπός της έρευνας....83
5.2. Αναγκαιότητα και σπουδαιότητα της έρευνας....83
5.3 Περιγραφή ερωτηματολογίου....84
5.4 Δημογραφικά χαρακτηριστικά του δείγματος....85
5.4.1. Φύλο....85
5.4.2. Ηλικία....85
5.4.3. Μορφωτικό επίπεδο....86
5.5 Συχνότητα χρήσης διαδικτύου....87
5.6 Κατοχή λογαριασμών στα social media....87
5.7 Λόγοι χρήσης διαδικτύου....88

5.8 Ενημέρωση από τα ΜΜΕ....89
5.9 Αντίληψη πληρότητας νόμων διαδικτύου για προστασία πολιτών....89
5.10 Επιλογή αποτελεσματικότητας νόμων κοινωνίας ή νόμων διαδικτύου....90
5.11 Δυσκολία εντοπισμού διαδικτυακού εγκληματία....91
5.12 Γνώση δικαιωμάτων Διαδικτύου....91
5.13 Ακολουθία νόμων κράτους με εξέλιξη τεχνολογίας....92
5.14 Νομική ενημερότητα αρμόδιων οργάνων για νόμους Διαδικτύου....93
5.15 Αντίληψη κατεύθυνσης σε περίπτωση διαδικτυακού εγκλήματος....94
ΣΥΜΠΕΡΑΣΜΑΤΑ....95
ΒΙΒΛΙΟΓΡΑΦΙΑ....97

ΕΙΣΑΓΩΓΗ

Το διαδίκτυο αποτελεί ένα από τα πιο σημαντικά επιτεύγματα του ανθρώπου, το οποίο συνέβαλε σε μια τεράστια τεχνολογικά ανάπτυξη και σε μια ψηφιακή επανάσταση που θα ερχόταν και θα άλλαζε τα μέχρι τότε δεδομένα της ζωής των ατόμων. Το διαδίκτυο εξελίχθηκε ραγδαία σε όλα τα μέρη του πλανήτη και εισήλθε με επιβλητικό τρόπο στη καθημερινότητα του κάθε πολίτη. Αυτή όμως η απότομη ανάπτυξη έδωσε το έναυσμα σε κάποιους επιτήδειους να εκμεταλλευτούν τη τεχνολογία για προσωπικό τους όφελος διαπράττοντας σοβαρά διαδικτυακά εγκλήματα. Έτσι, το κράτος για να περιορίσει και να ελέγξει αυτή τη παραβατικότητα δημιούργησε καινούριους νόμους ή τροποποίησε παλιούς με τη προσθήκη νέων εννοιών. Οι νόμοι αυτοί πρέπει συνεχώς πρέπει να εξελίσσονται και να συμβαδίζουν με τα νέα δεδομένα της τεχνολογίες πράγμα που δυσκολεύει και το ίδιο το κράτος και τις αρμόδιες αρχές.

Γενικά, δεν θα μπορούσε να εξηγήσει τίποτα καλύτερα από τη φράση «Ό,τι ανεβαίνει στο διαδίκτυο, μένει στο διαδίκτυο» αφού είναι σχεδόν αδύνατο να διαγραφεί κάθε δεδομένο που κοινοποιείται μέσω αυτού. Έτσι, συχνά ακούμε τα φαινόμενα κλοπής προσωπικών δεδομένων ανθρώπων και επιχειρήσεων, ηλεκτρονικών εγκλημάτων, παραπληροφόρησης των χρηστών για τα οποία γίνεται εκτενή ανάλυση στα παρακάτω κεφάλαια. Οι πιο πολλοί χρήστες, ιδιαίτερα όταν είναι νεαρής ηλικίας εντυπωσιάζονται από το νέο εικονικό κόσμο , προσκολλώνται σε αυτόν και εκθέτουν τα προσωπικά δεδομένα σε γνωστούς και αγνώστους.

Για αυτό, και θεώρησα σημαντική την έρευνα των δικαιωμάτων που έχει κάθε χρήστης του διαδικτύου αν πέσει θύμα απάτης. Στην έρευνα παρουσιάζονται τα είδη της παραβατικότητας και των εγκλημάτων που είναι τα πιο συνήθης και πρέπει ο κάθε πολίτης να είναι γνώστης των νόμων που τα περιστοιχίζουν.

Η παρούσα πτυχιακή χωρίζεται σε πέντε κεφάλαια. Στο πρώτο κεφάλαιο, γίνεται αναφορά στην ιστορική εξέλιξη του διαδικτύου μέχρι σήμερα και στα νέα μέσα που επέφερε με την ανάπτυξη του. Στο δεύτερο κεφάλαιο, παραπέμπεται η έννοια των προσωπικών δεδομένων, σε ποιες κατηγορίες χωρίζονται και η έννομη αντιμετώπιση τους αν αυτά παραβιαστούν. Στο τρίτο κεφάλαιο, αναλύονται τα είδη των ηλεκτρονικών εγκλημάτων , τα χαρακτηριστικά τους και οι τρόποι προστασία τους είτε μέσων εργαλείων είτε μέσω των νόμων που δεσπόζουν το Ελληνικό Κράτος. Στο τέταρτο κεφάλαιο, καθορίζεται η προσθήκη του διαδικτύου στην έννοια των Μέσων Μαζικής Ενημέρωσης και συγκρίνεται με τα παλαιότερα έτσι να γνωστοποιηθούν οι καλές πτυχές της ενημέρωσης από το διαδίκτυο αλλά και οι παγίδες που κρύβει. Όπως και στα προηγούμενα κεφάλαια έτσι και σε αυτό αναγράφονται οι εν ισχύ νόμοι που δεσπόζουν στα ΜΜΕ. Στο τελευταίο κεφάλαιο, παρατηρούνται τα αποτελέσματα του ερωτηματολογίου του διεξήχθη για τη προβολή των απόψεων των χρηστών σε σχέση με τη χρήση του διαδικτύου στην Ελλάδα.

ΚΕΦΑΛΑΙΟ 1ο – ΔΙΑΔΙΚΤΥΟ

1.1 Ιστορική εξέλιξη διαδικτύου

Το διαδίκτυο είναι ένας σύνδεσμος με εκατομμύρια υπολογιστές οι οποίοι είναι διασυνδεμένοι και δίνει τη δυνατότητα σε εκατομμύρια χρήστες σε κάθε πλευρά του πλανήτη να μπορούν να επικοινωνούν μεταξύ τους και με αυτό τον τρόπο να ανταλλάσσουν πληροφορίες (Laudon & Traver, 2011).

Αρχικά, οι πρώτες προσπάθειες για τη δημιουργία του διαδικτύου έγιναν κατά τη περίοδο του ψυχρού πολέμου στις ΗΠΑ. Οι αμερικανοί επειδή φοβόντουσαν για την προστασία της χώρας τους, διότι εκείνη τη περίοδο η Ρωσία είχε στείλει στο διάστημα τον δορυφόρο Σπούτνικ 1 ,αποφάσισαν να δημιουργήσουν την ARPA (Advanced Research Project Agency), όπου είναι η υπηρεσία προηγμένων αμυντικών ερευνών , γνωστή ως DARPA (Defense Advanced Research Projects Agency) στις μέρες μας. Έτσι, οι Αμερικανοί επειδή ζούσαν υπό το φόβο μιας πυρηνικής επίθεσης από τους Ρώσους θέλησαν για πρώτη φορά να στα χρονικά να κατασκευάσουν ένα σύστημα επικοινωνίας όπου δυο υπολογιστές θα συνδέονταν μεταξύ τους (Norton's, 2012).

Οι Αμερικανοί άρχισαν να επεξεργάζονται αυτή τη σκέψη, ώσπου μετά από ανάπτυξη και έρευνα πολλών επιστημόνων δημιουργήθηκε το 1969 το ARPANET (Advanced Research Projects Agency Network).

Ύστερα από τη λειτουργία αυτού του δικτύου, άρχισαν διαμέσου της DARPA , και συγκεκριμένα των δικτυώσεων της, να συνδέονται με το ARPAnet και άλλα πειραματικά δίκτυα. Τα πιο πολλά από αυτά χρησιμοποιούνταν για στρατιωτικές έρευνες, αλλά φάνηκαν ιδιαίτερα χρήσιμα και για ορισμένα πανεπιστήμια. Όσοι ερευνητές συμμετείχαν, τους δινόταν η δυνατότητα ανταλλαγής βάσεων δεδομένων, προγραμμάτων ακόμα και σκληρών δίσκων ενώ είχαν συνδεθεί από διαφορετικά κέντρα υπολογιστών. 23 κόμβοι είχαν συνδεθεί μέχρι το 1971, ενώ μέχρι το 1980 είχαν αυξηθεί στους 200 και ταυτόχρονα είχαν αρχίσει να δημιουργούνται τα πρώτα διεθνή δίκτυα(Laudon & Traver, 2011).

Το 1980, το ARPAnet διαχωρίστηκε σε δύο δίκτυα τα οποία εξακολουθούσαν να συνδέονταν μεταξύ τους.Το ένα τμήμα είχε αφιερωθεί στα στρατιωτικά και ονομάστηκε MILNET και το άλλο σε όλες τις υπόλοιπες χρήσεις και λεγόταν αρχικά DARPA Internet για να καταλήξει εντέλει να μετονομαστεί σε "δίκτυο του Internet". Στα τέλη του 70 και στις αρχές 80, φτιάχτηκαν 3 μεγάλα δίκτυα: το NSFnet (National Science Foundation Network), το BITNET (Because It's Time Network), και το CSNET(Computer Science Network). Το NSFnet μετατοπίστηκε στον κυριότερο κορμό (backbone) του Internet, εγκαθιστώντας μία γραμμή των 56 Kbps. Η DAPRA τη δεκαετία του '70 ανέπτυξε το πρωτόκολλο TCP/IP (Transmission Control Protocol/Internet Protocol), το οποίο χρησιμοποιήθηκε από το Internet το 1983 (Norton's, 2012).

Τη δεκαετία του'70 αναπτύχθηκε από την DARPA το πρωτόκολλο TCP/IP (Transmission Control Protocol/Internet Protocol) το οποίο άρχισε να χρησιμοποιείται από το internet το 1983. Ωστόσο, από τις αρχές του '80 ο ISO70 (International Standards Organization) όπου είναι ο Διεθνής Οργανισμός Προτύπων δημιούργησε πρωτόκολλα για λίγες χρήσεις Ανοικτής Διασύνδεσης Συστημάτων OSI (Open Systems Interconnection) (Laudon & Traver, 2011).

Το NSF(National Science Foundation), μια ομοσπονδιακή εταιρία των ΗΠΑ, αποφασίζει στα μέσα της δεκαετίας του 1980 να δημιουργήσει πέντε "κέντρα υπερυπολογιστών" τα οποία θα ήταν διαθέσιμα σε όποιον είχε την επιθυμία να τα χρησιμοποιήσει για ακαδημαϊκούς ερευνητικούς σκοπούς. Επειδή, όμως το φόρτο εργασίας δεν μπορούσε να το βγάλει εις πέρας το υφιστάμενο δίκτυο , η NSF δημιούργησε το 1986 ένα άλλο δίκτυο υψηλής χωρητικότητας που ονομάστηκε NSFnet , για να συμπληρώσει το μέχρι τότε υπερφορτωμένο δίκτυο ARPANET.

Η σύνδεση μεταξύ NSFnet, ARPANET και άλλων δικτύων αποτελούσαν το internet. Την ίδια χρονιά οι συνδεδεμένοι χρήστες του internet ήταν 5.000 ενώ τρία χρόνια αργότερα όπου αναβαθμίστηκε η γραμμή του κεντρικού κορμού της NSFnet ,ξεπέρασαν τους 100.000.Φτάνοντας στη δεκαετία του '90 οι συνδεδεμένοι στο internet είχαν αγγίξει τους 1.000.000 και το ενδιαφέρον για το διαδίκτυο επεκτεινόταν δραματικά.
Σιγά σιγά, το NSFnet άρχισε να υπερτερεί από το ARPAnet στις επιστημονικές διασυνδέσεις και μέχρι το Μάρτιο του 1990, το ARPAnet πλέον διαλύθηκε και επισήμως (Norton's, 2012).

1.1.1 Παγκόσμιος Ιστός (WWW)

Η Ελλάδα άρχισε να συνδέεται στο NSFnet το 1990. Μια χρονιά πριν, αναπτύσσετε από τον Tim Berners-Lee το World Wide Web(WWW) και το 1993, το Εργαστήριο Μοριακής Φυσικής στη Γενεύη της Ελβετίας αποφασίζει να το εκθέσει στο κόσμο ως ένα τρόπο πρόσβασης σε online έγραφα που ήταν αποθηκευμένα στο δίκτυο σε πολλούς υπολογιστές, σε όλο τον κόσμο του internet στις οποίες μπορεί να έχει πρόσβαση ο καθένας με τη χρήση ενός ποντικιού.

Μια τεράστια συλλογή από έγγραφα, τα οποία έχουν αποθηκευτεί σε διαφορετικά μέρη του κόσμου και με κάποιο τρόπο όλα είναι συνδεδεμένα μεταξύ τους μπορούν να δημιουργήσουν υποθετικά ένα 'ιστό' από αλληλένδετες πληροφορίες. Εάν αυτά τα έγγραφα και η σύνδεση μεταξύ τους καλύψουν όλη τη γη, τότε μιλάμε για ένα 'παγκόσμιο ιστό' και με άλλα λόγια για το Διαδίκτυο. Πολλοί συγχέουν τις έννοιες του WWW με το διαδίκτυο αλλά είναι δύο τελείως διαφορετικά πράγματα. Το Web είναι ένα σύστημα που υποστηρίζεται από το Διαδίκτυο(Laudon & Traver, 2011).

Το 1995 διατέθηκε στο κοινό Netscape το πρώτο πρόγραμμα περιήγησης που μπορούσε να μπει στο διαδίκτυο και να δει τις ιστοσελίδες του πράγμα που συντέλεσε στη μεγάλη του

εμπορευματοποίηση. Το διαδίκτυο άρχισε γρήγορα να αποτελεί μια εμπορική ευκαιρία και όχι ένα ερευνητικό δίκτυο και αυτό λόγω της ταχύτητας εξέλιξης και της έκτασης που πήρε. Στο δεύτερο μισό του ’90 άρχισαν να διανέμονται πολλά domain names(Norton’s, 2012).

Το 1996 το “.com” και “.net” που ήταν εμπορική, εξυπηρετούσαν το 1,8 των χρηστών έναντι του “.edu” που ήταν εκπαιδευτικός. Μέχρι το 2000 οι πιο πολλές νέες επιχείρησης που ιδρύονταν είχαν την κατάληξη “.com” οι οποίες ξεπερνούσαν κατά έξι φορές το “.edu” σε domain names.

Η περίοδος του Web 1.0 (1995-2003) είχε χαρακτηριστικό την ύπαρξη ιστοσελίδες που ήταν μόνο για ανάγνωση και στατικές και τη δημιουργία πολλών επιχειρήσεων που είχαν εμπορικό περιεχόμενο όπου οδήγησε στη λεγόμενη χρηματιστηριακή φούσκα του διαδικτύου(2000) (Norton’s, 2012).

Η εποχή του Web 2.0 που επήλθε το 2003 είχε ως χαρακτηριστικό τη μετεξέλιξη του διαδικτύου αφού η τεχνολογία γνώρισε σταδιακές εξελίξεις όπως γνώρισε και η κοινωνική επίδραση παγκόσμια. Το Web 2.0 Αποτελεί το εκμοντερνισμένο World Wide Web που χρησιμοποιείται σήμερα. Είναι ένας χαρακτηρισμός που περιγράφει μορφές όπως το YouTube, το Facebook, οι ιστοσελίδες κοινωνικής δικτύωσης, το MySpace, διαδραστικές μορφές λογισμικού, γλώσσες προγραμματισμού και εργαλεία που βοήθησαν στη δημιουργία του καινούριου Web.

Στην εποχή του Web 2.0 δόθηκε η δυνατότητα ελέγχου του περιεχομένου στους χρήστες και είχαν επομένως μεγαλύτερη διαδραστικότητα με το διαδίκτυο. Επίσης, είναι πιο γρήγορο από το προηγούμενο Web και έχει μεγαλύτερη διάρκεια στη σύνδεση το οποίο διευκολύνει τη πρόσβαση σε μουσική ,βίντεο, λογισμικό κ.τ.λ. (Laudon & Traver, 2011). Το νέο Web είναι εύκολο στη χρήση του για αυτό μπορούσαν οι ίδιοι οι χρήστες να το χρησιμοποιήσουν και υπήρχε η λεγόμενη διαδραστικότητα που ενθουσίασε τον κόσμο. Το διαδίκτυο άρχισε να παίρνει παγκόσμιο επίπεδο και ο κόσμος μπορούσε είτε να είναι σχολιαστής σε ιστότοπους , είτε δημιουργός μιας ιστοσελίδας, είτε χρήστης υπηρεσιών νέφους και γενικότερα να κατέχει ένα δυναμικό ρόλο σε αυτό το νέο διαδικτυακό κόσμο. Το διαδίκτυο ορίστηκε ως «διαδραστική υπολογιστική πλατφόρμα» (Norton’s, 2012).

Εικόνα 1 : Λογότυπο του παγκόσμιου ιστού (www)

Πηγή: http://www.freepngimg.com/png/19650-www-free-download-png

1.2 Το διαδίκτυο σήμερα

Η ευκολία πρόσβασης στο διαδίκτυο παράλληλα με την εμφάνιση του WWW προκάλεσε ‘έκρηξη’ στη προσέλευση καινούριων χρηστών στο διαδίκτυο. Σήμερα το διαδίκτυο απαριθμεί εκατομμύρια χρήστες που συνδέονται καθημερινά στα χιλιάδες δίκτυα που συνδέει. Χαρακτηριστικό του διαδικτύου είναι η έλλειψη ιδιοκτησίας που έχει ως αποτέλεσμα να είναι διαθέσιμο σε όποιον μπορεί να συνδεθεί. Πολλές οργανώσεις προτείνουν ιδέες και πρότυπα για τη σωστή χρήση των τεχνολογιών του διαδικτύου που καθολικά ,όμως, υποστηρίζουν την ελευθερία του διαδικτύου από κεντρικό έλεγχο. Το μόνο που χρειάζεται ο κάθε χρήστης του διαδικτύου σήμερα είναι ένα υπολογιστή και να είναι συνδεδεμένος στο διαδίκτυο για να συνδεθεί σε όποιον πόρο επιλέξει που έχει αναρτηθεί ή ακόμα και να δημιουργήσει αυτός ο ίδιος τους δικούς του. Αυτό δηλαδή σημαίνει ότι μπορεί να ανταλλάξει ηλεκτρονικά μηνύματα, έγγραφα, να κάνει ηλεκτρονικές αγορές σε υλικά αγαθά αλλά και να εκτελέσει σμήνος άλλων διεργασιών. Γενικά με το πέρασμα των χρόνων το διαδίκτυο γίνεται ένα μέρος της καθημερινότητας των ανθρώπων που πλέον δε μπορούν να ζήσουν χωρίς αυτό. Η τεχνολογία έχει εισβάλει καθοριστικά στη κοινωνία και με τα χρόνια παίρνει ραγδαίες και τρομακτικές διαστάσεις .

Οι δέκα πιο δημοφιλείς ιστοσελίδες σε παγκόσμια κλίμακα που έχει αναδειχθεί σύμφωνα με μια έρευνα(Alexa.com) αποτελούν :

- Google.com
- Facebook.com
- Youtube.com
- Yahoo.com
- Baidu.com, κινέζικη μηχανή αναζήτησης
- Amazon.com
- Wikipedia.org
- Taobao.com, ηλεκτρονικό κινέζικο πολυκατάστημα
- Twitter.com
- Qq.com, κινέζικη ηλεκτρονική πύλη.

1.2.1 Ψηφιακή Ανισότητα

Το διαδίκτυο εξελίσσεται ραγδαία και όλοι οι άνθρωποι προσπαθήσουν να συμβαδίσουν με τη νέα πραγματικότητα. Για κάποιους όμως είναι αδύνατον αφού άρχισαν να διεισδύουν σε αυτό τον κόσμο σε πολύ μεγάλη ηλικία και έτσι μπορούσαν να καταλάβουν μόνο λίγες λειτουργίες τους ή δεν είχαν τις ίδιες ευκαιρίες με άλλους για πρόσβαση στο διαδίκτυο λόγω κοινωνικοοικονομικών λόγων. Αυτό αποτελεί και την έννοια της «ψηφιακής ανισότητας» που διακρίνει τις διαφορές στον online πληθυσμό. Οι διαφορές αναφέρονται στη ποιότητα της σύνδεσης που έχει ο κάθε χρήστης όπως και το κόστος του. Επίσης, οι δεξιότητες που εμφανίζει ένας χρήστης στη διαχείριση των λειτουργιών του διαδικτύου όπως και οι γνώσεις

που κατέχει πάνω σε αυτόν. Άρα, το κύριο ζήτημα είναι πως θα χρησιμοποιήσουν οι άνθρωποι τη πρόσβαση στο διαδίκτυο και όχι αν έχουν απλά πρόσβαση σε αυτόν (Χατζόπουλο, 2010).

Λόγοι της ψηφιακής ανισότητας αποτελούν τα τεχνικά μέσα που προσφέρουν ένα φάσμα δυνατοτήτων διαδικτυακά αλλά έχουν μεγάλη χρηματική αξία, η αυτονομία χρήσης που επιβάλουν κάποιους περιορισμούς όπως είναι ο χρόνος πρόσβασης σε μια ηλεκτρονική βιβλιοθήκη, οι δεξιότητες που αφορά την εμπειρία, τη γνώση και την εκπαίδευση του κάθε χρήστη, η κοινωνική στήριξη που προσφέρουν άτομα εξοικειωμένα με νέες τεχνολογίες που παρακινούν άλλους και ο σκοπός της χρήσης που πιο σημαντικό αποτελεί η πρόσληψη γνώσεων (Κόλλια, 2017).

Η Cosmote πρόσφατα δημοσίευσε ένα σποτάκι σχετικά με τη κοινωνική ανισότητα υλοποιώντας μια βιωματική άσκηση διαδεδομένη στο εξωτερικό σχετικό με το ψηφιακό και τεχνολογικό φάσμα. Τοποθετούν λοιπόν πίσω από μια διαχωριστική γραμμή άτομα όλων των ηλικιών και διαφορετικών κοινωνικών στρωμάτων στην ίδια ευθεία αναφέροντας ότι στη ζωή δεν ακολουθούμε όλοι την ίδια διαδρομή αλλά «Όλοι θέλουμε να έχουμε ίσες ευκαιρίες όταν τη διανύουμε» . Αρχίζει λοιπόν ο εκφωνητής να αναγγέλλει κάποιες ερωτήσεις και ζητάει από τους ερωτηθέντες αν τους αφορά να κάνουν δυο βήματα μπροστά. Αρχίζει με ερωτήσεις για το τόπο διαμονής τους (αστικό κέντρο), συνεχίζει με ερωτήσεις που αφορούν το κοινωνικοοικονομικό τους επίπεδο που βρίσκονται, ύστερα ρωτάει για αυτούς που δε χρειάστηκαν να δουλέψουν έτσι ώστε να σπουδάσουν. Μετά περνάει σε τεχνολογικό επίπεδο ρωτώντας τους αν κάποιους από αυτούς χάρις της τεχνολογίας εξελίχτηκαν σε προσωπικό ή επαγγελματικό επίπεδο, αν σαν πρώτο κινητό είχαν smartphone, όσοι είχαν ιντερνέτ σε όλη τη διάρκεια της ζωής τους. Όταν όλοι κοιτάνε γύρω κάποιοι έχουν προχωρήσει ενώ άλλοι έχουν μείνει πίσω για λόγους που δεν έχουν να κάνουν με την αξία τους αλλά με τις συνθήκες όπως ακριβώς συμβαίνει με τη ζωή (Cosmote, 2018).

Αποτελεί γεγονός ότι διαφορετικές ομάδες ανθρώπων δεν έχουν τα ίδια οφέλη από τη πρόσβαση και χρήση της τεχνολογίας και αυτό αποτελεί το «ψηφιακό χάσμα».

1.3 Νέα Μέσα & Μέσα κοινωνικής δικτύωσης

Με τη ραγδαία εξέλιξη που έχει πάρει η τεχνολογία τα τελευταία χρόνια και με τον οραματισμό ολοένα και περισσότερων ανθρώπων να δημιουργήσουν κερδοφόρες και αναγνωρισμένες, σε όλο τον κόσμο, πλατφόρμες κοινωνικής δικτύωσης, τα μέσα κοινωνικής δικτύωσης έχουν καταφέρει να γίνουν αναπόσπαστο κομμάτι της καθημερινότητας μεγάλης μερίδας ανθρώπων. Έχουν εισβάλει και εξίσου καθοριστικά στις κοινωνικές αλληλεπιδράσεις της σημερινής κοινωνίας μέσω των δυνατοτήτων επικοινωνίας που προσφέρουν, οι ανάλογες ιστοσελίδες.

Εκατομμύρια άνθρωποι χρησιμοποιούν στις μέρες μας τα κοινωνικά δίκτυα σε όλο τον

κόσμο με σκοπό την επικοινωνία μεταξύ τους. Κάποιες από αυτές τις υπηρεσίες κοινωνικής δικτύωσης είναι το Facebook, το Twitter, το MySpace οι οποίες έχουν διεισδύσει τα τελευταία χρόνια στην καθημερινότητα όλο και περισσότερων ατόμων. Η πιο γνωστή από αυτές είναι σήμερα το Facebook που μετρά κάπου τους 1,5 δισεκατομμύρια χρήστες της. Αυτός ο εικονικός κόσμος, παρέχει σε οποιονδήποτε θελήσει να μοιραστεί τις σκέψεις του, τις ανησυχίες του , τις ανακαλύψεις του με όποιον επιλέξει, είτε είναι γνωστός του είτε είναι άγνωστος, με απλό και γρήγορο τρόπο.

Οι κυριότερες επιπτώσεις των μέσων κοινωνικής δικτύωσης μπορούν να ταξινομηθούν σε πέντε κατηγορίες.
Σαν πρώτη κατηγορία μπορεί να θεωρηθεί ότι έχουν πλέον γίνει από τις πιο σημαντικές πηγή πληροφοριών που κατατρέχουν κάθε μέρα χιλιάδες χρήστες για να ενημερωθούν για επίκαιρες ειδήσεις σε αντίστοιχες ιστοσελίδες του διαδικτύου. Η τηλεόραση, το ραδιόφωνο, οι εφημερίδες έχουν μπει σαν δεύτερη επιλογή στο τομέα της ενημέρωσης και κάθε μέρα χάνουν όλο και περισσότερο κοινό.
Ωστόσο, επειδή ο καθένας μπορεί να χει πρόσβαση στα νέα μέσα και να δημοσιεύει οτιδήποτε θελήσει χωρίς αυτό να ελέγχεται από ένα σύστημα ή κάποιον αρμόδιο, ορισμένες πληροφορίες ή πηγές μπορούν απλά να παραπληροφορούν τους χρήστες. Παρόλα αυτά, η άμεση διαθεσιμότητα των ειδήσεων προς το ευρύ κοινό, είτε της χώρας τους είτε κάποιας άλλης, και η μεγάλη ποσότητα πληροφοριών που προσφέρει καθιστά τα κοινωνικά δίκτυα πιο προσιτά από άλλες πηγές . Μέσα από τις διάφορες ιστοσελίδες του διαδικτύου τα νέα φτάνουν μέχρι την άκρη του κόσμου σε χρόνο μερικών δευτερολέπτων , κάνοντας την είδηση διαθέσιμη με ένα μόνο κλικ του ποντικιού(Κορδερά, 2010).

Σαν δεύτερη επίπτωση, επιτρέπουν στους ανθρώπους να επικοινωνούν μεταξύ τους καθημερινά ακόμα και αν τους χωρίζουν χιλιόμετρα. Αυτό πραγματοποιείται από διάφορες πλατφόρμες επικοινωνίας που είναι εγγεγραμμένος κάθε χρήστης και του δίνεται η δυνατότητα να επικοινωνήσει με όποιο άτομο επιθυμεί με το πάτημα ενός κουμπιού. Ταυτόχρονα, λόγω της μεγάλης έκτασης που έχουν αποκτήσει τα κοινωνικά δίκτυα παγκοσμίως, ο χρήστης μιας χώρας μπορεί να αναπτύξει επαφή με χρήστη άλλης χώρας, και ας είναι άγνωστοι μεταξύ τους, ανταλλάσσοντας ιδέες, απόψεις, πληροφορίες για τα ήθη και έθιμα της χώρας του, για τη κουλτούρα του, βρίσκοντας κοινά σημεία μεταξύ τους (Πλείος, 2014).

Τρίτον, τα μέσα κοινωνικής δικτύωσης έπαιξαν πολύ σημαντικό ρόλο στη μεγαλύτερη πολιτική οργάνωση αλλά και στην ευαισθητοποίηση των πολιτών, με αποτέλεσμα σε κάποιες περιπτώσεις να ξαναγραφτεί εξολοκλήρου ολόκληρο πολιτικό τοπίο. Με την εξέλιξη του κόσμου στο τεχνολογικό επίπεδο έπεται και η εξέλιξη και η μεταβολή στο πολιτικό πεδίο. Τρανταχτό παράδειγμα η χρήση του twitter στη Σαουδική Αραβία που μέσα σε σύντομο χρονικό διάστημα έχει πετύχει να γίνει ένα ελεύθερο σκαλοπάτι διαλόγου. Αυτή η αλλαγή έχει διαπιστωθεί και στην Ελλάδα όπου πολλοί πολιτικοί έχουν λογαριασμό στο twitter και τον χρησιμοποιούν ως φερέφωνο για τα γραπτά και το έργο τους αλλά και συμμετέχουν σε διαλόγους με άλλους πολιτικούς καθημερινά μπροστά στα “μάτια” εκατοντάδων

ψηφοφόρων. Έτσι η κοινωνία μπορεί να ασκήσει μεγαλύτερο έλεγχο προς το πολιτικό καθεστώς αλλά και έχει μια πιο στενή ματιά στις απόψεις των πολιτικών μέσα από τις αναρτήσεις τους.

Τέταρτον, δεν θα μπορούσαν τα νέα μέσα να μην έχουν αντίκτυπο, και μάλιστα μεγάλο, στη καλλιέργεια της παιδείας. Από πολύ νωρίς παρατηρείται ότι τα παιδιά αρχίζουν να χρησιμοποιούν τις υπηρεσίες που προσφέρει το διαδίκτυο και ιδιαίτερα πλατφόρμες παιχνιδιών σε μικρή ηλικία και πλατφόρμες επικοινωνίας σε μια μεγαλύτερη. Μέσα από τη πληθώρα πληροφοριών του διαδικτύου, ο καθένας διαλέγει τα θέματα που τον ενδιαφέρουν και επιλέγει το πόσο περίπλοκα θα είναι αυτά Γενικά οι άνθρωποι αρχίζουν να είναι πιο επικοινωνιακοί και εγγράμματοι (Πλείος, 2014).

Τέλος , τα μέσα κοινωνικής δικτύωσης έχουν φέρει ριζική αλλαγή στο χώρο του μάρκετινγκ αφού πλέον οι εταιρίες επιλέγουν να επενδύουν πάνω τους και στις ιστοσελίδες που τους ανήκουν λόγω των μεγάλων αλληλεπιδράσεων που φέρει με τον καταναλωτή. Έτσι η τηλεόραση αρχίζει και χάνει σιγά σιγά μεγάλο μέρος του κοινού της και σε εξακολούθηση οι εταιρίες παύουν να επενδύουν σε κανάλια και στις διαφημίσεις τους (Πλείος, 2014).

Υπάρχουν , πολλοί ακόμα τρόποι που τα μέσα κοινωνικής δικτύωσης αρχίζουν να αλλάζουν τη καθημερινότητα του κόσμου, απλά αυτοί οι πέντε είναι απτούς πιο σημαντικούς. Μέχρι τώρα, τα νέα μέσα έχουν ριζωθεί σταθερά στις ζωές των ανθρώπων και προβλέπεται στο μέλλον να έχουν ακόμη μεγαλύτερη επίδραση, ελπίζοντας όλοι ότι θα συμβάλουν θετικά στη διευκόλυνση της ζωής τους μέσω των διαδραστικών της πλατφορμών (Κορδερά, 2010).

1.3.1 Πλεονεκτήματα και μειονεκτήματα των μέσων κοινωνικών δικτύων

- ΠΛΕΟΝΕΚΤΗΜΑΤΑ

‘Άνθρωποι με κοινά ενδιαφέροντα έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους και να μοιράζονται πληροφορίες, ακόμα και να δημιουργούν κάποιες ομάδες για τη μελέτη σε εξετάσεις ή να ανταλλάσουν ιδέες και απόψεις σχετικά με ένα κλάδο κοινού ενδιαφέροντος. Ο πιο βασικός λόγος πρόσβασης των χρηστών στα μέσα κοινωνικής δικτύωσης είναι ότι βρίσκουν ένα ευχάριστο τρόπο να περνάνε το χρόνο τους όταν οι ίδιοι θέλουν να απαλλαχθούν από το διάβασμα ή τις εργασίες για τη δουλειά τους. Τα μέσα κοινωνικής δικτύωσης αποτελούν πλέον ένα εναλλακτικό τρόπο ζωής και δε θεωρούνται απλά εργαλεία (Πλείος, 2014).

Άλλος ένας λόγος είναι ότι μέσα από τις εφαρμογές των μέσων κοινωνικών δικτύωσης εκμηδενίζεται η απόσταση μεταξύ τν χρηστών, έτσι άνθρωποι που μένουν μακριά λόγω συγκυριών, είτε αυτά είτε συγγενικά πρόσωπα είτε φίλοι είτε απλοί γνωστοί, μπορούν τώρα να επανασυνδεθούν (Φέσιας, 2016).

Επίσης, έχουν την τύχη και την ευκαιρία να έρθουν σε επαφή και με νέα άτομα που δε

γνωρίζονταν αλλά τους ενώνουν κάποιες κοινές απόψεις για τη ζωή. Αυτά τα άτομα μπορεί να μένουν σε διαφορετική πόλη, σε άλλη χώρα αλλά να έχουν την θέληση να επικοινωνήσουν με καινούρια άτομα και να ανταλλάξουν απόψεις. Ιδιαίτερα, νέα άτομα που μένουν στις επαρχίες δεν έχουν πολλά άτομα να συναναστραφούν γι'αυτό και ψάχνουν συντροφιά στο διαδίκτυο (Πλείος, 2014).

Ακόμα, πολλοί χρήστες έχουν παραδεχτεί ότι θεωρούν τα μέσα κοινωνικής δικτύωσης σαν ένα υποκατάστατο για όσους στη πραγματική ζωή δεν έχουν το θάρρος να αναπτύξουν κάποια σχέση, είτε αυτή είναι φιλική είτε είναι ερωτική, με άλλα άτομα αλλά και για όσους το βαρύ φόρτο δουλειάς δεν τους αφήνει να έχουν καθόλου προσωπικό χρόνο (Φέσιας, 2016).

Επιπλέον, αυτή η έμμεση επικοινωνία που προσφέρουν τα μέσα κοινωνικής δικτύωσης, με χρήστες από όλες τις άκρες της γης να μπορούν να έρθουν σε επαφή και με αυτό τον τρόπο να γνωρίσουν νέα ήθη και έθιμα, νέες κουλτούρες, νέες πολιτισμούς είναι μοναδική (Φέσιας, 2016).

Επίσης, πολλοί κρύβονται πίσω από την οθόνη του υπολογιστή για να μπορούν να φανερώσουν τα συναισθήματα τους σε άτομα που τους ενδιαφέρουν αφού σε προσωπικές στιγμές μαζί τους δε τολμούσαν.

Τέλος, εν όψει οικονομικής κρίσης στην Ελλάδα δεν θα μπορούσε να μην ειπωθεί αυτή η δωρεάν επικοινωνία που προσφέρουν για όλα τα μέρη της γης τα μέσα κοινωνικής δικτύωσης (Πλείος, 2014).

- ΜΕΙΩΝΕΚΤΗΜΑΤΑ

Δυστυχώς, η μεγάλη προέκταση που έχει πάρει το διαδίκτυο και ο εθισμός που προσφέρει μέσω των εφαρμογών του έχει κάνει πολλούς έφηβους να αποσπούνται από το διάβασμα τους, έχει αποθαρρύνει την άμεση επικοινωνία, ενώ πολλοί χρήστες, απρόσωπα, πέφτουν θύματα διαδικτυακού εκφοβισμού.

Έφηβοι που χρησιμοποιούν συχνά μέσα κοινωνικής δικτύωσης και ιδιαίτερα το Facebook αρχίζουν να φανερώνουν τάσεις ναρκισσισμού ενώ κάποιοι ενήλικες σε νεαρή ηλικία που είναι καθημερινοί χρήστες εμφανίζουν σημάδια διαταραχών σε ψυχολογικό επίπεδο, μανίας αλλά και επιθετική συμπεριφορά. Αυτό συμβαίνει λόγω της υπερβολικής χρήσης της τεχνολογίας και των μέσων ,που αυτή προσφέρει, τα οποία επηρεάζουν την υγεία των εφήβων αφού πλέον καθίστανται πιο επιρρεπής στην κατάθλιψη, το άγχος και σε άλλα ψυχολογικά προβλήματα αλλά και πιο επιρρεπής σε θέματα μελλοντικής υγείας. Πιο μεγάλο μέσο επιρροής αποτελεί το Facebook, που μελέτες έδειξαν ότι φοιτητές και μαθητές κατατρέχουν σε αυτό ανά 15 λεπτά τη μέρα με αποτέλεσμα να αποσπούνται από τα μαθήματα τους(Κορδερά, 2010).

Αυτή η εξάρτηση στα μέσα κοινωνικής δικτύωσης που παρουσιάζουν κάποιοι χρήστες, προέρχεται από τη γενικότερη τους εξάρτηση από τον υπολογιστή και ότι συνάπτεται με αυτόν. Τα πιο μεγάλα μέσα της κοινωνικής δικτύωσης που είναι το Facebook και το Twitter παρέχουν ένα προσωπείο προς τους χρήστες που τους κάνει να έχουν αυτοεκτίμηση. Έτσι αποκτούν αυτοπεποίθηση και απελευθερώνουν τα συναισθήματα τους προς τα άτομα ενδιαφέροντος τους που στη πραγματική ζωή δε θα τολμούσαν. Όμως, αρκετοί χρήστες αρχίζουν να διατηρούν πολλαπλούς λογαριασμούς με διαφορετικά χαρακτηριστικά κάθε φορά καθιστώντας τους ψεύτικους και επικίνδυνους στη προσέγγιση τους με άλλα άτομα(Κορδερά, 2010).

Η ελληνική γλώσσα κατακρεουργείται στα μέσα από χυδαιολογίες και από τη χρήση των greeklish δηλαδή τη ταυτόχρονη χρησιμοποίηση αγγλικών και ελληνικών λέξεων. Η ελληνική γλώσσα αλλοιώνεται όλο και περισσότερο με την ανορθογραφία που κανέναν δεν απασχολεί στα social media, αλλά και με τη χρήση μόνο emoticons που φορτώνουν τη σελίδα με αποτέλεσμα να παίρνει πολύ ώρα να φορτώσει (Φέσιας, 2016).

Κάθε μέρα, μικρής ηλικίας χρήστες ανταγωνίζονται για το πόσους φίλους έχουν προσεγγίζει και το πόσο εμφανίσιμοι είναι αυτοί, ιδιαίτερα όταν είναι αντίθετου φίλου (Πλείος, 2014).

Οι φωτογραφίες που προβάλλονται στα μέσα και ειδικά των γυναικών πολλές φορές είναι προκλητικές, περιμένοντας τη προσέγγιση και τα σχόλια από κάποιο χρήστη εμφανίσιμο με ευχέρεια λόγου. Από την άλλη οι άντρες συνήθως προβάλλουν τα σωματικά τους προσόντα και τον δήθεν σκληρό χαρακτήρα τους.

1.3.2 Η αντικειμενικότητα και τα νέα μέσα

Τα νέα μέσα, ευτυχώς ή δυστυχώς, έχουν αναδείξει ότι οι ειδήσεις είναι κάποια γεγονότα που παρουσιάζονται μέσα από το φακό ορισμένων ατόμων και όπως αυτοί τα λαμβάνουν και αυτό αποτελεί εμφανές στοιχείο στην έλλειψη της αντικειμενικότητας. Οι τρόποι που έχουν οδηγήσει εκεί είναι πολλοί.
Αρχικά, μέσα στο τεχνολογικό περιβάλλον των μέσων τα γεγονότα εντυπώνονται έτσι όπως θεωρούνται πως έχουν συμβεί όχι όπως έχουν συμβεί στη πραγματικότητα και αυτό συμβαίνει λόγω της δυνητικής ή πλασματικής σύνθεσης των συμβάντων.

Στο διαδίκτυο πλέον αναρτώνται πολλά δημοσιογραφικά κείμενα τα οποία σχολιάζονται από χρήστες ,ανώνυμους ή επώνυμους ,και δημιουργούν μέσα από τη παρέμβαση του συντάκτη στα σχόλια τους ένα δημιουργικό διάλογο που φέρνει στο φώς κάτι που δεν ήταν τόσο εμφανές στα παλιά μέσα: Ότι η δημοσιογραφία, σε συνάρτηση με την ειδησεογραφία, ορίζεται σαν η πλαισίωση μιας είδησης με απόψεις(Κορδερά, 2010).

Ζούμε στην κοινωνία της πληροφορίας γι’αυτό η ανάγκη για πληροφόρηση είναι πολύ μεγαλύτερη απτό παρελθόν και οι λόγοι είναι πολιτικοί, κοινωνικοί, οικονομικοί κ.τ.λ. Ιδιαίτερα τα νέα μέσα χρειάζονται ένα τεράστιο όγκο πληροφοριών για να συνάπτονται και

με το εύρος των φωνών σε αυτά. Σαν αποτέλεσμα, ανύπαρκτα και ανεπιβεβαίωτα γεγονότα εμπλέκονται μέσα στις αληθές ειδήσεις των νέων μέσων. Ένα γεγονός διασπάται για να δημιουργήσει πολλές μικρές ειδήσεις που συντάσσονται για να ολοκληρωθούν με σχόλια και μεγεθύνονται για να μπορούν να δημοσιευτούν. Αυτό επεκτείνεται από τη συνεχείς και αυξανόμενη πρόσβαση των χρηστών των μέσων στην ειδησεογραφία. Για παράδειγμα στις ΗΠΑ, εν έτη 2013-2015, η πρόσβαση σε ειδήσεις στο Facebook από τους χρήστες της ανέβηκε από 52% σε 63% και στο Twitter το ποσοστό έφτασε τα 63% από 47%. Αυτό επίσης επηρεάζει και το είδος των ειδήσεων που οι δημοσιογράφοι αναγκάζονται να συντάξουν (Πλείος, 2014).
Οι δημοσιογράφοι ως εκ τούτου παρασύρονται και παράγουν πρόχειρες ειδήσεις με κατάληξη να κυκλοφορούν όλο και περισσότερες ανακριβείς ειδήσεις.
Πέρα από αυτή τη προχειρότητα των ειδήσεων παρατηρούνται όλο και περισσότερες παραβιάσεις σχετικά με τους κανόνες περιστοιχίζουν τη δημοσιογραφική δεοντολογία (Πλείος, 2014).

Η δημοσιογραφία που τείνει να εδραιωθεί στα μέσα κοινωνικής δικτύωσης χαρακτηρίζεται ως «δημοσιογραφία του συρμού» ή «δημοσιογραφία της περιρρέουσας ατμόσφαιρας» δηλαδή όχι αυτή που θα χαρακτηρίζαμε έγκυρη δημοσιογραφία.
Η έκταση που εξαπλώνεται μια πληροφορία(σε όλο τον κόσμο) όπως και η ταχύτητα της (μιας ανακριβής, πρόχειρης πληροφορίας) συνεισφέρουν δραματικά στην ιδέα της έλλειψης της αντικειμενικότητας.
Σε όλα αυτά προστίθεται και η «δημοσιογραφία των πολιτών» που μένουν περισσότερο στη θεωρία μιας πληροφορίας παρά στη πράξη(Κορδερά, 2010).

Η εξάπλωση της χρήσης του διαδικτύου όπως και το εμπλουτισμένο του περιεχόμενο άρχισε να κρίνει αναξιόπιστα τα παλιά μέσα και να έρχεται το ίδιο στο προσκήνιο ως η καλύτερη πηγή πληροφορίας. Σε συνδυασμό ,ακόμα, ότι μπορεί το διαδίκτυο να φιλοξενήσει τα πιο πρωτάκουστα θέματα και τις πιο ανατρεπτικές απόψεις, έχει με τον τρόπο του θεσμοθετήσει ότι τα νέα μέσα δεν αποδέχονται την αντικειμενικότητα (Πλείος, 2014).

Είναι σημαντικό να τονιστεί ότι πολλοί παράγοντες εμφανίζουν την αντικειμενικότητα σαν ουτοπία για τη σύγχρονη κοινωνία. Αυτοί οι παράγοντες κατονομάζονται ως ανθρωπιστικές ,οικονομικές και πολεμικές κρίσεις που συντείνουν έντονα στη στράτευση και στην ανάδειξη των μέσων. Ιδιαίτερα στην Ελλάδα το φαινόμενο αυτό αρχίζει να ναι όλο και περισσότερο εντονότερο λόγο της κρίσης που εκμεταλλεύονται να νέα μέσα για να αμολήσουν γρηγορότερα, σφοδρότερα και με πιο εμπλουτισμένο περιεχόμενο τις ειδήσεις στους προς το ελληνικό λαό(Κορδερά, 2010).

Τέσσερα πράγματα μπορούν να γίνουν για να ελεγχθεί η έλλειψη αντικειμενικότητας :

-Να ενωθούν οι δημοσιογράφοι, νέων και παλιών μέσων, σε νέα επαγγελματικά πλαίσια που έχουν ως στόχο την ορθή, αναβαθμισμένη άσκηση της δημοσιογραφίας πέρα από την επιρροή της λογοκρισίας.

-Να παρακολουθούνται επιστημονικά τα νέα και τα παλιά μέσα σχετικά με τη συμπεριφορά που προβάλουν γενικά αλλά και ειδικά στο ειδησεογραφικό τους κομμάτι και όλο αυτό να γίνει ανεξάρτητα από κάθε αρχή και να θεσμοθετηθεί. Η κοινή γνώμη πρέπει να έχει μια εκτεταμένη πρόσβαση σε αυτές τις γνώσεις που θα βρίσκεται σε κάποιο άλλο πεδίο από αυτό των ρυθμιστικών αρχών.

-Τα γεγονότα που βγαίνουν στη δημοσιότητα να τηρούνται από τους νόμους και τη δεοντολογία και από όλες τις σχετικές ρυθμίσεις. Γι'αυτό και είναι σημαντική η άνω παρακολούθηση.

-Οι διαφορετικές απόψεις που εκφέρονται να προβάλλονται ίσα χωρίς κάποια να υποβαθμίζεται ειδικά όταν τυπώνονται σε σημαντικά σημεία όπως είναι οι προεκλογικές περίοδοι (Φέσιας, 2016).

1.4 Νέο ψηφιακό τοπίο & Ψηφιακή επανάσταση

Ψηφιακή επανάσταση ονομάζεται η αλλαγή της αναλογικής τεχνολογίας σε ψηφιακής. Η επανάσταση αυτή άρχισε το 1980 και έχει αντίκτυπο ακόμα και σήμερα. Ταυτόχρονα, αναφέρεται στις ριζικές αλλαγές που έφερε η τεχνολογία και η πληροφορική στα μέσα του 20^{ου} αιώνα στο κόσμο των επικοινωνιών. Μια νέα εποχή ξεκινά μετά την έναρξη της ψηφιακής επανάστασης με κύριο σηματοδότη της τη ψηφιακή πληροφορία. Η όλο αυξανόμενη παραγωγή χρήση του κινητού τηλεφώνου, του υπολογιστή και του φαξ θα αποτελέσουν κεντρικό ρόλο στη ψηφιακή επανάσταση.

Η αντικατάσταση της αναλογικής τεχνολογίας σε ψηφιακή, έκανε εφικτή την ανάπτυξη πολλών αντιγράφων σχεδόν ίδιων με αυτόν που είχαν δημιουργηθεί αρχικά. Με αυτό τον τρόπο οι πληροφορίες κατά την εκπομπή του σήματος ήταν απόλυτα ασφαλές στις ψηφιακές επικοινωνίες (Economist, 2018).

Από τη μεριά των πολυμέσων , επήλθαν σημαντικές αλλαγές στην αποθήκευση της εκάστοτε πληροφορίας λόγω της ψηφιακής επανάστασης. Πλέον τα δεδομένα άρχισαν να αποθηκεύονται σε μια μορφή που μπορούσε αμέσως να αποθηκευτεί και να μεταφερθεί σε όλα τα είδη μέσων. Σημαντικής σημασίας, θεωρείται και η δημιουργία της ασύρματης επεξεργασίας και μεταφοράς των πληροφοριών (Καλησπεράκη, 2016).

Όλα τα εργαλεία που χρησιμοποιούσαν τη ψηφιακή τεχνολογία αντικαταστάθηκαν από άλλες πιο ανεπτυγμένες που προσέφεραν και μεγαλύτερο εύρος δυνατοτήτων. Έτσι, οι τότε κασέτες και πικ-απ αντικαταστήθηκαν από τα σημερινά cd που διαθέτουν μεγαλύτερο χώρο αποθήκευσης. Οι βιντεοταινίες περάστηκαν σε dvd. Η αναλογική αναμετάδοση που υπήρχε μετατράπηκε σε ψηφιακή όπως και το αναλογικό τηλέφωνο σε ψηφιακό. Η παλιά κλασσική μηχανή μετατράπηκε σε ένα απαραίτητο εργαλείο του σήμερα τον εκτυπωτή. Πολλά από τα

βιβλία που κυκλοφορούνε στην αγορά μετατράπηκαν σε ψηφιακά και πλέον είναι διαθέσιμα στο διαδίκτυο δωρεάν. Τέλος, το καθημερινό μέσο μετάδοσης των ειδήσεων στους ανθρώπους που είναι η τηλεόραση μετέτρεψε τη μετάδοση των καναλιών της σε ψηφιακή μορφή για να χαρίσει μεγαλύτερη ευκρίνεια και εύρος χρωμάτων στην εικόνα του τηλεθεατή (Economist, 2018).

Δεν θα μπορούσε να διευκρινιστεί η ψηφιακή επανάσταση χωρίς να γίνει λόγος για τη μεγάλη ζήτηση που άρχισαν να έχουν οι υπολογιστές και ιδιαίτερα ο μικροεπεξεργαστής που διέθεταν, ο οποίος κατάφερε να ενσωματώσει τα υπολογιστικά συστήματα ανάμεσα σε πολλές άλλες συσκευές. Ίδια σημαντική σημασία κατείχε και η ανάπτυξη του Διαδικτύου, της ψηφιακής αναμετάδοσης και γενικά όλων των τηλεπικοινωνιακών τεχνολογιών. Το 2000, άρχισαν να μπαίνουν με γρήγορο ρυθμό στη κοινωνία τα κινητά τηλέφωνα της τελευταίας τεχνολογίας που παρείχαν σημαντικές υπηρεσίες στο λογισμικό τους όπως την επικοινωνία, την διασκέδαση και φυσικά τη πρόσβαση στο διαδίκτυο (Καλησπεράκη, 2016).

Παρόλο που τα οφέλη της ψηφιακής επανάστασης στην κοινωνία είναι τεράστια, όπως είναι η διασύνδεση πολλών υπολογιστών σε όλη τη γη, η ευκολία της επικοινωνίας σε παγκόσμιο επίπεδο και η προσβασιμότητα σε πολλές πληροφορίες που έχουν δημοσιευτεί στο διαδίκτυο, υπάρχουν κάποιες ανησυχίες. Όλες αυτές οι δυνατότητες που παρέχονται στους χρήστες λόγω των νέων τεχνολογιών έφεραν στο προσκήνιο τις πιθανότητες της εκμετάλλευσης που τις περιστοιχίζουν. Τα δεδομένα που προσφέρονται στο διαδίκτυο άρχισαν να συζητιούνται λόγω των πληροφοριών τους που ήταν εύκολο να αντιγραφούν από οποιοδήποτε χρήστη αλλά παράλληλα δεν μπορούσαν να ελεγχτούν για την αξιοπιστία τους. Νέα πολιτικά και ανθρώπινα δικαιώματα άρχισαν να εγκαινιάζονται με την έλευση της ψηφιακής επανάστασης που είχαν σαν αποτέλεσμα την επιτήρηση των άρθρων που δημοσιεύονται αλλά και των γεγονότων (Economist, 2018).

Με την εύκολη διάθεση των πληροφοριών διαδίκτυο και τη μαζική τους διάδοση ήταν πλέον εύκολο σε οποιοδήποτε να δημιουργήσει ένα άρθρο που είχε τις βάσεις του σε αναληθείς πηγές. Είναι πολύ εύκολο ο καθένας να φτιάξει ψεύτικες ειδήσεις, όσο και να τροποποιήσει κάποιες αληθείς σε μη. Ειδικά αν αλλάξει τη μορφή που έχουν αποθηκευτεί τα δεδομένα , γίνεται ιδιαίτερα δύσκολη η ανάκτηση τους και έπειτα η ανάγνωση τους. Δηλαδή, οι αυθεντικές πληροφορίες που δημοσιεύονται στο διαδίκτυο και επέρχονται από αποτελέσματα έρευνας , πρέπει οπωσδήποτε να επαληθεύονται ως ακριβείς για να διατηρούνται έτσι στο κυβερνοχώρο (Καλησπεράκη, 2016).

Σε όλα αυτά τα προβλήματα έρχονται να προστεθούν και κάποια δικαιώματα που υπάρχουν στο ψηφιακό κόσμο άλλα και άλλες τεχνολογίες σχετικές με τις αντίγραφες των δεδομένων στο διαδίκτυο, οι οποίες σιγουρεύουν ότι τα δεδομένα που είναι διαθέσιμα θα μπορούν να διαβαστούν μόνο από συσκευές που έχουν προκαθοριστεί. Έτσι πληροφορίες που έχουν αποθηκευτεί σε παλιά μέσα επικοινωνίας κάνουν σχεδόν αδύνατη τη μελλοντική τους αναπαραγωγή από κάποιο άλλο μηχάνημα (Economist, 2018).

Εικόνα 2 : Νέες συσκευές επικοινωνίας

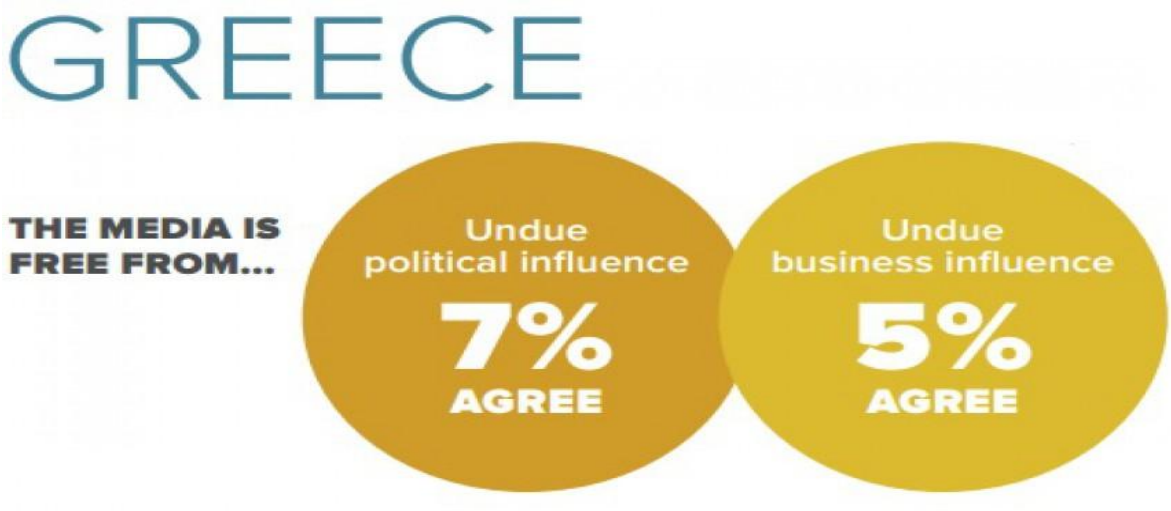
Πηγή: https://patimes.org/internet-social-media-citizens-public-services-needing-renewed-rules/

1.4.1 Το τοπίο της ψηφιακής ενημέρωσης στην Ελλάδα και τον κόσμο.

Σύμφωνα με μια έρευνα που διεξήχθη στο Ινστιτούτο Reuters στο πέμπτο ετήσιο 'Digital News Report' σχετικά με τη ψηφιακή ενημέρωση της Ελλάδας αλλά και του κόσμου, έδωσε τα συμπεράσματα ότι τα κοινωνικά δίκτυα που έχουν ως αντικείμενο την ενημέρωση έχουν ανοδική πορεία στη χρήση τους τα τελευταία χρόνια και ότι μεγάλη δυσαρέσκεια αποτυπώνεται από τους χρήστες σχετικά με τη διαδικτυακή διαφήμιση όλο και περισσότερο. Επίσης, σε συνδυασμό ότι πολύ λίγοι χρήστες προθυμοποιούνται να πληρώνουν για να έχουν πρόσβαση στις ειδήσεις που αναρτώνται καθημερινά σε ιστοσελίδες στο διαδίκτυο, ενδείκνυται να υπάρξουν επιπτώσεις μελλοντικά τα Μέσα Ενημέρωσης (Καλογερόπουλος, 2016).

Τα αποτελέσματα της δημοσκόπησης, που έγινε διαδικτυακά, βασίζονται σε απαντήσεις 50.000 ατόμων προερχόμενοι από 26 χώρες. Η Ελλάδα βρίσκεται στα πιο υψηλά επίπεδα σε σχέση με τη χρήση που κάνει στα κοινωνικά δίκτυα κυρίως για σκοπούς ενημέρωσης και στα προγράμματα ad-blocking ενώ στα πιο χαμηλά εμφανίζεται η εμπιστοσύνη που δείχνει στη δημοσιογραφία και τα Μ.Μ.Ε.

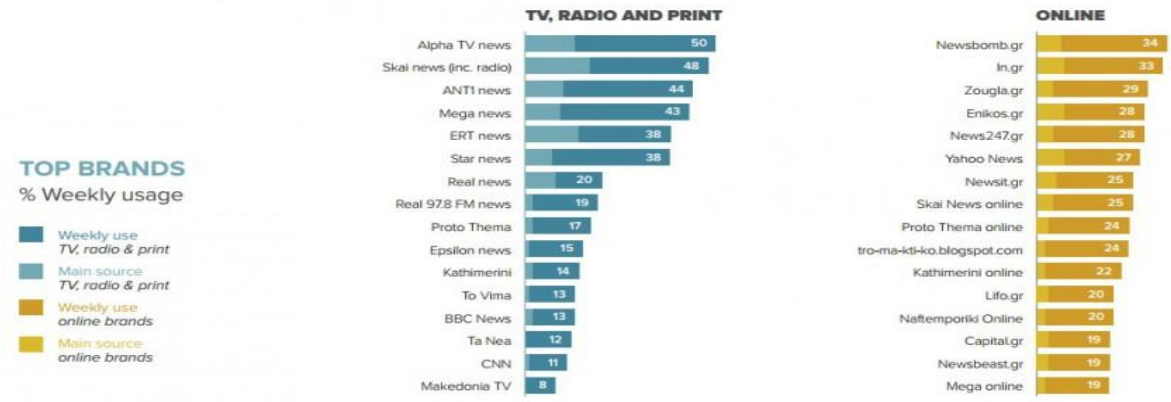
Η Ελλάδα αναδείχτηκε σαν τη τελευταία από τις 26 χώρες που θεωρούν ότι τα Μέσα Ενημέρωσης δεν επηρεάζονται από τη κακόβουλη πολιτική επίδραση με μόλις 7% των Ελλήνων να το υποστηρίζουν ενώ μόλις το 5% πιστεύει πως τα Μέσα Ενημέρωσης δε διακινούνται από επιχειρηματικά συμφέροντα.



Εικόνα 3 : Αποτελέσματα έρευνας για τη γνώμη των Ελλήνων σχετικά με την επιρροή των ΜΜΕ από κακόβουλη πολιτικά και επιχειρηματικά συμφέροντα.

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

Ενώ στις περισσότερες χώρες, οι κάτοικοι τους προτιμούν να ενημερώνονται από τις σελίδες των brands που έχουν συνηθίσει τόσα χρόνια στο διαδίκτυο, οι Έλληνες προτιμούν η ενημέρωση τους να προέρχεται από καινούριες διαδικτυακές σελίδες.
Βέβαια, τα αποτελέσματα της έρευνας δεν είναι τελείως αντιπροσωπευτικά για την Ελλάδα εφόσον μόνο το 63% αυτών κατευθύνονται για την ενημέρωση τους στο διαδίκτυο.

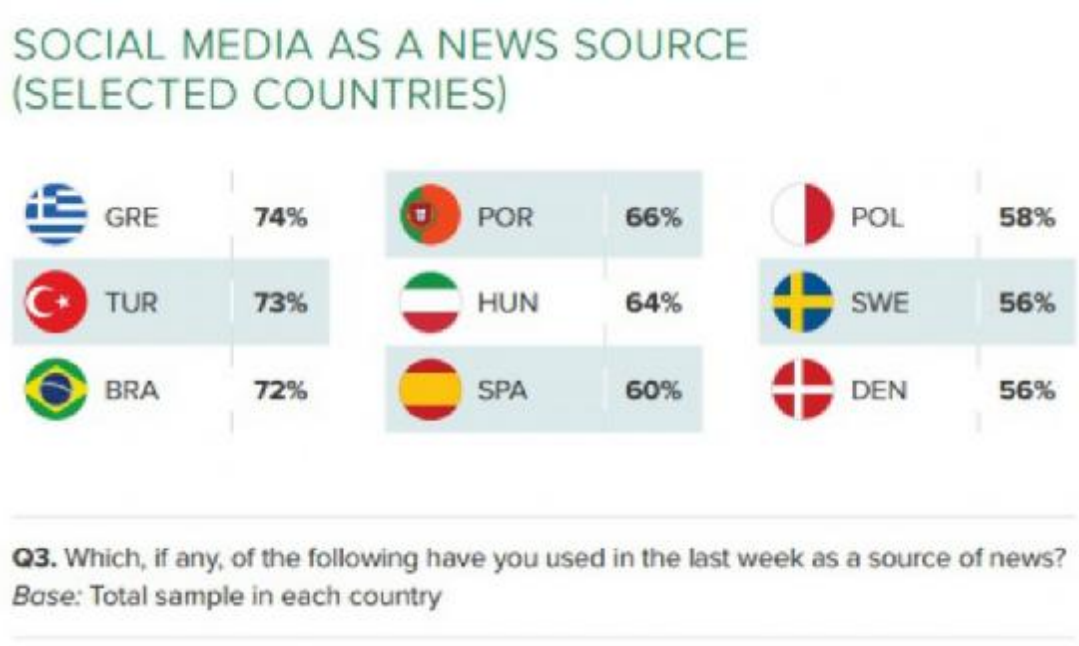


Εικόνα 4 : Αποτελέσματα επιλογής ενημέρωσης

Πηγή: http://www.lifo.gr/articles/digital-media_articles/10433

Το 86% των Ελλήνων είναι δραστήριο στο σχολιασμό των ειδήσεων , αντιδρώντας με like ή αποστέλλοντας τα με mail ενώ το 74% διαβάζει τα νέα γεγονότα στα κοινωνικά δίκτυα και συνάμα τα σχολιάζει περισσότερο από ότι οι κάτοικοι των άλλων χωρών και αυτό

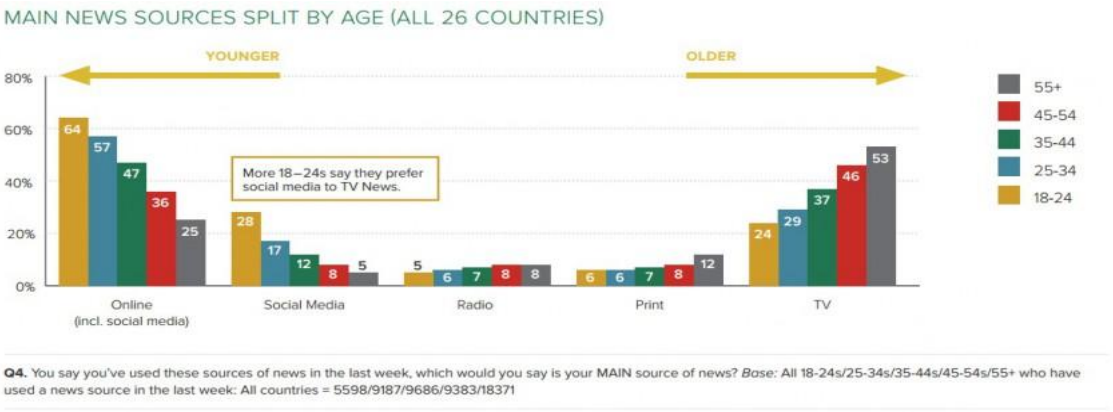
προσδίδεται στο γεγονός ότι η πολιτική ειδησεογραφία είναι πολύ έντονη τελευταία όπως και η οικονομική.



Εικόνα 5 : Τα κοινωνικά δίκτυα ως νέα πηγή ενημέρωσης

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

Η μεγαλύτερη ηλικία διαπιστώθηκε ότι προτιμά να ενημερώνεται από τη τηλεόραση ενώ η νεολαία μεταξύ 18-24 ετών προτιμά να ενημερώνεται από τα κοινωνικά δίκτυα με ποσοστό 28% έναντι αυτό της τηλεόρασης που φτάνει το 24%. Γενικά, από τις 26 χώρες που έγινε η έρευνα οι μισοί(51%) προτιμούν την ενημέρωση από τα social media έναντι του 12% που προτιμούν τα κοινωνικά δίκτυα.



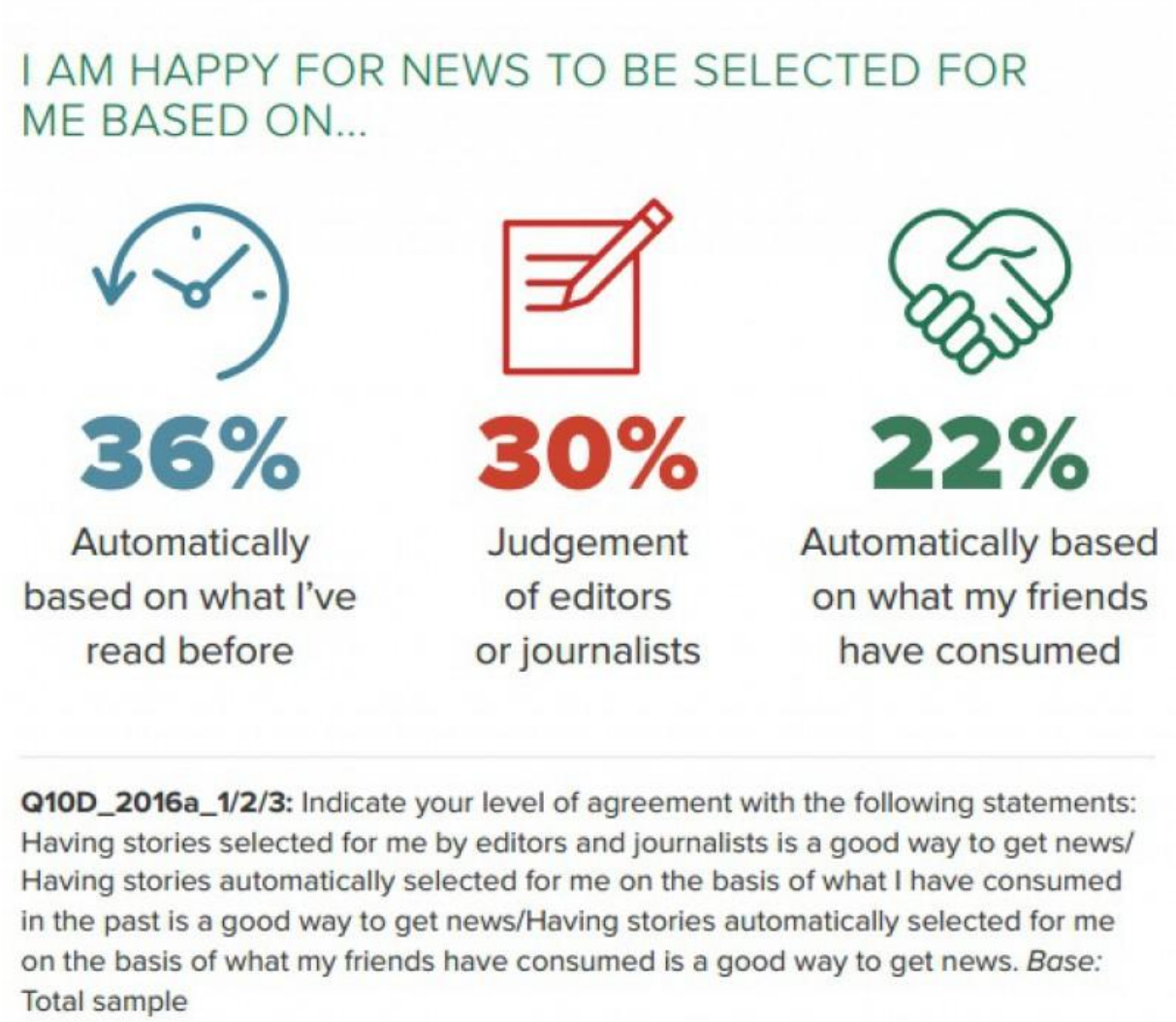
Εικόνα 6 : Η ενημέρωση διαχωρισμένη ανά ηλικία

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

Πολύ εξέχουσα θέση έχει πάρει το Facebook στη καθημερινότητα των ανθρώπων καθώς

καθημερινά το 44% αυτών το χρησιμοποιεί για να διαβάσει ειδήσεις , να μοιραστεί πληροφορίες, να βρει κάποια είδηση που τους ενδιαφέρει κ.τ.λ. Το YouTube έρχεται δεύτερο με μόλις 19% ποσοστό ενώ το Twitter τρίτο με 10% παρόλο που προτιμάται από πολλούς χρήστες λόγω του ειδησεογραφικού ενδιαφέροντος που προσφέρει. Επίπτωση της χρήσης αυτών των μέσων για ενημέρωση είναι οι περισσότεροι χρήστες να μη προσέχουν από πού προέρχεται η είδηση και απλά να τις διαβάζουν δίχως να γνωρίζουν την πηγή τους.

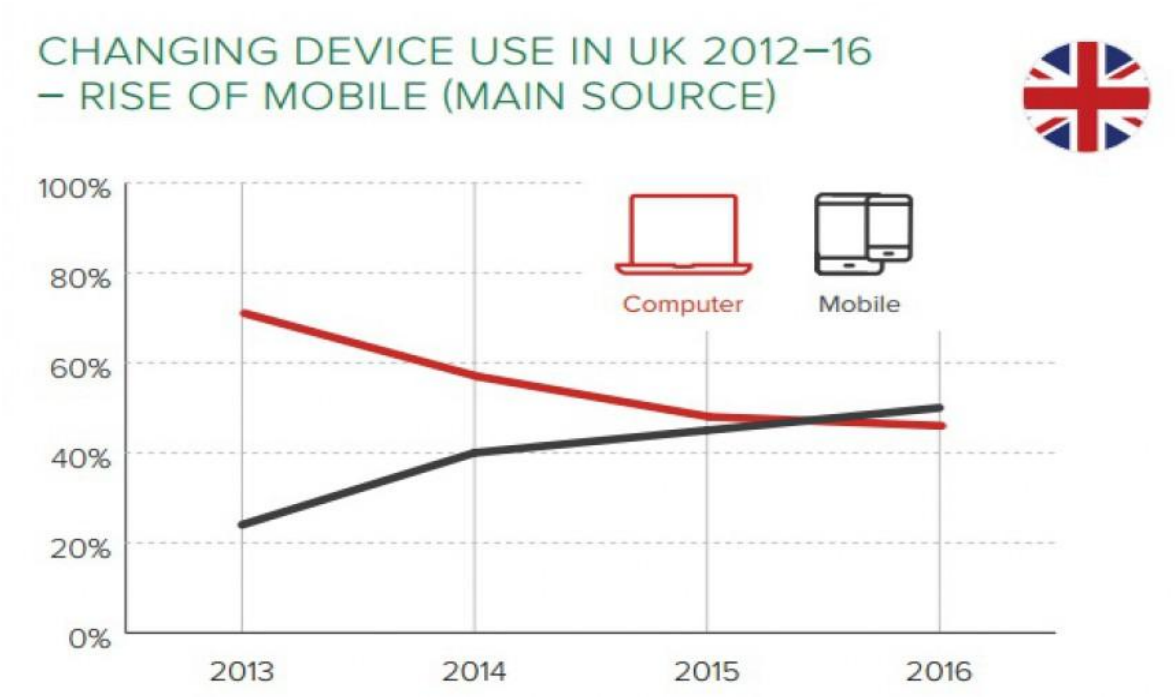
Η έρευνα έδειξε επίσης ότι οι χρήστες κατά 36% προτιμούν να διαβάζουν τις πιο δημοφιλείς ειδήσεις του διαδικτύου που έχουν αναδειχθεί βάσης επισκεψιμότητας και όχι ειδήσεις που έχουν επιλεχθεί σαν οι πιο ενδιαφέρουσες από συντάκτες ή και από δημοσιογράφους(30%).



Εικόνα 7: Λόγοι επιλογή ειδήσεων στο διαδίκτυο

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

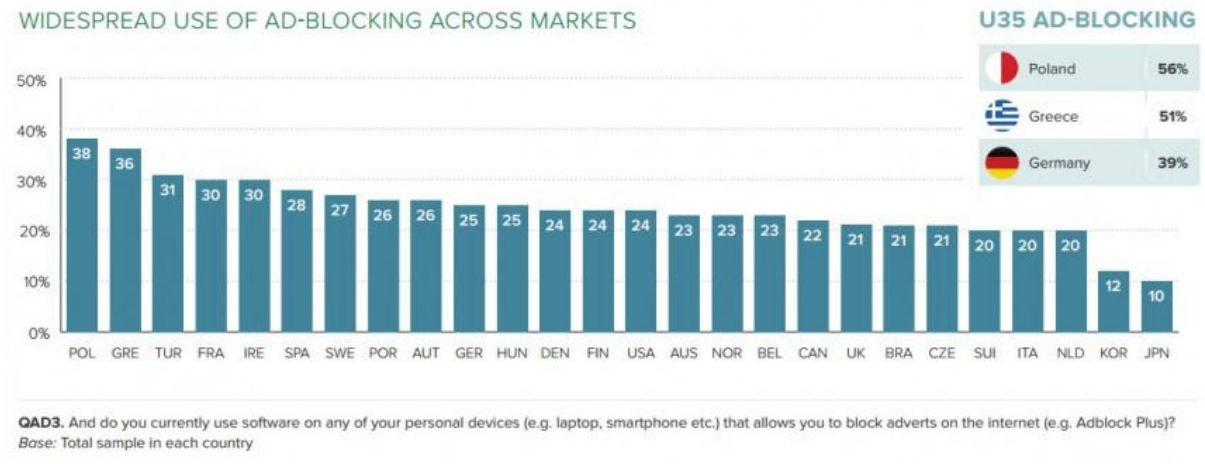
Ακόμα, η χρήση των tablet με τα χρόνια έχει γίνει σταθερή σε σχέση με την αυξημένη χρήση των smartphones στην επιλογή των ειδήσεων προς ανάγνωση. Συγκεκριμένα στο Ηνωμένο Βασίλειο οι υπολογιστές χρησιμοποιούνται σε μικρότερο βαθμό σε σχέση με τις φορητές συσκευές για ενημέρωση.



Εικόνα 8: Σχεδιάγραμμα χρήσης υπολογιστών και φορητών συσκευών για ενημέρωση στο Ηνωμένο Βασίλειο

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

Στην Ελλάδα, οι μισοί χρήστες της (51%) που είναι κάτω των 35 ετών έχουν κατεβάσει στον υπολογιστή τους το ad-blocking το οποίο αφαιρεί τις διαφημίσεις από τη περιήγηση στο διαδίκτυο.



Εικόνα 9: Διαδεδομένη χρήση του ad-blocking

Πηγή: http://www.lifo.gr/articles/digital-media_articles/104332

Τέλος, το μεγαλύτερο ποσοστό των χρηστών(76%) δεν βλέπει ενημερωτικά βίντεο στο διαδίκτυο αλλά προτιμά να διαβάζει τις ειδήσεις μέσω άρθρων που αναρτώνται γιατί τα

θεωρεί πιο βολικά και γιατί δεν μπορεί τις διαφημίσεις που συνεχώς διακόπτουν τα βίντεο.

Γενικά το διαδίκτυο έχει εισβάλει και έχει ριζωθεί για τα καλά στις ζωές των ανθρώπων με αποτέλεσμα να τους παρασύρει σε όλα τα τεχνολογικά επιτεύγματα που τη περιστοιχίζουν. Ιδιαίτερα τα μέσα κοινωνικής δικτύωσης έχουν διευκολύνει με τις εφαρμογές τους σε πολλά επίπεδα τη καθημερινότητα των χρηστών του και ιδιαίτερα στην ενημέρωση. Οι τεράστιες ποσότητες πληροφοριών που προσφέρει και η διευκόλυνση της επικοινωνίας σε παγκόσμιο επίπεδο το καθιστά ένα από τα πιο χρήσιμα επιτεύγματα της ανθρωπότητας. Κάθε μέρα όλο και πιο πολλές παλιές τεχνολογίες αντικαθιστούνται με νέες για να συμβάλουν στο νέο ψηφιακό τοπίο που ρυθμίζεται με τις ανάγκες της εκάστοτε χώρας και εποχής. Βέβαια, με αυτό τον έντονο ρυθμό που μεταβάλλεται κάθε μέρα η τεχνολογία στο διαδίκτυο τόσο πιο πολλές ανησυχίες και κενά αφήνει σχετικά με τη διαχείριση και παρακολούθηση των δεδομένων της. Γι'αυτό, για την ασφαλή περιήγηση των χρηστών κάποια πράγματα έπρεπε να θεσμοθετηθούν σχετικά με τη χρήση και τα όρια που θα έχει η κάθε διαδικτυακή εταιρία και ο κάθε χρήστης.

ΚΕΦΑΛΑΙΟ 2ο - ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

2.1 Ορισμός των προσωπικών δεδομένων

Σαν ορισμός τα προσωπικά δεδομένα , μπορούν να θεωρηθούν όλες οι πληροφορίες που έχουν σχέση με ένα άτομο και μέσα από αυτές να γίνει η αναγνώριση του. Προσωπικά δεδομένα θεωρούνται στη καθημερινή ζωή το όνομα, ο αριθμός τηλεφώνου, η διεύθυνση, οι φωτογραφίες , οι πολιτικές απόψεις, το θρήσκευμα αλλά και αυτά που υπάρχουν στο διαδίκτυο όπως ο λογαριασμός στο Facebook, το ηλεκτρονικό ταχυδρομείο, οι κωδικοί σε όλες τις on-line πλατφόρμες που είναι κάποιος εγγεγραμμένος κ.τ.λ. (Dimsis, 2011).

Τα προσωπικά δεδομένα προκύπτει δηλαδή ότι είναι άμεσα συνδεδεμένα με την ιδιωτική ζωή εφόσον περιέχουν πληροφορίες κάποιου ατόμου που ο ίδιος δε θα ήθελε να τις μοιραστεί με άλλους ανθρώπους. Αυτό συμβαίνει γιατί είναι κάποια προσωπικά δεδομένα που θέλει ο καθένας να τα κρατάει για τον εαυτό του και φοβάται ότι αν γίνουν γνωστά σε λάθος άτομα μπορεί να βρεθεί υπό την απειλή αυτών. Οπότε όσο καλύτερα διαφυλάσσονται τα προσωπικά δεδομένα τόσο προστατευμένη είναι και η ιδιωτική ζωή (Βασιλόπουλου, 2015).

Τα τελευταία χρόνια, γίνεται όλο και πιο αναγκαία προστασία των προσωπικών δεδομένων στο Διαδίκτυο εφόσον τόσο η ανάπτυξη του είναι ραγδαία όσο και ο αριθμός των ανθρώπων που το χρησιμοποιεί καθημερινά. Το διαδίκτυο είναι ένας τεράστιος κυβερνοχώρος και είναι δύσκολο να ελεγχθεί κάθε χρήστης και ιστότοπος που προσπαθεί να αποκτήσει πρόσβαση στα προσωπικά δεδομένου κάποιου χρήστη χωρίς καν ο ίδιος να το γνωρίζει τις περισσότερες

φορές. Για παράδειγμα, κάθε υπολογιστής έχει μια διεύθυνση IP όταν αποκτά πρόσβαση στο διαδίκτυο και αρχίζει να «σερφάρει». Παρά το γεγονός ότι αυτή η διεύθυνση συνεχώς μεταβάλλεται και ότι ο υπολογιστής τις περισσότερες φορές είναι κοινόχρηστος για όλα τα μέλη της οικογένειας , θεωρείται και ο ίδιος ένα προσωπικό δεδομένο εφόσον μπορεί κάποια στιγμή να ταυτοποιήσει τον πάροχο του υπολογιστή εάν κάποιος προβεί σε έρευνα και διασταυρώσει ορισμένες πληροφορίες. Για αυτούς τους λόγους, έχει αποκτήσει ιδιαίτερη σημασία να υπάρχουν κατάλληλα μέτρα έτσι ώστε να προστατευτούν τα προσωπικά δεδομένα των χρηστών του διαδικτύου (Dimsis, 2011).

2.1.1 Χρήση προσωπικών δεδομένων στο Διαδίκτυο

Οποιαδήποτε χρήση του Διαδικτύου σχεδόν πάντα οδηγεί σε επεξεργασία προσωπικών δεδομένων του χρήστη:

α) Αρχικά, όταν λαμβάνει ένας χρήστης κάποιο e-mail και το διαβάζει αυτομάτως καταγράφεται η ώρα εισόδου του, ο αποστολέας του και η ώρα που αποστάλθηκε το μήνυμα από τον πάροχο ηλεκτρονικών επικοινωνιών. Οπότε έχει πρόσβαση σε προσωπικά δεδομένα.

β) Όταν πλοηγείται ο χρήστης από τη μία ιστοσελίδα στην άλλη στο διαδίκτυο ο browser τις καταγράφει και κάποιες από αυτές εγκαθιστούν αρχεία cookies στον υπολογιστή έτσι ώστε όταν τις ξανά επισκεφτεί να τον αναγνωρίσουν.

γ) Όταν ένας χρήστης ψάχνει πληροφορίες στο διαδίκτυο μέσω κάποια μηχανής αναζήτησης αποτυπώνεται η διεύθυνση IP του υπολογιστή του χρήστη μαζί με τις αναζητήσεις που κάνει αλλά και την ώρα που πραγματοποιεί κάθε αναζήτηση.

δ) Για τη συμμετοχή του κάθε χρήστη σε έναν διαγωνισμό ή για να εκτελέσει μια ηλεκτρονική παραγγελία καλείτε να συμπληρώσει κάποια πεδία που απαιτούν να εισάγει προσωπικά του στοιχεία όπως το ονοματεπώνυμο του, τη διεύθυνση του, το τηλέφωνο του κ.τ.λ.

ε) Οι υπηρεσίες κοινωνικής δικτύωσης χρησιμοποιούνται από μεγάλο πλήθος ανθρώπων σε όλο τον κόσμο οι οποίοι κοινοποιούν διάφορα προσωπικά δεδομένα στο λογαριασμό τους. Το Facebook, που ναι το δημοφιλέστερο από αυτά, δίνει τη δυνατότητα στους χρήστες του να δημοσιεύουν τις φωτογραφίες τους και ναι είναι διαθέσιμες είτε στους «φίλους» τους είτε δημόσια, σε όλους. Εάν άλλος χρήστης κλέψει και ανεβάσει αυτές τις φωτογραφίες στο λογαριασμό του χωρίς την άδεια του ιδιοκτήτη του τότε έχει καταχραστεί προσωπικά δεδομένα (Βασιλόπουλου, 2015).

Γενικά, η κάθε κίνηση στο Διαδίκτυο συνάπτει με επεξεργασία των προσωπικών δεδομένων του χρήστη για αυτό είναι δύσκολο να βγει ένας κατάλογος που να περιέχει όλες τις πιθανότητες επεξεργασίας κατά την πλοήγηση. Τα προσωπικά δεδομένα ενός χρήστη είναι πολύ επίφοβο με τις διαστάσεις που έχει πάρει το Διαδίκτυο να βρεθούν σε λάθος χέρια και

να χρησιμοποιηθούν εναντίον του κάποια στιγμή στο μέλλον. Για παράδειγμα, όταν σε ένα προφίλ κοινωνικής δικτύωσης ένας χρήστης δημοσιεύει κάποιες απόψεις του σχετικά με ένα θέμα πρέπει να τις επικροτεί γενικά στη ζωή του γιατί μπορεί στο μέλλον να επηρεάσει την επαγγελματική του πορεία ή και κάποια προσωπική σχέση. Είναι λογικό, κάποιοι εργοδότες να παρακολουθούν ακόμα και τα προφίλ των εργαζομένων του για να έχουν μια ολοκληρωμένη άποψη για αυτούς που μέσα στα ορόρια της δουλειάς τους να μην προλαβαίνουν να αντιληφθούν την πραγματική προσωπικότητα τους. Πρέπει γενικά να υπάρχει μεγάλη προσοχή στο τι δημοσιεύεται στο Διαδίκτυο γιατί είναι πολύ δύσκολο αργότερα να διαγραφεί τελείως. «Τα γραπτά μένουν» λέει ένα ρητό και περιγράφει ακριβώς αυτή τη κατάσταση και μπορεί να δημοσιεύονται σε ιστότοπους χωρίς την έγκριση κανενός. Είναι πλέον πολύ σύνηθες φαινόμενο, να υποκλέπτεται ακόμα και η ταυτότητα κάποιου χρήστη του Διαδικτύου από κάποιον κακόβουλο που γνωρίζει πολλά προσωπικά του δεδομένα με σκοπό να εξαπατήσει ή ακόμα και να βλάψει τον ίδιο ή και τους φίλους του (Dimsis, 2011).

2.1.2. Προστασία των προσωπικών δεδομένων

Για να προστατευτούν τα άτομα που χρησιμοποιούν χωρίς όριο τα προσωπικά τους δεδομένα στο διαδίκτυο θεσπίστηκε νομοθεσία τόσο στην Ελλάδα όσο και στις άλλες χώρες που είναι μέλη της Ευρωπαϊκής Ένωσης. Αρμόδια για την εφαρμογή της νομοθεσίας στην Ελλάδα είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (νόμοι 2472/1997 και 3471/2006). Ο κύριος κανόνας των παραπάνω νόμων είναι: ότι είναι απαραίτητη η συγκατάθεση του υποκειμένου για να χρησιμοποιούν τα προσωπικά δεδομένα από κάποιον άλλον. Αυτή είναι και η πιο συνηθισμένη περίπτωση που γίνεται επεξεργασία των προσωπικών δεδομένων και πρέπει ουσιαστικά το άτομο που είναι δικά του τα προσωπικά δεδομένα να δώσει προφορική συγκατάθεση για να χρησιμοποιηθούν τα δεδομένα του από άλλο χρήστη και να τη γνωστοποιήσει στην ΑΠΔΠΧ. Βέβαια το υποκείμενο από μόνο του πρέπει να σιγουρευτεί για το ποιος ακριβώς είναι ο χρήστης που ζητά πρόσβαση στα δεδομένα, για ποιο λόγο που θέλει να χρησιμοποιήσει τα δεδομένα του, τα ακριβή στοιχεία που ζητά και σε ποιόν ιστότοπο ή σε ποιους ακριβώς θα τα διαβιβάσει. Κάποια δεδομένα απαγορεύεται να υποστούν επεξεργασία όπως είναι οι πολιτικές πεποιθήσεις, το θρήσκευμα, η καταγωγή, η ερωτική ζωή, η υγεία κ.τ.λ. Κατά εξαίρεση επιτρέπεται η επεξεργασία σε αυτά τα δεδομένα μόνο μέσω ειδικής άδειας από την ΑΠΔΠΧ. Για τη λήψη αυτής της άδειας θα πρέπει να υπάρχουν ειδικοί λόγοι (αρ.7 ν.2472/1997), οι οποίοι είναι:

1) Να υπάρχει μια γραπτή συγκατάθεση του ατόμου που αφορά τα δεδομένα
2) Πρέπει να διαφυλάσσεται το προσωπικό συμφέρον του ατόμου ή το ζωτικό συμφέρον κάποιου τρίτου όπως αυτός θα οριστεί από το νόμο, εάν το υποκείμενο δε μπορεί να δώσει τη συγκατάθεση το ίδιο.
3) Υπό την παρουσία κάποιου πειθαρχικού οργάνου ή δικαστηρίου να γίνει άσκηση του δικαιώματος όπως και αναγνώρισης και υπεράσπισης βεβαίως. (αρ.22 ν.3471/2006)
4) Η διαχείριση υπηρεσιών υγείας και γενικά να γίνει κάθε ιατρική εξέταση για να

βεβαιωθεί ότι δε συντρέχουν προβλήματα υγείας(η ιατρική διάγνωση, πρόληψη, περίθαλψη) (αρ.34 ν.2915/2001)

5) Να εξακριβωθεί ότι το άτομο που ζητά την άδεια δεν έχει πάρει μέρος σε ποινικά αδικήματα ή έχει γενικά εκκρεμότητες με το νόμο.
6) Να ασκηθεί δημόσιος φορολογικός έλεγχος και να προστατευθεί η δημόσια υγεία.(αρ. 34 ν.2915/2001)
7) Έλεγχος της τήρησης των προσωπικών δεδομένων παράλληλα με τη διεξαγωγή επιστημονικής έρευνας.(ν.2472/1997)

2.2 Η ιδιωτικότητα στο Διαδίκτυο

Τα προσωπικά δεδομένα αντανακλούν την προσωπικότητα ενός ατόμου και παρουσιάζει στοιχεία της ιδιωτικής του ζωής για αυτό και όταν προστατεύονται τα προσωπικά δεδομένα στο Διαδίκτυο ουσιαστικά προστατεύεται και η ιδιωτικότητα του υποκειμένου. Όταν αναφέρεται κάποιος στην ιδιωτικότητα, περιγράφει την ανάγκη του για απομόνωση, την αυτονομία του, την μοναχικότητα του. Γενικά, είναι αυτός που επιζητά να μην βρίσκεται στο επίκεντρο προσοχής αλλά να βρίσκεται στην αφάνεια δίχως κάποιος να τον παρατηρεί. Η έννοια της ιδιωτικότητας, στις ΗΠΑ, ταυτίζεται με τα προσωπικά δεδομένα ιδιαίτερα όταν έχει να κάνει για τη προστασία τους. Τα προσωπικά δεδομένα σαν ορισμός συνήθως χρησιμοποιούνται ως μια νομική ορολογία αλλά όταν μιλάμε για έμπρακτα παραδείγματα οι δυο έννοιες δε διαχωρίζονται (Dimsis, 2011).

2.2.1 Η διαδικτυακή ιδιωτικότητα

Η διαδικτυακή ιδιωτικότητα έχει να κάνει με την επιθυμία προφύλαξης των ιδιωτικών στοιχείων ενός ατόμου όταν τα εισάγει στο διαδίκτυο. Δηλαδή ο ίδιος προλαμβάνεται για τις πληροφορίες που θα παρουσιάσει σε τρίτους να μείνουν ιδιωτικές. Αυτή η ιδιωτικότητα της πληροφορίας απαιτείται από το κάτοχο της για να μην κλαπούν από άλλους οργανισμούς αλλά και άλλα άτομα. Όταν ένα τρίτο άτομο έχει στην ιδιοκτησία του προσωπικά δεδομένα ενός άλλου ατόμου τότε η ιδιωτικότητα σαφηνίζεται ως η ικανότητα που έχει ένα άτομο να ελέγχει σε μεγάλο βαθμό αυτόν που έχει πρόσβαση στα προσωπικά του δεδομένα (Dimsis, 2011).

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης όρισε σαν προσωπικά δεδομένα οποιαδήποτε πληροφορία μπορεί να ταυτοποιήσει ένα άτομο στο Διαδίκτυο. Τα προσωπικά δεδομένα επειδή είναι πολυπληθείς περιλαμβάνουν τους ακόλουθους τύπους:

- Δεδομένα που φανερώνουν τη τοποθεσία που βρίσκεται το υποκείμενο είτε μέσω του GPS που διαθέτουν τα κινητά τηλέφωνα είτε μέσω του IP address που διαθέτουν οι υπολογιστές μόλις συνδεθούν στο Διαδίκτυο.

- Οτιδήποτε έχει δημιουργήσει ένας χρήστης στο Διαδίκτυο. Για παράδειγμα ένα προσωπικό blog, ένα βίντεο, ένα σχόλιο κ.τ.λ.
- Όλα τα κοινωνικά δεδομένα που περιστοιχίζουν ένα χρήση στα μέσα κοινωνικής δικτύωσης (όπως φίλοι, επαφές).
- Όλη η συμπεριφορά που προβάλλουν στο διαδίκτυο όπως είναι οι αγορές on-line και τρόπος αναζήτησης και πληρωμής του.
- Να γίνει αναγνώριση σε δεδομένα του χρήστη τα όποια αναφέρουν το όνομα του, οι λογαριασμοί τραπέζης του, ο αριθμός μητρώος του , οι οικονομικές συναλλαγές του δηλαδή στοιχεία επίσημης φύσης.
- Στοιχεία όπως το φύλο, οι πολιτικές πεποιθήσεις, η φυλή, η ηλικία, το εισόδημα τα οποία απαρτίζουν τα δημογραφικά στοιχεία (Βασιλόπουλου, 2015).

Τα προσωπικά δεδομένα έχουν κατηγοριοποιηθεί κατά καιρούς με διάφορους τρόπους. Γνωστό παράδειγμα αυτό του Schneier που το 2010 ταξινόμησε τα προσωπικά δεδομένα σύμφωνα με τα κοινωνικά δίκτυα όπως, δηλαδή, τα σχόλια που γίνονται σε δημοσιεύσεις άλλου χρήστη ονομάστηκαν εμπιστευτικά δεδομένα. Συχνά βέβαια τα προσωπικά δεδομένα κατηγοριοποιούνται λαμβάνοντας υπόψη τη χρήση που έχουν στο διαδίκτυο δηλαδή ξεχωρίζουν τα δεδομένα που χρησιμοποιούνται άμεσα για κάποια εργασία από αυτά που αποθηκεύονται για μετέπειτα χρήση(FTC,2009). Στη δεύτερη κατηγορία ταξινομούνται τα δεδομένα σε δύο κατηγορίες με βάση αν οι πληροφορίες που περιλαμβάνουν τα δεδομένα δεν μετατραπούν σε μεγάλο βαθμό κατά το πέρασμα του χρόνου ,άρα κατά κάποιο τρόπο μείνουν στατικές, και αν οι πληροφορίες αλλάξουν δραματικά αλλά δίνουν τη δυνατότητα αν συλλεχθούν και εξεταστούν να μπορούν να αποδώσουν ένα καλά πληροφορημένο προφίλ ενός ανθρώπου, άρα οι πληροφορίες αυτές να είναι δυναμικές (sofokleousin, 2017.)

2.2.2 Δεδομένα προσωπικής και μη προσωπικής ταυτοποίησης του χρήστη

Μια γνωστή διάκριση που γίνεται ανάμεσα στα προσωπικά δεδομένα είναι αυτή της προσωπικής και μη προσωπικής ταυτοποίησης του χρήστη. Στη πρώτη κατηγορία υπάρχουν πληροφορίες που οδηγούν στην απευθείας ταυτοποίηση του χρήστη ενώ στη δεύτερη κατηγορία που περιλαμβάνει πληροφορίες σχετικά με τη επισκεψιμότητα του χρήστη σε ιστοσελίδες, με τη συμπεριφορά που εμφανίζει στο Διαδίκτυο, με την αναζήτηση που κάνει σε όλες τις υπηρεσίες του διαδικτύου που δύσκολα ταυτοποιούν τη ταυτότητα του εν λόγο χρήστη. Στις πληροφορίες προσωπικής ταυτοποίησης κατανέμονται για παράδειγμα μοναδικά στοιχεία του χρήστη όπως είναι ο αριθμός ταυτότητας του, η διεύθυνση, το όνομα, το ΑΦΜ του ενώ στις πληροφορίες μη προσωπικής ταυτοποίησης συναντάμε τις διαδικτυακές αγορές, τις αναζητήσεις στο παγκόσμιο ιστό, της επισκεψιμότητα στις ιστοσελίδες (Dimsis, 2011).

Καθώς βελτιώνονται όλο και περισσότερο οι μέθοδοι που αναλύονται τα δεδομένα και προσφέρουν πλέον τη δυνατότητα να αναλυθούν ευρέως κάποιες μη ταυτοποιήσιμες πληροφορίες και έτσι να ταυτοποιηθεί σε τελική βάση ο χρήστης, επέρχεται μια αβεβαιότητα

στο τρόπο που θα κατηγοριοποιηθούν κάποιες πληροφορίες. Πληροφορίες μη προσωπικής ταυτοποίησης όπως η διεύθυνση IP και η γεωγραφική θέση όταν συσχετιστούν μεταξύ τους μαζί με άλλες πληροφορίες, όπως η αναζήτηση ορολογιών, η επίσκεψη σε συγκεκριμένες ιστοσελίδες μπορούν να ταυτοποιήσουν ένα χρήστη. Έτσι, όμως, πλέον παύεται να υφίσταται ιδιωτικότητα και ανωνυμία στο διαδίκτυο (Βασιλόπουλου, 2015).

2.2.3 Ανησυχίες για την ιδιωτικότητα

Ένα από τα πιο σημαντικά ζητήματα της εποχής της τεχνολογίας και συνάμα της πληροφορίας είναι η προστασία της ιδιωτικότητας του κάθε ατόμου και ο έλεγχος των πληροφοριών του έναντι τρίτων ατόμων. Από την αρχή της ίδρυσης των υπολογιστικών συστημάτων εκφράστηκαν ανησυχίες για το ενδεχόμενο παραβατικότητας των προσωπικών δεδομένων λόγω της δυσκολίας παρατήρησης ενός τέτοιου μεγάλου κυβερνοχώρου. Όσο περισσότερο εξελίσσεται η τεχνολογία και μαζί με αυτή όλες οι υπηρεσίες της τόσο περισσότερο ευάλωτα γίνονται τα προσωπικά δεδομένα των χρηστών στην έκθεση τους. Οι διαδικτυακές υπηρεσίες, πλέον, ζητούν μεγάλο όγκο προσωπικών πληροφοριών για τη χρήση τους όπως και τα επιχειρηματικά λογισμικά που συλλέγουν ακατάπαυστα προσωπικά δεδομένα αλλά και οι χρήστες από μόνοι τους δημοσιεύουν σε προσωπικά τους blogs ή σε σελίδες κοινωνικής δικτύωσης περιεχόμενα με στοιχεία από τη προσωπική τους ζωή (Βασιλόπουλου, 2015).

2.2.4 Παραβίαση Ιδιωτικής Ζωής

Κάθε φορά που «σερφάρει» κάποιος στο διαδίκτυο «προσφέρει» πληροφορίες από τη προσωπική του ζωή. Οι πληροφορίες αυτές αποτελούν ένα γρίφο που μόλις συμπληρωθεί με τις σωστές πληροφορίες ταυτοποιεί έναν άνθρωπο. Η ζωή στο φυσικό κόσμο έχει μεγάλη συσχέτιση με τη ζωή στο διαδίκτυο. Σε όποια πράξη και αν προβεί κάποιος στο διαδίκτυο αφήνει ίχνη πίσω του για αυτό και πρέπει να υπάρχει τεράστια προσοχή (Βασιλόπουλου, 2015).

Όταν κάποιος ανταλλάσει e-mail με κάποιον άλλον συνήθως ανταλλάσουν πληροφορίες για τη καθημερινότητα τους. Εάν δεν υπάρχει προσοχή, τότε πολλά άτομα μπορεί να πάρουν τις πληροφορίες αυτού του ατόμου και ανάμεσα σε αυτούς μπορεί να είναι ο εργοδότης του, ο παροχέας το e-mail, η κυβέρνηση και πολλοί άλλοι (Dimsis, 2011).

Επίσης, όταν κάποιος συμμετέχει σε ομαδικές συζητήσεις στο Διαδίκτυο πρέπει να προσέχει για το ποιες πληροφορίες μοιράζεται με τα άλλα μέλη της ομάδας (π.χ. e-mail) διότι μπορεί κάποιος μέλος της να τις διασύρει σε άλλα άτομα χωρίς να υπάρξει απαγόρευση (sofokleousin, 2017.)

Ακόμα, όταν χρησιμοποιείται ένας web browser (περιηγητής ιστού) στο Διαδίκτυο αφήνει ίχνη και έτσι πολύ πιθανόν να διανέμονται πληροφορίες στον παροχέα διαδικτύου σχετικά με τον αριθμό IP του υπολογιστή που χρησιμοποιήθηκε αλλά και τις σελίδες που επισκέφτηκε. Αν ακόμα ο web browser χειρίζεται το e-mail τότε μπορεί να παρέχει και το τηλέφωνο το χρήστη και την ηλεκτρονική του διεύθυνση (Dimsis, 2011).

Πολλές ιστοσελίδες, για να θυμούνται όταν ένας ίδιος χρήστης τις επισκεφτεί ξανά, αποθηκεύουν κάποια δεδομένα, τα "Cookies" όπως ονομάζονται. Τα Cookies είναι κάποια μικρά αρχεία που αποθηκεύουν πληροφορίες ενός χρήστη όπως είναι το διαδικτυακό του όνομα, η φόρμα εγγραφής σε μια ιστοσελίδα, οι αγορές του κ.τ.λ. Τα Cookies που χρησιμοποιούνται από νόμιμες εταιρίες είναι ουσιαστικά για λόγους διαφήμισης ενώ αυτά που χρησιμοποιούνται από παράνομες είναι για λόγους Marketing (για να πουλήσουν τα προσωπικά δεδομένα σε εταιρίες) (Dimsis, 2011).

Επιπλέον, ιδιαίτερη προσοχή πρέπει να υπάρχει σε αποστολή μηνύματος της στιγμής όπως είναι το Google Talk που αυτόματα κάνουν αποθηκεύσει των μηνυμάτων εκτός και αν έχουν προγραμματιστεί συγκεκριμένες ρυθμίσεις (sofokleousin, 2017.)

Κάθε μέρα, οι άνθρωποι αναζητούν τη μεταξύ τους επικοινωνίας και αρχίζουν να αλληλεπιδρούν μέσω της αποστολής φωτογραφιών με τη χρήση κοινωνικών δικτύων. Αυτά τα δίκτυα, όπως είναι το MySpace, το Instagram, το Facebook, μπορεί να εθίσουν ένα χρήστη και να του δημιουργήσουν με το πέρασμα του χρόνου πρόβλημα στη δουλειά του , στο σχολείο του αλλά και σε όλες τις πτυχές της καθημερινότητας του. Επίσης, όλο και πιο συχνά ακούγονται περιπτώσεις παιδόφιλων που «ψαρεύουν» τα θύματα τους από τα κοινωνικά δίκτυα είτε για να τα αποπλανήσουν είτε για να τα εκβιάσουν αργότερα με τις ίδιες τους τις φωτογραφίες (Dimsis, 2011).

Εκτεταμένη είναι σήμερα και η χρήση ιστολογιών(blog), τα οποία αφήνουν ίχνη στο Διαδίκτυο, και δημιουργούνται ιδιαίτερα από άτομα νεαρής ηλικίας και είναι κάτι σαν ενημερωτική εφημερίδα. Τα ιστολόγια έχουν ελεύθερη πρόσβαση και ανανεώνονται καθημερινά αφού εισάγουν νέες πληροφορίες για να κρατήσουν το ενδιαφέρον του κοινού τους. Όσοι χρήστες επιθυμούν μπορούν να αφήσουν τα σχόλια τους για να πουν τη γνώμη τους για ένα θέμα. Σε κάποια από αυτά απαιτείται να γίνει εγγραφή για να μπορούν οι χρήστες τους να σχολιάσουν και έτσι αυτομάτως δίνουν προσωπικά τους δεδομένα όπως είναι το όνομα, το e-mail κ.τ.λ. (MADRIGAL, 2012).

2.2.5 Facebook και ιδιωτικότητα

Κάπου στους 1,5 δισεκατομμύρια χρήστες χρησιμοποιούν στην σημερινή εποχή το Facebook, που ναι το δημοφιλέστερο μέσο κοινωνικής δικτύωσης και έχει μπει στα σπίτια των περισσότερων ανθρώπων σε όλο το πλανήτη. Έχει γίνει ένας εθισμός, ιδιαίτερα στα άτομα νεαρής ηλικίας, που μπαίνουν κάθε δεκαπεντάλεπτο κατά μέσο όρο για να ελέγχουν το

λογαριασμό τους (sofokleousin, 2017.)

Το Facebook δίνει τη δυνατότητα στους χρήστες του να ανταλλάσουν πληροφορίες γρήγορα και πολύ εύκολα είτε αυτές είναι φωτογραφίες και βίντεο είτε είναι σχόλια και μηνύματα. Το Facebook, με αυτόν τον τρόπο έχει τη δυνατότητα να προσφέρει υπηρεσίες διαδικτυακής διαφήμισης και να αποκτά τεράστια ποσά από τη προώθηση τους. Για να μπει κάποιος και να συμμετέχει σε αυτόν τον μικρόκοσμο της πληροφορίας θα πρέπει να δημιουργήσει ένα δικό του «προφίλ» παρέχοντας όμως μεγάλο αριθμό από τα προσωπικά του δεδομένα στην υπηρεσία κοινωνικής δικτύωσης, όπως είναι το όνομα του, το e-mail του και στη συνέχεια το φύλο του, την εργασία του, τη προσωπική του κατάσταση κ.τ.λ. Μέσω αυτών ο χρήστης καταλήγει να προσφέρει απροκάλυπτα τον «εαυτό του» σε χιλιάδες χρήστες του Facebook (ΕφΑθ 175/2014) (Βασιλόπουλου, 2015).

Ενόψει αυτών η νομοθεσία για τη προστασία των προσωπικών δεδομένων έπρεπε να θέσει ένα πλαίσιο για την παραχώρηση των κοινωνικών δικτύων και να παρέχει κάποιο τρόπο προστασίας των χρηστών του που να θεμελιώνεται νομικά.

Κάθε πληροφορία που μπορεί να χαρακτηρίσει έναν άνθρωπο θεωρείται προσωπικό δεδομένο. Για παράδειγμα η ηλικία, το όνομα, το τηλέφωνο, η διεύθυνση, τα ενδιαφέροντα θεωρούνται προσωπικά δεδομένα και μπορούν ακόμα και να περιέχουν την ερωτική του ζωή, το θρήσκευμα του, την πολιτική του πεποίθηση, την οικονομική του κατάσταση αλλά επίσης και τη κατάσταση της υγείας του (άρθρο 2α και γ Ν. 2472/1997) (Broumas, 2015).

Καθημερινές δραστηριότητες που πραγματοποιούνται στα μέσα κοινωνικής δικτύωσης έχουν ως αντίκτυπο την επεξεργασία προσωπικών δεδομένων. Κάθε ενέργεια που τελείτε πάνω σε δεδομένα προσωπικού χαρακτήρα όπως μια φόρμα συμμετοχής σε διαγωνισμό ηλεκτρονικού παιχνιδιού που περιέχει όνομα, διεύθυνση, τηλέφωνο, ηλικία ή η εγγραφή σε κάποιο on-line κατάστημα συγγραμμάτων ή ένα ηλεκτρονικό site με μουσική που αποθηκεύει τους καλλιτέχνες και το είδος μουσικής που αρέσει στο χρήστη του ή το προφίλ στο Facebook που κρατά φωτογραφίες αλλά και πληροφορίες με φίλους βασίζονται πάνω στην επεξεργασία των προσωπικών δεδομένων. Άρα και η διαγραφή και συσχέτιση δεδομένων, η καταγραφή, η συλλογή, η επικοινωνία, που επιμελείται κατά τη παραχώρηση σε κάποια κοινωνικά δίκτυα αποτελεί επεξεργασία προσωπικών πληροφοριών και δεδομένων σύμφωνα με τον Ν. 2472/1997 (Koumentakis, 2017).

«Υποκείμενο των δεδομένων» θεωρείται οποιοδήποτε φυσικό πρόσωπο από τον οποίον μπορεί η ταυτότητα του είτε να βεβαιωθεί είτε να είναι γνωστή δηλαδή μπορεί να εξακριβωθεί η ζωή του με βάση τη πολιτιστική, τη κοινωνική, τη πολιτική, τη βιολογική, τη φυσική, τη ψυχική του υπόσταση (άρθρο 2 γ’ Ν. 2472/1997). Οπότε τα δεδομένα που επεξεργάζονται και συλλέγονται και ανήκουν σε κάποιο χρήστη που χρησιμοποιεί μια υπηρεσία κοινωνικής δικτύωσης συνιστούν υποκείμενα δεδομένων και κατέχουν δικαιώματα του Ν. 2472/1997. (Broumas, 2015).

«Υπεύθυνος επεξεργασίας» θεωρείται ο καθένας να προσδιορίσει τον τρόπο επεξεργασίας και τον σκοπό των προσωπικών δεδομένων, όπως μια υπηρεσία ή δημόσια αρχή, ή κάποιο

νομικό ή φυσικό πρόσωπο ή ο κάθε άλλος οργανισμός (άρθρο 2 ζ' Ν. 2472/1997). Υπεύθυνοι επεξεργασίας θεωρούνται επίσης και οι αυτοί που παρέχουν υπηρεσίες κοινωνικής δικτύωσης , με εξαίρεση λίγες περιπτώσεις, σύμφωνα με το Ν. 2472/1997 (Broumas, 2015).

Κατά εξακολούθηση και οι χρήστες μπορούν να χαρακτηριστούν ως υπεύθυνοι επεξεργασίας αν και εφόσον αντιπροσωπεύουν ένα οργανισμό ή μια εταιρία οι οποίοι να χρησιμοποιούν τις υπηρεσίες τους ως πλατφόρμα με σκοπό φιλανθρωπικούς, διαφημιστικούς ή πολιτικούς σκοπούς (Koumentakis, 2017).

2.2.6 Συνέπειες παραβίασης προσωπικών δεδομένων

Η ανησυχία που υπάρχει γύρω από τη χρήση του διαδικτύου είναι η παραβίασης της ασφάλειας των προσωπικών δεδομένων των χρηστών έχοντας κοινωνικές, οικονομικές φυσικές συνέπειες με αρνητικό αποτέλεσμα. Ανάλογα με τα προσωπικά δεδομένα που παραβιάζονται, μπορούν να χωριστούν οι συνέπειες της σε χαμηλές, μέσες και υψηλές. Στο χαμηλό επίπεδο της παραβίασης της εμπιστευτικότητας, κατανέμεται η αναστάτωση που βιώνει ένας χρήστης όταν για παράδειγμα αναγκαστεί να αλλάξει τον αριθμό του τηλεφώνου του επειδή έχει διαρρεύσει στο διαδίκτυο. Στο μεσαίο επίπεδο κατανέμεται οι επιπτώσεις στον οικονομικό τομέα όπως για παράδειγμα αν πέσει θύμα εκβιασμού για να μην δημοσιευτούν προσωπικά του στοιχεία ή αν ταπεινωθεί δημόσια ή αν κλαπούν τα στοιχεία που έχει στη ταυτότητα του. Τέλος, στο υψηλό επίπεδο κατατάσσονται οι οικονομικές ζημιές όπως και οι κοινωνικές, οι σωματικές βλάβες με χειρότερη κατάληξη την απώλεια ζωής ενός ατόμου ή η πτώχευση του (Βασιλόπουλου, 2015).

Διάφορες μηνύσεις έχουν γίνει σε πολύ δημοφιλείς ιστοσελίδες όπως είναι η Facebook Beacon , η Google Buzz και η AOL Value Click με αφορμή τις παραβιάσεις που γίνονται σε βάρος της ιδιωτικότητας στο διαδίκτυο αλλά ακόμα έχουν δημιουργηθεί και νόμοι σχετικά με τη προστασία των προσωπικών δεδομένων στο διαδίκτυο, γεγονότα που αποδεικνύουν το ύψιστο ενδιαφέρον που έχει στραφεί στη διαδικτυακή ιδιωτικότητα. Αρκετοί ερευνητές έχουν επανεξετάσει το ζήτημα της προστασίας των δεδομένων έτσι ώστε αυτό να συμβαδίζει με την εξέλιξη και την δυναμικότητα της εποχής αφού όλο και περισσότερες τεχνολογίες εμφανίζονται στο προσκήνιο που προσφέρουν νέες υπηρεσίες και είναι τελείως διαφορετικός ο τρόπος λειτουργίας τους από το τις προηγούμενες (Dampali, 2011).

2.3 Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων στην Ελλάδα

Το 1948 κατοχυρώθηκε, σε διεθνές νομικό κείμενο για πρώτη φορά , το δικαίωμα που έχει κάθε άτομο να προστατεύσει τα προσωπικά του δεδομένα έναντι παρεμβολής τρίτων. Η Οικουμενική Διακήρυξη Ηνωμένων Εθνών στο άρθρο 12 που αφορά τα ανθρώπινα δικαιώματα θέσπισαν το σεβασμό που πρέπει να υπάρχει τόσο στην οικογενειακή όσο και

στην ιδιωτική ζωή (Οργανισμός Ηνωμένων Εθνών-ΟΗΕ, Οικουμενική Διακήρυξη για τα ανθρώπινα δικαιώματα,10/12/1948).

Έκτοτε, ύψιστη σημασία όλων των νομοθετημάτων που κατοχυρώθηκαν ήταν το δικαίωμα της προστασίας των προσωπικών δεδομένων του ανθρώπου αλλά και το δικαίωμα του απορρήτου. Επειδή δεν γινόταν να απαγορευτεί εξ ολοκλήρου η συλλογή και η επεξεργασία των προσωπικών δεδομένων τέθηκε ένα νομικό πλαίσιο για να τα οριοθετήσει (Ι. Κ. Καράκωστας 2009).

Τα βασικά νομοθετικά κείμενα στην Ελλάδα σχετικά με την προστασία των προσωπικών δεδομένων όσον αφορά το φυσικό και τον ηλεκτρονικό χώρο είναι οι:

- Ν.2472/1997 «Περί προστασίας του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.»
- Ν.3471/2006 «Προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.»
- Ν.3783/2009 «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις.»
- Ν.3917/2011 «Διατήρηση δεδομένων που παράγονται και υποβάλλονται σε επεξεργασία σε συνάρτηση με τη 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.»
  Ακόμα,

- Ν.4070/2012 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις.»
- Ν.3051/2002 «Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις.»

1)Ν.2472/1997 «Περί προστασίας του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.»

Σύμφωνα με τη Σύμβαση της 28^{η}ς Ιανουαρίου 1981 του Συμβουλίου της Ευρώπης και κατά επιταγή της Οδηγίας 95/46/ΕΚ θεσπίστηκε στην Ελλάδα ο Ν.2472/1997 «Περί προστασίας του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» ο οποίος ορίζει ότι για να επεξεργαστεί κάποιος τα δεδομένα ενός άλλου χρήστη πρέπει να έχει πάρει τη συγκατάθεση του και να τον ενημερώσει διεξοδικά για το είδος της επεξεργασίας, για ποιο σκοπό θα προβεί σε αυτήν αλλά και από ποιον θα γίνει.

Αυτές τις προϋποθέσεις προβλέπει αυτός ο νόμος που έχει ως σκοπό να προστατέψει τα

διαδικτυακά δικαιώματα του κάθε χρήστη αλλά και την ελευθερία να κινείτε κάποιος άφοβα στο διαδίκτυο χωρίς να φοβάται μήπως εκτεθεί και επηρεαστεί η προσωπική του ζωή.(Άρθρο 1 του Ν.2472/1997).

Όταν γίνεται στις ηλεκτρονικές επικοινωνίες επεξεργασία των προσωπικών δεδομένων τότε αυτή περιλαμβάνει τη διαδικασία της δέσμευσης, συσχέτισης, τροποποίησης, διαγραφής, χρήσης, συλλογής, καταχώρισης, διατήρησης, καταστροφής, αποθήκευσης, διάδοσης, διαβίβασης(άρθρο 2 του Ν.2472/1997). Για να επιτραπεί η επεξεργασία θα πρέπει να δηλωθεί κάποιος συγκεκριμένος σκοπός που να είναι σύμφωνος με το νόμο (άρθρο 4 του Ν.2472/1997).

Για να πραγματοποιηθεί και να γίνει η επεξεργασία πρέπει πρώτα από όλα να ενημερωθεί το υποκείμενο των δεδομένων και να συμφωνήσει με την όλη διαδικασία. Βέβαια, βασικές προϋποθέσεις είναι τα δεδομένα αυτά να μην είναι ευαίσθητα και να είναι αναγκαία για το πρόσωπο που θέλει να τα χρησιμοποιήσει αλλά και το μόνο προβαλλόμενο άτομο από αυτά να είναι το υποκείμενο (άρθρο 5 του Ν.2472/1997). Η συλλογή των προσωπικών δεδομένων από μια υπηρεσία πρέπει να γίνει τη στιγμή που θα αποδεχτεί το υποκείμενο τους όρους χρήσης του και όχι πιο πριν (Θ. Σιδηρόπουλος 2008).

Για να ελέγχεται και να τηρείτε ο νόμος σχετικά με τη προστασία προσωπικών δεδομένων ιδρύθηκε η δημόσια αρχή που ονομάστηκε “Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα” έχοντας τρία συστήματα ελέγχου.

Πρώτον, το σύστημα που γνωστοποιεί έγγραφα στην ΑΠΔΠΧ όλη τη συλλογή που έχει γίνει στα δεδομένα αλλά και της αρχειοθέτησης και της επεξεργασίας που έχουν υποστεί από όλους τους κατόχους τους.

Δεύτερον, το σύστημα άδειας για τη συλλογή και την επεξεργασία των δεδομένων που θεωρούνται ευαίσθητα από την ΑΠΔΠΧ.

Τρίτον, το σύστημα ενημέρωσης των ατόμων πριν υποστούν επεξεργασία τα προσωπικά τους δεδομένα (Α. Γέροντας 2002).

Από την παράβαση των κανόνων προκύπτουν στον ίδιο νόμο αστικές, διοικητικές, ποινικές κυρώσεις που ορίζουν τις ποινές τους ανάλογα με το βαθμό και τη βαρύτητα που διεπράχθη μια παραβατικότητα και την καθορίζουν με την αρχή της αναλογικότητας(άθρο21-23 του Ν.2472/1997).

2) Ν.3471/2006 «Προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν .2472/1997.»

Η οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και επίσης του Συμβουλίου της 12ης Ιουλίου του 2002 ενσωματώθηκε στο ελληνικό δίκαιο μέσω του Ν.3471/2006 και έχει σχέση με την επεξεργασία που υπόκεινται τα προσωπικά δεδομένα στο χώρο της ηλεκτρονικής επικοινωνίας αλλά και την προστασία της προσωπικής ζωής του υποκειμένου όταν αυτά τα δεδομένα δημοσιοποιηθούν(ΕΕ L 201/37 της 31ης Ιουλίου 2002). Πρέπει να υπάρξουν

κάποιες προϋποθέσεις όταν ένας τρίτος μπει στη διαδικασία να επεξεργαστεί τα προσωπικά δεδομένα κάπου άλλου και αυτό ακριβώς ορίζει αυτός ο νόμος. Επίσης, διασφαλίζει στις ηλεκτρονικές επικοινωνίες που γίνονται μεταξύ των χρηστών του διαδικτύου να υπάρχει απόρρητο ώστε να μην μπορούν να υποκλαπούν από άλλους.

Στο άρθρο 5 παρ.1 του Ν.3471/2006 ορίστηκε ότι για να επεξεργαστούν τα προσωπικά δεδομένα θα πρέπει να περιοριστεί όσο το δυνατόν περισσότερο η επεξεργασία τους για να οριστεί ένα μέτρο και να μπορεί να εξυπηρετήσει, παράλληλα, το σκοπό της (περιλαμβάνονται τα δεδομένα κίνησης και θέσης).

Βέβαια, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα ενδέχεται να επιτραπεί μόνο εάν ένας χρήστης ή ένας συνδρομητής μιας ιστοσελίδας ο οποίος είναι συμβαλλόμενο μέρος αποδεχτεί την επεξεργασία γιατί είναι απαραίτητη για να πραγματοποιηθεί κάποια σύμβαση ή αν ο συνδρομητής κάνει αίτηση για να λάβει κάποια μέτρα πριν υπογράψει τη σύμβαση. Η άλλη περίπτωση είναι ο χρήστης ή ο συνδρομητής εφόσον έχει ενημερωθεί διεξοδικά για την έκταση της επεξεργασίας που θα γίνουν στα δεδομένα αλλά και το σκοπό αυτής της ενέργειας και το είδος που θα τροποποιηθούν να συγκαταθέσει για τους αποδέκτες αυτών.

Πέρα από όλα αυτά, πρέπει να παρέχεται στον επισκέπτη μιας ιστοσελίδας η δυνατότητα να εισέλθει σε αυτήν με κάποιο ψευδώνυμο αντί να κάνει εγγραφή με τα αληθινά της στοιχεία(αρ.5 παρ. 7 Ν.3471/2006).

Στην επιβολή πολύ μεγάλων προστίμων καταφεύγει η δικαιοσύνη αν καταπατηθούν τα παραπάνω δικαιώματα (άρθρο 15 του Ν.3471/2006).

Δηλαδή, αν κάποιος εκμεταλλευτεί με οποιοδήποτε τρόπο τα δεδομένα προσωπικού χαρακτήρα κάποιου συνδρομητή ή χρήστη, είτε αυτό σημαίνει να τα χρησιμοποιήσει, να τα συλλέξει, να τα αποθηκεύσει, να τα μεταδώσει, να τα δημοσιοποιήσει, να τα ανακοινώσει είτε αυτό σημαίνει να τα αλλοιώσει, να τα αφαιρέσει ,να τα καταστρέψει και σε περίπτωση που αυτά γίνουν προσιτά και γνωστοποιηθούν σε μη δικαιούμενα πρόσωπα προβλέπεται τιμωρία με ενός έτους φυλάκισης και πρόστιμο που κυμαίνεται από τα δέκα χιλιάδες ευρώ μέχρι τα εκατό χιλιάδες ευρώ ανάλογα με τη πράξη. (άρθρο 15 παρ. 1 του Ν.3471/2006).

Όποιος ευθύνεται για την άνομη επεξεργασία ή ο εκπρόσωπος του και δεν αποδέχεται τις διοικητικές κυρώσεις που του χουν επιβληθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τιμωρείται με διετή φυλάκιση και με πρόστιμο από δώδεκα χιλιάδες ευρώ μέχρι εκατόν είκοσι χιλιάδες ευρώ (άρθρο 15 παρ. 2 του Ν.3471/2006). Οι διοικητικές αυτές κυρώσεις αφορούν την προσωρινή ή οριστική ανάκληση άδειας του κατηγορούμενου και την καταστροφή ολοκλήρου του παράνομου αρχείου ή την διακοπή της επεξεργασίας των δεδομένων που έχουν καταχραστεί και την καταστροφή του.

Αν ο δράστης είχε σκοπό να κλέψει τα προσωπικά στοιχεία για να παραλάβει κάποιο χρηματικό ποσοστό είτε για τον εαυτό του είτε για κάποιον άλλον ή ακόμα ήθελε με αυτά τα στοιχεία να βλάψει τον ιδιοκτήτη του τότε τα χρόνια φυλάκισης ανεβαίνουν στα δεκαπέντε και το χρηματικό ποσό ορίζεται από δεκαπέντε χιλιάδες ευρώ μέχρι εκατόν πενήντα χιλιάδες

ευρώ. Σε περίπτωση που διακυβεύτηκε κίνδυνος στην ελευθερία που προσδίδει το δημοκρατικό πολίτευμα ή στην εθνική ασφάλεια, τότε η τιμωρία που επιβάλλεται είναι η κάθειρξη και η ποινή για το χρηματικό ποσό μπορεί να αγγίξει στη χειρότερη τα τριακόσια πενήντα χιλιάδες ευρώ ή στη καλύτερη τα πενήντα χιλιάδες ευρώ (άρθρο 15 παρ. 3 του Ν.3471/2006).

Αν το δικαστήριο υποψιαστεί αμέλεια στις πράξεις των παραγράφων 1 και 2 (Ν.3471/2006) η ποινή φυλάκισης είναι μόνο 18 μήνες και το χρηματικό ποσό ορίζεται σε δέκα χιλιάδες ευρώ (άρθρο 15 παρ. 4 του Ν.3471/2006). .

3) Ν.3917/2011 «Διατήρηση δεδομένων που παράγονται και υποβάλλονται σε επεξεργασία σε συνάρτηση με τη 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.»

Η οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και της 15ης Μαρτίου που ενσωματώθηκε στο Ν.3917/2011 έδωσε το έναυσμα να διατηρηθούν τα δεδομένα που παράγονται στο διαδίκτυο αλλά και αυτά που υποβάλλονται σε επεξεργασία να διατηρηθούν στον κυβερνοχώρο στην τελική τους επεξεργασμένη μορφή. Παράλληλα, να είναι διαθέσιμα στο κοινό υπηρεσίες ή δημόσια δίκτυα που προωθούν την επικοινωνία των χρηστών μέσω της ανταλλαγής μηνυμάτων ή άλλων μέσων. Αυτός ο νόμος τροποποίηση την οδηγία 2002/25/ΕΚ που επικρατούσε μέχρι τότε.

Κατά γενική ομολογία το νομοθετικό πλαίσιο είναι επαρκές στην Ελλάδα, ωστόσο προβλήματα προκύπτουν στην εφαρμογή του. «Το πρόβλημα είναι στην εκτέλεση της απόφασης», εξηγεί στην «Κ» ο διδάκτωρ της Νομικής και διδάσκων Διακυβερνητική στο Πάντειο Πανεπιστήμιο Θέμης Σοφός. Όπως ο ίδιος διευκρινίζει, πολλές εταιρείες, όπως η Google, δεν εδρεύουν στην Ελλάδα και στην καλύτερη των περιπτώσεων έχουν θυγατρικές εταιρείες σε χώρες της Ευρωπαϊκής Ένωσης. «Στην περίπτωση της Google, εκδόθηκε απόφαση από το Ευρωπαϊκό Δικαστήριο με την οποία οφείλει να συμμορφωθεί η θυγατρική της στη Γερμανία, όχι όμως και η μητρική εταιρεία που εδρεύει στην Αμερική», επισημαίνει ο κ. Σοφός. Το θέμα με το Διαδίκτυο είναι ότι δεν υπάρχει γεωγραφικός περιορισμός, με αποτέλεσμα σε πολλές περιπτώσεις να είναι δύσκολη η εφαρμογή των αποφάσεων». Υπέρ της επάρκειας της νομοθεσίας τίθεται και ο νομικός Γιώργος Βουκελάτος. «Το πλαίσιο είναι επαρκές. Το ζήτημα είναι η εφαρμογή του νόμου από τα θεσμικά όργανα καθώς και η ενημέρωση των πολιτών για τα δικαιώματά τους».

Γενικά, το νομοθετικό πλαίσιο θεωρείται επαρκές στην Ελλάδα αλλά αντιμετωπίζει και κάποια προβλήματα όταν φτάνει η ώρα της εφαρμογής του. Όλο το πρόβλημα προκύπτει στην εκτέλεση της όποια απόφασης. Αυτό συμβαίνει γιατί γενικά πολλές εταιρίες δεν έχουν ως έδρα την Ελλάδα και ως έσχατη των περιπτώσεων διατηρούν θυγατρικές σε χώρες της Ευρωπαϊκής Ένωσης. Το διαδίκτυο είναι παγκόσμιο και δεν μπορεί να περιοριστεί με αποτέλεσμα η εφαρμογή των αποφάσεων να γίνεται πολύ δύσκολη υπόθεση. Οπότε το βάρος πέφτει στα θεσμικά όργανα της επιβολής των νόμων αλλά και στην ενημέρωση που πρέπει να έχουν όλοι οι πολίτες σχετικά με τα προσωπικά τους δεδομένα στο διαδίκτυο (Koumentakis,

2017).

2.3.1 Τρόποι προστασίας προσωπικών δεδομένων

Πολλές φορές οι νόμοι παραβιάζονται και τα προσωπικά δεδομένα συλλέγονται, επεξεργάζονται και χρησιμοποιούνται από τρίτα πρόσωπα ή επιχειρήσεις για αυτό και ο ίδιος ο χρήστης πρέπει να διατηρήσει την ανωνυμία του όσο αυτό είναι εφικτό και να λάβει κάποια μέτρα για να προφυλάξει την ιδιωτική του ζωή. Έχουν δημιουργηθεί τεχνολογίες προστασίας για να επιτελέσουν αυτό το σκοπό. Επίσης, κάθε επιχείρηση διαθέτει πολιτική ιδιωτικότητας σχετικά με τα προσωπικά δεδομένα που καταχωρεί κάθε χρήστης (Dampali, 2011).

Οι πολιτικές ιδιωτικότητας αποτελούν κείμενα σχετικά με τη χρήση που θα γίνει στα προσωπικά δεδομένα του κάθε χρήστη (δηλαδή τον τρόπο που θα χρησιμοποιηθούν και τον χρόνο) που αναρτώνται στις ιστοσελίδες των επιχειρήσεων ή των οργανισμών. Ο χρήστης μπορεί να διαλέξει όποια επιχείρηση επιθυμεί με βάση τη πολιτική ιδιωτικότητας της για να γνωρίζει επακριβώς τη διαχείριση που θα γίνει στα προσωπικά του δεδομένα. Οι μεγάλες επιχειρήσεις συνήθως διαθέτουν έγγραφα πολιτικών ιδιωτικότητας ωστόσο οι καταναλωτές σπάνια τα διαβάζουν διότι θεωρούν τα έγγραφα δυσανάγνωστα και δύσκολα (Koumentakis, 2017).

Οι πολιτικές ιδιωτικότητας μπορεί να μεταβληθούν χωρίς ενημέρωση και διαφέρουν σε κάθε ιστοσελίδα και έτσι μένουν αφανείς στους περισσότερους χρήστες (Dampali, 2011).

2.3.2 Τεχνολογίες προστασίας των χρηστών του διαδικτύου

Οι χρήστες του Διαδικτύου που δεν ανησυχούν ιδιαίτερα για τα προσωπικά τους δεδομένα προστατεύουν την ιδιωτικότητα τους μέσω των έλεγχων των δεδομένων που επιλέγουν να γνωστοποιηθούν όπως είναι η διεύθυνση IP τους και οι πληροφορίες μη προσωπικής ταυτοποίησης (Koumentakis, 2017).

Από τη άλλη, οι χρήστες που ανησυχούν για την ιδιωτικότητα τους επιθυμούν καλύτερους μεθόδους προστασίας και επιζητούν τη διαδικτυακή τους ανωνυμία προκειμένου να μην αποκαλυφθούν πληροφορίες σε τρίτους προσωπικής ταυτοποίησης. Επίσης, αρκετές κυβερνητικές οργανώσεις δραστηριοποιούνται έτσι ώστε να προστατέψουν την ιδιωτικότητα των ανθρώπων αλλά και την ανωνυμία τους(Dampali, 2011).

Συμπερασματικά, τα προσωπικά δεδομένα που διανέμονται στο διαδίκτυο πρέπει να εξετάζονται λεπτομερώς από τους χρήστες τους. Μέσα από τη παραβίαση τους, ο χρήστης μπορεί να βρεθεί σε πολύ δυσάρεστη θέση και να κινδυνέψει η ιδιωτική του ζωή. Επειδή με κάθε κίνηση στο διαδίκτυο εκθέτεται και ένα προσωπικό δεδομένο πρέπει ο κάθε άνθρωπος πριν χρησιμοποιήσει τις λειτουργίες που προσφέρει το διαδίκτυο να ενημερωθεί για τα

δικαιώματα του και να λάβει κάποια μέτρα πρόληψης έτσι ώστε να είναι ασφαλής. Όσο, εξελίσσεται η τεχνολογία τόσο αυξάνονται και οι υπηρεσίες που προσφέρει στον άνθρωπο αλλά τόσο ακόμα αυξάνονται τα ηλεκτρονικά εγκλήματα που πραγματοποιούνται μπροστά από την οθόνη του υπολογιστή με τη χρήση του διαδικτύου.

ΚΕΦΑΛΑΙΟ 3^{ο} - ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

3.1 Ορισμός ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό έγκλημα έχει οριστεί από το Forester και Morrison τη δεκαετία του 90 ως «μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως κυριότερο μέσο τέλεσης της». Πρόκειται ουσιαστικά για τα ίδια εγκλήματα που συναντά κανείς στη καθημερινότητα του απλώς σε αυτή τη περίπτωση τελούνται μέσω ενός υπολογιστή. Στην Ελλάδα, τον συναντάμε συχνά με τους όρους έγκλημα του κυβερνοχώρου και διαδικτυακό έγκλημα (Ψαρά, 2016).

Όπως αποκαλύπτουν και οι ίδιες οι λέξεις, για να τελεστεί ένα ηλεκτρονικό έγκλημα είναι απαραίτητη η ύπαρξη ενός υπολογιστή. Ο υπολογιστής μπορεί να αποτελέσει τρείς ρόλους στο ηλεκτρονικό έγκλημα, είτε να είναι ένα βοηθητικό μέσο, είτε να είναι το ίδιο το μέσο της ηλεκτρονικής επίθεσης, είτε να θεωρηθεί το «θύμα» της επίθεσης (Γιαγκουδάκης, 2013).

Ο νομοθέτης γενικά αποφεύγει να δώσει ένα ορισμό στο ηλεκτρονικό έγκλημα εξαιτίας της πολυμορφίας του και συνήθως αναθέτει αυτή την αρμοδιότητα στα δικαστήρια και τους νόμους που το περικλείουν ή δανείζεται όρους από τη τεχνολογία (Γκαρτζώνη, 2017).

Κατηγοριοποίηση του Ηλεκτρονικού εγκλήματος:

- Σε εγκλήματα που ο ηλεκτρονικός υπολογιστής αποτελεί το μέσο για τη διάπραξη του και γίνεται στο περιβάλλον του ή σε άλλο συμβατικό. Ένα παράδειγμα αποτελεί η εξύβριση και η παραπλάνηση ενός ατόμου από μια ιστοσελίδα.
- Σε εγκλήματα που διαπράττονται δίχως να κάνουν χρήση του διαδικτύου όπως είναι η αντιγραφή κάποιου ξένου λογισμικού δίχως την άδεια του δημιουργού του.
- Σε εγκλήματα που το διαδίκτυο κατέχει απαραίτητο ρόλο, όπως η περίπτωση της εξάπλωσης των ιών.

Κάθε μέρα όλο και περισσότερο αυξάνεται η χρήση του διαδικτύου και ταυτόχρονα εκείνων

που θέλουν να εκμεταλλευτούν αυτή τη χρήση προς δικό τους όφελος. Αυτό αποτελεί το ηλεκτρονικό έγκλημα όπου ο δράστης μπορεί να βρίσκεται στην άλλη άκρη της γης και να το τελεί απλά μέσω ενός δικτυωμένου υπολογιστή. Μια τέτοια εισβολή δεν αποτελεί δύσκολη υπόθεση εφόσον στο διαδίκτυο είναι διαθέσιμες εφαρμογές λογισμικού, που μπορεί ο καθένας να χρησιμοποιήσει αφού δεν απαιτεί εξειδικευμένη γνώση, που παραχωρούν εύκολα στους εισβολείς τη δυνατότητα διάπραξης ενός ηλεκτρονικού εγκλήματος. Οι εισβολείς αυτοί, που ονομάζονται και hackers, σαμποτάρουν τα συστήματα με την εισβολή τους σε αυτά και σε άλλα δίκτυα οι οποίοι πολλές φορές ελευθερώνουν ιούς στο χώρο τους και τα καταστρέφουν. Σε σχέση με το συμβατικό περιβάλλον, στο περιβάλλον ηλεκτρονικών υπολογιστών διαπράττονται πιο εύκολα τα εγκλήματα (Γιαγκουδάκης, 2013).

Μια επανάσταση της εποχής αποτελεί η επικοινωνία, μέσω του διαδικτύου, μεταξύ ατόμων που βρίσκονται σε κάθε γωνιά του πλανήτη και επικοινωνούν μεταξύ τους μέσω ομάδων ειδήσεων ή μέσω ηλεκτρονικού ταχυδρομείου ή μέσω δωματίων συζητήσεων σε πραγματικό χρόνο. Αποτελούν αυτοί οι δίαυλοι επικοινωνίας έναν εύκολο και ανέξοδο τρόπο να επικοινωνήσουν πολλά άτομα μεταξύ τους ταυτόχρονα που μέσω του τηλεφώνου για παράδειγμα δεν θα ήταν εφικτό. Μέσω αυτών των ομάδων συζητήσεων πολλοί δράστες βρίσκουν την ευκαιρία να ψαρέψουν τα υποψήφια θύματα τους. Η πιο συχνή επίθεση αποτελεί το spam που είναι η ανεπιθύμητη αλληλογραφία αλλά και σε πιο σοβαρές καταστάσεις η αιμοφιλία και η παιδική πορνογραφία (Αυγουστάκη, 2010).

Το μόνο που χρειάζεται για να διαπραχτεί ένα ηλεκτρονικό έγκλημα είναι να υπάρχει ένας συνδεδεμένος στο διαδίκτυο ένας ηλεκτρονικός υπολογιστής σε όποιο μέρος του πλανήτη και αν είναι αυτός. Επομένως, ο ρόλος των αρμόδιων αρχών για αυτά τα εγκλήματα καθιστάτε πολύ δύσκολος αφού είναι σχεδόν αδύνατο να εντοπίσουν το τόπο που τέλεσε το έγκλημα ο δράστης αλλά και το πότε ειδικά αν έχει προνοήσει να διαγράψει τα ηλεκτρονικά του ίχνη. Για αυτό και οι αρμόδιες αρχές δίωξης πρέπει να ενημερώνονται και να εκπαιδεύονται συνεχώς στις νέες τεχνολογίες που εμφανίζονται (ΜΠΟΛΑΡΗ, 2017).

3.2 Κυβερνοέγκλημα

Το Κυβερνοέγκλημα ορίστηκε από τον Donn Parker ως το έγκλημα στο οποίο αυτός που το διαπράττει έχει συγκεκριμένες και σαφείς γνώσεις γύρω από το κυβερνοχώρο. Το κυβερνοέγκλημα μπήκε στο στόχαστρο της Εξεταστικής Επιτροπής της Μεγάλης Βρετανίας και την απασχόλησε από της απαρχές της δημιουργίας της(τη δεκαετία του ΄80). Άρχισε, λοιπόν, να κάνει έρευνες σχετικά με την έκταση που έχει πάρει το έγκλημα στον ιδιωτικό και στο δημόσιο τομέα μέσω της χρήσης του ηλεκτρονικού υπολογιστή. Η έρευνα φανέρωσε ότι όσο περνούσαν τα χρόνια όλο και αυξάνονταν τα ποσοστά των εγκλημάτων. Οι μελέτες που έγιναν το 1981 έδειξαν ότι τα μόνα εγκλήματα που διώκονταν, επειδή για αυτά γίνονταν κατηγορίες, ήταν η κλοπή και η απάτη ενώ το 1998 και τη προσθήκη και άλλων εγκλημάτων όπως η κλοπή δεδομένων λογισμικού και η παράνομη χρήση τους, η κακή χρήση προσωπικών δεδομένων, η διάχυση ιών σε ένα πρόγραμμα, η πορνογραφία κ.α. το ποσοστό

υπετετραπλασιάστικε (Γιαγκουδάκης, 2013).

Στα εγκλήματα που ο υπολογιστής έχει βοηθητικό ρόλο μπορούν να διαπραχθούν και δίχως αυτόν ενώ στα εγκλήματα που κατέχει πρωταγωνιστικό ρόλο, το έγκλημα αποτελεί κύριο αποτέλεσμα της τεχνολογίας των υπολογιστών χωρίς να εμφανίζεται ταυτόχρονα και σε άλλους τομείς. Σε αυτή τη περίπτωση εμφανίζονται και οι περιπτώσεις hacking και ιών. Βέβαια, στη πρώτη περίπτωση που ο υπολογιστής έχει βοηθητικό ρόλο πρέπει να σημειωθεί ότι είναι το ίδιο σοβαρή με τα δεύτερη, απλά στην δεύτερη κατηγορία εμφανίζονται οι κυβερνοεγκληματίες οι οποίοι επικεντρώνονται στις τεχνολογίες όπου είναι διάχυτες οι πληροφορίες (Γιαγκουδάκης, 2013).

Όταν γίνεται χρήση παράνομου υλικού, που συνήθως συσχετίζονται με ζητήματα που έχουν να κάνουν με την πνευματική ιδιοκτησία, αποτελεί και αυτό έγκλημα εφόσον είναι απαραίτητη η ύπαρξη του υπολογιστή, άρα ανήκει στη δεύτερη κατηγορία εγκλήματος (Γκαρτζώνη, 2017).

3.3 Ηλεκτρονικοί εγκληματίες

Στην ανάπτυξη της τεχνολογίας, όσοι προσπάθησαν να την εκμεταλλευτούν κατηγοριοποιήθηκαν ως εξωτερικοί και εσωτερικοί δράστες το 1980 από το James Anderson (Ψαρά, 2016).

Α) Ως εξωτερικοί δράστες αναφέρονται τα πρόσωπα τα οποία εισχωρούν στο σύστημα χωρίς να έχουν κάποια εξουσιοδότηση δηλαδή είναι άτομα που προέρχονται από τον εξωτερικό χώρο. Είναι αλλιώς γνωστοί με την ονομασία hacker που είναι παράνομοι στο όλο το ηλεκτρονικό σύστημα. Οι στόχοι τους συνήθως έχουν οικονομικό όφελος για αυτό και στοχεύουν συστήματα που φυλάσσουν εμπιστευτικές πληροφορίες.

Β) Ως εσωτερικοί δράστες αναφέρονται οι χρήστες που έχουν εξουσιοδότηση στο σύστημα αλλά εισχωρούν σε πληροφορίες και δεδομένα που δεν τους ανήκουν. Οι χρήστες αυτοί διαχωρίζονται σε αυτούς που εισχωρούν σε ξένα αρχεία παράνομα για να εξετάσουν το περιεχόμενο τους (ονομάζονται ως κρυφοί χρήστες), αυτούς που κλέβουν τη ταυτότητα κάποιου άλλου χρήστη για να εισχωρήσουν στα συστήματα (ονομάζονται ως μεταμφιεσμένοι) και τέλος αυτούς που εκμεταλλεύονται τα προνόμια που έχουν στο σύστημα, δηλαδή της χρήσης του και των πηγών της, και αποκαλούνται ως έκπτωτοι (Γκαρτζώνη, 2017).

3.3.1 Εξωτερικές απειλές-hackers

Όταν αναφερόμαστε στη λέξη hacker ουσιαστικά μιλάμε για έναν εισβολέα στο διαδίκτυο

που έχει ειδικές γνώσεις πάνω σε αυτόν και εκμαιεύεται πληροφορίες τρίτων για μελλοντική τους χρήση. Η ετυμολογία προέρχεται από το τον όρο «hack writer» και εννοεί εκείνον που έχει πλήρη έλεγχο του κειμένου πριν αυτό ολοκληρωθεί (Barlow, 1990). Ο χαρακτηρισμός αυτός άρχισε αργότερα να υποδηλώνει αυτούς που γνωρίζει άριστα τους υπολογιστές αλλά και όσους μπορούσαν να διαχειριστούν πολύπλοκα συστήματα (δεκαετία ’60 και ’70). Σκοπός τους είναι να πάρουν στοιχεία από το διαδίκτυο που τους ενδιαφέρουν και όχι η πρόκληση βλάβης στα άτομα που κλέβουν τις πληροφορίες. Είναι βέβαια ευνόητο ότι κάποιοι από αυτούς θα κρατάνε τα στοιχεία που συλλέγουν για προσωπικό τους όφελος και αυτοί είναι που ονομάζονται crackers. Εκτός από αυτούς στο διαδίκτυο συναντάει κανείς και τους hactivists οι οποίοι διαχέουν κακόβουλο υλικό, στέλνουν πολλά μαζικά μηνύματα στο ηλεκτρονικό ταχυδρομείου κάποιου χρήστη κ.τ.λ. Επίσης, υπάρχουν οι vandals οι λειτουργούν παραπλανώντας τους χρήστες στους δικτυακούς τόπους αλλάζοντας τις αληθινές πληροφορίες σε ψεύτικες με αποτέλεσμα να πλήξουν την αξιοπιστία τους. Τέλος, από τους χειρότερους εγκληματίες στον κυβερνοχώρο θεωρούνται οι cyberterrorists οι οποίοι πραγματοποιούν τρομοκρατικές επιθέσεις με τη χρήση του διαδικτύου. Όπλο των τρομοκρατικών επιθέσεων αποτελούν οι διασυνδεμένοι ηλεκτρονικοί υπολογιστές και έτσι η όλη ενέργεια ονομάζεται ως cyber terrorism (Ψαρά, 2016).

Οι δράστες που μπαίνουν στη διαδικασία της παρανομίας μόνο και μόνο από περιέργεια αποκαλούνται ερασιτέχνες και συνήθως χρησιμοποιούν έτοιμα εργαλεία περιμένοντας κάποια ευκαιρία για να εισβάλλουν σε ένα υπολογιστικό σύστημα (Γιαγκουδάκης, 2013).

Αντιθέτως, αυτοί γνωρίζουν άριστα το χειρισμό των υπολογιστών, του προγραμματισμού και του διαδικτύου ολόκληρου αποκαλούνται ως επαγγελματίες εισβολείς και διαπράττουν σοβαρά εγκλήματα όπως είναι η κατασκοπεία (ΜΠΟΛΑΡΗ, 2017).

Οι hackers, γενικά, θεωρούν ότι δεν είναι εγκληματίες για αυτό και διαφοροποιούν τη θέση τους από αυτών των crackers. Ωστόσο, είναι δύσκολο να θεωρηθεί αυτό λογικό αφού διεισδύουν καθημερινά σε μη εξουσιοδοτημένες πληροφορίες και είναι οι ίδιοι που δημιουργούν κακόβουλο λογισμικό. Φυσικά, όπως σε κάθε κοινωνία έτσι και στην κοινωνία του hacking κυριαρχούν κάποιοι κανόνες σχετικά με τη κουλτούρα τους όπως είναι το casual ντύσιμο και τα μακριά γένια και μαλλιά (οι πλειοψηφία είναι άντρες). Προσάπτουν ιδιαίτερη προσοχή και ενδιαφέρον στα έργα τέχνης, τα βιβλία, τα παιχνίδια ευφυΐας και επειδή ασχολούνται συνήθως με προγράμματα προγραμματισμού χρησιμοποιούν την αγγλική γλώσσα (Lawspot.gr , 2014).

Εικόνα 10: Hacker

Πηγή: https://hacked.com/coincheck-halts-withdrawals/

3.3.2 Εσωτερικές απειλές

Το βασικότερο κίνδυνο για έναν οργανισμό αποτελούν οι εσωτερικές απειλές. Σύμφωνα με έρευνες που έχουν διεξαχθεί, το 75% των επιθέσεων προέρχεται από άτομα με διευθυντικές θέσεις και από υπαλλήλους εταιριών και αυτό γιατί κατέχουν κωδικούς πρόσβασης σε συστήματα και είναι ενήμεροι για καθετί λεπτομέρεια σχετικά με την ασφάλεια τους (Ψαρά, 2016).

Από το 1990 και μετά, κατατέθηκαν όλο και περισσότερα περιστατικά προσβολής από ιούς σε συστήματα διότι οι hackers άρχισαν να έχουν ελάχιστα τεχνολογικά εμπόδια και σήμερα έχουν αυτοματοποιημένη βοήθεια από πολλά εργαλεία. Ετησίως μελέτες πραγματοποιούνταν από το 1996 από το Ίδρυμα Ασφάλειας Υπολογιστών(CSI) στις ΗΠΑ για να παρουσιάσουν και να γνωστοποιήσουν στο κοινό την έκταση του προβλήματος. Το 1996, τα στοιχεία έδειξαν αύξηση του προβλήματος και ιδιαίτερα σε οργανισμούς σχετικά με την παράνομη χρήση των συστημάτων του διαδικτύου που ανερχόταν σε 42% με κατακόρυφη έξαρση το 2000 που έφτασε το 70% (Lawspot.gr , 2014).

Στα πρώτα χρόνια τα ηλεκτρονικά εγκλήματα περιορίζονταν στην κλοπή και την απάτη ενώ αργότερα, με τη διάδοση του διαδικτύου, παρουσιάζονταν και άλλα εγκλήματα όπως είναι οι ιοί αλλά και μορφές παρενόχλησης . Τα εγκλήματα έχουν εξελιχθεί σε διάφορες μορφές που πλέον αποτελούν τον ίδιο το στόχο και όχι απλά ένα μέσο. Η φράση «οι υπολογιστές είναι το μέλλον του εγκλήματος…» που ειπώθηκε από τον Clive Blake αποτυπώνει την έννοια του ηλεκτρονικού εγκλήματος (Γιαγκουδάκης, 2013).

3.4 Μορφές ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό έγκλημα για να γίνει σαφές θα πρέπει να αρχικά να οριστεί σε δυο

κατηγορίες. Στην πρώτη κατηγορία κατατάσσονται τα γνήσια ηλεκτρονικά εγκλήματα που εμφανίστηκαν παράλληλα με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο και στη δεύτερη κατηγορία κατατάσσονται στα εγκλήματα με τη χρήση του υπολογιστή που προϋπήρχαν δηλαδή πριν εμφανιστούν οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο αλλά με την άφιξη τους συντέλεσαν στην ανάπτυξη τους (ΜΠΟΛΑΡΗ, 2017).

3.4.1 Γνήσια ηλεκτρονικά εγκλήματα

Στα γνήσια ηλεκτρονικά εγκλήματα συμπεριλαμβάνονται το hacking(κακόβουλη εισβολή), το spamming(ανεπιθύμητη αλληλογραφία), το phishing(ψάρεμα), η πειρατεία ονομάτων χώρου, η πειρατεία λογισμικού, το κακόβουλο λογισμικό, οι επιθέσεις σε δικτυακούς τόπους και οι επιθέσεις άρνησης εξυπηρέτησης (Γκαρτζώνη, 2017).

-Στον 21^{ο} αιώνα το πιο διαδεδομένο διαδικτυακό έγκλημα είναι το hacking. Σκοπός τους είναι να εισβάλουν σε ηλεκτρονικά συστήματα ή γενικά σε υπολογιστές , αποκτώντας πλήρης γνώση της ασφάλειας τους και ανακαλύπτοντας της αδυναμίες τους έτσι ώστε να μπορούν να επιτεθούν πιο εύκολα. Ο εισβολέας μπορεί να επιχειρήσει και να καταφέρει τη πλήρη διείσδυση στα δικαιώματα του συστήματος και στη διαχείριση του και με αυτό τον τρόπο να προκαλέσει σοβαρές επιπτώσεις ή να διεισδύσει σε δικαιώματα που έχει ένας απλός χρήστης του συστήματος (Ψαρά, 2016).

Μια συνήθης τεχνική hacking αποτελούν τα cookies που είναι μικρά αρχεία που αποθηκεύονται στον υπολογιστή αυτόματα από τις ιστοσελίδες που έχει επισκεφτεί ο χρήστης για να τον θυμούνται αν τις ξαναεπισκεφτεί. Αυτά τα αρχεία αποθηκεύουν οπότε κάποια προσωπικά στοιχεία του χρήστη που αν ένας hacker αποκτήσει πρόσβαση μπορεί να ανακαλύψει προσωπικά στοιχεία όπως είναι το όνομα χρήστη, οι κωδικοί πρόσβασης κ.α. (Γκαρτζώνη, 2017).

Μια άλλη τεχνική hacking είναι η ανίχνευση δικτυακών υπηρεσιών συστημάτων όπου οι εισβολείς στέλνουν ερωτήσεις τους διακομιστές του συστήματος για να συλλέξουν πληροφορίες σχετικά με την ασφάλεια και τις υπηρεσίες του συστήματος έτσι ώστε να εισβάλουν στο σύστημα εύκολα και μεθοδικά (Γιαννακοπούλου, 2017).

Επίσης υπάρχουν οι ανιχνευτές δικτυακών πακέτων που λειτουργούν μέσω των packet sniffers, που είναι εφαρμογές λογισμικού, και εντοπίζουν όλα τα πακέτα του διαδικτύου. Αν τα πακέτα αυτά δεν είναι κρυπτογραφημένα τότε ο hacker μπορεί να ανακτήσει προσωπικές πληροφορίες (Γκαρτζώνη, 2017).

Ακόμα, οι hackers δρουν μέσω πλαστών διευθύνσεων για να εισέλθουν σε δικτυακές υπηρεσίες. Οι hackers, δηλαδή, τροποποιούν επικεφαλίδες πακέτων έτσι ώστε να δίνουν την εντύπωση ότι προέρχονται από μια νόμιμη πηγή (Γιαννακοπούλου, 2017).

Οι πλοηγοί ιστού(web browser) έχουν συχνά πρόβλημα με την ασφάλεια που παρέχουν για

αυτό και οι hackers χρησιμοποιούν την τεχνική της επίθεσης σε επίπεδο εφαρμογής σε δικτυακές εφαρμογές.

-Οι επιθέσεις άρνησης εξυπηρέτησης γίνονται ώστε να εξαντλήσουν τους πόρους ενός υπολογιστικού συστήματος για να μη μπορεί ούτε να μεταδίδει δεδομένα σε κάποιο δίκτυο ούτε να συνδέεται με υπηρεσίες, ούτε να προσφέρει άριστη ποιότητα στο χρήστη. Οι πιο σημαντικές τεχνικές επιθέσεων άρνησης εξυπηρέτησης είναι οι Ping of death, Fragmentation, SYN Flood Attacks (Γκαρτζώνη, 2017).

-Πολύ συχνά χρησιμοποιείται στο διαδίκτυο από έναν εγκληματία το κακόβουλο λογισμικό που αποσκοπεί στην πρόκληση ζημιάς σε έναν ηλεκτρονικό υπολογιστή με τη διαγραφή ή υποκλοπή δεδομένων, την αλλοίωση προγραμμάτων, τη δυσλειτουργία ενός συστήματος. Ο κακόβουλος κώδικας διακρίνεται σε σκουλήκια, δούρειους ίππους και ιούς (Ψαρά, 2016).

-Τον όρο spam τον ακούει κανείς πλέον συχνά αφού συνεχώς κατακλύζει τους χρήστες του διαδικτύου με μαζικά μηνύματα, που αφορούν συνήθως διαφημιστικά σχετικά με τη προώθηση υπηρεσιών ή προϊόντων. Οι spammers συνήθως συλλέγουν διευθύνσεις από καταλόγους εταιριών που τους ανήκουν ηλεκτρονικά καταστήματα ή “τρέχουν” το harvester, που είναι ένα λογισμικό σάρωσης διευθύνσεων από όλο το διαδίκτυο. Αυτή η εφαρμογή αποτελεί μια ευκαιρία για επιθέσεις για τους εγκληματίες του διαδικτύου (Γιαγκουδάκης, 2013).

-Οι επιθέσεις σε διαδικτυακούς τόπους συνήθως έχουν στο στόχαστρο κυβερνητικές υπηρεσίες και οργανισμούς και γίνεται επίθεση στο περιεχόμενο της ιστοσελίδας τους, το οποίο παραποιούν. Η παραποίηση αυτή μπορεί να διορθωθεί όταν εντοπιστεί αλλά ανάλογα με το μέγεθος της, αν είναι δηλαδή σε μεγάλο βαθμό, ο δικτυακός τόπος θα χρειαστεί να μείνει κλειστός για λίγες ώρες ώσπου να διορθωθεί το πρόβλημα (Γιαννακοπούλου, 2017).

-Μια “γνήσια” επίθεση, ειδικά στις απαρχές λειτουργίας του διαδικτύου, ήταν η πειρατεία ονομάτων χώρου όπου διάφοροι επιτήδειοι έπαιρναν διευθύνσεις στο διαδίκτυο πριν προλάβουν να κατοχυρωθούν από τις ενδιαφερόμενες εταιρίες και ύστερα τις πουλούσαν σε αυτές έναντι μεγάλης χρηματικής αμοιβής είτε βασιζόμενοι στο όνομα μιας εταιρίας έκαναν προσβλητικές αναρτήσεις (Γιαγκουδάκης, 2013).

-Το phishing είναι μια από τις πιο επικίνδυνες τεχνικές εξαπάτησης διότι στοχεύει τα προσωπικά δεδομένα των καταναλωτών ενός οργανισμού ώστε αργότερα να τα καταχραστεί και να εκβιάσει τους κατόχους τους για προσωπικό κερδοσκοπικό σκοπό. Με τη χρήση διαφόρων μεθόδων, όπως το spam, οι phishers εμφανίζονται στα επιλεγμένα θύματα τους ως εκπρόσωποι κάποιου γνωστού οργανισμού για να τους πείσουν να εισάγουν στο σύστημα προσωπικά δεδομένα τους έτσι ώστε να καταχραστούν τα περιουσιακά τους στοιχεία. Για παράδειγμα, το θύμα μέσω ένα παραπλανητικού e-mail, που θα προέρχεται από μια τραπεζική υπηρεσία ,θα του ζητηθεί να επιβεβαιώσει τους κωδικούς τραπέζης τους λόγω μιας συντήρησης που πραγματοποιούν και έτσι θα αποκαλύψει προσωπικά του στοιχεία στους δράστες που θα φροντίσουν να τα καταχραστούν. Ο phisher φροντίζει με μια σειρά από ψεύτικες πληροφορίες να καθησυχάσει το θύμα για την εγκυρότητα της υπηρεσίας του και

ότι είναι άξιος εμπιστοσύνης έτσι ώστε να μπορεί να αλιεύσει όσες περισσότερες πληροφορίες μπορεί για να διευκολύνει τη δουλειά του. Στην επικοινωνία που γίνεται κατά το phishing χρησιμοποιούνται είτε τα εργαλεία στιγμιαίας επικοινωνίας, είτε από παραβιασμένους διακοσμητές, είτε με το ηλεκτρονικό ταχυδρομείο, είτε με τηλεφωνική επικοινωνία, είτε με τη χρήση ψεύτικων διαδικτυακών (Rouse, 2017).

-Η πειρατεία λογισμικού είναι ουσιαστικά ότι λένε και οι όροι της, δηλαδή η κατάχρηση προγραμμάτων λογισμικού και η μετέπειτα διακίνηση και αναπαραγωγή τους για προσωπικό όφελος. Οι εταιρίες επειδή πλήττονται καθημερινά από αυτή τη πειρατεία εφαρμόζουν τεχνολογικά μέτρα για να την αποτρέψουν όμως με την εξέλιξη που έχουν πάρει οι hackers μπορούν εύκολα να τα παραμερίσουν αυτά τα μέτρα και να αντιγράψουν το λογισμικό (Γιαγκουδάκης, 2013).

3.4.2 Εγκλήματα με τη χρήση υπολογιστή

Σε μια δεύτερη κατηγορία του ηλεκτρονικού εγκλήματος μπορούν να ενταχθούν τα εγκλήματα τα όποια γίνονται με τη χρήση ηλεκτρονικού υπολογιστή, αν και προϋπήρχαν πριν αυτών. Ο υπολογιστής βοηθάει στη διάδοση πληροφοριών που δεν είναι έγκυρες και οδηγούν στην παραπληροφόρηση όπως και στην εύρεση πληροφοριών που συνάπτουν με παράνομες ενέργειες. Επίσης, μέσω του υπολογιστή μπορεί ένας χρήστης να αποθηκεύσει προσωπικά δεδομένα κάποιου άλλου χρήστη χωρίς την έγκριση του. Ακόμα, μέσω του διαδικτύου ένας χρήστης υπολογιστή μπορεί να κάνει παράνομες ηλεκτρονικές αγορές με μια κλοπιμαία πιστωτική κάρτα αλλά και να διαδώσει παράνομο υλικό όπως για παράδειγμα είναι η πορνογραφία (Ψαρά, 2016).

3.5 Η απάτη στο διαδίκτυο

Σίγουρα το διαδίκτυο έχει γίνει ένας βασικός παράγοντας για τη διάπραξη ηλεκτρονικών εγκλημάτων που πολλές φορές στοχεύουν στην απόσπαση μεγάλων χρηματικών αμοιβών από τα θύματα του. Ένας εύκολος τρόπος είναι μέσω της αποστολής e-mail. Για παράδειγμα, ένας εγκληματίας αρχίζει να στέλνει πολλά e-mails ταυτόχρονα προς τα θύματα του για να τους παραπλανήσει και με έξυπνο τρόπο να πετύχει το στόχο του. Αρχίζει , λοιπόν, να λέει μέσω του e-mail ότι είναι από την Αφρική και θέλει να μετακινηθεί, λόγο πολέμου, καταστροφών, άθλιων συνθηκών κ.α., προς τη χώρα του θύματος ζητώντας του να ανοίξει ένα τραπεζικό λογαριασμό στο οποίο θα καταθέσει ένα χρηματικό ποσό και θα ναι συνδικαιούχος και μόλις τελειώσει η περιπέτεια του θα τον ανταμείψει. Σκοπός του εννοείται ότι είναι να κλέψει το χρηματικό ποσό και ύστερα να καταστρέψει το λογαριασμό (Lawspot.gr , 2014).

Ένα άλλο παράδειγμα είναι η απάτη με το ΛΟΤΤΟ στην Ισπανία. Κάτοικοι της Ισπανίας με

αφρικανική καταγωγή, στέλνουν e-mail στα θύματα τους ότι τάχα κέρδισε το ΛΟΤΤΟ και του ζητούν τον αριθμό τραπέζης του και κάποια άλλα προσωπικά στοιχεία ώστε να του καταθέσουν, και καλά, το κερδισμένο ποσό αλλά του ζητούν και του θύματος να στείλει κάποια χρήματα σε αυτούς για τα διαδικαστικά έξοδα. Βέβαια, το μόνο που έχουν οι δράστες σκοπό είναι να εντοπίσουν το τραπεζικό λογαριασμό του θύματος και να του αποσπάσουν όλο το ποσό.

Με την εξάπλωση του ηλεκτρονικού εμπορίου όλο και περισσότερα εγκλήματα διαδραματίζονται με τη χρήση πιστωτικής κάρτας αφού οι χρήστες τη χρησιμοποιούν για κάθε ηλεκτρονική εμπορική συναλλαγή. Έτσι στο διαδίκτυο συσπειρώνονται πολλοί αριθμοί τραπεζικών λογαριασμών που γίνονται εύκολα προσβάσιμοι με την τεχνολογία «web sniffer» που παρακολουθεί όποια μετάδοση δεδομένων γίνεται (Γιαγκουδάκης, 2013).

-Ένα πολύ σοβαρό έγκλημα είναι η κλοπή ταυτότητας ιδιαίτερα όταν αυτό γίνεται διαδικτυακά παίρνει πιο επικίνδυνες διαστάσεις. Αρχικά ο εγκληματίας προσπαθεί να συγκεντρώσει όσο πιο πολλές πληροφορίες μπορεί από το επιλεγμένο θύμα του είτε έμμεσα χακάροντας προσωπικά του δεδομένα είτε άμεσα κλέβοντας τη τσάντα του για να ανακτήσει στοιχεία της ταυτότητας του ή την αλληλογραφία του ακόμα. Με τις πληροφορίες που έχει συγκεντρώσει αρχίζει να δημιουργεί τραπεζικούς λογαριασμούς, πλαστή ταυτότητα, πιστωτικές κάρτες με το πρόσωπο του θύματος (Lawspot.gr , 2014).

-Στο διαδίκτυο από παράνομες συναλλαγές έρχεται και παράνομο χρήματα που οι κάτοχοι του για να τα αποκρύψουν κάνουν ξέπλυμα χρήματος. Το χρήμα κρύβεται από τη παράνομη πηγή με τη μεταφορά του σε άλλες οικονομικές συναλλαγές έτσι ώστε να διασπαστεί το ποσό και στο τέλος εμφανίζεται με διάφορες διαδικασίες σε νόμιμο εισόδημα. Στο διαδίκτυο επικρατεί ο νόμος της ανωνυμίας του πελάτη οπότε και να εντοπιστεί η παράνομη συναλλαγή είναι δύσκολο να εντοπιστούν οι κάτοχοι του (Ψαρά, 2016).

-Η πορνογραφία και η διακίνηση του υλικού της προϋπήρχε πολύ πιο πριν το διαδίκτυο, απλά εξαπλώθηκε ραγδαία με την έλευση του. Όσο και αν καταβάλλεται να εντοπιστεί η πηγή της διακίνησης παραμένει ακόμα και σήμερα πολύ δύσκολο αφού έχουν δημιουργηθεί πολλοί ψεύτικοι λογαριασμοί για τη κάλυψη του. Το υλικό αυτό συγκεντρώνεται πολλές φορές από ανυποψίαστα θύματα που ενώ νομίζουν ότι στέλνουν ακατάλληλο υλικό στο σύντροφο τους, στη πραγματικότητα το στέλνουν σε ένα άγνωστο άτομο. Το πορνογραφικό υλικό κυμαίνεται από φωτογραφίες μέχρι βίντεο που πλέον ανακτώνται πολύ εύκολα από οποιοδήποτε κάτοχο διαδικτύου. Η πιο ανήσυχη περίπτωση αποτελεί η παιδική πορνογραφία που ανακτώνται από νεαρά αφελή θύματα που εμπιστεύονται πολλοί εύκολα αγνώστους και στο τέλος μπλέκονται στα δίκτυα τους και απειλούνται δίχως να μπορούν να γλιτώσουν. Δύσκολα αυτοί οι εγκληματίες εντοπίζονται και πιάνονται από τις αρχές εφόσον δρουν πίσω από την οθόνη ενός υπολογιστή (Ψαρά, 2016).

-Όπως ανακαλύπτει και το ίδιο το όνομα, δικτυακή τρομοκρατία είναι η τρομοκρατία που γίνεται με εργαλείο το διαδίκτυο. Δυστυχώς έχει πολύ τραγικά αποτελέσματα αφού βοηθάει στη μαζική επικοινωνία των δραστών και την οργάνωση επιθέσεων που μπορεί να γίνουν ταυτόχρονα σε πολλά μέρη της γης. Η επικοινωνία αυτή, πέρα του ότι είναι ανέξοδη, είναι

και δύσκολη να εντοπιστεί από τις αρμόδιες αρχές. Η Κυβερνο-τρομοκρατία ορίζεται από το FBI ως μια καλά προσχεδιασμένη επίθεση κατά των ηλεκτρονικών δεδομένων και προγραμμάτων που έχει πολιτικούς σκοπούς και αποτελείται από μυστικούς πράκτορες και υπερεθνικές ομάδες που ασκούν εν τέλει βία σε άμαχο στόχο (Ψαρά, 2016).

-Η παρενόχληση υπάρχει στη καθημερινότητα ενός ατόμου και σε λεκτική και σε πρακτική μορφή. Το δίκτυο όμως την διευκόλυνε και την έκανε απρόσωπη μέσω των e-mail. Το θύμα παρενοχλείτε είτε άμεσα με την αποστολή προσβλητικού ή απειλητικού μηνύματος απευθείας σε αυτό είτε έμμεσα με το προσβλητικό ή το απειλητικό μήνυμα να προέρχεται από διαφορετικούς λογαριασμούς (ΜΠΟΛΑΡΗ, 2017).

-Μορφή ηλεκτρονικού εγκλήματος μπορεί να θεωρηθούν και τα κινητά τηλέφωνα τα οποία περιέχουν πολλά προσωπικά δεδομένα. Τα κινητά τηλέφωνα μπορούν να ελεγχθούν από απόσταση μέσω ενός bluetooth ή αν έχουν ενεργοποιήσει το hot-spot άρα μπορεί να ανακτηθούν δεδομένα τους από μακριά. Έτσι, κλήσεις στο εξωτερικό μπορεί να πραγματοποιηθεί και να επιφέρει τεράστιες χρεώσεις στο θέμα ή μέσω του hot-spot κάποιος να μπει στο λογισμικό του κινητού του θύματος κα να ανακτήσει ότι δεδομένα επιθυμεί(φωτογραφίες, κωδικοί ηλεκτρονικών υπηρεσιών κ.τ.λ.) (Lawspot.gr , 2014).

Τα ηλεκτρονικά παιχνίδια μπορούν να αποτελέσουν άλλο ένα μέσο ηλεκτρονικού εγκλήματος αφού απαιτούν ειδικά προγράμματα και ασύρματη σύνδεση που αν γίνουν θύμα hacking μπορούν να επιτρέψουν τη διαχείριση του υπολογιστή από απόσταση (Ψαρά, 2016).

Τέλος, ακόμα και ένα μέσο που θεωρείτε έμπιστο στη καθημερινότητα μπορεί να συντελέσει σε ηλεκτρονικό έγκλημα και αυτό είναι το ΑΤΜ. Οι δράστες τοποθετούν μικρές κάμερες για να κλέβουν τους κωδικούς από τις κάρτες ή δημιουργούν μηχανισμούς που μπλοκάρουν και κρατούν τις κάρτες ή τοποθετούν περίπου ίδια πληκτρολόγια πάνω από τα κανονικά για να βρουν τους αριθμούς των κωδικών (Γκαρτζώνη, 2017).

3.6 Ασφάλεια στο διαδίκτυο και ηλεκτρονικό έγκλημα

Το διαδίκτυο είναι πλέον ένα κομμάτι του πολιτισμού των ανθρώπων που καταφεύγουν καθημερινά σε αυτόν για κάθε είδους βοήθεια που χρειάζονται και αυτό γεννά το ερώτημα πόσο ασφαλής είναι η περιήγηση στο διαδίκτυο. Αρχικά, ο όρος ασφάλεια στο διαδίκτυο σχετίζεται με τη δυνατότητα του κάθε ξεχωριστά οργανισμού να προστατεύει τις πληροφορίες τους από τις απειλές που καταδιώκουν συνεχώς στο κυβερνοχώρο. Η ασφάλεια των συστημάτων μπορεί να ρυθμιστεί με τη πρόληψη αποφυγής ξένων ενεργειών από το σύστημα, με την ανίχνευση κάθε απειλής και επίθεσης και με την άμεση αντίδραση του συστήματος για αποκατάσταση της ζημιάς. Αυτά τα τρία στοιχεία λαμβάνει κάθε οργανισμός για τη πολιτική του ασφάλεια (Γιαγκουδάκης, 2013).

Η ασφάλεια ακολουθείται από τρείς βασικές έννοιες:

α) τη διαθεσιμότητα, που είναι η παρουσίαση κάθε πληροφορίας εύκολα και γρήγορα.

β) την εμπιστευτικότητα, δηλαδή την άκρως μυστικότητα της ίδιας της ύπαρξης των δεδομένων

γ) την ακεραιότητα, που είναι η ακέραιη διατήρηση των πληροφοριών ενός συστήματος

3.6.1 Ηλεκτρονικό έγκλημα και πρόληψη

Η πρόληψη είναι ο πιο σημαντικός παράγοντας στην ασφάλεια ενός συστήματος αφού μεροληπτεί για τυχόν επιθέσεις. Αρχικά, κάθε σύστημα και οργανισμός πρέπει να διαθέτει τη διαδικασία της αυθεντικοποίησης όπου ταυτοποιεί τη ταυτότητα ενός χρήστη είτε με τους κωδικούς πρόσβασης είτε με τα φυσικά χαρακτηριστικά του (δαχτυλικά αποτυπώματα) για να αποφεύγει ξένες εισβολές (Ψαρά, 2016).

Οι κωδικοί πρόσβασης είναι οι πιο διαδεδομένοι αφού αποτελεί το πιο απλό τρόπο προστασίας δεδομένων αφού το μόνο που χρειάζεται είναι η επιλογή ενός όνομα χρήστη και ο κωδικός πρόσβασης. Ο κωδικός μπορεί να αλλάξει από τον ίδιο το χρήστη όποτε το χρειαστεί και είναι εύκολο να απομνημονευτεί αφού ο χρήστης επιλέγει να χρησιμοποιήσει κωδικούς που αφορά τον ίδιο και είναι δύσκολο να τους ξεχάσει. Όμως, οι κωδικοί είναι εύκολο πλέον να αποκαλυφθούν με τη χρήση εργαλείων λογισμικού που διακινούνται στο διαδίκτυο αλλά και συνήθως ειδικά μεταξύ συναδέλφων φανερώνονται μεταξύ τους οι κωδικοί για να εξυπηρετηθούν ο ένας από τον άλλον (Lawspot.gr , 2014).

Επίσης, σαν πιο εξελιγμένη τεχνική στην ασφάλεια των συστημάτων θεωρείται η βιομετρία που χρησιμοποιεί τη ψηφιακή τεχνολογία για να κάνει επαλήθευση της ταυτότητας ενός ατόμου με βάση τα μοναδικά του χαρακτηριστικά. Στις βιομετρικές τεχνικές εντάσσονται η σάρωση υπογραφής, φωνής, χεριού, πατήματος πλήκτρο, ίριδας, δαχτυλικού αποτυπώματος και η αναγνώριση προσώπου.

Ακόμα, στα μέτρα πρόληψης περιλαμβάνεται η χρήση λογισμικού ασφάλειας όπως είναι τα antivirus και τα firewalls που είναι οι πιο διαδεδομένες (ΜΠΟΛΑΡΗ, 2017).

Οι ιοί παραμονεύουν πίσω από κάθε κλικ του ποντικιού για αυτό και η χρήση λογισμικού ασφάλειας αποτελεί ζωτική σημασία για τον υπολογιστή. Ανάλογα με το εύρος της επίθεσης του ιού μπορεί να επιφέρει ακόμα και ανεπανόρθωτη ζημιά σε ένα σύστημα. Το λογισμικό antivirus ανιχνεύει αρχικά τον ιό που έχει προσβάλει το σύστημα, το ταυτοποιεί για να δει τη πρόκληση της ζημιάς που έχει επιφέρει και ύστερα τα εξουδετερώνει τους ιούς εντοπίζοντας τα αρχεία που έχει προσβάλει. Επειδή, βέβαια, καθημερινά δημιουργούνται χιλιάδες ιοί οι εταιρίες λογισμικού ασφάλειας δίνουν το δικαίωμα στο χρήστη της on-line ενημέρωσης στις βάσεις δεδομένων σχετικά με τους νέους ιούς που κυκλοφορούν (Γιαγκουδάκης, 2013).

Ο ορισμός της λέξης firewall προσδίδεται σε ένα τοίχος προστασίας που αποτρέπει την εισαγωγή ενός μη ασφαλούς πακέτου στον υπολογιστή του χρήστη. Οι βασικές λειτουργίες

του firewall είναι το φιλτράρισμα πακέτων, όπου επιτρέπει ή απαγορεύει τη κίνηση πακέτων στο διαδίκτυο, και οι πύλες εφαρμογών, όπου οι εσωτερικοί χρήστες μπορούν να χρησιμοποιήσουν κάποιες υπηρεσίες που έχουν εξεταστεί από ιούς και οι hosts είναι προστατευμένοι. Στη σημερινές μέρες, που το ηλεκτρονικό έγκλημα έχει αυξηθεί και διεκπεραιωθεί ραγδαία, η χρήση των firewalls είναι αναγκαία για αυτό και η τεχνολογία τους αναπτύσσεται συνεχώς ώστε να μπορούν να επιτελούν πολλές εργασίες την ίδια στιγμή (Lawspot.gr , 2014).

Μια αρχαία μέθοδος που συναντάει κανείς και σήμερα στην ασφάλεια των συστημάτων είναι η κρυπτογραφία μ που γίνεται με τη χρήση κωδικών-συμβόλων. Στην κρυπτογράφηση μετατρέπεται μια κατανοητή πληροφορία σε ένα κωδικό-γρίφο που μπορεί έλθει ξανά στην κανονική της μορφή μέσω της διαδικασίας της αποκρυπτογράφησης (ΜΠΟΛΑΡΗ, 2017).

Η κρυπτογραφία χωρίζεται σε δύο κατηγορίες:

- Στη συμμετρική κρυπτογραφία όπου υπάρχει ένα κλειδί που συντελεί και τη διαδικασία της κρυπτογράφησης και τη διαδικασία αποκρυπτογράφησης. Ο αποστολέας ενός μηνύματος το κρυπτογραφεί με τη χρήση του κλειδιού και ύστερα ο παραλήπτης το αποκρυπτογραφεί με τη χρήση του ίδιου κλειδιού μέσω ενός ασφαλούς καναλιού επικοινωνίας.
- Στην ασύμμετρη κρυπτογραφία όπου υπάρχουν δύο κλειδιά. Το ένα είναι γνωστό σε όλους για να μπορούν να κρυπτογραφούν ένα μήνυμα και το άλλο είναι γνωστό μόνο σε αυτόν που θα προβεί στην αποκρυπτογράφηση (Γκαρτζώνη, 2017).

Αδύναμα σημεία έχουν και οι δύο περιπτώσεις, με τη συμμετρική κρυπτογραφία να εμφανίζει πρόβλημα στην εύρεση ενός ασφαλούς καναλιού επικοινωνίας και στην ασύμμετρη να υπάρχει πρόβλημα λόγω της απαίτησης μεγαλύτερων κλειδιών για την αποκρυπτογράφηση πράγμα καταντά τη διαδικασία πολύ χρονοβόρα. Έτσι συνδυάστηκαν οι δυο κρυπτογραφήσεις δημιουργώντας το υβριδικό σύστημα όπου στην ανταλλαγή μυστικού κλειδιού χρησιμοποιείται η ασύμμετρη και στην επικοινωνία η ασύμμετρη (Γιαννακοπούλου, 2017).

Ένας τομέας που είναι παραμελημένος αλλά έχει μεγάλη σημασία για έναν οργανισμό και ένα χρήστη είναι η φυσική ασφάλεια. Οι πιο πολλοί επικεντρώνονται στη σύγχρονη προστασία του συστήματος με εξελιγμένο λογισμικό και δεν σκέπτονται ότι αυτό το λογισμικό έρχεται σε δεύτερη μοίρα αν κάποιος αφαιρέσει το σκληρό δίσκο ενός υπολογιστή. Στη φυσική ασφάλεια συμπεριλαμβάνονται τα μέτρα από μια πιθανή εισβολή εγκληματία όπως και οι κατασκευές ύψιστης ασφάλειας που προστατεύουν το κτίριο από φυσικά αίτια όπως είναι η φωτιά, οι πλημμύρες, ο σεισμός (Lawspot.gr , 2014).

Πολλές φορές οι ηλεκτρονικές συσκευές είναι εκτεθειμένες στο κοινό και βρίσκονται σε κίνδυνο να χακαριστούν με σκοπό την κλοπή δεδομένων του χρήστη, τη καταστροφή του δικτύου, τη παρεμβολή συσκευών. Επίσης, πρέπει να προστατεύονται ιδιαίτερα οι αποθηκευτικές μονάδες όπου υπάρχουν σημαντικές πληροφορίες που αφορούν είτε το χρήστη

είτε το σύστημα του υπολογιστή του και η ασφάλεια αυτού. Η πιο εξελιγμένη μέθοδος είναι η βιομετρική που περιλαμβάνει μεθόδους όπως το δακτυλικό αποτύπωμα κ.α. (Ψαρά, 2016).

Όταν τα μέτρα πρόληψης παραλειφθούν και ο εισβολέας μπει στο σύστημα του υπολογιστή τότε θα πρέπει απευθείας να εντοπιστεί η απειλή. Αυτό το τομέα το αναλαμβάνει το Σύστημα Ανίχνευσης επιθέσεων που εγκαθίσταται από τον διαχειριστή και έχει ως βασική λειτουργία του τον εντοπισμό οποιαδήποτε ξένης πρόσβασης στο σύστημα που θα προκαλέσει ζημιές στο σύστημα.

Τρία μοντέλα αποτελούν ανίχνευσης επιθέσεων αποτελούν:

- η ανίχνευση ανωμαλιών όπου είναι ένα σύστημα που τυποποιεί τις ροές και τις διαδικασίες δεδομένων έτσι ώστε να εντοπίζει τις ανωμαλίες μόλις εισβάλουν. Ωστόσο, αν τα συστήματα δεν είναι καλά ρυθμισμένα τότε δίνουν λανθασμένες εντολές σχετικά με νόμιμες κινήσεις.
- η ανίχνευση υπογραφών που είναι μια μέθοδος ταυτοποίησης και εντοπισμό ιού που στηρίζονται στο γεγονός ότι κάθε επίθεση έχει μοναδική υπογραφή. Η υπογραφή αποθηκεύεται για μετέπειτα σύγκριση. Απαιτείται συνεχής ενημέρωση βάσης.

το υβριδικό μοντέλο όπου συνδυάζει τα δύο προηγούμενα μοντέλα τα οποία παρακολουθούν την κίνηση στο δίκτυο για τυχόν απειλές, εντοπίζει κακόβουλα δεδομένα, ανωμαλίες, δυσλειτουργίες και εστιάζει κυρίως στις εσωτερικές απειλές (Γιαγκουδάκης, 2013).

3.6.2 Αντιμετώπιση καταστροφών

Η πρόληψη και η αντιμετώπισης μιας απειλής είναι δυο στάδια εξαιρετικής σημασίας για τη προστασία ενός υπολογιστικού συστήματος που πολλές φορές δεν αρκεί για να εμποδίσουν την απειλή και σε εκείνο το σημείο μπαίνει η διαδικασία που αντιμετωπίζονται οι καταστροφές μετά από την εισχώρηση του εισβολέα. Πρέπει οπωσδήποτε οι οργανισμοί ιδιαίτερα αλλά και οι χρήστες να αποθηκεύουν το σημαντικό υλικό τους σε μονάδες αποθήκευσης έτσι ώστε να μη χαθούν αν πάθει κάποια βλάβη ο υπολογιστής. Βέβαια, υπάρχει και η περίπτωση της φυσικής καταστροφής των δεδομένων που γίνεται με πλημμύρες σεισμό, πυρκαγιά και σε περίπτωση που συμβεί σε έναν οργανισμό και χαθούν όλα τα δεδομένα του ενδέχεται να επιφέρει ολοκληρωτική καταστροφή στην οικονομία του. Για αυτό το λόγο θα πρέπει να έχουν ληφθεί κατάλληλα μέτρα με τη λήψη εφεδρικών αντιγράφων που με τα επιμέρους υποσυστήματα που διαθέτει αυτό το σύστημα διασφαλίζει τα δεδομένα από όλες τις καταστροφές που μπορεί να συμβούν. Ένα τέτοιο σύστημα είναι ζωτικής σημασίας για κάθε οργανισμό για αυτό και πρέπει να υπάρχει αλλά αν και ο οργανισμός δεν διαθέτει το κεφάλαιο για να το αποκτήσει, μπορεί να εξασφαλίσει τα δεδομένα του με τη χρήση εφαρμογών που κυκλοφορούν στην αγορά. Ο χρήστης ή η επιχείρηση ή ο οργανισμός μεταφέρει όλα τα αρχεία που χρειάζεται σε ένα σκληρό δίσκο του υπολογιστή του έτσι ώστε όταν ένας δίσκος του καταστραφεί να αντικατασταθεί κατευθείαν

από το νέο (ΜΠΟΛΑΡΗ, 2017).

-Το ηλεκτρονικό ταχυδρομείο που χρησιμοποιείται ανελλιπώς σήμερα προσφέρει ταχύτητα , είναι δωρεάν και αποστέλλει μαζικά μηνύματα. Αυτό που αναζητά κάθε χρήστης του διαδικτύου είναι η εμπιστευτικότητα και η αυθεντικότητα κάθε μηνύματος που συχνά απειλείται επειδή γίνεται στόχος επιθέσεων των ιών. Οι ιοί εμφανίζονται με τη μορφή μηνύματος αγνώστου προέλευσης που περιέχει εκκεντρικό περιεχόμενο για να ξεγελάσει το παραλήπτη έτσι ώστε να το ανοίξει. Ο υπολογιστής οπότε θα πρέπει να έχει οπωσδήποτε ένα λογισμικό antivirus και να το ενημερώνει συνεχώς για τη πιθανότητα νέων ιών (ΜΠΟΛΑΡΗ, 2017).

Πέρα από το antivirus ένας υπολογιστής θα πρέπει να προμηθευτεί και λογισμικό που αποτρέπει το spamming όταν αυτό φτάσει σε ενοχλητικό βαθμό. Το spamming συνήθως περιέχει παραπλανητικά διαφημιστικά και κάνει μαζική αποστολή αυτών.

Γενικά , θα πρέπει να δίνεται ιδιαίτερη προσοχή στα ηλεκτρονικά μηνύματα που ανταλλάσσονται μέσω του e-mail και ιδανικά να μην αναφέρονται στο περιεχόμενο τους ευαίσθητα δεδομένα όπως είναι κωδικοί πρόσβασης, τραπεζικοί λογαριασμοί κ.τ.λ. όσο προχωρά η τεχνολογία τόσο πιο εύκολο γίνεται να παραβιαστούν οι κωδικοί και να πέσουν τα προσωπικά στοιχεία σε τρίτους για αυτό και οι κωδικοί επιτάσσεται να ανανεώνονται συνεχώς (ΜΠΟΛΑΡΗ, 2017).

-Οι πιο πολλές αγορές πλέον γίνονται on-line διότι υπάρχει μεγάλη προσφορά εύρος επιλογών και τιμών. Οι αγορές γίνονται γρήγορα και εύκολα με το πάτημα ενός πλήκτρου και με τη χρήση πιστωτικής ή χρεωστικής κάρτας. Έτσι όσο το ηλεκτρονικό εμπόριο αυξάνεται τόσο οι επιτήδειοι βρίσκουν την ευκαιρία να διαπράξουν απάτη. Πρέπει δηλαδή να υπάρχει τεράστια προσοχή στις σελίδες που γίνονται οι αγορές. Για να επιτευχθεί αυτή η ασφαλής επικοινωνία μεταξύ σελίδας και χρήστη δημιουργήθηκαν πρωτόκολλα επικοινωνίας που θα προστατεύουν τα προσωπικά δεδομένα του χρήστη (ΜΠΟΛΑΡΗ, 2017).

Ένα από αυτά τα πρωτόκολλα είναι το SSL που κρυπτογραφεί τα μηνύματα, σύμφωνα με τη συμμετρική και ασύμμετρη κρυπτογράφηση, που εξετάζει την αυθεντικότητα των συναλλασσόμενων και το ακέραιο περιεχόμενο. Το πρωτόκολλο SSL χρησιμοποιείται ως πρόσθετη ασφάλεια σε ιστοσελίδες γιατί προκαλεί μεγάλο όγκο στα δεδομένα με αποτέλεσμα να αργεί πολύ η μετάδοση του (ΜΠΟΛΑΡΗ, 2017).

Το δεύτερο είναι το πρωτόκολλο SET που εξασφαλίζει τις εμπιστευτικές συναλλαγές και ταυτοποιεί αυτόματα τους συναλλασσόμενους. Αυτό το πρωτόκολλο αποτελεί μια υλοποιήσιμη ιδέα εταιρειών πιστωτικών καρτών που θέλησαν να προστατέψουν τον αριθμό της πιστωτικής κάρτα σε εμπορικές συναλλαγές από τυχόν κλοπή. Η αποκρυπτογράφηση γίνεται μόνο από την εταιρία της κάρτας και όχι την εταιρία πώλησης.

-Το 90% ενός υπολογιστικού συστήματος αποτελείται από βάσεις δεδομένων και χρειάζεται τη μέγιστη δυνατή ασφάλεια. Τα δεδομένα στις βάσεις δεδομένων είναι πολύ ευαίσθητα και σημαντικά. Χρειάζονται πολύπλοκα εργαλεία και εξειδικευμένα για τη προστασία κάθε βάση

δεδομένων (Αυγουστάκη, 2010).

Οι βάσεις δεδομένων πρέπει να έχουν φυσική ακεραιότητα για να προστατευθούν από φυσικά προβλήματα και λογική ακεραιότητα για έναν σωστό σχεδιασμό για μη επιρροή άλλου πεδίου σε τυχόν μεταβολή τιμής σε ένα πεδίο (ΜΠΟΛΑΡΗ, 2017).

Επίσης, πρέπει να ενδείκνυται ακεραιότητα προσπέλασης στις βάσεις δεδομένων για να είναι σωστές οι τιμές των πεδίων και πρέπει να γίνεται έλεγχος προσπέλασης των χρηστών για να εισάγουν μόνο τα εξουσιοδοτημένα δεδομένα τους (ΜΠΟΛΑΡΗ, 2017).

Ακόμα, να υπάρχει αυθεντικοποίση χρηστών και τέλος να υπάρχει διαθεσιμότητα για να επιβεβαιώνει τη πρόσβαση στα δεδομένα όλη την ώρα.

-Κάθε οργανισμός οφείλει να έχει ένα γραπτό κείμενο που εξασφαλίζει την ασφάλεια του πληροφοριακού συστήματος προς τους κινδύνους μέσω κανόνων και αυτό αποτελεί την πολιτική ασφάλεια ενός οργανισμού. Η σύνταξη του κειμένου αποτελείται από δύο στάδια. Αρχικά, στο προσδιορισμό των κινδύνων με ποσοτική και ποιοτική ανάλυση (Αυγουστάκη, 2010).

Στην ποσοτική ανάλυση καθορίζεται το είδος των κινδύνων, η πιθανότητα να προκύψει και το κόστος που θα επέλθει σε τυχόν εισβολή.

Στην ποιοτική ανάλυση καθορίζονται οι πιθανές απειλές και η ευαισθητοποίηση του συστήματος έναντι απειλών. Σε αυτό το στάδιο συντάσσεται το κείμενο που θα περιγράφει τις γενικές πολιτικές και τις συγκεκριμένες διαδικασίες που θα τελεστούν για την αντιμετώπιση της εισβολής και συντάσσεται από ένα γνώμονα άνθρωπο του αντικειμένου (ΜΠΟΛΑΡΗ, 2017).

-Για τη προστασία πληροφοριακών συστημάτων έναντι του phishing χρησιμοποιούνται τεχνολογικά μέσα που έχουν τρία επίπεδα προστασίας (Rouse, 2017).

Αρχικά, ενδείκνυται το client-side επίπεδο που αντιμετωπίζει το phishing από τους τελικούς χρήστες και χρησιμοποιεί desktop protection agents, ψηφιακή υπογραφή και πιστοποίηση ηλεκτρονικής αλληλογραφίας, κατάλληλη διαρρύθμιση των παραμέτρων επικοινωνίας, εγρήγορση σε ζητήματα ασφαλείας και απενεργοποίηση των παραμέτρων του λογισμικού web-browser ιστοσελίδων (ΜΠΟΛΑΡΗ, 2017).

Το desktop protection agents αποσκοπεί στην ανίχνευση και παράλληλα στο μπλοκάρισμα κάθε εξωτερικής απειλής που προσπαθεί να διαρρήξει το σύστημα σε πραγματικό χρόνο. Αυτό το καταφέρνει με συνεχή ενημέρωση των anti-virus και anti-spam και τη χρήση firewall. Επίσης, με τη προστασία του υπολογιστή από κακόβουλα λογισμικά αλλά και με το σύστημα που ανιχνεύει κάθε προσπάθεια παραβίασης της ασφάλειας (ΜΠΟΛΑΡΗ, 2017).

Ύστερα υπάρχει το server-side επίπεδο που αντιμετωπίζει την επίθεση phishing στα πληροφορικά συστήματα μιας επιχείρησης και περιλαμβάνει τη ταυτοποίηση της προέλευσης των πληροφοριών, την συνεχή παρακολούθηση της ασφάλειας του συστήματος για άμεση αντιμετώπιση σε περίπτωση εισβολής και στη χρήση token-based συστημάτων για τη

πιστοποίηση ενός εξωτερικού παράγοντα (Γκαρτζώνη, 2017).

Τέλος, υπάρχει το services provider-side επίπεδο που αντιμετωπίζει το phishing από παρόχους υπηρεσιών με την περιμετρική προστασία με gateway protection agents, τη διαρκής παρακολούθηση του διαδικτύου, τη ψηφιακή υπογραφή των e-mails, την ταυτοποίηση διευθύνσεων e-mail αυτόματα και την προστασία του ονόματος χώρου.

Η προστασία με gateway protection agents γίνεται με gateway φιλτράρισμα περιεχομένου της εισβολής, με gateway anti-virus σκανάρισμα μη τυχών απειλείται το σύστημα από ιούς και από gateway anti-spam φιλτράρισμα για να αποφευχθούν τα παραπλανητικά διαφημιστικά (ΜΠΟΛΑΡΗ, 2017).

Η διαρκής παρακολούθηση που γίνεται από πάροχους υπηρεσιών στο διαδίκτυο δίνουν ώθηση στα agent-based bots να ανιχνεύσουν περιεχόμενο που ανήκει νομικά στον οργανισμό όπως είναι το λογότυπο του και ύστερα λαμβάνοντα τα κατάλληλα μέτρα για την αντιμετώπιση του προβλήματος (ΜΠΟΛΑΡΗ, 2017).

3.7 Η νομοθεσία στο ηλεκτρονικό έγκλημα

Το ηλεκτρονικό έγκλημα έχει προκληθεί λόγω της τεράστιας εξέλιξης της τεχνολογίας στα υπολογιστικά συστήματα και αυτό έφερε στο προσκήνιο την ανάγκη για ύπαρξη νομοθεσίας. Το ηλεκτρονικό έγκλημα αποτελεί ένα κλάδο ξεχωριστό και για να θεσμοθετηθεί πρέπει να γίνει προσέγγιση και από τεχνολογική πλευρά. Είναι εξαιρετικά δύσκολη η νομική ρύθμιση του Διαδικτύου γιατί ένας απρόσωπος χώρος, χωρίς χρόνο και χώρο, χωρίς γεωγραφικά όρια και με αμέτρητες δυνατότητες στην ανταλλαγή των πληροφοριών. Η παγκόσμια διάσταση του έχει προβληματίσει ιδιαίτερα τους νομοθέτες γιατί το κάθε έγκλημα αντιμετωπίζεται αλλιώς σε κάθε χώρα σύμφωνα με τις παραδόσεις, τα ήθη και τα έθιμα του κάθε λαού. Είναι επιτακτική οπότε η νομική συνεννόηση των χωρών γιατί ένα έγκλημα μπορεί να διαπραχθεί σε πολλές χώρες ταυτόχρονα και έτσι πρέπει να επιβληθεί μια κοινή ποινή, όσο είναι δυνατόν. Στην Ελλάδα δημοσιεύτηκε στις 3 Αυγούστου το 2016 ο νόμος 4411/2016 σχετικά με την αντιμετώπιση του ηλεκτρονικού εγκλήματος σε νομοθετικό επίπεδο. Ουσιαστικά κυρώθηκε η Σύμβαση του Συμβουλίου της Ευρώπης, που υπογράφτηκε στη Βουδαπέστη στις 21 Νοεμβρίου 2001,για το έγκλημα στο Κυβερνοχώρο και του Πρόσθετου Πρωτοκόλλου της σχετικά με τα εγκλήματα που διαπράττονται μέσω της χρήσης υπολογιστικών συστημάτων. Με αυτό το νόμο τιμωρούνται ενέργειες που τελούνται εναντίων των δικτύων, όπως η πρόκληση βλάβης τους ή η αλλοίωση και καταστροφή των δεδομένων τους, και οι πράξεις που αφορούν την υποκλοπή, τη παράνομη πρόσβαση, τις παρεμβολές σε συστήματα και δεδομένα. Πολύ σημαντική είναι και η ενσωμάτωση της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου, στο μέρος δεύτερο του νόμου 4411/2016, για τις επιθέσεις που γίνονται έναντι των συστημάτων των πληροφοριών και περιλαμβάνει τα εργαλεία που γίνονται οι επιθέσεις. Ο νέος νόμος τροποποιεί και εισάγει νέους νόμους σχετικά με τα εγκλήματα που διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή και μέχρι

τότε αντιμετωπίζονταν με το Ν.1805/1988.

- Πληροφοριακά συστήματα και ψηφιακά δεδομένα

Καταρχάς διερευνήθηκε η έννοια του εγγράφου με νομοθετικό ορισμό με τον Ν.1805/1988. Στην έννοια του εγγράφου περιλαμβάνονται το χαρτί, οι εκτυπωτές, οι σκληροί δίσκοι, οι πιστωτικές κάρτες, οι βάσεις δεδομένων και γενικά τα ηλεκτρονικά αρχεία που μπορεί να περιέχει ένα υπολογιστικό σύστημα κ.τ.λ.

Στο τέλος της περίπτωσης γ του άρθρου 13 του Ποινικού Κώδικα προστίθεται το ακόλουθο εδάφιο: «Εγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιοδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος. αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία».

Με τον νέο νόμο εισάγονται δύο πρόσθετοι ορισμοί στο άρθρο 13 του Ποινικού Κώδικα, τα στοιχεία η' και θ', των ψηφιακών δεδομένων και του πληροφοριακού συστήματος οι οποίοι είναι απαραίτητοι για να κατανοηθεί το νόημα των νέων διατάξεων αλλά και αυτών που πρόκειται να τροποποιηθούν και από τα έννομα όργανα και από το κοινό που παρακολουθεί την εξέλιξη των νόμων.

«η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο)»

- Εγκλήματα σε Σχέση με Εργαλεία για την Τέλεση Κυβερνοεγκλημάτων

Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

Το αδίκημα της Παρακώλησης λειτουργίας πληροφοριακών συστημάτων εισήχθη στο νέο

άρθρο 292Β του Ποινικού Κώδικα μετά το 292 Α με το οποίο προβλέπεται η ποινική πρόβλεψη με γνώμονα τις επιθέσεις έναντι συστημάτων τηλεφωνικών επικοινωνιών σύμφωνα πάντα με αυτά που προβλέπουν οι ποινές της οδηγίας περί νομικής προστασίας που προβάλει την αρχή της αναλογικότητας. Δηλαδή, όσο μεγαλύτερη είναι η ζημιά στα πληροφοριακά συστήματα τα οποία αποτελούν μέρος ζωτικών υπηρεσιών για τη κοινωνία και που γίνεται προσχεδιασμένα με τη χρήση εργαλείων, τόσο μεγαλύτερή είναι και η ποινή που επιβάλλεται και προβλέπεται, με συνδυασμό το άρθρο 187 του Ποινικού Κώδικα , ως εγκληματική πράξη.

« Άρθρο 292Β: Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

1.Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση μέχρι τριών (3) ετών.

2.Η πράξη της πρώτης παραγράφου τιμωρείται:

α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4.Γ ια την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση»(Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο)

- Ποινικοποίηση αυτοτελών συμπεριφορών

Προστίθεται νέο άρθρο 292Γ στο Ποινικό Κώδικα, μετά το άρθρο 292Β,στο οποίο ποινικοποιούνται όποιος χωρίς δικαίωμα και έχοντας ως στόχο το έγκλημα εισάγει, παράγει

κ.τ.λ. προγράμματα σχεδιασμένες να τελέσουν μια άνομη πράξη, σύμφωνα με το άρθρο 7 της Οδηγίας και του άρθρου 292Β Π.Κ.

« Άρθρο 292Γ

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη των εγκλημάτων του άρθρου 292Β παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης των εγκλημάτων του άρθρου 292Β, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

4.Οι παράγραφοι 2 και 5 του άρθρου 348Α του Ποινικού Κώδικα αντικαθίστανται ως εξής:

«2. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.

5.Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

- Πορνογραφία ανηλίκων

Η πορνογραφία αποτελεί ένα από τα πιο ειδεχθή εγκλήματα το οποίο αυξάνεται όλο και περισσότερο τα τελευταία χρόνια κάνοντας το έργο των διωκτικών αρχών όλο και πιο δύσκολο. Η διαδικτυακή πορνογραφία μπορεί να πάρει τη μορφή βίντεο, φωτογραφιών και γενικά όλων των πολυμέσων. Οι δράστες της παιδικής πορνογραφίας τιμωρούνται με τις διατάξεις του Ποινικού Κώδικα που φέρουν τα άρθρα 337 «Προσβολή της γενετήσιας αξιοπρέπειας», 339 «Αποπλάνηση παιδιών», 342 «Κατάχρηση ανηλίκων σε ασέλγεια», 348Α «Πορνογραφία ανηλίκων», 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους», 348Γ «Πορνογραφικές παραστάσεις ανηλίκων» και 351Α Π.Κ. «Ασέλγεια με ανήλικο έναντι αμοιβής».

Το άρθρο που τροποποιήθηκε στο Ποινικό Κώδικα είναι το 348Β «Προσέλκυση παιδιών για γενετήσιους λόγους» και όπως ορίζεται από το άρθρο 13 Π.Κ. εισάγεται στη 2 και στη 5 παράγραφο του πληροφοριακού συστήματος για να αποκλειστεί πιθανή ομοιογένεια με άλλες διατάξεις του Π.Κ.

Για αυτούς τους λόγους αλλάζει και το άρθρο 348Β Π.Κ. διότι εισάγεται ο όρος « πληροφοριακά συστήματα».

«Άρθρο 348Β: Προσέλκυση παιδιών για γενετήσιους λόγους

Όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαοχτώ έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

- Παράνομη πρόσβαση σε πληροφοριακό σύστημα

Το hacking μπαίνει στις διατάξεις του Ποινικού Κώδικα με το άρθρο 370Γ ως η άνομη πρόσβαση σε ένα τμήμα ή σύνολο πληροφοριακού συστήματος. Ο όρος αυτός χρησιμοποιείται συνεχώς στη γλώσσα των δραστών ονόματι hacker που όλο και περισσότεροι προστίθενται στην άτυπη οργάνωση τους αφού κυκλοφορούν πολλά εργαλεία στο Διαδίκτυο που διευκολύνουν τη παραβίαση δεδομένων.

«Άρθρο 370Γ: Παράνομη πρόσβαση σε πληροφοριακό σύστημα

1.Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι (6) μήνες και με χρηματική ποινή διακοσίων ενενήντα (290) ευρώ έως πέντε χιλιάδων εννιακοσίων (5.900) ευρώ.

2.Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχός του, τιμωρείται με φυλάκιση. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή την ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148.

3.Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

4.Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

- Παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων

Τιμωρείται ως αδίκημα σύμφωνα με το άρθρο 370 του Π.Κ. η παραβίαση του απορρήτου που

πρέπει να έχει κάθε επικοινωνία και γίνεται στο χώρο των πληροφοριακών συστημάτων και η μετέπειτα χρήση των πληροφοριών που έχει εκλάβει αυτή την επικοινωνία ο δράστης. Οι ποινές που επιβάλλονται είναι σύμφωνες με το άρθρο 370 Π.Κ. που σχετίζεται με το απόρρητο των τηλεφωνικών επικοινωνιών και προβλέπει κάθειρξη δέκα ετών. Αν οι πράξεις έχουν αντίκτυπο την ασφάλεια του κράτους σε μια εμπόλεμη περίοδο τότε τιμωρούνται με βάση το άρθρο 146 Π.Κ.

Μετά το άρθρο 370Γ του Ποινικού Κώδικα προστίθεται άρθρο 370Δ ως εξής:

«Άρθρο 370Δ

1.Όποιος, αθέμιτα, με τη χρήση τεχνικών μέσων, παρακολουθεί ή αποτυπώνει σε υλικό φορέα μη δημόσιες διαβιβάσεις δεδομένων ή ηλεκτρομαγνητικές εκπομπές από, προς ή εντός πληροφοριακού συστήματος ή παρεμβαίνει σε αυτές με σκοπό ο ίδιος ή άλλος να πληροφορηθεί το περιεχόμενό τους, τιμωρείται με κάθειρξη μέχρι δέκα (10) ετών.

2.Με την ποινή της παραγράφου 1 τιμωρείται όποιος κάνει χρήση της πληροφορίας ή του υλικού φορέα επί του οποίου αυτή έχει αποτυπωθεί με τους τρόπους που προβλέπεται στην παράγραφο 1.

3.Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

- Παρεμβολές σε δεδομένα - Παράνομη Υποκλοπή Ψηφιακών Δεδομένων

Μια νέα διάταξη (άρθρο 370 Ε Π.Κ.) έρχεται να τιμωρήσει όσους διαθέτουν, διανέμουν προγράμματα τα οποία δείχνουν τον τρόπο και διαθέτουν τα μέσα για μια μη εξουσιοδοτημένη πρόσβαση σε ένα πληροφοριακό σύστημα με σκοπό το έγκλημα (άρθρα 370 Α μέχρι 370Δ Π.Κ.). Με την εισαγωγή του νέου άρθρου (38ΙΑ Π.Κ.) προστατεύονται πλέον τα ψηφιακά δεδομένα από την διαγραφή, την υποκλοπή, την αλλοίωση κ.τ.λ. Έτσι καλύπτεται το κενό που είχε η ελληνική νομοθεσία(άρθρο 4 της Σύμβασης και άρθρο 5 της Οδηγίας) στο να προστατεύεται μόνο ο υλικός φορέας που περιλαμβάνει τα ψηφιακά δεδομένα.

«Άρθρο 370^{E}

Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται ενός χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό ενός διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ,

β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος» (Νόμος 4411/2016 – ΦΕΚ 142/Α/3-8-2016 – Άρθρο Δεύτερο).

- Παράνομη Παρεμβολή σε Ψηφιακά Δεδομένα –Φθορά ηλεκτρονικών δεδομένων

Η ελληνική νομοθεσία με το άρθρο 381Α του Π.Κ. «Φθορά ηλεκτρονικών δεδομένων» εναρμονίζεται με το άρθρο 7 της οδηγίας που προσδίδει την ποινική ευθύνη στα πρόσωπα που πουλάνε, αγοράζουν κ.τ.λ. κωδικούς και προγράμματα από το διαδίκτυο με σκοπό να τα χρησιμοποιούσουν αργότερα για τη τέλεση κάποιας αξιόποινης πράξης(38ΙΑ Π.Κ.)

«Άρθρο 381^{Α}: Φθορά ηλεκτρονικών δεδομένων

1.Όποιος χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός συστήματος πληροφοριών, καθιστά ανέφικτη τη χρήση τους ή με οποιονδήποτε τρόπο αποκλείει την πρόσβαση στα δεδομένα αυτά, τιμωρείται με φυλάκιση έως τρία (3) έτη. Σε ιδιαίτερα ελαφρές περιπτώσεις, το δικαστήριο μπορεί, εκτιμώντας τις περιστάσεις τέλεσης, να κρίνει την πράξη ατιμώρητη.

2.Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.

4.Γ ια την ποινική δίωξη της πράξης της παραγράφου 1απαιτείται έγκληση»(Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

- Απάτη σχετική με υπολογιστές

Στις περιπτώσεις που αφορούν την απάτη με υπολογιστή, τροποποιείται το άρθρο 386 Α Π.Κ. (άρθρο 8 της Σύμβασης) και προστίθεται και η χρήση των δεδομένων που γίνεται δίχως να τους έχει παραχωρηθεί κάποιο δικαίωμα.

«Άρθρο 386Α

Απάτη με υπολογιστή

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα» (Νόμος 4411/2016 - ΦΕΚ 142/Α/3-8-2016 - Άρθρο Δεύτερο).

3.7.1 Ειδικότερες διατάξεις που έχουν σχέση με το ηλεκτρονικό έγκλημα

Α) Όσον αφορά το ηλεκτρονικό εμπόριο βρίσκονται σε ισχύ το Ποινικό Δίκαιο 131/2003 που έχει ως κύριο μέρος την ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam mail) και την ευθύνη που πρέπει να αναλάβουν αυτοί που παρέχουν υπηρεσίες στο Διαδίκτυο για τις πράξεις που προβαίνουν οι χρήστες τους. Το Π.Δ. 150/2001 αφορά το κοινοτικό πλαίσιο των ηλεκτρονικών υπογραφών και θα επιτευχθεί με τη προσαρμογή της Κοινοτικής Οδηγίας 99/93/ΕΕ

Β) Στις ηλεκτρονικές επικοινωνίες συναντάμε τους νόμους:

- 2867/2000 για την «Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις.»
- 3431/2006 «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις.»
- 3783/2009 για την «Ταυτοποίηση και κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις.»

Γ) Ως προς την πνευματική ιδιοκτησία, τα δικαιώματα των πολιτών προστατεύονται από το Ν.2819/2000 και ιδιαίτερα όταν αφορά τη προστασία βάσεων δεδομένων.

Δ) Για την προστασία των απορρήτων των επικοινωνιών βρίσκουν ισχύ οι νόμοι:

- 2225/1994 σχετικά με τη «προστασία της ελευθερίας της ανταπόκρισης της επικοινωνίας και άλλες διατάξεις.»

- 3674/2008 για την «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις.»
- Π.Δ. 47/2005 σχετικά με τις «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για τη άρση του απορρήτου των επικοινωνιών και για τη διασφάλιση του.»

Ε) Όταν γίνετε αναφορά σχετικά με τη διατήρηση δεδομένων ο Ν.3917/2011 μιλάει για τη «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με τη 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.»

3.7.2 Το πρόβλημα δικαιοδοσίας στο διαδίκτυο

Η δικαιοδοσία στο Διαδίκτυο είναι αρμοδιότητα του Δικαστηρίου που θα κληθεί να δικάσει μια υπόθεση καθώς και των διωκτικών αρχών που θα κληθούν να ερευνήσουν μια εγκληματική συμπεριφορά.

Η επιλογή του δικαίου που θα εφαρμοστεί αποτελεί ένα από το δυσκολότερο ζήτημα ειδικά όταν αφορά έγκλημα που έχει τελεστεί στο διαδίκτυο. Ο προσδιορισμός της δικαιοδοσίας γίνεται με βάσει γεωγραφικά κριτήρια, οπότε το έγκλημα που έχει τελεστεί στο έδαφος ενός κράτους το αναλαμβάνει αυτό και μόνο, αλλά και γίνεται με βάσει εθνικά κριτήρια που το κράτος αναλαμβάνει δικαιοδοσία όταν ένα έγκλημα έχει τελεστεί από τους πολίτες του. Όμως, όταν το έγκλημα γίνει διαδικτυακά το έργο της δικαιοδοσίας γίνεται εξαιρετικά δύσκολο, εφόσον δεν υφίσταστε γεωγραφική κυριαρχία και ο τόπος όπου τελέστηκε το ηλεκτρονικό έγκλημα είναι δύσκολο να προσδιοριστεί. Όλες οι πληροφορίες που διανέμονται στο διαδίκτυο δεν έχουν στόχο μόνο ένα αποδέκτη αλλά πολλούς οι οποίοι είναι διαμοιρασμένοι σε παγκόσμιο επίπεδο επηρεάζοντας νομικά άτομα διαφορετικής δικαιοδοσίας και ταυτόχρονα διαφορετικού νομικού πλαισίου (Γκαρτζώνη, 2017).

Το ζήτημα αυτό καθορίζεται με βάση διεθνείς συμβάσεις, εθνικές νομοθεσίες και νομολογία.

Η επιλογή του Δικαίου που θα εφαρμοστεί σε μια υπόθεση ηλεκτρονικού εγκλήματος στο Διαδίκτυο βασίζεται:

1) Στο τόπο που βρίσκεται ο server που περιέχει τα βλαπτικά ψηφιακά δεδομένα που θα καθορίσει το δίκαιο της χώρας που θα εφαρμόσει τους κανόνες. Ωστόσο, τα ψηφιακά δεδομένα συνήθως είναι προσωρινά σε ένα διακοσμητή και ο διακοσμητής να μην είναι καν γνωστός στο χρήστη του.
2) Στη διεύθυνση της ιστοσελίδας του παροχέα με βάση τη χώρα που έχει έδρα άρα αποσαφηνίζεται το δίκαιο που θα εφαρμοστεί.
3) Στη χώρα που ο χρήστης θα πραγματοποιήσει τις εμπορικές του συναλλαγές αποτελεί κριτήριο.
4) Το δίκαιο της χώρας όπου γίνεται η επικοινωνία του συναλλασσόμενου και του

χρήστη.

Τα διαδικτυακά εγκλήματα, γενικά, ως τόπος που τελέστηκε το έγκλημα είναι από τη μια μεριά ο τόπος που εκδηλώθηκε η εγκληματική συμπεριφορά(π.χ. εισαγωγή δεδομένων) ή από την άλλη ο τόπος επέλευσης του αποτελέσματος όπως είναι ο τόπος που βρίσκονται τα ψηφιακά δεδομένα του θύματος (Γκαρτζώνη, 2017).

Συμπερασματικά, τα ηλεκτρονικά εγκλήματα μπορούν να τελεστούν από οπουδήποτε και σε οποιονδήποτε για αυτό και αποτελεί δύσκολη ενέργεια ο εντοπισμός του και πόσον μάλλον η εξιχνίαση του με το Δίκαιο μιας χώρας. Γενικά, οι νόμοι είναι δύσκολο να συμβαδίσουν με τη ραγδαία εξέλιξη της τεχνολογίας έτσι ώστε να την οριοθετήσουν για αυτό και η νομοθεσία παρουσιάζει κενά στην τέλεση τους. Ο ίδιος ο χρήστης θα πρέπει να είναι ενήμερος και να φροντίζει για την ασφάλεια του πρωτίστως για να μην φτάσει να χρειαστεί τη παρέμβαση του κράτους. Επίσης, ο χρήστης πρέπει να φιλτράρει και να εξετάζει προσεκτικά την ενημέρωση που παίρνει από το διαδίκτυο αφού έχουν δημιουργηθεί εκατοντάδες ιστότοποι ενημέρωσης που προσπαθούν με κάθε είδηση που δημοσιεύουν να δελεάσουν τον κόσμο για αυτό πέφτουν στη παγίδα της σύντομης και μη έγκυρης είδησης. Εννοείται, και στον τομέα της διαδικτυακής ενημέρωσης τροποποιούνται και προσαρμόζονται νόμοι έτσι ώστε να καλυφθεί νομικά και αυτός ο τομέας του διαδικτύου.

ΚΕΦΑΛΑΙΟ 4^{ο} - ΜΕΣΑ ΜΑΖΙΚΗΣ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

4.1 Η αλλαγή του τοπίου της Ενημέρωσης από τα Νέα Μέσα

Η επικοινωνία αποτελεί ένα κύριο συστατικό μιας κοινωνίας και είναι αυτό που συντάσσει ένα πολιτισμό. Κάθε δραστηριότητα που προβαίνει ένα άτομο συνάπτει μια επικοινωνιακή λειτουργία προς τη κοινωνία και τους συνανθρώπους του με τη παραγωγή, τη μετάδοση και τη κατανόηση του μηνύματος. Τα Μ.Μ.Ε. αναλαμβάνουν μια τέτοια δραστηριότητα με τη μετάδοση μηνυμάτων και συμβάντων που διαδραματίζονται στη καθημερινότητα με σκοπό τη γνωστοποίηση τους προς το ευρύ κοινό. Ως ορισμός των Μέσων Μαζικής Ενημέρωσης εννοούνται όλα τα μέσα που είναι διαθέσιμα στο κοινό και μέσω αυτών μπορεί να ενημερωθούν για όλα τα τρέχοντα γεγονότα.

Οι ανακαλύψεις που συμβαίνουν σε κάθε εποχή θεωρούνται εξαρχής πρωτοποριακές μέχρι να κάνουν την εμφάνιση τους οι επόμενες που θα είναι βελτιωμένες και ανατρεπτικές. Κάτι τέτοιο συμβαίνει και με τα μέσα ενημέρωσης που συνεχώς άλλαζαν το τοπίο με τις νέες εφευρέσεις που παρουσιάζονταν. Όλα τα παλιά μέσα έπρεπε να προσαρμοστούν με τα εκσυγχρονισμένα μέσα και τα νέα δεδομένα που έφερναν στο προσκήνιο. (Καβακόπουλος,

2006)

Τα πρώτα μέσα που εμφανίστηκαν στο πλανήτη ήταν τα έντυπα και ακολούθησαν τα μέσα της εικόνας και του ήχου που επηρέασαν ολόκληρη τη καθημερινότητα του ανθρώπου και έφεραν μια επαναστατική τάση προς την ενημέρωση και την επικοινωνία της εποχής. Στα τέλη του 19^{ου} αιώνα, ύστερα από τις εφημερίδες ως νέο μέσο θεωρούταν ο κινηματογράφος και λίγες δεκαετίες αργότερα, στις αρχές του 20^{ου} αιώνα(δεκαετίες,'20, '30) το ραδιόφωνο. Λίγο αργότερα, εμφανίστηκε η τηλεόραση, όπου άρχισε να χρησιμοποιείται ευρέως τη δεκαετία του '60.

Τα μέσα, με την εξέλιξη που πήραν, άρχισαν να επηρεάζουν ιστορικές και κοινωνικές εξελίξεις όπως ήταν η διάδοση του Διαφωτισμού που βοηθήθηκε ιδιαίτερα από τον γραπτό λόγο και τον διαμοιρασμό εντύπων. Επίσης, επανάσταση προκλήθηκε στα μέσα επικοινωνίας από την εφεύρεση και ανάπτυξη του ραδιοφώνου ,της τηλεόρασης, του κινηματογράφου. Όλες αυτές οι αλλαγές ήταν μηδαμινές μπροστά στις ανατροπές που έφερε το διαδίκτυο παράλληλα με τα νέα μέσα σε όλες τις πτυχές της κοινωνίας. (Ρήγου, 2014).

Σημαντικό ρόλο έπαιξαν στην ενημέρωση τα νέα μέσα και το διαδίκτυο όπου άλλαξαν ολοκληρωτικά το σκηνικό που επικρατούσε μέχρι τότε. Αναλογικά μέσα όπως ήταν η τηλεόραση, ο Τύπος, το ραδιόφωνο μετατράπηκαν σε ψηφιακά για να συγκλίνουν με την εξέλιξη της εποχής τους.

Σιγά σιγά άρχιζαν οι εφημερίδες να ανεβαίνουν και στο διαδίκτυο κατά τις αρχές της δεκαετίας του '90 και αυτό γιατί τα έντυπα μέσα άρχιζαν να φθίνουν μπροστά στις ηλεκτρονικές υπηρεσίες που πρόσφερε το διαδίκτυο και έτσι μετατράπηκαν και σε ηλεκτρονικές. Οι ιστοσελίδες με ενημερωτικό περιεχόμενο όλο και αυξάνονται και γενικά το διαδίκτυο αρχίζει να μεταβάλει συνεχώς το τοπίο της ενημέρωσης (Τσενέ, 2012).

Τα ΜΜΕ έχουν τόση μεγάλη επιρροή στους ανθρώπους που πλέον είναι γνωστή και ως «τέταρτη εξουσία». Τα γεγονότα τα οποία παρουσιάζουν και περιγράφουν επηρεάζουν τη γνώμη του κοινού και γενικότερα συνδιαμορφώνουν την πραγματικότητα τους σχετικά με ένα γεγονός. Τα ΜΜΕ δίνουν ειδήσεις στο κοινό που το ίδιο ζητά ή παρουσιάζει μεγάλο ενδιαφέρον για αυτά. Μέσω των ΜΜΕ προβάλλονται κοινωνικά πρότυπα, διαμορφώνονται αξίες αλλά και νοοτροπίες για αυτό πρέπει να είναι πολύ προσεκτικά με την περιγραφή τους αλλά και με τη κάθε τους κίνηση. Επίσης, είναι ένα μέσο ψυχαγωγίας αλλά και το πιο δυνατό μέσο επικοινωνίας του κράτους και του πολίτη (Φωτόπουλος, 2014).

Τα ΜΜΕ έφεραν μια μεγάλη επανάσταση που «απελευθέρωσε» τον άνθρωπο από τη περιορισμένη τοπική ενημέρωση που είχε, την απομόνωση, την άγνοια των συμβάντων στον υπόλοιπο κόσμο αλλά και να γνωρίσει εικονικά τον κόσμο, να ανταλλάξει ιδέες, σκέψεις κ.τ.λ. Αυτή όμως η εικονική πραγματικότητα άρχισε να αποπροσανατολίζει τον άνθρωπο με σκοπό να τον οδηγήσει στο μονοπάτι που η ίδια ήθελε(Παπαθανασόπουλος, 2004).

Τα ΜΜΕ χωρίζονται στα ασύγχρονα μέσα, που είναι ο τύπος και το διαδίκτυο, διότι η πληροφορία μεταδίδεται ασύγχρονα για κάθε χρήστη, δηλαδή σε διαφορετικές χρονικές στιγμές, και στα σύγχρονα που συγκαταλέγονται η τηλεόραση και το ραδιόφωνο και η

πληροφορία μεταδίδεται συγχρονισμένη στους χρήστες.

Ο Τύπος υπάρχει πλέον σε παραδοσιακή και ηλεκτρονική μορφή. Παραδοσιακός τύπος θεωρείται τα περιοδικά, οι εφημερίδες, το ραδιόφωνο ενώ ηλεκτρονικός οι ιστοσελίδες, η τηλεόραση κ.τ.λ.

Το ραδιόφωνο χρησιμοποιείται ακόμα από πολλούς ως μέσο ενημέρωσης αφού διαθέτει ευχάριστα ψυχαγωγικά προγράμματα και ειδήσεις με άποψη. Μπορεί να μεταφερθεί και να χρησιμοποιηθεί παντού και προσφέρει συγχρόνως και μη άκουσμα μουσικής και ειδήσεις (Ψυχογιός, 2004).

Η τηλεόραση ασκεί μεγάλη επιρροή στους τηλεθεατές αφού είναι κάθε μέρα και ώρα διαθέσιμο συμβάλλοντας μέσα από το πρόγραμμα του στη διαμόρφωση απόψεων, ιδεών του θεατή. Βέβαια, καμιά φορά προβάλλει λάθος πρότυπα και μηνύματα και μπορεί να προκαλέσει προβλήματα υγείας όπως μυωπία, πονοκέφαλο κ.α. (Ψυχογιός, 2004).

Ο ρόλος που έχουν αναλάβει τα ΜΜΕ είναι να παρέχουν έγκαιρη και έγκυρη ενημέρωση στους πολίτες, να ελέγχουν την πολιτική εξουσία, τη προπαγάνδα και τη παραπληροφόρηση, να ενεργοποιούν τους πολίτες για θέματα της κοινωνίας. Βέβαια, όλα αυτά πλέον απέχουν από τη πραγματικότητα αφού τα τελευταία χρόνια παρατηρείται να γίνεται επιλεκτική ενημέρωση με βάση την εξυπηρέτηση συμφερόντων, να φιλτράρονται οι ειδήσεις και να παρουσιάζουν ένα μέρος της αλήθειας αποσιωπώντας τα σημαντικά γεγονότα και τονίζοντας τα πιο ασήμαντα για να κατευθύνουν το κοινό στη κατεύθυνση που αυτά θέλουν.

Η κύρια πηγή από τα έσοδα των ΜΜΕ είναι οι διαφημίσεις από τα οποία αποσκοπούν μεγάλο κέρδος και έτσι επιλέγονται να διαφημιστούν τα προϊόντα με το μεγαλύτερο κέρδος. Ο ανταγωνισμός που υπάρχει στα ΜΜΕ τα κάνουν να περιορίζονται σε θέματα που ευχαριστούν τους καταναλωτές της προσφέροντας έτσι μικρή ποικιλία των θεμάτων της (ithageneis, 2010).

Σύμφωνα με μια έρευνα που πραγματοποιήθηκε στην Ελλάδα από δημοσιογράφους σε τοπικά αλλά και εθνικά μέσα προήλθαν συμπεράσματα για την αντίληψη των πολιτών στη δραστηριότητα των ΜΜΕ(Καρακατσάνης, 2010).

Καταρχήν, οι πιο πολλοί από τους ερωτηθέντες της έρευνας πιστεύουν ότι είναι καλό που υπάρχουν πολλές πηγές ενημέρωσης γιατί προωθούν τη πολυφωνία άρα και την δυνατότητα της κοινωνίας να αναπτύξει κριτική σκέψη σχετικά με τα οικονομικά και κοινωνικά δρώμενα.

Επιπλέον, οι περισσότεροι όρισαν τα ΜΜΕ ως ένα «ιδιωτικό ολιγοπώλιο» που κατευθύνεται από ανθρώπους που είναι μέρος του χώρου των επιχειρήσεων και όχι της επικοινωνίας, όπως θα έπρεπε, για αυτό και η ανταγωνιστικότητα που υπάρχει ανάμεσα στα ΜΜΕ έχει καταλυτική επιρροή στην μορφή της ενημέρωσης.

Ακόμα, πολλοί από τους ερωτηθέντες εντόπισαν μια σχέση εξάρτισης που έχει αναπτυχθεί μεταξύ του χώρου της πολιτικής και του χώρου των ΜΜΕ.

Τέλος, αναφέρθηκε η οικονομική εξάρτηση των ΜΜΕ από πόρους για να είναι λειτουργικά

και να έχουν κέρδος όπως ακριβώς δηλαδή λειτουργεί κάθε επιχείρηση.

Η έρευνα έδειξε ότι η ύπαρξη πολλών πηγών πληροφόρησης έκανε τους συμμετέχοντες να μην υιοθετούν απόψεις εύκολα και χωρίς να τις επεξεργαστούν με βάση τη κριτική τους σκέψη.

Η κρίση έπληξε το 2007 τα ΜΜΕ σε διεθνές επίπεδο, αφού η οικονομική κρίση, που χτύπησε τις αγορές ΗΠΑ και Ευρώπης, αποτέλεσε στη μείωση των διαφημιστικών και των πωλήσεων του τύπου. Η κρίση έφτασε στην Ελλάδα ένα χρόνο αργότερα(2008).Το αποτέλεσμα της κρίσης ήταν να μειωθεί η διαφημιστική δαπάνη σε δύο χρόνια 30% και να μην αγοράζουν οι πολίτες τόσο συχνά περιοδικά και εφημερίδες. Οι λόγοι της κρίσης ήταν πέρα από οικονομικές δυσκολίες η άνοδος του δωρεάν Τύπου, η αλλαγή στις συνήθειες που είχε το κοινό, η έλλειψη της ταύτισης της γνώμης των ΜΜΕ με το κοινό του, η κρίση εμπιστοσύνης των ειδήσεων των ΜΜΕ και η άνοδος του Διαδικτύου.

Εικόνα 11: Social Media

Πηγή: https://sproutsocial.com/insights/social-media-ideas/

4.1.1 Μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης αποτελούν τη κύρια πηγή ενημέρωσης, ψυχαγωγίας και επικοινωνίας των χρηστών του διαδικτύου. Μέσα κοινωνικής δικτύωσης αποτελούν το Facebook, Instagram, to Twitter κ.τ.λ. τα οποία έχουν δημιουργήσει ένα νέο κόσμο στον οποίο ο καθένας μπορεί να εκφράσει την άποψη του, τα συναισθήματα του, τις ιδέες του ελεύθερα, γρήγορα και εύκολα.

Τα μέσα κοινωνικής δικτύωσης παρέχουν πολλές θετικές επιπτώσεις όπως είναι η κοινωνικοποίηση με νέα άτομα που επιτρέπουν την αλληλεπίδραση των χρηστών τους με σκοπό να ανταλλάσουν μεταξύ τους πληροφορίες και να επικοινωνούν όσο τακτά οι ίδιοι επιθυμούν. Οι χρήστες μπορούν με αυτόν τον τρόπο να έρθουν σε επαφή με άτομα που βρίσκονται σε άλλη πόλη, χώρα σε μηδέν χρόνο και να επικοινωνήσουν με άτομα που δεν θα μπορούσαν να γνωρίσουν στη καθημερινή τους ζωή. Οι χρήστες, λοιπόν, μέσω κάποιας εφαρμογής που προσφέρουν τα μέσα κοινωνικής δικτύωσης μπορούν να ενημερωθούν έμμεσα από συνομιλητή τους για ένα συμβάν που συνέβη στη χώρα τους, για τα ήθη και τα

έθιμα τους, για τη κουλτούρα τους κ.τ.λ. Ο ένας τρόπος ενημέρωσης είναι αυτός και ο άλλος τρόπος είναι μέσω των προφίλ που φιλοξενούν τα μέσα κοινωνικής δικτύωσης ή μέσω των ιστοσελίδων που έχουν δημιουργηθεί και έχουν ως θέμα τους την ενημέρωση των χρηστών τους. Τα μέσα κοινωνικής δικτύωσης αποτελούν μια σημαντική πηγή ειδήσεων που είναι πιο προσιτά στο κοινό τους και μπορούν να μεταφέρουν τα νέα από της μια μεριά του κόσμου μέχρι την άλλη με μεγάλη ταχύτητα. Επίσης, δίνουν φωνή στους χρήστες τους, αφού τους αφήνουν να σχολιάσουν μια είδηση και να εκφράσουν τη γνώμη τους φέροντας στο προσκήνιο μια νέα συμμετοχική δημοσιογραφία. Επομένως, οι πολίτες μπορούν να επικοινωνούν και να ενημερώνονται ταυτόχρονα έχοντας πλέον κατακτήσει μια εξουσία στο κόσμο της ενημέρωσης αφού μπορούν να επηρεάσουν με τα σχόλια τους την σημασιολογία μιας είδησης (Κόνσουλας, 2014).

Ακόμα, έχουν συμβάλλει και στο τομές της παιδείας αφού τα παιδιά από πολύ μικρή ηλικία πλέον ξεκινούν να διαχειρίζονται τις πλατφόρμες κοινωνικής δικτύωσης και να μπορούν να επικοινωνήσουν μέσω αυτών. Το χρησιμοποιούν, επιπλέον, και για να τελειοποιήσουν μια εργασία στο σχολείο τους αφού το φάσμα των πληροφοριών για ότι και αν ψάχνουν είναι τεράστιο. Έχουν την δυνατότητα να πληροφορηθούν είτε για πληροφορίες απλοϊκές είτε περίπλοκες και άρα να επιλέξουν οι ίδιοι το βαθμό της δυσκολίας που επιλέγουν.

Η πληροφόρηση, γενικά, από τα μέσα κοινωνικής δικτύωσης είναι πιο ευχάριστη διότι συνοδεύεται συνήθως από υλικό όπως εικόνες, βίντεο, ήχο κ.α. και έτσι κάνουν μια είδηση πιο ευχάριστη και πιο κατανοητή σε σχέση με ένα απλό άρθρο. Όταν μια πληροφορία, οποιασδήποτε προέλευσης, παρουσιάζεται με ευφάνταστο τρόπο και με χρήση οπτικοακουστικού υλικού προτιμάται από έναν χρήστη και επαληθεύει με κάποιο τρόπο την αντικειμενικότητά της.

Η δυνατότητα αλληλεπίδρασης που προσφέρουν τα μέσα κοινωνικής δικτύωσης σε εικόνες, άρθρα, βίντεο ενός χρήστη με κάποιου άλλου ή ιστοσελίδας οδηγεί και σε ένα τρόπο ψυχαγωγίας των χρηστών του. Ακόμα και οι σελίδες με εκπαιδευτικό χαρακτήρα που φιλοξενούνται στο διαδίκτυο βάζουν κουΐζ και κάποιου είδους παιχνιδιού στους χρήστες τους για να λάβουν γνώσεις με το πιο εύκολο και διασκεδαστικό τρόπο που γίνεται. Πέρα από αυτά προσφέρονται και παιχνίδια ηλεκτρονικά προς τους χρήστες τους που τα πιο εξελιγμένα τους παραπλανούν σε ένα εικονικό κόσμο που αγγίζει τα όρια του αληθινού. Επιπλέον, σε πολλά παιχνίδια των μέσων κοινωνικής δικτύωσης, τα μέλη τους πρέπει να συνεργάζονται μεταξύ τους για να παίξουν σε ένα παιχνίδι οπότε αρχίζουν άγνωστοι μεταξύ αγνώστων να επικοινωνούν μεταξύ τους (Κόνσουλας, 2014).

Τα μέσα κοινωνικής δικτύωσης, έχουν εισβάλει σε πολλούς τομείς της καθημερινότητας ενός ανθρώπου λόγω των απεριόριστων δυνατοτήτων που προσφέρει και αποτελεί μια νέα αναπτυσσόμενη δύναμη της τεχνολογίας.

4.2 ΔΙΑΔΙΚΤΥΑΚΗ ΕΝΗΜΕΡΩΣΗ

Η διαδικτυακή ενημέρωση έχει πάρει της σκυτάλη της ενημέρωσης αφήνοντας πίσω της τη τηλεόραση και την έντυπη δημοσιογραφία. Το διαδίκτυο με τη ποικιλομορφία και το εύρος της ενημέρωσης που προσφέρει έχει κεντρίσει το ενδιαφέρον του κοινού που πλέον επιλέγουν να ενημερωθούν από ιστοσελίδες ενημέρωσης και από ψηφιακά μέσα. Μεγάλο ποσοστό του κοινού ενημερώνονται από τους ισότοπους κατά τη διάρκεια της εργασίας του για 3 με 5 λεπτά δηλαδή σε όσο χρόνο μπορούν να ξεκλέψουν από τη δουλειά τους για να πάρουν μια ανάσα. Η ενημέρωση γίνεται δωρεάν και είναι διαθέσιμη όλο το 24ωρο για το κοινό του στο διαδίκτυο. Οι αναγνώστες μπορούν να συμμετέχουν στις ειδήσεις ανώνυμα γράφοντας τα σχόλια τους ή συμμετέχοντας σε ομαδικές συζητήσεις. Ακόμη και οι δημιουργοί των ιστοσελίδων μπορούν να κρατήσουν την ανωνυμία τη δική τους και των πηγών τους αν θελήσουν. Έτσι το διαδίκτυο με την ευχρηστία του και τις δυνατότητες που προσφέρει αρχίζει να κερδίζει έδαφος στη προτίμηση του κοινού για ενημέρωση παίρνοντας τη πρωτοκαθεδρία από τα παραδοσιακά ΜΜΕ. (Χατζηαναστασίου, 2011).

Η επικοινωνία που αναπτύσσεται στο Διαδίκτυο γίνεται άμεση μέσω τη πληροφόρηση του πολίτη από ιστότοπους αλλά και αμφίδρομη με την ανταλλαγή απόψεων κάτω από τις ειδήσεις αλλά και τη δημιουργία μιας πληροφορίας από τον ίδιο τον πολίτη, που αρχίζει να αποκτά σιγά σιγά την ιδιότητα του παγκόσμιου πολίτη. Το πιο γνωστό μέσω αλληλεπίδρασης αναγνωστών είναι τα ιστολόγια (blogs) που μπορεί ο καθένας να εκφράσει τη γνώμη του για όλα τα θέματα (Φέσιας, 2016).

Ο χρήστης του διαδικτύου μπορεί να επιλέξει όποια είδηση θέλει για ανάγνωση η οποία είναι συνήθως σύντομη και παραπέμπει και σε άλλες ιστοσελίδες μέσω των υπερσυνδέσμων για παραπάνω ενημέρωση αν ο χρήστης το επιθυμεί. Η είδηση είναι επίκαιρη και ζωντανή για επιτόπου ενημέρωση του χρήστη αλλά και για ταυτόχρονη αλληλεπίδραση με άλλους χρήστες.(Κόμλου, 2011).

Επίσης, ο χρήστης όποτε θελήσει μπορεί να κατατρέξει σε παλιότερες ειδήσεις που δεν πρόλαβε να ενημερωθεί και τον ενδιαφέρουν. Οι ειδήσεις δεν έχουν γεωγραφικό όριο αφού είναι διεθνείς και είναι διαχωρισμένες ανάλογα με το περιεχόμενο τους(πολιτικές, κοινωνικές, αθλητικές κ.τ.λ.) Ο χρήστης επιλέγει όποιο τομέα ενημέρωσης επιθυμεί χωρίς να χρειάζεται να προσπεράσει τους άλλους. Γενικά, είναι αυτόνομος στην ενημέρωση που θέλει να εκλάβει και να ενημερωθεί. Ενημερώνεται άμεσα ακόμη και για γεγονότα που συμβαίνουν στην άλλη άκρη της γης αφού όλες οι ειδήσεις αναρτώνται απευθείας στο διαδίκτυο από ιστοσελίδες που σκοπό για τη καθεμία να είναι η πρώτη που θα την “ανεβάσει”. Έτσι μπορεί ακόμα ο ελληνικός λαός να επικοινωνήσει με ένα ξένο λαό για να σιγουρευτεί για την εγκυρότητα της ειδήσεις και να μάθει περισσότερες πληροφορίες. (Χατζηαγγελάκη, 2013).

Μια νέα εποχή έχει επέλθει στην ενημέρωση με κύριο πρωταγωνιστή της το Διαδίκτυο. Οι πολίτες αν και ακόμα ενημερώνονται από τα παραδοσιακά μέσα, ταυτόχρονα αρχίζουν να γοητεύονται από τη πληθωρικότητα που συσπειρώνουν τις ειδήσεις στο διαδίκτυο. Το διαδίκτυο διαθέτει ευελιξία και δίνει τη δυνατότητα στους χρήστες του να γίνουν μέρος της παραγωγικής διαδικασίας των ειδήσεων της εύκολα και γρήγορα. Μια φράση που λέει πολλά είναι «η φωνή ενός άγνωστου blogger μπορεί να ακουστεί σε χιλιάδες χρήστες, δυνατότητα,

που στα ΜΜΕ πληρώνεται ακριβά. Το διαδίκτυο εγγυάται ότι αυτή η φωνή έχει ίση αξία, ειδικά αν συνδεθεί με τους κεντρικούς πόλους του παγκόσμιου ιστού» (Παπάνης Ε., 2011)

Για την επιτυχία ενός ηλεκτρονικού εντύπου σημαντικό συστατικό παίζει η αμφίδρομη επικοινωνία που αναπτύσσεται μεταξύ των αναγνωστών και της ιστοσελίδας. Οι αναγνώστες επιλέγουν να ξαναεπισκέπτονται σελίδες που έχουν ειδήσεις που τους ενδιαφέρουν και που δίνουν τη δυνατότητα να εκφέρουν την άποψη τους και να επικοινωνήσουν. (Χατζηαναστασίου, 2011).

Τα ΜΜΕ εννοείται πως είναι ένα αναπόσπαστο κομμάτι της κοινωνίας που πρέπει να έχουν κάποια κανονιστικά πλαίσια έτσι ώστε να παρέχουν έγκυρη και ακριβής επικαιρότητα χωρίς την αλλοίωση της από απολιτικές και άλλες παρεμβάσεις. Ο πολίτης με αυτό τον τρόπο θα έχει μια καθαρή εικόνα για τα δρώμενα και θα έχει αναπτύξει τη κριτική του σκέψη ανεπηρέαστος από εξωτερικά συμβάντα.

4.2.1 Παθητικοί θεατές

Η νεολαία είναι ο τομέας της κοινωνίας που έχει επηρεαστεί περισσότερο από τη ψηφιακή εποχή και που είναι γνώστες της διαχείρισης του. Κάθε μέρα περνούν όλο και περισσότερες ώρες μπροστά από τον υπολογιστή και διαβάζουν ειδήσεις, στέλνουν μηνύματα μέσω των μέσων κοινωνικής δικτύωσης, παίζουν παιχνίδια, κάνουν chat με αγνώστους, δημοσιεύουν υλικό στους λογαριασμούς που διαθέτουν, χρησιμοποιούν το λεξιλόγιο greeklish κ.τ.λ. Γενικά ενημερώνονται από το διαδίκτυο και όχι από τα παραδοσιακά μέσα (Παπασίμος , 2016).

Οι νέοι αρχίζουν να εμπιστεύονται περισσότερο ότι θα διαβάσουν σε ένα blog ή site και όχι αυτό που θα ακούσουν από την τηλεόραση. Ο κάθε ένας ανάλογα με αυτά που διαβάζει στο επώνυμο ή ανώνυμο site και ανάλογα τα πιστεύω(τη κουλτούρα, το πολιτισμό του) κ.τ.λ. του αποφασίζει αν θα εμπιστευτεί ή όχι την είδηση.

Η τηλεόραση που αποτελεί το ισχυρότερο μέσο επικοινωνίας διεθνώς αρχίζει σταδιακά να χάνει έδαφος και να υπερισχύει έναντι αυτής οι νέες μορφές επικοινωνίας που προσφέρει το διαδίκτυο(διαδραστικές και αμφίδρομες)(Γιακουμής, 2012).

Δυστυχώς όμως ξεκίνησε με λάθος τρόπο στην Ελλάδα αυτή η νέα τάση όπως ακριβώς είχε συμβεί και με τα ιδιωτικά ΜΜΕ. Το 1989, τα ιδιωτικά ΜΜΕ, άνοιξαν τις πύλες τους και επέβαλαν απευθείας ένα συγκεκριμένο τρόπο παρακολούθησης που ακόμα και σήμερα σοκάρει όπως ακριβώς συνέβη και με κάποια μέσα του διαδικτύου που προφανώς δημιουργήθηκαν με διαφορετικούς σκοπούς αντί την ενημέρωση (προσωπικό κέρδος, φιλοδοξίες, άνομους στόχους κ.τ.λ.). Βέβαια, υπάρχουν εξαιρέσεις με σοβαρούς ιστότοπους ενημέρωσης.

Ο κυριότερος λόγος στροφής των πολιτών στο Διαδίκτυο είναι ότι έχουν καταλάβει ότι τα

παραδοσιακά ΜΜΕ επηρεάζονται από την πολιτική και τα συμφέροντα της κάθε επιχείρησης ενώ πιστεύουν ότι το διαδίκτυο τους χαρίζει την ελευθερία κρίσης και γνώμης (Τατάλια-Λίτσου, 2014).

Γνωστό είναι οι εξωτερικές δραστηριότητες των ιδιοκτητών των ΜΜΕ σε κάδους όπως την ναυτιλία (Αλαφούζος, Μαρινάκης, Κυριακού), στις κατασκευές(Μπόμπολα), στα πετρέλαια (Βαρδινογιάννης) κ.α. Οπότε, το MEGA δεν θα ανέφερε ποτέ αρνητικά στα διόδια που έχουν επιβληθεί στις εθνικές οδούς, ο ΣΚΑΙ θα υποστηρίζει έμμεσα τον Παναθηναϊκό κ.τ.λ. Άρα, στην Ελλάδα δε μπορεί κανείς να μιλήσει για ανεξαρτησία των ΜΜΕ αφού προπαγανδίζουν πολιτικές απόψεις, παραπληροφορούν με απόκρυψη ειδήσεων, αναπαράγουν επιλεκτικές ειδήσεις και γενικά διαστρεβλώνουν τη πραγματικότητα και προγραμματίζουν την επικαιρότητα (Ασλανίδου, 2012).

Παράλληλα, τα παραδοσιακά ΜΜΕ έχουν διεκπεραιωθεί και ηλεκτρονικά. Μονοπωλιακοί όμιλοι και ολόκληρες κυβερνήσεις στην πραγματικότητα ελέγχουν το διαδίκτυο. Κάθε πληροφορία που κινείται στο διαδίκτυο μεσολαβεί μέσω μηχανισμών και διακοσμητών που διαχειρίζονται από οργανισμούς.

Υπάρχουν πολλά διαδικτυακά μέσα ενημέρωσης για να αναδειχτεί μόνο ένα και κάθε μέρα κατοχυρώνονται χιλιάδες μηνύματα αναγνωστών έτσι είναι δύσκολο να αναδειχτεί μια «φωνή»(Σιφναίος, 2011).

Τα περισσότερα διαδικτυακά μέσα δρουν στο σκοτάδι, χωρίς επωνυμία, και δε προσφέρουν κάποια γνώση στους αναγνώστες τους. Γενικά, λόγω της ανωνυμίας και της δωρεάν διατήρησης τους δεν διαθέτουν κάποια υπευθυνότητα και τα άρθρα δε διακρίνονται από επαγγελματισμό. Αυτά με τη μεγαλύτερη επισκεψιμότητα δε σημαίνει ότι είναι και τα πιο έγκυρα για αυτό και η πολιτεία θα έπρεπε να θέσει ορισμένους κανόνες για τον τρόπο ενημέρωσης που φέρει το διαδίκτυο, γιατί προσφέρει μεγάλη ελευθερία λόγου, αφού όποιος θέλει γράφει, όποιος θέλει σχολιάζει, όποιος θέλει δημιουργεί ιστοσελίδα και γενικά οτιδήποτε θέλει κάνει ο καθένας. Δηλαδή, μπορεί και ο καθένας να βρίζει, να βγάζει τα απωθημένα του, να προσβάλλει ανώνυμα ή με ψεύτικο όνομα (Τσενέ, 2012).

Για τους νέους, δεν θα πρέπει να αρκεί μόνο η πληροφόρηση αλλά πρέπει να πηγαίνουν και πιο μακριά από εκεί δηλαδή στην κατανόηση, στην ερμηνεία, στην επεξήγηση. Σίγουρα, το διαδίκτυο προσφέρει πληθώρα πληροφοριών αλλά συνήθως σύντομων που δεν μπορούν να αντικαταστήσουν την ανάγνωση βιβλίων , εφημερίδων που προσφέρουν ολοκληρωμένη γνώση για ένα ζήτημα. Όπως και μια ζωντανή συζήτηση δεν μπορεί να αντικατασταθεί από τα comments, τα tweets και γενικά τα μισόλογα των social media. (Σιφναίος, 2011).

Το θέμα είναι να μην γίνει το κοινό παθητικοί θεατές του διαδικτύου και να φιλτράρουν τις ειδήσεις που δέχονται ξεχωρίζοντας τις έγκυρες από τις δόλιες και τις ψεύτικες.

4.3 Η ελευθερία της έκφρασης στο διαδίκτυο

Η διαδικτυακή ενημέρωση έχει πάρει τα ηνία της γενικής ενημέρωσης του κοινού. Η άμεση ενημέρωση που προσφέρει στα δρώμενα αλλά και οι πολλοί διαδικτυακοί τόποι που έχουν αναπτυχθεί στο διαδίκτυο και προσφέρουν μεγάλο εύρος απόψεων έχουν κερδίσει το ενδιαφέρον του κοινού. Επίσης, τα εκατοντάδες ιστολόγια(blogs) που υπάρχουν, όπως και το πλήθος των ιστοσελίδων(sites) και του ηλεκτρονικού τύπου προσφέρουν πολλούς διαφορετικούς τύπους ενημέρωσης και συμμέτοχης των ίδιων των αναγνωστών στο σχολιασμό μιας είδησης. Επιπλέον, τα μέσα κοινωνικής δικτύωσης δεν θα μπορούσαν να μην προσφέρουν ενημέρωση πέρα από τη ψυχαγωγία εφόσον χρησιμοποιούνται από εκατομμύρια χρήστες καθημερινά (Τσενέ, 2012).

Στο άρθρο 14 παρ.1 του Συνάγματος και στο άρθρο 10 παρ.1 του ΕΣΔΑ κατοχυρώνει την ελευθερία της έκφρασης που πρέπει να υπάρχει στην ενημέρωση και να εφαρμόζεται από κάθε φορέας της αλλά και τη διάδοση των στοχασμών που πρέπει να γίνεται χωρίς φραγμούς και αποτελεί ένα βασικό στοιχείο μιας υγιής προσωπικότητας.

Το άρθρο 14 του Συντάγματος έχει ως στόχο τη «γραπτή και δια του τύπου έκφραση» οπότε κατοχυρώνει και την έκφραση γνώμης σε όλους τους φορείς της ενημέρωσης που πλέον περιλαμβάνει και το διαδίκτυο. Κάθε άποψη που εκφέρεται από ένα πρόσωπο και εκφράζει τα πιστεύω και συναισθήματα του αποτελεί έκφραση γνώμης. Δηλαδή κάθε μήνυμα, ιδέα, γεγονός είδηση που μεταδίδεται στο διαδίκτυο προστατεύεται πλέον από το Σύνταγμα ως ελευθερία έκφρασης. Επομένως, ο κάθε άνθρωπος μπορεί να μεταδίδει την άποψη του ελεύθερα είτε με τη μορφή λόγου είτε με τη μορφή μέσων(π.χ. εικόνα) σε όποιο ενημερωτικό μέσο θέλει και σε όποια στιγμή μπορεί χωρίς να αντιμετωπίσει κυρώσεις. Άρα, όροι δεν μπορούν να τεθούν ούτε από το κράτος αλλά ούτε από τον παροχέα ενός ενημερωτικού μέσου. Όπως, και το περιεχόμενο ενός ιστότοπου επικοινωνίας δεν μπορεί να οριστεί από νόμους αλλά και οι εξωτερικές συνθήκες που το επηρεάζουν (Ματζούφας , 2008).

Το κράτος υποχρεούται να καταστήσει προσιτή, σε οικονομικό αλλά και τεχνολογικό επίπεδο την πρόσβαση στο διαδίκτυο ,δίχως αυτό να σημαίνει ότι θα είναι τελείως δωρεάν, και να διευκολύνει τη πρόσβαση με όποιο υλικό μέσο μπορεί σύμφωνα με τη συνταγματική επιταγή(άρθρο 5 παρ.2 του Συντάγματος).

Είναι λογικό κάθε πληροφορία να μην είναι προσιτή σε όλους ειδικά όταν αυτή η πληροφορία αναφέρεται σε προσωπικά δεδομένα και ουσιαστικά διεισδύει στην ιδιωτική ζωή των πολιτών. Επίσης, αν αυτή η πληροφορία αφορά την ιατρική δραστηριότητα ενός πολίτη, ή αν αναφέρεται στα επαγγελματικά και τα δικηγορικά πεδία ενός πολίτη που είναι απόρρητα και τον μόνο που θα πρέπει να απασχολεί και να ενδιαφέρει είναι τον ίδιο αλλά και δραστηριότητες του κράτους που δεν πρέπει να γίνονται γνωστές. Γενικά, αν και η ελευθερία της έκφρασης συνάπτει με την «ελευθερία του πληροφορείν και του πληροφορείσθαι» πρέπει να υπάρχουν κάποια όρια και δε περιλαμβάνει το δικαίωμα της παράνομης πρόσβασης σε απόρρητα προσωπικά και κρατικά αρχεία (Φωτόπουλος, 2014).

4.3.1 Σύγκριση ενημέρωσης διαδικτύου από τα παραδοσιακά μέσα

Το διαδίκτυο διευκολύνει πολύ τους χρήστες με τις υπηρεσίες που διαθέτει στην ενημέρωση για αυτό και προτιμάτε πλέον από το μεγαλύτερο μέρος του πληθυσμού του πλανήτη ωστόσο κρύβει κάποιες παγίδες. Κάποια από τα πλεονεκτήματα και τα μειονεκτήματα που εντοπίζονται είναι:

- Στο διαδίκτυο ο κάθε άνθρωπος μπορεί να επιλέξει για ποιους τομείς της καθημερινότητας θέλει να ενημερωθεί και μπορεί να έχει ενεργητική στάση σε μια είδηση μέσω του σχολιασμού του αλλά και να αποτελεί συνάμα πομπό και δέκτη ειδήσεων και κατά εξακολούθηση πληροφοριών. Στα παραδοσιακά ΜΜΕ δεν υφίσταται κάτι τέτοιο αφού εκπέμπονται ειδήσεις που έχουν προαποφασιστεί από άλλους.
- Στο διαδίκτυο η επικοινωνία παίρνει πολλές μορφές όπως η αποστολή εικόνων, βίντεο, οι εμπορικές συναλλαγές κ.τ.λ.
- ενώ στα άλλα ΜΜΕ σπανίως υπάρχει. Συνήθως η πρόσβαση και σε εκπαιδευτικό υλικό και σε όλες τις άλλες γνώσεις είναι πιο ευχάριστη διότι κάθε υλικό συνδυάζει γραπτό με ήχο, εικόνα, βίντεο ενώ στα άλλα ΜΜΕ η είδηση μπορεί απλά να τυπώνεται.
- Αν και το διαδίκτυο χρησιμοποιείται από πολλούς ανθρώπους , ένα μεγάλο μέρος δε ξέρει ακόμα να τον χρησιμοποιεί ούτε διαθέτει έναν για αυτό και καταφεύγουν στα παραδοσιακά ΜΜΕ που είναι εύκολα διαχειρίσιμα για όλους και υπάρχουν σε κάθε σπίτι (Τσενέ, 2012).
- Ενώ και το διαδίκτυο και τα παραδοσιακά ΜΜΕ πληροφορούν για διεθνή θέματα. Τα δεύτερα επικεντρώνονται πιο πολύ στα θέματα της χώρας τους.
- Στο διαδίκτυο η σχέση πομπού και δέκτη είναι αμφίδρομη ενώ στα άλλα ΜΜΕ συνήθως όχι.
- Το διαδίκτυο ενστερνίζεται τις προτιμήσεις του κοινού στο θέμα τις ενημέρωσης και προσαρμόζεται.
- Επειδή στο διαδίκτυο ο καθένας μπορεί να δημιουργήσει ένα ιστότοπο ενημέρωσης και να μεταδίδει πληροφορίες δημιουργείται μεγάλος όγκος πληροφοριών που μπορεί να περιέχει μη έγκυρες κακογραμμένες πληροφορίες. Επίσης, μπορεί να γίνει προώθηση επικίνδυνων κυκλωμάτων μέσα από τη μετάδοση τόσων πολλών πληροφοριών. Αντίθετα, η πληροφόρηση στα άλλα μέσα ελέγχεται από ένα πλήθος ατόμων για να μην υπάρχει κατάχρηση και παραπληροφόρηση(όπως δημοσιογράφοι, εκδότες, ραδιοτηλεοπτικό συμβούλιο, ένωση συντακτών κ.α.). Ειδικά, στην εφημερίδα ή στο σταθμό-κανάλι όλες οι ειδήσεις και απόψεις που εκφέρονται είναι επώνυμα έτσι ώστε σε περίπτωση λάθους να αναλάβει ο καθένας της ευθύνες του.
- Ο Ε.Παπανούτσος έγραψε ότι το διαδίκτυο περιλαμβάνει «μια επικοινωνία πολυεπίπεδη, πολυπρόσωπη, μαζική και εξατομικευμένη» έχοντας φέρει μια επανάσταση στην ιστορία της.
- Κρίση ιδιαίτερα περνά η γλώσσα στο διαδίκτυο αφού χρησιμοποιείται

κωδικοποιημένη, με συντομεύσεις, με χρήση λεξιλογίου greeklish, με υβριστικό περιεχόμενο ενώ στα άλλα ΜΜΕ ο λόγος προσέχετε και ελέγχεται (Χαραλαμπάκης, 2011).

4.3.2 Παραπληροφόρηση

Ως παραπληροφόρηση ορίζεται η μεταφορά ψευδών πληροφοριών που δεν είναι επαληθευμένες από κάποια αληθινή πηγή. Θεωρείται ως κακή πράξη αφού συνήθως είναι σκόπιμη και αποσκοπεί σε προσωπικό όφελος έναντι του παραπληροφορούντος. Με εξαίρεση, αν η απόκρυψη πληροφοριών γίνεται με σκοπό τη προστασία ατόμων που αν γίνονταν γνωστές θα είχαν άσχημα αποτελέσματα προς αυτούς οπότε θεωρείται ως καλή και έννομη πράξη.

Ο άνθρωπος που είναι ο ίδιος πηγή παραπληροφόρηση έχει την απόλυτη ευθύνη ενώ αυτός που απλά μεταφέρει όσα έχει ακούσει ή όσα νομίζει ότι έχει γνώσεις δεν έχει μεγάλες ευθύνες αφού απλά δεν έχει ελέγξει τις πηγές του. Στη παραπληροφόρηση κατασκευάζονται πληροφορίες, παραποιούνται γεγονότα, διαβάλλονται πρόσωπα (Χαραλαμπάκης, 2011).

Όσον αφορά τις ειδήσεις που μπαίνουν στα ΜΜΕ μπορεί να είναι προϊόντα παραπληροφόρησης. Η παραπληροφόρηση μπορεί να οφείλεται στη λειτουργία των ΜΜΕ με βάση κομματικών συμφερόντων ή στη προστασία συμφερόντων που οδηγεί στην απόκρυψη στοιχείων. Οι τηλεθεατές, ακροατές, χρήστες πρέπει να ελέγχουν τη πηγή των πληροφοριών τους για να αποτραπούν από τη παραπληροφόρηση (Φωτόπουλος, 2014).

Ο Νίκος Καζαντζάκης αναφέρει ότι τα ΜΜΕ κατά κάποιον τρόπο θέτουν όρια στην ζωή ενός ανθρώπου αφού παραπέμπει στην Ασκητική τις ακόλουθες προτάσεις «Δεν ζυγιάζω, δεν μετρώ, δεν βολεύομαι! Ακολουθώ το βαθύ μου χτυποκάρδι. Ρωτώ, ξαναρωτώ χτυπώντας το χάος: ποιος μας φυτεύει στη γη σε τούτη χωρίς να μας ζητήσει την άδεια; Ποιος μας ξεριζώνει από τη γη σε τούτη χωρίς να ζητήσει την άδεια;» Με αυτές παραπέμπει τους ανθρώπους να ζήσουν τη ζωή τους χωρίς στερεότυπα και ιδανικά όπως υποδεικνύουν τα Μ.Μ.Ε.

Μέχρι πρότινος στο προσκήνιο της ενημέρωσης υπήρχαν οι ειδήσεις και οι «μη ειδήσεις». Δηλαδή, υπήρχαν τα κοινωνικοοικονομικά και πολιτικά γεγονότα που απευθύνονταν στο ευρύ κοινό και οι «μη ειδήσεις» που απευθύνονταν στο πιο ψαγμένο κοινό που ήθελε να γνωρίζει παραπάνω πληροφορίες για ένα γεγονός (Παυλίδης, 2017).

Ο διαχωρισμός αυτός των ειδήσεων αλλάζει μορφή και προστίθεται ο όρος ψεύτικες ειδήσεις (“fake news”). Οι ψεύτικες ειδήσεις υπήρχαν πάντα στο χώρο των ΜΜΕ αλλά τα τελευταία χρόνια έχουν πάρει απειλητικές και μεγάλες διαστάσεις (Καλαντζής,2018).

Οι ψεύτικες ειδήσεις δεν έχουν όλες το ίδιο βάρος εφόσον κάποιες από αυτές οφείλονται στην έλλειψη επαγγελματισμού του δημοσιογράφου ή στην άγνοια του προς το περιεχόμενο

της είδησης ενώ άλλες αλλοιώνονται σκόπιμα έτσι ώστε να εξυπηρετήσουν συγκεκριμένα συμφέροντα. Ο Αντρέας Βλάχος που είναι ένας έλληνας ερευνητής ανέφερε ότι: « άλλο είναι η λανθασμένη πληροφορία το (misinformation) κι άλλο η παραπληροφόρηση (disinformation), που γίνεται με κακή πρόθεση» (Καλαντζής,2018).

Οι ψεύτικες ειδήσεις, σήμερα, μπορούν να έχουν απτές συνέπειες και στον πραγματικό κόσμο αφού ασκούν μεγάλη επιρροή διότι αναπαράγονται και δημοσιεύονται σε πολύ μεγαλύτερο βαθμό από ότι γινόταν παλαιότερα. Το διαδίκτυο και ιδιαίτερα τα μέσα κοινωνικής δικτύωσης έχουν παίξει σημαντικό ρόλο στη διασπορά των ψεύτικων ειδήσεων αφού έχουν κάνει πολύ πιο εύκολη τη διαδικασία και πολύ πιο μαζική. Επιπλέον, στο χώρο της δημοσιογραφίας δεν υπάρχουν, πλέον, μόνο οι επαγγελματίες αλλά και οι δημοσιογράφοι-πολίτες οι οποίοι έχουν αυξήσει τον ανταγωνισμό με αποτέλεσμα να διαχέονται πλήθος ψευδών ειδήσεων. Στο διαδίκτυο, αυτό που έχει ύψιστη σημασία στις ειδήσεις είναι η επισκεψιμότητα των χρηστών για αυτό πολλοί διαδικτυακοί τόποι επιλέγουν την εύκολη λύση να χρησιμοποιήσουν τις ειδήσεις δολώματα που δεν έχουν καμία σχέση με τη πραγματικότητα (click-bait). Επίσης, επειδή όλοι οι ιστότοποι θέλουν να έχουν τα πρωτεία μιας είδησης, κάποιες από αυτές προτρέχουν να δημοσιεύσουν μια είδηση πριν τη διασταυρώσουν. Έτσι, οι χρήστες διαβάζουν και αναδημοσιεύουν μια ψεύτικη είδηση χωρίς να το έχουν καταλάβει και αυτό οφείλεται και στο φαινόμενο του ψηφιακού αναλφαβητισμού των χρηστών του διαδικτύου που δεν μπορούν να κρίνουν οι ίδιοι την εγκυρότητα του μηνύματος που λαμβάνουν (Παυλίδης, 2017).

4.4 Ο ρόλος των ΜΜΕ στη ζωή των εφήβων

Οι έφηβοι τείνουν να βρίσκονται στη δική τους πραγματικότητα και να βλέπουν τον κόσμο με άλλα μάτια. Σε αυτό τον κόσμο έρχεται να προστεθεί και ο νέος πολύπλοκος κόσμος του διαδικτύου. Ο κόσμος αυτός έχει εισβάλει σαρωτικά στη ζωή όλων των ανθρώπων αλλά ιδιαίτερα των εφήβων που τείνουν να έχουν εθιστική τάση σε όλα τα νέα μέσα που προσφέρει το διαδίκτυο.

Τα κινητά τηλέφωνα είναι ένα μέσο επικοινωνίας των ανθρώπων και χρησιμοποιείται ευρέως από όλες τις ηλικίες. Με τη πάροδο του χρόνου τα κινητά τηλέφωνα εξελίχθηκαν και πλέον προσφέρουν, πέραν της τηλεφωνικής επικοινωνίας και την αποστολή μηνυμάτων, τη πλοήγηση στο διαδίκτυο, την αποστολή φωτογραφιών και βίντεο, την ηλεκτρονική αλληλογραφία, την ηλεκτρονική αγορά (Χαραλαμπάκης, 2011).

Τα καινούρια κινητά διαθέτουν όλα σύνδεση στο διαδίκτυο μέσω των mb ή του wifi και έχει σταθερή διάρκεια όλη τη μέρα. Το κινητό τηλέφωνο έχει γίνει προέκταση της ζωής του εφήβου που το χρησιμοποιεί ανελλιπώς για κάθε είδους επικοινωνία καθημερινά (Φέσιας, 2016).

Είναι ένα μέσο που έχει γίνει μια κύρια πηγή σύνδεσης στο διαδίκτυο και ενημέρωσης από

αυτόν. Ένας έφηβος περνά ώρες για να εξερευνήσει τις νέες δυνατότητες που του προσφέρει το διαδίκτυο και γενικά είναι μια περίοδος της ζωής του που εξερευνά και την ίδια τη προσωπικότητα του. Οι έφηβοι χρησιμοποιούν σε μεγάλο βαθμό το διαδίκτυο σε σχέση με τα παιδιά αλλά όσο περνάει ο καιρός τα παιδιά αρχίζουν να μπαίνουν στο χώρο της τεχνολογίας σε όλο και μικρότερη ηλικία με αποτέλεσμα πολλές φορές να γνωρίζουν περισσότερα από τους ίδιους τους γονείς. Τα παιδιά παροτρύνονται, πλέον, από τους δασκάλους τους να ψάξουν πληροφορίες στο διαδίκτυο για μια εργασία τους και στη τάξη μέσω διαδραστικών παιχνιδιών μαθαίνουν πώς να το χρησιμοποιούν. Τα παιδιά μαθαίνουν πώς να έρχονται σε επαφή με τον κόσμο, πώς να πληροφορούνται μέσα από αυτόν, πως θα τους διευκολύνει σε θέματα της καθημερινότητας του (Βερβέρη, 2017).

Τα παιδιά, όμως, όπως και οι έφηβοι που τα ζούνε όλα στο έπακρο αρχίζουν να προσκολλώνται στον υπολογιστή και να απομακρύνονται από τις αληθινές σχέσεις που προσφέρει ο πραγματικός κόσμος. Το διαδίκτυο τους προσφέρει τον αλληλεπιδραστικό ρόλο που αναζητούν και τους βγάζει από τη θέση του θεατή που είχαν μέχρι τότε στα άλλα μέσα ενημέρωσης (Χαραλαμπάκης, 2011).

Στο διαδίκτυο, οι έφηβοι μπορούν να ασχολούνται με πολλές δραστηριότητες ταυτόχρονα όπως είναι τα ηλεκτρονικά παιχνίδια, οι ηλεκτρονικές αγορές, να κάνουν τα μαθήματα τους, να κατεβάζουν μουσικής. Γενικά, οι έφηβοι το χρησιμοποιούν για την επικοινωνία τους με τους φίλους τους είτε είναι γνωστοί και άγνωστοι, ως ένα πολιτισμικό εργαλείο, ως μια πηγή γνώσης.

Το διαδίκτυο είναι πολύπλοκο και κοινωνικά όπως είναι η τηλεόραση και τεχνικά όπως είναι ο υπολογιστής. Οι έφηβοι το χρησιμοποιούν πιο πολύ ως κοινωνικό μέσο στο οποίο συναναστρέφονται ευκολότερα με άλλα άτομα και ανταλλάσουν γνώσεις με αυτά αλλά και ενημερώνονται για θέματα που τους ενδιαφέρουν όπως είναι η σεξουαλικότητα, οι σχέσεις μεταξύ ανθρώπων που στη καθημερινότητα τους θα ντρεπόντουσαν να ρωτήσουν (Βερβέρη, 2017).

Στο διαδίκτυο, οι περισσότεροι άνθρωποι εκφράζονται ευκολότερα και μοιράζονται σκέψεις που σε μια «κατά πρόσωπο» επικοινωνία δε θα τολμούσαν. Έτσι ανοίγονται συναισθηματικά ακόμα και σε ξένους και ανταλλάσουν πληροφορίες για όλα τα πιστεύω τους, χωρίς ενδοιασμούς, ενημερώνοντας ο ένας τον άλλον για αληθινά γεγονότα.

Αυτή η επικοινωνία μπορεί να γίνει και με ανθρώπους από άλλες χώρες και άρα να μάθουν οι έφηβοι έγκυρες πληροφορίες σχετικά με τα ήθη και έθιμα άλλου πολιτισμού, σχετικά με τα κοινωνικά φαινόμενα που επικρατούν εκεί και γενικά να απορροφήσουν γνώσεις που οι ίδιοι θα επιλέξουν να πληροφορηθούν και όχι όσα οι άλλοι θέλουν να προβάλλουν όπως συμβαίνει στη τηλεόραση. Επίσης, μπορεί να θέλει να ρωτήσει για ένα συμβάν που είδε στη τηλεόραση και δεν επαρκούσαν οι πληροφορίες που έδινε για να το καταλάβει (Χαραλαμπάκης, 2011).

Ακόμα, πέρα από τα μηνύματα μπορεί να ενημερωθεί και μέσω ιστότοπων που έχουν παγκόσμιο χαρακτήρα στο διαδίκτυο και πληροφορούν άμεσα για όλες τις ειδήσεις. Ιδιαίτερα, η δυνατότητα σχολιασμού που προσφέρει κεντράρει ένα έφηβο να κάνει ερωτήσεις

για ένα συμβάν που στη καθημερινότητα του θα ντρεπόταν να ειπωθεί μην τυχόν και τον περάσουν για ανίδεο, αλλά και να δει τις γνώμες άλλων ατόμων και να υιοθετήσει όποια τον κεντράρει.

Επίσης, ακόμα και στα ηλεκτρονικά παιχνίδια υπάρχει φόρμα επικοινωνίας των παικτών για να συνεννοούνται μεταξύ τους και να συνεργάζονται ως προς τις νίκες. Ο καθένας, μπορεί να αναφέρει όρους και κανόνες που γνωρίζει για το παιχνίδι και οι άλλοι αγνοούν(Βερβέρη, 2017).

Επιπλέον υπάρχουν και τόποι ομαδικών συζητήσεων όπως τα chat rooms που έφηβοι μπαίνουν, γνωστοί και άγνωστοι μεταξύ τους, για να επικοινωνήσουν μεταξύ τους και να πληροφορήσουν για αυτά που έμαθαν σήμερα ή για το πώς πέρασαν τη γνώμη τους μεταδίδοντας γνώσεις χωρίς τον γνωρίζουν. Είναι ένα πολύ καλό μέσο που προσφέρει το διαδίκτυο γιατί γενικά οι έφηβοι ενστερνίζονται πιο εύκολα απόψεις και πληροφορίες από συνομήλικους τους παρά από ενήλικες (Φέσιας, 2016).

4.4.1 Mobile journalism

Η εξέλιξη των μέσων κοινωνικής δικτύωσης επέφερε μεγάλες αλλαγές στο καταμερισμό του ειδησεογραφικού περιεχομένου όπως και στην ενημέρωση και γενικότερα στη πρόσβαση σε αυτά. Μέρος αυτής της εξέλιξης υπήρχε και η κινητή τηλεφωνία όπου τα κινητά της νέας γενιάς που ήρθαν στο προσκήνιο πρόσφεραν στους κατόχους τους τη δυνατότητα πρόσβασης τις ειδήσεις εικοσιτέσσερις ώρες το εικοσιτετράωρο σε οποιοδήποτε μέρος και αν βρίσκονται. Υπάρχουν ειδικές εφαρμογές πρόσβασης, τα mobile applications, από τα οποία ο χρήστης μπορεί να ενημερώνεται είτε από το κινητό του είτε από το tablet για ότι συμβαίνει σε όλο τον κόσμο. Αυτή η νέα μορφή δημοσιογραφίας είναι που αποτελεί το «mobile journalism». Το περισσότερο χρόνο οι χρήστες των «έξυπνων» κινητών συνήθως το περνάνε στο Facebook και στα κοινωνικά δίκτυα.

Αξιότιμες εταιρίες πληροφορικής και εξέχουσας σημασίας ΜΜΕ όπως και τα ίδια τα social media αρχίζουν να επενδύουν στο καταμερισμό ειδησεογραφικού περιεχόμενου σε μέσα κοινωνικής δικτύωσης διότι προβάλει μεγάλη ανάπτυξη (Μαργαρίτη, 2016).

Πρώτα από όλα, το Facebook δημιούργησε ένα λογισμικό που αφορά τα κινητά με λογισμικό iPhone και Android, και δίνει πρόσβαση στους δικτυωμένους χρήστες σε περιεχόμενα ειδησεογραφικών μέσων που χρησιμοποιούν την υπηρεσία «Instant Articles». Παράλληλα, το Facebook σε συνεργασία με το Storyful έχει κατασκευάσει μια υπηρεσία που απευθύνεται αποκλειστικά σε δημοσιογράφους με υλικό όπως βίντεο, φωτογραφίες, θέματα που να έχουν σχέση με την ενημέρωση και ονομάζεται «Facebook Newswire»(Roberts, 2016).

Το Twitter, όντας ένα ακόμη διαδεδομένο μέσον κοινωνικής δικτύωσης, δημιούργησε την υπηρεσία «Moments» που προσφέρει ενημέρωση από μεγάλα δίκτυα ειδήσεων παγκοσμίως με χρήση ζωντανού υλικού και απευθύνεται τόσο στους χρήστες όσο και τους

δημοσιογράφους.

Στο Facebook ανήκει και η πλατφόρμα WhatsApp, στην όποια ανταλλάσσονται μηνύματα από τους εκατομμύρια χρήστες που τη χρησιμοποιούν και είναι οι πιο πολύ σε νεαρή ηλικία, και τη χρησιμοποιούν ο Guardian, το BBC, η Huffington Post, οι Financial Times και άλλα που είναι ειδησεογραφικά μέσα και θέλουν να μεταδώσουν το περιεχόμενο τους (Bell, 2016).

Η Google δημιούργησε και αυτή με τη σειρά της μια πλατφόρμα ενημέρωσης με την οποία κατάφερε να επιταχύνει τη σύνδεση στο διαδίκτυο στα κινητά που ονομάζεται «Accelerated Mobile Pages» (AMP). Επεκτάθηκε, επίσης και στη δημιουργία μιας εφαρμογής που συνεργαζόταν με πολλά κοινωνικά δίκτυα και παροχείς τεχνολογίας (Pinterest, Chartbeat, Twitter, Parsely LinkedIn), αλλά και μέσα ενημέρωσης (The Financial Times, The New York Times, Hearst, , The Posts Washington and Huffington Post Vox Media, Gannett). με σκοπό την επιλογή της είδησης από τους χρήστες από μεγάλη ποσότητα παροχών. Οι συνεργάτες αυτής της εφαρμογής από την άλλη πλευρά μπορούν να διαφημίζουν τα προϊόντα τους (Galvin, 2016).

Η ενημέρωση όπως αποδεικνύεται γίνεται πιο εύκολα και γρήγορα μέσω των social media και κατ επέκταση του κινητού τηλεφώνου που έχουν πρόσβαση σε ειδησεογραφικά προϊόντα. Η πρόσβαση στην ενημέρωση πλέον για τους πολίτες είναι δωρεάν ή με ελάχιστο κόστος και γίνεται σε οποιοδήποτε μέρος βρίσκονται, σε απευθείας σύνδεση αν επιθυμούν και παγκόσμια. Η κατανομή του ειδησεογραφικού προϊόντος έχει απεξαρτηθεί από τα παραδοσιακά μέσα (ραδιόφωνο, εφημερίδα, τηλεόραση) που έχουν βρεθεί στο περιθώριο στο τομέα της ενημέρωσης σε σχέση με το Διαδίκτυο. Οι κινητές συσκευές κερδίζουν έδαφος στην ενημέρωση και εμφανίζονται συνεχώς καινούριες όπως είναι τα smart watch που λειτουργούν επακριβώς όπως ένα κινητό, έχουν δυνατότητα πρόσβασης στο διαδίκτυο, εφαρμογές, λειτουργίες όπως τα κινητά, πολυμεσικό υλικό (Φέσιας, 2016).

4.4.2 Διαδικτυακός εθισμός

Αυτό που απασχολεί ιδιαίτερα είναι ο χρόνος που αφιερώνουν στα ΜΜΕ οι έφηβοι (διαδίκτυο, τηλεόραση, βιντεοπαιχνίδια κ.τ.λ.). Οι γονείς προσπαθούν συνήθως με χρονικά όρια να περιορίσουν τη πλοήγηση των παιδιών τους, προσπάθεια που αντιμετωπίζεται αρνητικά από εκείνα αλλά και εμφανίζει δυσκολίες στην εφαρμογή τους.

Καταρχήν, όταν οι γονείς έχουν μια πολυάσχολη μέρα, προτρέπουν οι ίδιοι τα παιδιά τους να χρησιμοποιήσουν τα μέσα ως μέθοδο αντιπερισπασμού και ελέγχου. Επίσης, οι ίδιοι οι γονείς περνούν πολλές ώρες να ασχολούνται με τα μέσα αλλά και αποτελούν ένα εργαλείο για όλες τις δουλειές της καθημερινότητας. Τέλος, υπάρχει ένας άγραφος κανόνας ότι τα παιδιά μπορούν να περνούν το σαββατοκύριακο με όποιο τρόπο θέλουν (Χαραλαμπάκης, 2011).

Γενικά ο εθισμός στο διαδίκτυο αποτελεί ένα φαινόμενο συχνό στους εφήβους ειδικά όταν οι

έφηβοι έχουν μια καταθλιπτική τάση ή είναι υπερκίνητα και προέρχονται από οικογένεια με έναν γονέα ή από οικογένεια που είναι δυσλειτουργική. Δυστυχώς, αυτή η μορφή εξάρτισης είναι καταστροφική με αποτέλεσμα τα παιδιά να προσκολλώνται στο διαδίκτυο και να αποκολλώνται από τον πραγματικό κόσμο (Φέσιας, 2016).

Αρχικά, ο χρήστης θεωρεί ως τη πιο σημαντική πτυχή της ζωής του τον υπολογιστή του. Το άτομο για να νιώσει ευχαρίστηση θέλει να περνά πολλές ώρες μπροστά από τον υπολογιστή. Οι έφηβοι περνάει αμέτρητες ώρες σε διαδραστικές λειτουργίες του διαδικτύου όπως είναι οι ομαδικές λειτουργίες, αποκόπτοντας του από το πραγματικό κόσμο και δημιουργώντας του την εντύπωση ότι κάπου αρχίζει να έχει πρόβλημα και να υστερεί. Όλα αυτά προκαλούν δυσλειτουργία για τη καθημερινότητα του εφήβου αφού τον απομακρύνει από την οικογένεια και τους συνομήλικους του, περιορίζει τα χόμπι του και αυξάνει το κίνδυνο της παχυσαρκίας, αρχίζει να εμφανίζει προβλήματα όρασης λόγω των ωρών που περνά μπροστά από την οθόνη του υπολογιστή. (Χαραλαμπάκης, 2011).

Με την ανεξέλικτη χρήση αργότερα εμφανίζονται και πιο σοβαρές επιπτώσεις που έχει να κάνει με την ασφάλεια τους όπως είναι η πορνογραφία, η κλοπή προσωπικών δεδομένα, η διαδικτυακή εγκληματικότητα, το cyber bullying κ.τ.λ. Οι γονείς θα παίξουν καίριο μέρος στο περιορισμού αυτού του εθισμού και στην ασφάλεια των παιδιών τους με τον έλεγχο του χειρισμού του διαδικτύου, με τη συνεχή επαγρύπνηση, με τη παρότρυνση των παιδιών τους για εξωσχολικές δραστηριότητες, με την ενεργή αντιμετώπιση όλων των εμποδίων που θα εμφανιστούν(Τατάλια-Λίτσου, 2014).

Αν οι γονείς δεν καταφέρουν να προλάβουν κάποια άνομη δραστηριότητα ενάντια των παιδιών τους τότε το κράτος και οι νόμοι του είναι εκεί για να επιλύσουν το πρόβλημα.

4.5 Νομιμοποίηση των ΜΜΕ

«Νόμος για το διαδίκτυο, δεν υπάρχει. Για την ακρίβεια, νόμος δεν χρειάζεται. Όπως δεν υπάρχει νόμος για το χαρτί, για τη μηχανή του fax, τη συσκευή της τηλεόρασης και του ραδιοφώνου. Εφαρμόζεται όμως στο διαδίκτυο όλο το γνωστό νομικό πλαίσιο που ισχύει για τα υπόλοιπα μέσα επικοινωνίας.»(«Δίκαιο & Internet» του Ιωάννη Καράκωστα, 2009).

Η έννοια «Μέσο Ενημέρωσης» ταυτίζεται με το περιεχόμενο και όχι με το περίβλημα που συνθέτει την εμφάνιση του (τεχνολογία μετάδοσης, υλικό κατασκευής). Έτσι το διαδίκτυο μπορεί να θεωρηθεί ένα Μέσο Ενημέρωσης (Μπαζαίος, 2009).

Αν πρωταρχικό ρόλο έπαιζε η εξωτερική εμφάνιση τότε θα υπήρχε νόμος σχετικά με τις προδιαγραφές που θα έπρεπε να χει το χαρτί ή τα υλικά κατασκευής του ή ο εκτυπωτής κ.α. για να τυπωθεί μια εφημερίδα. Φυσικά, νόμοι σαν αυτούς δεν πρόκειται να υπάρξουν για αυτό και μια εφημερίδα μπορεί να εκτυπωθεί με οποιοδήποτε τρόπο ακόμα και να προβληθεί στη τηλεόραση, σε ένα ολόγραμμα και γενικά σε όποιο μέσο αφήνει η τεχνολογία.

Όποιοι κανόνες ισχύουν σε μια κοινωνία οι ίδιοι ισχύουν και στο διαδίκτυο εφόσον αποτελεί μια καινούρια κοινωνική πραγματικότητα. Μια κοινωνία οπότε δεν γίνεται να μην περιβάλλεται από κανόνες που θα διασφαλίσει την ήρεμη ροή της.

Επειδή ένα μέσο ενημέρωσης ορίζεται από το περιεχόμενο του μια ιστοσελίδα που ποστάρει πληροφορίες θεωρείται μέσο ενημέρωσης και οι πληροφορίες αυτές παρουσιάζονται ως μέσο ενημέρωσης.

Άλλος ένας όρος που πρέπει να διευκρινιστεί είναι η «Επιχείρηση Μέσων Ενημέρωσης». Συνεπώς, όπως ο νόμος 3414/2005 (ΦΕΚ Α' 279/2005) ορίζει την «Επιχείρηση Μέσων Ενημέρωσης» ως μια νομική οντότητα που λειτουργεί με βάση της δικαιοδοσίας του Ελληνικού κράτους ανάλογα με τις διατάξεις που έχει θεσπίσει στο άρθρο 3 του ποινικού κώδικα 100/2000 (ΦΕΚ 98 Α΄) και δραστηριοποιείται :

« α) την έκδοση εφημερίδων ή περιοδικών, σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία, ή εντύπων που περιέχουν ύλη, πολιτικού ή οικονομικού χαρακτήρα, σε οποιαδήποτε μορφή εκδίδονται, διαδίδονται ή διανέμονται, συμπεριλαμβανομένης της ηλεκτρονικής, ή

β) την εγκατάσταση και λειτουργία ή τη διαχείριση τηλεοπτικού σταθμού ή την εκπομπή ή μετάδοση τηλεοπτικού σήματος, με οποιαδήποτε μορφή ή τρόπο, όπως είναι η ελεύθερη λήψη, καλωδιακή, συνδρομητική, δορυφορική, ψηφιακή, ενσύρματη, ασύρματη, σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία [1], ή

γ) την εγκατάσταση και λειτουργία ή τη διαχείριση ραδιοφωνικού σταθμού ή εκπομπής ραδιοφωνικού σήματος με οποιαδήποτε μορφή, σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία, ή

δ) την παροχή μέσω του διαδικτύου υπηρεσιών οπτικού ή/και ακουστικού περιεχομένου, εφόσον το περιεχόμενο αυτό έχει ενημερωτικό χαρακτήρα και ειδικότερα περιλαμβάνει, κατά το πρότυπο των έντυπων εφημερίδων, ειδήσεις για πολιτικά ή κοινωνικά ή οικονομικά γεγονότα και εκδηλώσεις, καθώς και άρθρα, σχόλια, συνεντεύξεις ή συζητήσεις για τα θέματα αυτά.»

Στο άρθρο 15 του α.ν. 248/1967 ορίζεται η έννοια «μη ημερήσια εφημερίδα ή περιοδικό» που ορίζεται και για τις ημερήσιες εφημερίδες με τη μόνη διαφορά να έπεται στη περιοδικότητα έκδοσης (άρθρο 15 παρ. 2 του α.ν. 248/1967). Όποια μορφή και να έχει ένα έντυπο και όποια εμφάνιση και αν το περιτυλίγει θεωρείται ως εφημερίδα ή περιοδικό.

Ο α.ν. 248/1967 αντικαταστήθηκε από το άρθρο 14 παρ. 9 του ν. 3232/2004 που περιγράφει λεπτομερώς τη σημασία της περιοδικότητας. Στο ρυθμιστικό πεδίο αυτού του νόμου

διατυπώνονται οι εφημερίδες που παρουσιάζουν το υλικό τους στα ψηφιακά μέσα όπως είναι ο υπολογιστής. Το διαδίκτυο, δηλαδή, λειτουργεί ως μέσο εμφάνισης της ύλης μιας εκδοτικής επιχείρησης και όχι ως μέσο ενημέρωσης. Άρα, εφόσον αποτυπώνονται εφημερίδες και περιοδικά στο διαδίκτυο θα υπάρχουν και διαφημίσεις στις ιστοσελίδες που αποτυπώνονται και θα πρέπει αυτές να καταβάλλουν αγγελιόσημο (α.ν. 248/1967). Το ίδιο ισχύει για όλα τα ραδιοτηλεοπτικά μέσα.

Το διαδίκτυο παρέχει πολλές λειτουργίες σε ραδιοφωνικές και τηλεοπτικές εκπομπές (άρθρο 15 του Συντάγματος) για αυτό και πρέπει στον όρο «εκπομπή» να εξομοιωθεί και η έννοια διαδικτυακή. Το νέο περιβάλλον στα μέσα ενημέρωσης περιλαμβάνει ιντερνετικό ραδιόφωνο, ψηφιακή εφημερίδα, ipTV. Με αυτά τα νέα μέσα καταργείται ο διαχωρισμός των παραδοσιακών μέσων(όπως είναι το ραδιόφωνο, το περιοδικό, η τηλεόραση, η εφημερίδα) από το διαδίκτυο και ενοποιούνται ως ΜΜΕ.

Η «διαδικτυακή διανομή των μέσων ενημέρωσης» όσο αφορά τις συναλλαγές και τη φορολόγηση έχει διατυπωθεί αλλά όσο αφορά τη ΓΓΕ-ΓΓΕ και τους φορείς ασφάλισης η νομοθεσία αυτή πρέπει να ερμηνευτεί.

Με τη ΠΟΛ. 1144/2003 (Πολυγραφημένη Υπουργική Εγκύκλιος) τα Οικονομικά Υπουργεία έχουν ερμηνεύσει του όρους Adbrite, Text-link-ads, e-book ,Google, Adsense/Adwords κ.τ.λ.

ΚΕΦΑΛΑΙΟ 5ο- Έρευνα μέσω ερωτηματολογίου - Αποτελέσματα

5.1. Θέμα και σκοπός της έρευνας

Θέμα της παρούσης έρευνας είναι η διερεύνηση του τρόπου που χρησιμοποιείται το διαδίκτυο και της ασφάλειας που το περιστοιχίζει. Σκοπός της εργασίας είναι η καταγραφή των χαρακτηριστικών των ατόμων που χρησιμοποιούν το διαδίκτυο και την αντίληψη που έχουν για την ασφάλεια τους κατά της διάρκεια χρήσης του. Η διαδικτυακή συμπεριφορά που παρουσιάζουν οι χρήστες ανακαλύπτει πολλά στοιχεία του χαρακτήρα του και έτσι μπορεί με προφυλάξεις να γίνει σκιαγράφηση του προφίλ του.

5.2. Αναγκαιότητα και σπουδαιότητα της έρευνας

Η μεθοδολογία που χρησιμοποιείται είναι ποσοτική και ερευνητική έρευνα μέσω της συμπλήρωσης ερωτηματολογίου. Το ερωτηματολόγιο συντάχθηκε μέσω του διαδικτυακού προγράμματος Google Forms και κοινοποιήθηκε στο Facebook για τυχαία δειγματοληψία ατόμων που είναι όμως χρήστες του διαδικτύου. Οι τύποι των ερωτήσεων ήταν κλειστού τύπου και πολλαπλής επιλογής όπου ο ερωτηθέν μπορούσε να επιλέξει μόνο μια απάντηση. Στα πλεονεκτήματα της συγκεκριμένης μεθόδου συγκαταλέγονται η συλλογή μεγάλο εύρος

απαντήσεων σε μικρό διάστημα ενώ στα μειονεκτήματα ότι μπορεί κάποιος χρήστης να απαντήσει πάν από μια φορά στο ερωτηματολόγιο και έτσι να χαθεί η αντικειμενικότητα που οφείλει να έχει μια έρευνα.

5.3 Περιγραφή ερωτηματολογίου

Το ερωτηματολόγιο συντάχθηκε για να γίνει συλλογή των δεδομένων που παρουσιάζουν τη συχνότητα χρήσης του διαδικτύου, τις επιλογές των υπηρεσιών του , και τον τρόπο χρήσης που μπορεί να φέρει αρνητικά αποτελέσματα. Το ερωτηματολόγιο διεξήχθη σε 95 ενήλικα άτομα και περιείχε 13 ερωτήσεις που είχαν όλες σχέση με το διαδίκτυο.
Σε πρώτο επίπεδο έγινε σκιαγράφηση του προφίλ των ερωτηθέντων και διερευνήθηκε ο βαθμός εξοικείωσης με το διαδίκτυο. Οι χρήστες ερωτήθηκαν τα εξής:
1) Συμπληρώστε το φύλο σας.
2) Η ηλικία σας είναι:
3) Το μορφωτικό σας επίπεδο είναι:
4) Πόσο συχνά χρησιμοποιείτε το διαδίκτυο;
5) Σε πόσα από τα social media διαθέτετε λογαριαμό;
όπως είναι το facebook, instagram, twitter...
6) Ο λόγος που χρησιμοποιείτε τα social media είναι:
7) Όταν θέλετε να ενημερωθείτε ποιό ΜΜΕ επιλέγετε;

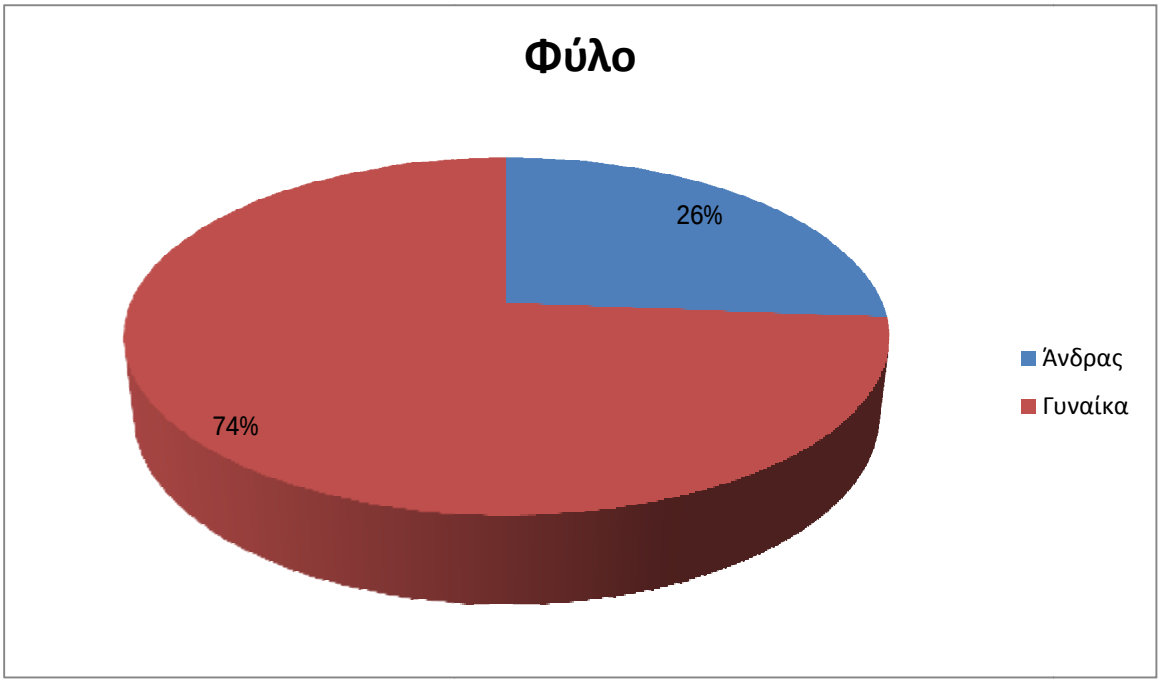
Στο δεύτερο επίπεδο διερευνάται το ζήτημα του θεσμικού πλαισίου που περιβάλει το διαδίκτυο για να γνωστοποιηθεί αν οι χρήστες είναι γνώστες για τα δικαιώματα που έχουν κατά τη πλοήγηση στο διαδικτύου και το πόσο αποτελεσματικούς θεωρούν τους νόμους αλλά και τα θεσμικά όργανα που τους. Τα ζητούμενα που τέθηκαν στους ερωτηθέντες ήταν τα εξής:
1)Πιστεύετε ότι οι νόμοι που διέπουν το κράτος σχετικά με το Διαδίκτυο είναι αρκετοί για τη προστασία των πολιτών της;
2)Πιο αποτελεσματικοί πιστεύεται ότι είναι οι νόμοι που περιστοιχίζουν την κοινωνία ή το διαδίκτυο;
3)Πόσο δύσκολο θεωρείτε ότι είναι ο εντοπισμός ενός διαδικτυακού εγκληματία;
4)Είστε ενήμεροι για τα δικαιώματα που έχετε σχετικά με τη χρήση των εφαρμογών του Διαδικτύου;
5)Οι νόμοι του κράτους θεωρείτε ότι συμβαδίζουν με την εξέλιξη της τεχνολογίας;
6) Πόσο ενήμερα θεωρείτε ότι είναι τα αρμόδια όργανα επιβολής των νόμων του Διαδικτύου;
7)Που θα απευθυνθείτε σε περίπτωση που πέσετε θύμα διαδικτυακού εγκλήματος;

Η έρευνα πραγματοποιήθηκε από 30/3/2018 – 8/4/2018. Μετά τη ολοκλήρωση της ποσοτικής έρευνας, τα ερωτηματολόγια συγκεντρώθηκαν και ελέγχθηκαν για τυχόν παρασπονδίες. Οι συμμετέχοντες έπρεπε να έχουν συμπληρώσει όλη την έρευνα ώστε να θεωρηθούν έγκυρες οι απαντήσεις τους. Στη συνέχεια ακολούθησε η καταγραφή των στοιχείων και η στατιστική επεξεργασία τους, για την οποία χρησιμοποιήθηκε το πρόγραμμα Excel. Στη συνέχεια έγινε ανάλυση των δεδομένων και ο σχολιασμός τους με βάση τα αποτελέσματα της έρευνας, για να διεξαχθούν ορθά συμπεράσματα.

5.4 Δημογραφικά χαρακτηριστικά του δείγματος

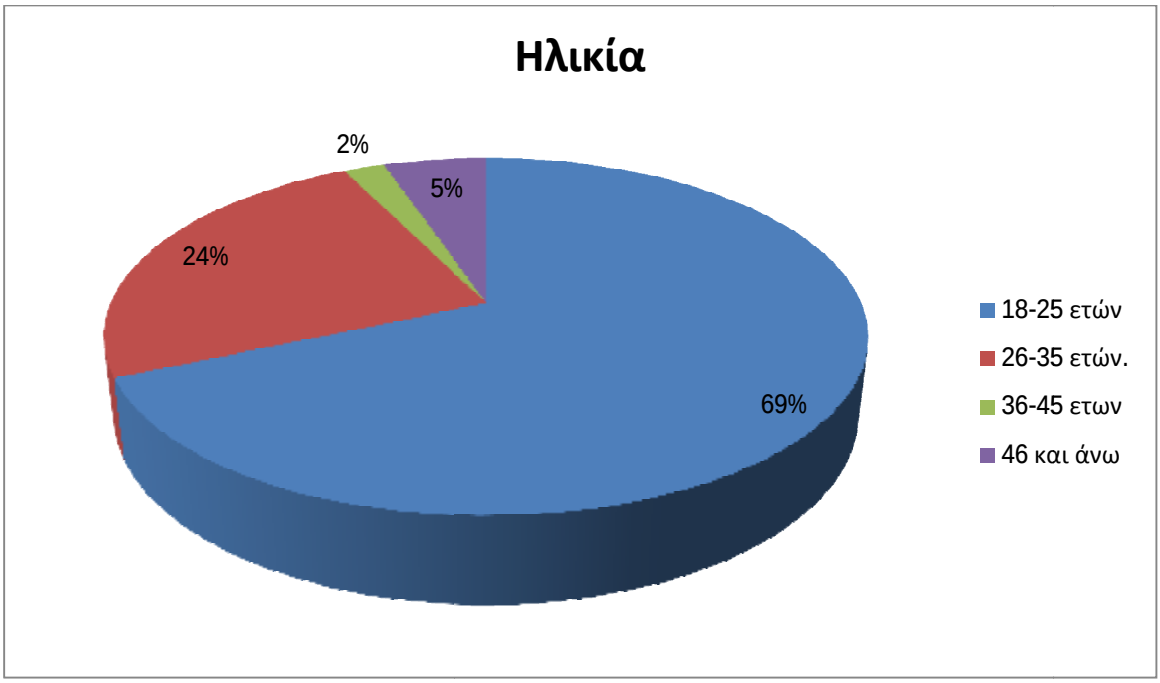
5.4.1. Φύλο

Από την ανάλυση της κατανομής του δείγματος κατά φύλο, διαπιστώθηκε ότι οι συμμετέχοντες αποτελούνταν λιγότερο από άνδρες (N = 25, 26%) και περισσότερο από γυναίκες (N =70, 74%).



5.4.2. Ηλικία

Ως προς την ηλικία των συμμετεχόντων , το μεγαλύτερο δείγμα αποτελείται από τις ηλικίες 18-25 (N =65, 71%). Ένα μικρότερο ποσοστό έχουν οι ηλικίες 26-35 ετών (N =23, 25%) και ελάχιστοι συμμετείχαν με ηλικίες 36-45(N =2, 2%) ετών και 46 και άνω (N =5, 5%).

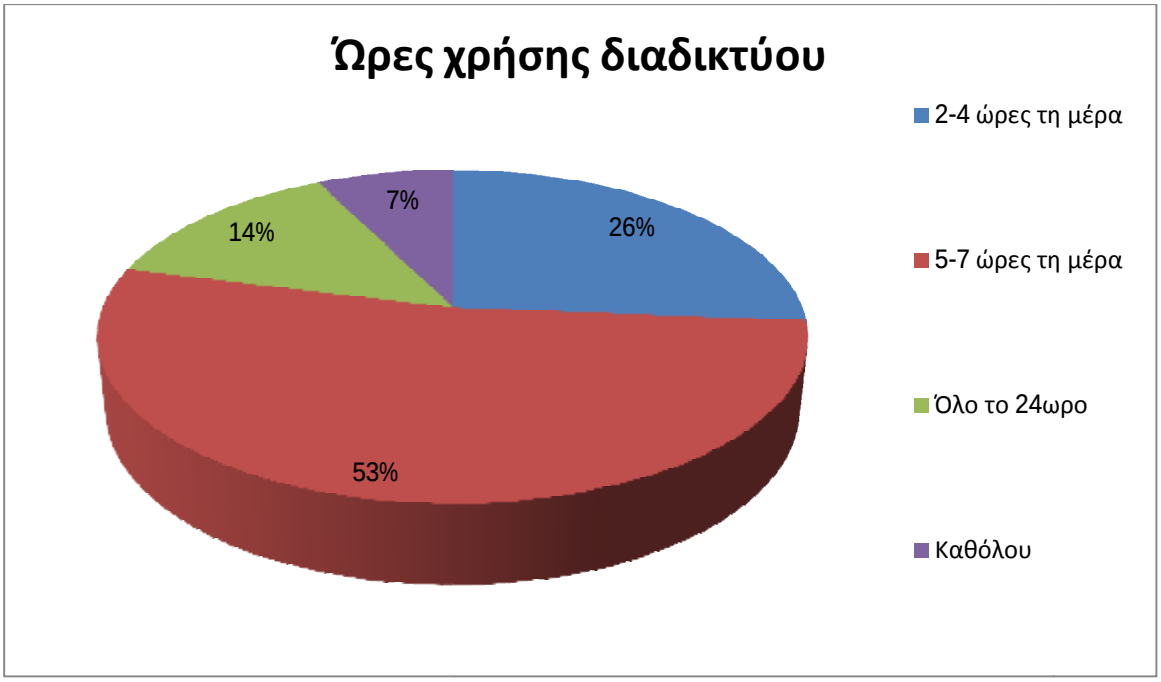


5.4.3. Μορφωτικό επίπεδο

Οι συμμετέχοντες της έρευνας ανέφεραν ότι έχουν ολοκληρώσει τη δευτεροβάθμια εκπαίδευση (N =30, 32%) με το μεγαλύτερο μέρος εξ αυτών να είναι απόφοιτοι ΤΕΙ-Πανεπιστημίου (N =53, 56%) και των υπόλοιπων να βρίσκονται ή να έχουν ήδη ολοκληρώσει ανώτερες σπουδές.

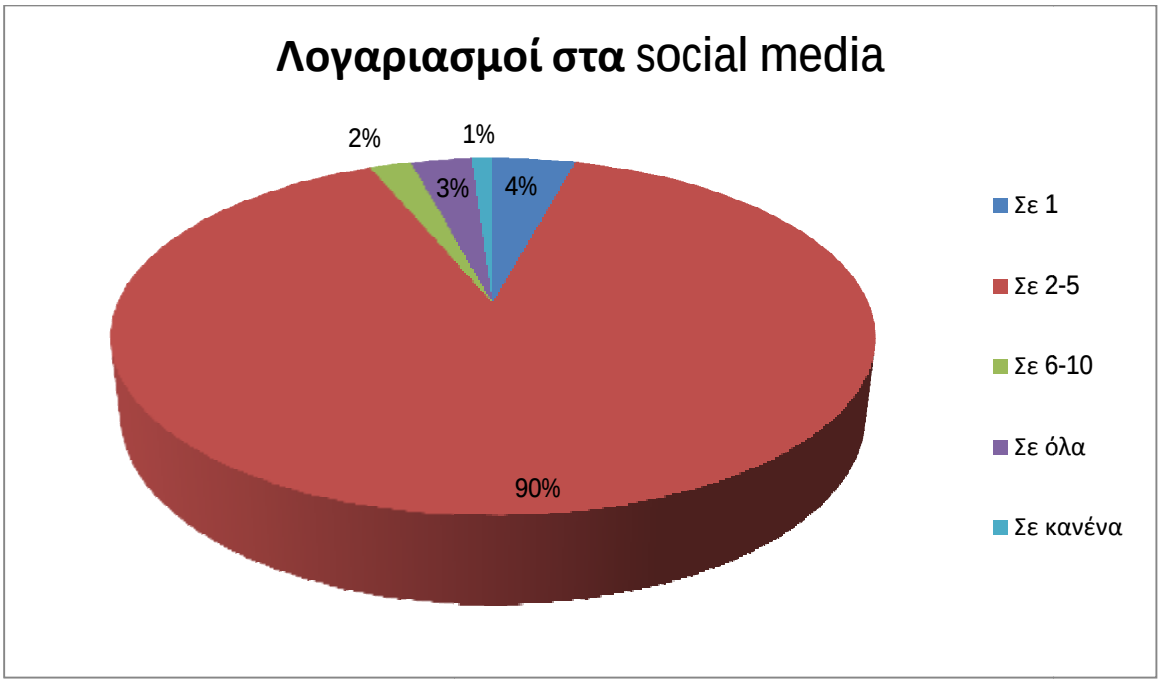
5.5 Συχνότητα χρήσης διαδικτύου

Η συντριπτική πλειοψηφία των ερωτηθέντων συνδέονται 5-7 ώρες την ημέρα στο διαδίκτυο (N =50, 53%) ενώ μερικοί παρουσιάζουν εθισμό προς το διαδίκτυο αφού είναι όλο το 24ωρο συνδεδεμένοι (N =13, 14%). Οι υπόλοιποι είναι σε κανονικά πλαίσια συνδεδεμένοι με 2-4 ώρες την ημέρα (N =25, 26%).



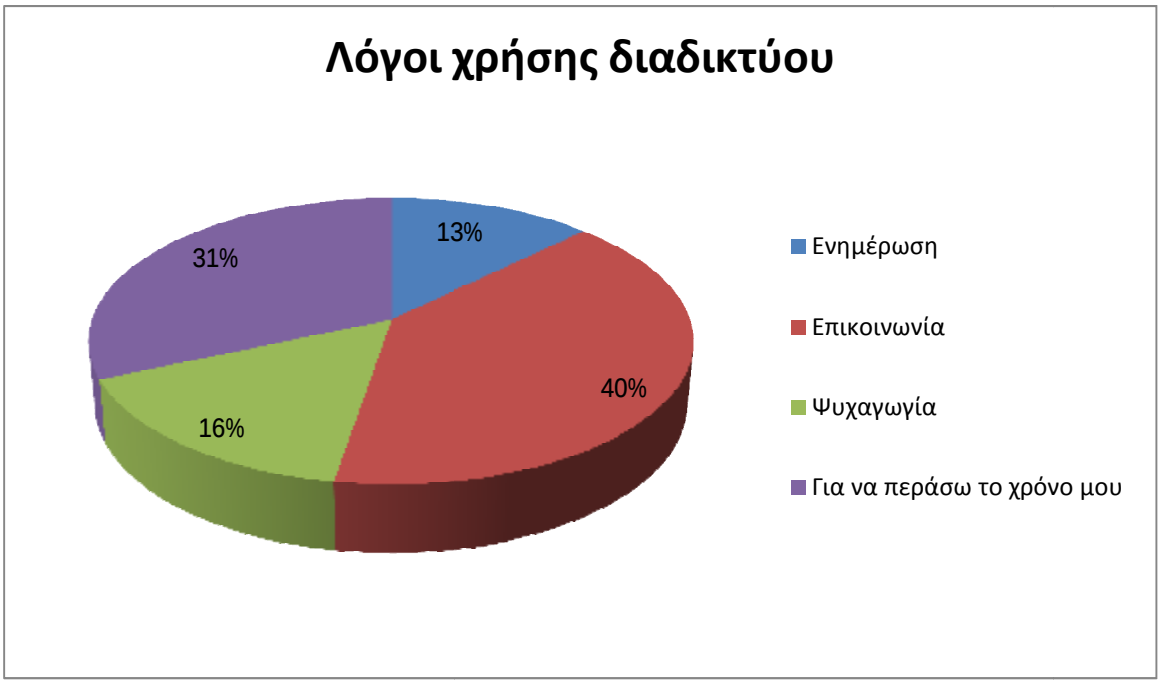
5.6 Κατοχή λογαριασμών στα social media

Το συντριπτικό ποσοστό των ερωτηθέντων είναι ενεργά μέλη των υπηρεσιών που προσφέρει το διαδίκτυο με το 90% (N=85) εξ αυτών να διαθέτουν λογαριασμούς σε 2-5 social media. Οι υπόλοιποι ερωτηθέντες της έρευνας είτε διαθέτουν περισσότερους λογαριασμούς 6-10 (N=2, 2%), σε όλα (N=3, 3%), είτε σε λιγότερους σε 1 (N=4, 4%), σε κανένα (N=1, 1%).



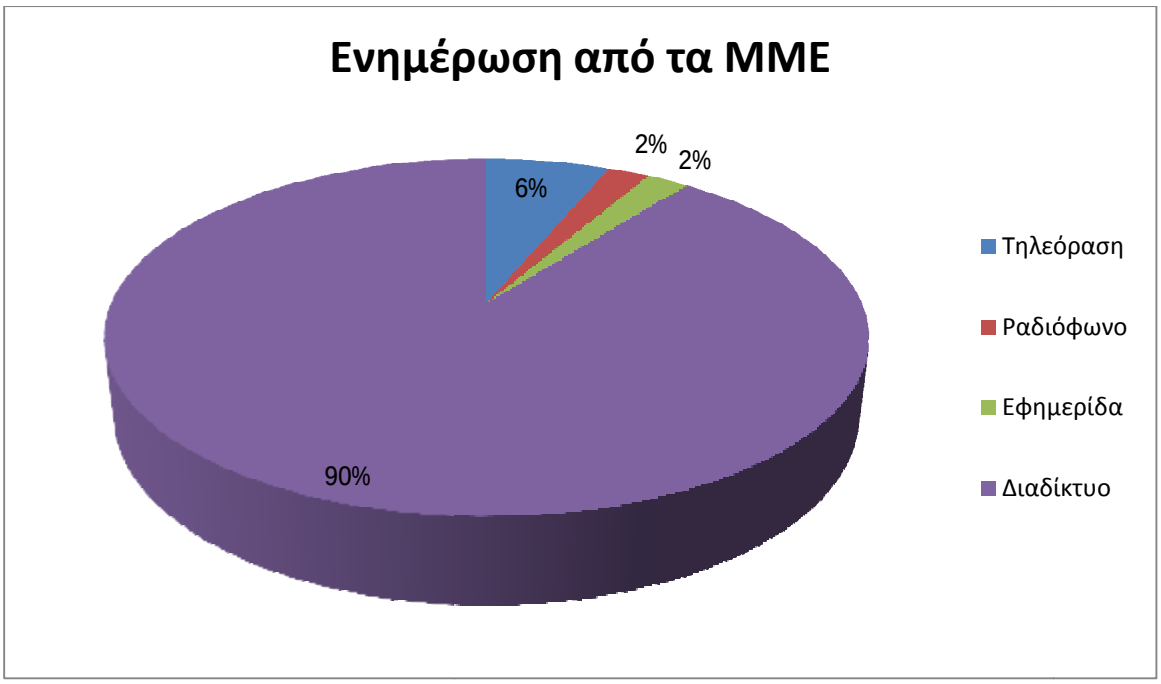
5.7 Λόγοι χρήσης διαδικτύου

Στους λόγους που οι πιο πολύ άνθρωποι χρησιμοποιούν το διαδίκτυο οι ερωτήσεις διαμοιράστηκαν σε κοντινά ποσοστά εκτός από το πεδίο της Ενημέρωσης που επιλέχθηκε μόνο από το 13% (N=12) των ερωτηθέντων. Μεγαλύτερο ποσοστό συγκέντρωσε η Επικοινωνία με 40% (N= 38), ακολουθεί η απάντηση Για να περάσω το χρόνο μου με 30%(N=31%) και στη συνέχεια με μικρή διαφορά η Ψυχαγωγία με 16% (N=15).



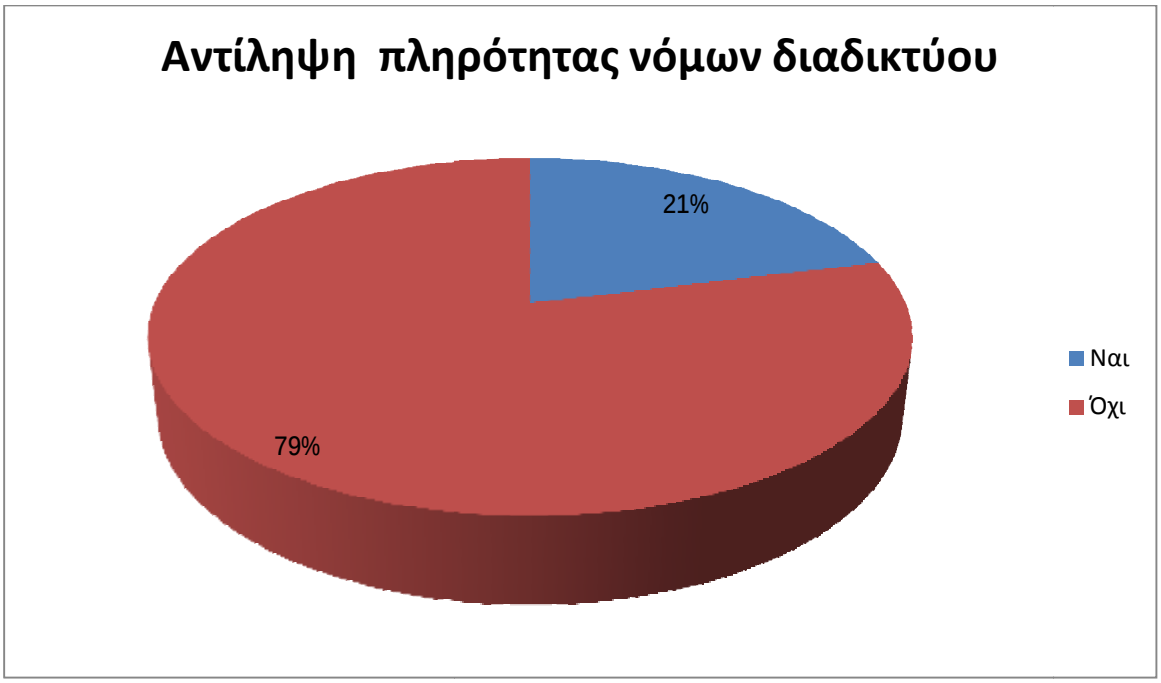
5.8 Ενημέρωση από τα ΜΜΕ

Σε αυτήν την ερώτηση, φαίνεται πόσο έχει διεισδύσει το διαδίκτυο στις καθημερινές λειτουργίες του άνθρωπου όπως είναι η ενημέρωση. Σχεδόν όλοι οι ερωτηθέντες επιλέγουν να ενημερωθούν από το διαδίκτυο(N=85, 90%) και όχι από τα παραδοσιακά μέσα.



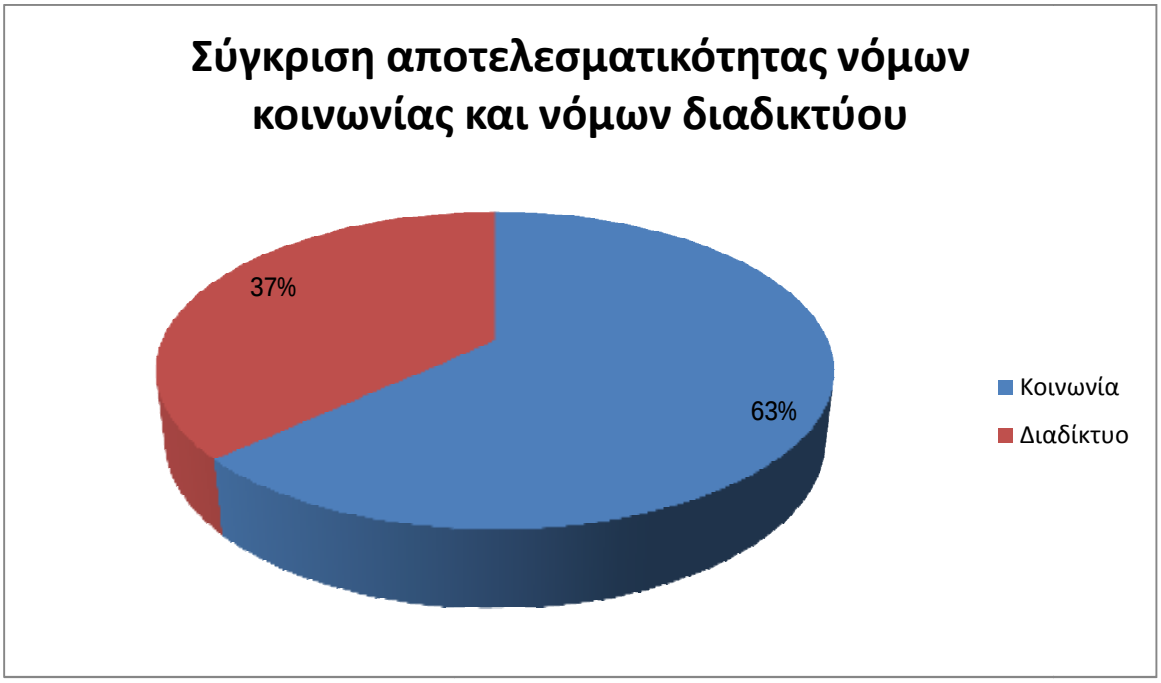
5.9 Αντίληψη πληρότητας νόμων διαδικτύου για προστασία πολιτών

Οι νόμοι σύμφωνα με τη πλειονότητα των ερωτηθέντων (N=75,79%) δεν είναι αρκετοί ώστε να προστατέψουν τους πολίτες του κράτους σε όποια εγκληματική πράξη προκύψει σε βάρος τους εν ώρα πλοήγησης.



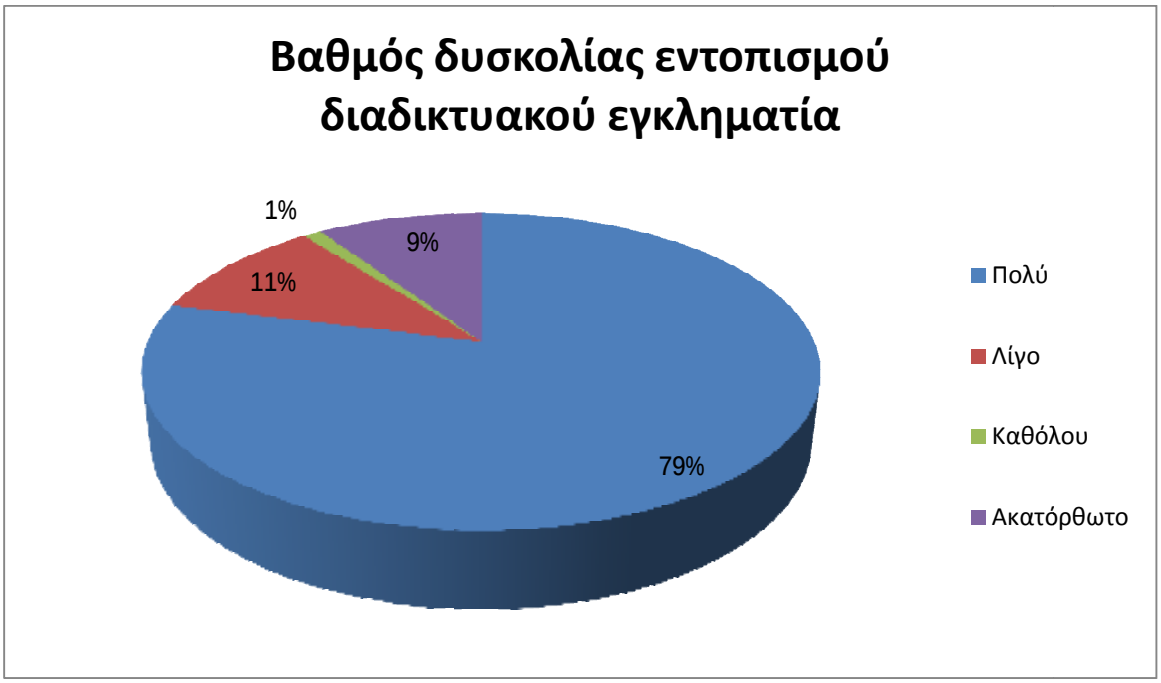
5.10 Επιλογή αποτελεσματικότητας νόμων κοινωνίας ή νόμων διαδικτύου

Στην ερώτηση σύγκρισης μεταξύ των νόμων της κοινωνίας και των νόμων του διαδικτύου σε σχέση με την αποτελεσματικότητα που εμφανίζουν κατά την επιβολή τους, οι περισσότεροι ερωτηθέντες απάντησαν θετικά προς του νόμους της κοινωνίας με ποσοστό 63% ενώ λίγοι είναι αυτοί που πιστεύουν ότι οι νόμοι που περιστοιχίζουν το διαδίκτυο είναι στη πράξη τους αποτελεσματικοί (37%) και άρα μπορούν να επιλύσουν μια δικαστική απόφαση.



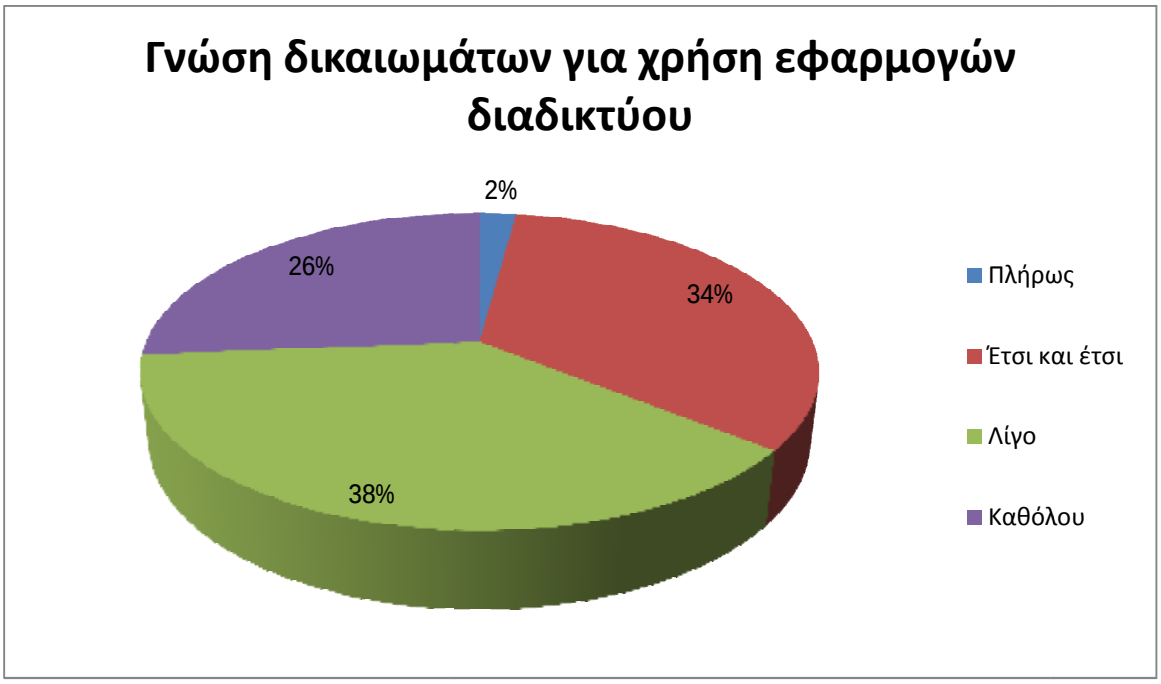
5.11 Δυσκολία εντοπισμού διαδικτυακού εγκληματία

Το διαδίκτυο είναι ένα πολύπλοκο σύστημα και αποτελεί μια νέα πραγματικότητα που δεν είναι ιδιαίτερα προσιτή σε όλους λόγω των γνώσεων που απαιτεί για τη διαχείριση του. Έτσι όταν γίνει προσπάθεια να εντοπιστεί ένας διαδικτυακός εγκληματίας από το κράτος, οι περισσότεροι πολίτες του πιστεύουν ότι είναι πολύ δύσκολο να βρεθεί (N=75,79%) ενώ άλλοι πιστεύουν ότι είναι και ακατόρθωτο (9%).



5.12 Γνώση δικαιωμάτων Διαδικτύου

Τα αποτελέσματα αυτής της έρευνας είναι επί το πλείστον ενθαρρυντικά αφού το μεγαλύτερο ποσοστό των ερωτηθέντων γνωρίζει λίγο(N=36, 38%) ή έτσι κι έτσι(N=32, 34%) τα δικαιώματα που έχουν όταν χρησιμοποιούν τις εφαρμογές του διαδικτύου ενώ μόνο το 2% δηλώνει πλήρως ενήμερο. Βέβαια, υπάρχει και ένα σημαντικό ποσοστό ατόμων(26%) που δηλώνει ότι δεν γνωρίζει τίποτα σχετικά που τα δικαιώματα που έχει προς το διαδίκτυο.

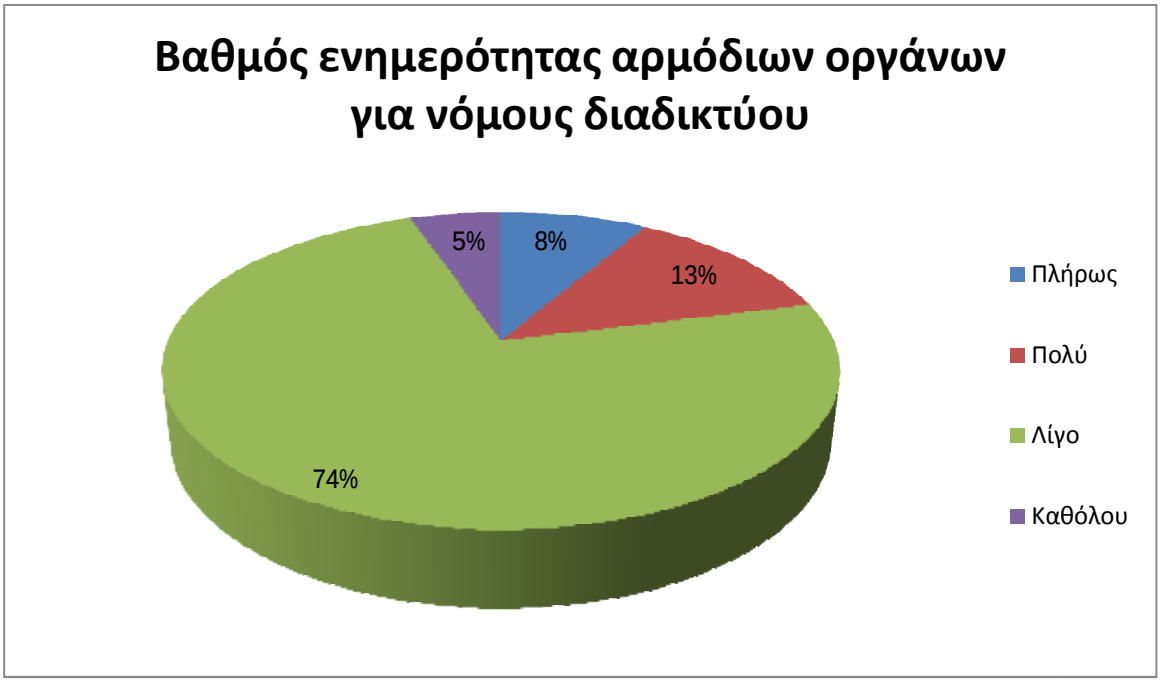


5.13 Ακολουθία νόμων κράτους με εξέλιξη τεχνολογίας

Η τεχνολογία εξελίσσεται διαρκώς και ραγδαία τα τελευταία χρόνια με αποτέλεσμα το κράτος να βρίσκεται σε συνεχή επαγρύπνηση για το συγχρονισμό των νόμων του με την εξέλιξη αυτή. Έτσι οι πιο πολλοί είναι δύσπιστοι στην ακολουθία αυτή των νόμων προς τη τεχνολογία (N=45, 43%) ενώ διαμοιρασμένοι στο 24% είναι αυτή που πιστεύουν ότι συμβαδίζουν ελάχιστα και αυτοί που πιστεύουν σε μεγάλο βαθμό. Μόλις το 9% δείχνει την απόλυτη εμπιστοσύνη στο έργο του κράτους.

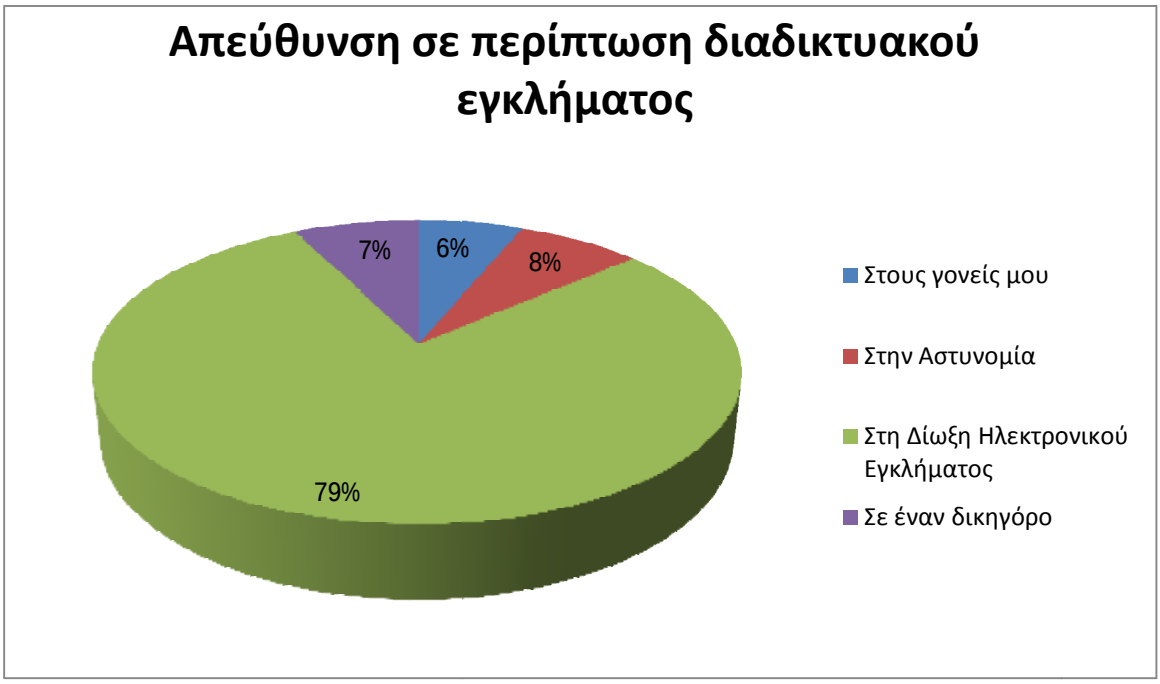
5.14 Νομική ενημερότητα αρμόδιων οργάνων για νόμους Διαδικτύου

Τα αρμόδια όργανα οφείλουν να είναι ενήμερα πλήρως για τους νόμους που περιστοιχίζουν το διαδίκτυο και για την εξέλιξη που συναντά η τεχνολογία καθημερινά για να αναγνωρίζουν κάθε πρόβλημα που καλούνται να λύσουν στο διαδίκτυο. Ωστόσο, μόνο το 8% των ατόμων πιστεύει στην πλήρη ενημέρωση των αρμόδιων οργάνων ενώ το συντριπτικό ποσοστό των 74% πιστεύει ότι είναι λίγο.



5.15 Αντίληψη κατεύθυνσης σε περίπτωση διαδικτυακού εγκλήματος

Οι πιο πολλοί χρήστες είτε είναι ενήμεροι είτε έχουν ακουστά που ακριβώς πρέπει να απευθυνθούν σε περίπτωση που πέσουν θύμα ηλεκτρονικού εγκλήματος. Έτσι, οι περισσότεροι γνωρίζουν ότι πρέπει να απευθυνθούν στη Δίωξη Ηλεκτρονικού Εγκλήματος σε όποια απάτη αντιληφθούν στο διαδίκτυο(N=75,79%). Οι υπόλοιποι επιλέγουν μια πιο γνώριμη μορφή πάταξης εγκλήματος που είναι η αστυνομία(8%) είτε ένα έννομο όργανο που να γνωρίζει τα δικαιώματα του όπως είναι ο δικηγόρος(7%). Οι λιγότεροι επιθυμούν τη βοήθεια από το συγγενικό τους περιβάλλον (6%).



ΣΥΜΠΕΡΑΣΜΑΤΑ

Με την έρευνα που έγινε σχετικά με το θεσμικό πλαίσιο του διαδικτύου που επικρατεί στην Ελλάδα στους τομείς των προσωπικών δεδομένων, Μέσων Μαζικής Ενημέρωσης, ηλεκτρονικών εγκλημάτων παρουσιάζονται οι τρόποι αντιμετώπισης της παραβίασης τους από τους νόμους που έχει ορίσει το κράτος και ενημερώνει τους χρήστες για τους τρόπους πρόληψης από μια διαδικτυακή απάτη και για τα δικαιώματα που έχουν σε κάθε περίπτωση.

Παράλληλα, επιδιώχθηκε η καταγραφή των αντιλήψεων ενός δείγματος 95 ενηλίκων για τον τρόπο που διαχειρίζονται το διαδίκτυο αλλά και την ενημέρωση που έχουν οι ίδιοι για τα διαδικτυακά τους δικαιώματα. Αποτυπώθηκε, επιπλέον, η γνώμη τους σε σχέση με την αποτελεσματικότητα που φέρει το κράτος και τα αρμόδια όργανα που το περιστοιχίζουν στην επιβολή των νόμων του διαδικτύου αλλά και η γνώση που έχουν πάνω στους νόμους αυτούς.

Η ανάλυση των αποτελεσμάτων έδειξε ότι οι πιο πολλοί συμμετέχοντες δαπανούν στο διαδίκτυο 5-7 ώρες της καθημερινότητας του στο διαδίκτυο χρησιμοποιώντας τις υπηρεσίες του διαδικτύου πιο πολύ για την επικοινωνία και όταν έπεται το θέμα της ενημέρωσης από κάποιο μέσο μαζικής ενημέρωσης τότε υποστηρίζουν και εκεί το διαδίκτυο ως ένα σύγχρονο μέσο που διαθέτει μεγάλο εύρος ειδήσεων αλλά και ως ένα διαδραστικό αφού μπορεί ο κάθε χρήστης να συμμετέχει ενεργά στο σχολιασμό της κάθε είδησης..

Συνολικά, οι συμμετέχοντες ανέφεραν ότι είναι ενεργοί χρήστες του διαδικτύου διατηρώντας 2-5 λογαριασμούς στα social media. Βέβαια, οι πιο πολλοί δηλώνουν ότι έχουν λίγη έως καθόλου γνώση των δικαιωμάτων τους σε σχέση με τις εφαρμογές που χρησιμοποιούν στο διαδίκτυο θέτοντας τους έτσι εύκολα και πιθανά θύματα ηλεκτρονικών εγκληματιών. Προφανώς οι χρήστες πιστεύουν ότι δεν πρόκειται να πέσουν θύματα κάποιου ηλεκτρονικού εγκλήματος και αν πέσουν τότε η πλειοψηφία αναφέρει ότι θα απευθυνθεί στη Δίωξη Ηλεκτρονικού Εγκλήματος για να τους βοηθήσει με το εκάστοτε πρόβλημα τους.

Έκπληξη αποτέλεσε η γνώμη που ανέδειξαν οι χρήστες σχετικά με τους νόμους που περιστοιχίζουν το διαδίκτυο. Οι πιο πολλοί, λοιπόν, από τους ερωτηθέντες φάνηκαν ότι θεωρούν ελλιπές τους νόμους που διέπουν το διαδίκτυο με σκοπό τη προστασία τους και βρήκαν το κράτος αδύναμο ως προς το συγχρονισμό των νόμων του με αυτό της τεχνολογίας. Έτσι, θεώρησαν και τα αρμόδια όργανα ελάχιστα ενήμερα σε σχέση με την εξέλιξη που εμφανίζει η τεχνολογία και άρα ακατάλληλα ως προς την επιβολή των νόμων με σωστό και εμπεριστατωμένο λόγο. Συμπερασματικά με τα προηγούμενα είναι λογικό να θεωρήσουν και ως μια πολύ δύσκολη διαδικασία τον εντοπισμό ενός ηλεκτρονικού εγκληματία που έδρασε εις βάρος κάποιου χρήστη και για να ανακαλυφθεί πρέπει να βρεθούν όλες οι παράνομες ενέργειες που προέβη μέχρι να φτάσει στη διάπραξη του εγκλήματος. Για αυτή όμως τη διαδικασία χρειάζεται πλήρη γνώση και όλων των πτυχών της τεχνολογίας και των νόμων που τη περιστοιχίζουν. Έτσι, τα άτομα δηλώνουν πιο σίγουρα με τους νόμους που

περιβάλουν τη κοινωνία παρά με αυτούς του διαδικτύου.

Οι αναλύσεις συσχετίσεων κατέδειξαν ότι υπάρχει στατιστικώς σημαντική σχέση ανάμεσα στην ηλικία, στο μορφωτικό επίπεδο και τις ώρες χρήσης του διαδικτύου, με τη νεολαία να υποστηρίζει ένθερμα το διαδίκτυο και τις δυνατότητες που προσφέρει. Οι πιο πολλοί ερωτηθέντες είναι απόφοιτοι ΤΕΙ-Πανεπιστημίου, οπότε χρησιμοποιούν το διαδίκτυο και ως βοήθημα για τη καλύτερη τέλεση των σπουδών τους, έχοντας αποκτήσει με αυτό τον τρόπο μεγαλύτερη εξοικείωση με τη τεχνολογία σε σχέση με μεγαλύτερης ηλικίας άτομα. Η άγνοια σχετικά με τα δικαιώματα που έχει κάθε χρήστης στο διαδίκτυο συνεχίζει να υπάρχει, θεωρώντας και το κράτος ανίκανο προστασίας τους λόγω των ελλιπών νόμων και οργάνων που το περιβάλλουν. Γενικά, το διαδίκτυο, παρόλο που αποτελεί έναν επικίνδυνο κόσμο με τις παγίδες που κρύβει στο κάθε κλικ του πληκτρολογίου, έχει γίνει μέρος της καθημερινότητας της νεολαίας.

Παρατηρείται ότι όσο αναπτύσσεται η τεχνολογία και όσο περνούν τα χρόνια τόσο οι άνθρωποι προτιμούν το διαδίκτυο για την εξυπηρέτηση των αναγκών τους και τόσο αυξάνονται οι επιτήδειοι που εκμεταλλεύονται το γεγονός αυτό. Η ηλικία που κάποιος έρχεται σε επαφή με το διαδίκτυο συνεχώς μειώνεται και έτσι οι άνθρωποι από νωρίς διεισδύουν στο κόσμο της τεχνολογίας και περνούν ώρες εξερευνώντας τον είτε παίρνοντας γνώσεις από αυτό είτε βαδίζοντας στο μονοπάτι προσωπικού συμφέροντος που μπορεί να εκμεταλλευτεί από αυτό. Πλέον έχουν αναπτυχθεί λογισμικά που είναι εύκολο να χρησιμοποιηθούν από κάθε χρήστη που έχει λίγες γνώσεις τεχνολογίας και να κλέψει προσωπικά δεδομένα από κάποιον άλλον προβαίνοντας σε έγκλημα.

Το διαδίκτυο αποτελεί ένα τεχνολογικό φαινόμενο που συνεχώς αναπτύσσει νέες λειτουργίες ή αναβαθμίζει παλιές με αποτέλεσμα οι νόμοι που το περιστοιχίζουν να μην μπορούν να συμβαδίσουν με τη τεχνολογική του εξέλιξη και να είναι ελλιπές όπως και τα όργανα επιβολής των νόμων αυτών να είναι ανήμερα και ανεκπαίδευτα. Αποτελεί ένα κόσμο ανεξέλεγκτο αλλά και πολύ εθιστικό προς τους έφηβους χρήστες του ιδιαίτερα και έχει ενσωματωθεί σε όλους τους τομείς της καθημερινότητας του.

Οι χρήστες του διαδικτύου πρέπει να πάρουν μέτρα προστασίας οι ίδιοι για να προφυλάξουν τη προσωπική τους ζωή και τα αγαθά τους και το κράτος να ναι σε μόνη επαγρύπνηση για κάθε εξέλιξη που έπεται στην τεχνολογική ενότητα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

*Ρήγου, Μ. (2014). Από την ψηφιακή επανάσταση στην ψηφιακή επιτήρηση. Νέα Μέσα, δημοσιότητα και πολιτική. Αθήνα, Σιδέρης.

* Τσενέ, Λ. (2012), Από την κρίση των ΜΜΕ στα social media: ένα νέο μοντέλο κοινωνικής ευθύνης, Αθήνα, Αιώρα

* Ψυχογιός, Δ. (2004), Τα Έντυπα Μέσα Επικοινωνίας. Από τον Πηλό στο Δίκτυο. Αθήνα, Καστανιώτης

* Παπαθανασόπουλος, Στ. (2004), Πολιτική και ΜΜΕ. Η περίπτωση της Νότιας Ευρώπης, Αθήνα, Καστανιώτης

* Σιδηρόπουλος, Γ. Κ. (2008) "Το δίκαιο του Διαδικτύου", Αθήνα, Αντ. Ν. Σάκκουλα

Μεταφρασμένη βιβλιογραφία

* Laudon, K. C. & Traver, C. G. (2011). Ηλεκτρονικό εμπόριο. Επιχειρήσεις. Τεχνολογία. Κοινωνία. μτφρ. Α.Μήλιος. Αθήνα, Παπασωτηρίου.

* Norton's, P. (2012). Εισαγωγή στους υπολογιστές. Μτφρ. Μ. Γ. Δημόπουλος. Αθήνα, Τζιόλα.

Χρήση άρθρων, ισοτόπων και αναφορών από το διαδίκτυο

*Καλαντζής, Δ. (2018) Ψεύτικες ειδήσεις: Η κερδοφόρος παραπληροφόρηση της εποχής, https://www.huffingtonpost.gr/dimitris-kalantzis/-_10256_b_14955702.html (τελευταία πρόσβαση 31 Μαρτίου 2018)

*Παυλίδης, Γ. (2017) Fake news και δημοσιογραφία... http://politis.com.cy/article/fake-news-ke-dimosiografia (τελευταία πρόσβαση 30 Μαρτίου 2018)

*Κόνσουλας, Θ. (2014) Social Media σχολείο: Μαθαίνουμε τα δημοφιλή Μέσα Κοινωνικής Δικτύωσης, http://www.socialmedialife.gr/110286/social-media-sxoleio/ (τελευταία πρόσβαση 31 Μαρτίου 2018)

*Cosmote, (2018) Ένας κόσμος, καλύτερος για όλους., https://www.youtube.com/watch?v=wh1yq7V8aP0 (τελευταία πρόσβαση 11 Μαρτίου 2018)

* Κορδερά, Ε. (2010) Τα Μέσα Κοινωνικής Δικτύωσης και οι Επιπτώσεις τους στην Ψυχική μας Υγεία., http://www.psychologos-kordera.gr/index.jsp?CMRCode=19HC1PL3B&extLang (τελευταία πρόσβαση 12 Οκτωβρίου 2017)

* Παπαθανοσόπουλου, Σ. & Αθανασιάδη, Η. & Ξενοφώντος, Μ. (2014) Facebook και ιδιωτικότητα: αντίρροπες δυνάμεις; , http://dimosiografia.com/facebook-idiotikothta/ (τελευταία πρόσβαση 17 Οκτωβρίου 2017)

* Καλογερόπουλος, Α. (2016) Ποιο είναι το τοπίο της ψηφιακής ενημέρωσης στην Ελλάδα και τον κόσμο; http://www.lifo.gr/articles/digital-media_articles/104332 (τελευταία πρόσβαση 25 Οκτωβρίου 2017)

* Καλησπεράκη, Χ. (2016) Η Ψηφιακή Επανάσταση προ των πυλών http://www.anysma.gr/rethemniotika-nea/articles/i-psifiaki-epanastasi-pro-ton-pulon.html (τελευταία πρόσβαση 20 Οκτωβρίου 2017)

* Economist, (2018) Economist :Η ψηφιακή επανάσταση γίνεται ζήτημα επιβίωσης το 2018, http://www.insider.gr/epiheiriseis/diethni/71840/economist-i-psifiaki-epanastasi-ginetai-zitima-epiviosis-2018 (τελευταία πρόσβαση 25 Φεβρουαρίου 2018)

* Φέσιας, Λ. (2016) «Η δημοσιογραφία σήμερα, αλλαγές και προκλήσεις», http://www.ant1iwo.com/news/cyprus/article/235788/-i-dimosiografia-simera-allages-kai-prokliseis/ (τελευταία πρόσβαση 18 Οκτωβρίου 2017)

* Πλείος, Γ. (2014) Τα νέα μέσα και η ουτοπία της αντικειμενικότητας , http://tvxs.gr/news/blogarontas/ta-nea-mesa-kai-i-oytopia-tis-antikeimenikotitas (τελευταία πρόσβαση 10 Οκτωβρίου 2017)

* Κόλλια, Κ. (2017) Ψηφιακή ανισότητα και ευρωπαϊκός πολιτισμός, http://www.liberal.gr/arthro/182105/apopsi/arthra/psifiaki-anisotita-kai-europaikos-politismos-.html *(τελευταία πρόσβαση 2 Οκτωβρίου 2017)*

* Καβακόπουλος, Λ. (2006) *Η Πραγματική Ιστορία των Μ.Μ.Ε.*, *https://antidogma.gr/2008/11/12/history-of-mass-media/ (τελευταία πρόσβαση 2 Μαρτίου 2018)*

* *Χατζόπουλο, Α. (2010) Ψηφιακό χάσμα = νέες ανισότητες, http://tvxs.gr/news/sci-tech/%CF%88%CE%B7%CF%86%CE%B9%CE%B1%CE%BA%CF%8C-%CF%87%CE%AC%CF%83%CE%BC%CE%B1-%CE%BD%CE%AD%CE%B5%CF%82-%CE%B1%CE%BD%CE%B9%CF%83%CF%8C%CF%84%CE%B7%CF%84%CE%B5%CF%82 (τελευταία πρόσβαση 5 Οκτωβρίου 2017)*

**Σιφναίος, Χ.(2011) «Πως το διαδίκτυο μπορεί να αποτελέσει μορφή αντίδρασης στην κατάσταση των Μ.Μ.Ε.;»*, http://ereuna-mps.blogspot.gr/ (τελευταία πρόσβαση 17 Φεβρουαρίου 2018)

* *ithageneis (2010) Παρουσίαση βιβλίου: «Η ιστορία των ΜΜΕ», https://ithageneis.wordpress.com/2010/09/13/%CF%80%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%AF%CE%B1%CF%83%CE%B7-%CE%B2%CE%B9%CE%B2%CE%BB%CE%AF%CE%BF%CF%85-%CE%B7-%CE%B9%CF%83%CF%84%CE%BF%CF%81%CE%AF%CE%B1-%CF%84%CF%89%CE%BD-%CE%BC%CE%BC%CE%B5/ (τελευταία πρόσβαση 26 Φεβρουαρίου 2018)*

* Barthel, M., Shearer, E., Gottfried, J., & Mitchell, A. (2015) *The Evolving Role of News on Twitter and Facebook* στο http://www.pewresearch.org. Online στο http://www.journalism.org/2015/07/14/the-evolving-role-of-news-on-twitter-and-facebook/,

(τελευταία πρόσβαση 5 Μαρτίου 2018).

* Κόμλου, Β. (2011) ΤΟ ΔΙΑΔΙΚΤΥΟ ΩΣ ΑΝΤΙΔΡΑΣΗ ΣΤΗΝ ΚΡΙΣΗ ΤΩΝ ΜΜΕ, http://ereuna-mps.blogspot.gr/ (τελευταία πρόσβαση 6 Φεβρουαρίου 2018)

* Χατζηαναστασίου, Χ.(2011) «Μ.Μ.Ε. ΚΑΙ ΚΡΙΣΗ. ΜΠΟΡΕΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΝΑ ΑΠΟΤΕΛΕΣΕΙ ΑΝΤΙΔΡΑΣΗ ΣΤΑ Μ.Μ.Ε.;», http://ereuna-mps.blogspot.gr/ (τελευταία πρόσβαση 17 Φεβρουαρίου 2018)

*Παπασίμος, Γ. (2016) Παθητικοί θεατές μιας δυσώδους πραγματικότητας που φτωχοποιεί και περιθωριοποιεί, https://www.atticacoast.gr/99675-2/ (τελευταία πρόσβαση 16 Ιανουαρίου 2018)

*Μπαζαίος Γ. (2009) New Media στην Ελλάδα, https://newmediagr.wordpress.com/2009/12/10/ngtddyogtx/ (τελευταία πρόσβαση 3 Ιανουαρίου 2018)

*Χαραλαμπάκης, Μ. (2011) ΔΙΑΔΊΚΤΥΟ (ΠΛΕΟΝΕΚΤΗΜΑΤΑ - ΜΕΙΟΝΕΚΤΗΜΑΤΑ) – ΚΕΙΜΕΝΑ, https://tassos-filologos.blogspot.gr/2011/07/blog-post_12.html (τελευταία πρόσβαση 14 Ιανουαρίου 2018)

*Βερβέρη, Μ. (2017) «Η επίδραση των ΜΜΕ στην ανάπτυξη των παιδιών», http://www.lesvosnews.net/articles/news-categories/psyhologia/i-epidrasi-ton-mme-stin-anaptyxi-ton-paidion (τελευταία πρόσβαση 14 Οκτωβρίου 2017).

Γιακουμής, Β. (2012) Τα ΜΜΕ και το διαδίκτυο, http://www.protagon.gr/epikairotita/ellada/ta-mme-kai-to-diadiktyo-12407000000 (τελευταία πρόσβαση 5 Ιανουαρίου 2018)

*Τατάλια-Λίτσου, Γ. (2014) Τα ΜΜΕ, οι αρνητικές επιδράσεις τους και τρόποι αντιμετώπισης, http://blogs.sch.gr/apontes/2014/02/22/mme/ (τελευταία πρόσβαση 1 Μαρτίου 2018).

*Ασλανίδου, Σ. (2012) Παγκοσμιοποίηση –τηλεόραση –εκπαίδευση:Μια μεθοδολογική στροφή στην έρευνα της τηλεόρασης, http://www.pee.gr/wp-content/uploads/praktika_synedrion_files/e10_11_03/meros_c_th_en_vii/aslanidoy.htm (τελευταία πρόσβαση 20 Ιανουαρίου 2017)

*Καρακατσάνης, Γ. (2010) Έρευνα: Blogs & Δημοσιογραφία, https://www.xblog.gr/έρευνα-blogs-δημοσιογραφία/ (τελευταία πρόσβαση 4 Φεβρουαρίου 2018)

* Χατζηαγγελάκη, Δ.(2013) Έρευνα για τα Μέσα Μαζικής Επικοινωνίας, http://www.arsakeio.gr/gr/psychico/psychico-high-school-b/events-activities/15085-erevna-gia-ta-mesa-mazikhs-enhmerwshs (τελευταία πρόσβαση 7 Φεβρουαρίου 2018)

* Μαργαρίτη, Κ. (2016) *Οι ειδησεογραφικές εφαρμογές στη δημοσιογραφική πρακτική* στο medianalysis.net. Online στο https://medianalysis.net/2016/06/17/%CE%BF%CE%B9-%CE%B5%CE%B9%CE%B4%CE%B7%CF%83%CE%B5%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%B9%CE%BA%CE%AD%CF%82-%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82-%CF%83%CF%84%CE%B7-%CE%B4%CE%B7%CE%BC/ (τελευταία πρόσβαση 2

Φεβρουαρίου 2017).

* Ένωση Συντακτών Ημερησίων Εφημερίδων Αθηνών (ΕΣΗΕΑ), *Περί ΕΣΗΕΑ-ιστορικό* στο www.esiea.gr. Online στο http://www.esiea.gr/istoriko/ (τελευταία πρόσβαση 24 Ιανουαρίου 2017)

* Ρέππα, Ε. (2011) ΔΙΑΔΙΚΤΥΟ VERSUS M.M.E., http://ereuna-mps.blogspot.gr/ (τελευταία πρόσβαση 5 Ιανουαρίου 2018)

* Δουλγκέρη. Φ, (2014) *Τα social media εισβάλλουν στην ενημέρωση. Η περίπτωση του Facebook Newswire* στο Medianalysis.net. Online στο http://medianalysis.net/2014/10/21/facebook_newswire/ (τελευταία πρόσβαση 14 Ιανουαρίου 2018).

* Ευσταθίου, Ν. (2017) *Τα «fake news» και η Δημοκρατία*, στο kathimerini.gr. Online στο http://www.kathimerini.gr/893925/article/epikairothta/kosmos/ta-fake-news-kai-h-dhmokratia (τελευταία πρόσβαση 22 Φεβρουαρίου 2018).

* Constine, J. (2016) *Facebook Live Audio makes talk radio social, starting with the BBC*, στο Techcrunch.com. Online στο https://techcrunch.com/2016/12/20/facebook-live-audio/?utm_source=Pew+Research+Center&utm_campaign=a11ef44fe9-EMAIL_CAMPAIGN_2016_12_21&utm_medium=email&utm_term=0_3e953b9b70-a11ef44fe9-399993749 (τελευταία πρόσβαση 17 Δεκεμβρίου 2017).

* Fenton, W. (2016) *How the Internet Affects What (and How) We Read*, στο PC. Online στο http://www.pcmag.com/commentary/344583/how-the-internet-affects-what-and-how-we-read, (τελευταία πρόσβαση 21 Δεκεμβρίου 2017).

* Zuckerberg. M. (2017) *Building Global Community*, στο Facebook. Online στο https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10103508221158471/

* Roberts, J. (2016) Opening up Instant Articles to All Publishers, στο media.fb.com. Online στο http://media.fb.com/2016/02/17/opening-up-instant-articles/ (τελευταία πρόσβαση 25 Δεκεμβρίου 2017).

* Bell, E. (2016) Facebook is eating the world, στο Columbia Journalism Review. Online στο http://www.cjr.org/analysis/facebook_and_media.php, (τελευταία πρόσβαση 14 Νοεμβρίου 2017).

* Galvin, J. (2016) Brussels, and the Perils of Rip and Ship Journalism στο blog.storyful.com. Online στο http://blog.storyful.com/2016/03/31/brussels-and-the-perils-of-rip-and-ship-journalism/#.V11a6PmLTIX, (τελευταία πρόσβαση 20 Νοεμβρίου 2017).

* Ματζούφας, Π. (2008) Ελευθερία έκφρασης και διαδίκτυο, https://www.constitutionalism.gr/1834-eleyteria-ekfrasis-kai-diadiktyo/ (τελευταία πρόσβαση 21Νοεμβρίου 2017).

*Φωτόπουλος, Τ. (2014) Ελευθερία Λόγου και Διαδίκτυο, http://www.inclusivedemocracy.org/fotopoulos/greek/grE/gre2014/2014_11_16.html

(τελευταία πρόσβαση 21 Νοεμβρίου 2017).

* Dimsis, (2011) Προσωπικά δεδομένα και Διαδίκτυο, http://www.log.gr/prosopika-dedomena-ke-diadiktuo/ (τελευταία πρόσβαση 5 Νοεμβρίου 2017).

* Βασιλόπουλου, Κ. (2015) Προστασία δεδομένων, ιδιωτικότητα και ασφάλεια στο Διαδίκτυο http://www.kathimerini.gr/836171/article/oikonomia/ellhnikh-oikonomia/apoyh-prostasia-dedomenwn-idiwtikothta-kai-asfaleia-sto-diadiktyo (τελευταία πρόσβαση 7 Νοεμβρίου 2017).

* sofokleousin,(2017) Τι αλλάζει για τα προσωπικά δεδομένα στο διαδίκτυο https://iservices.gr/blog/2017/02/02/ti-allazei-gia-ta-prosopika-dedomena-sto-diadiktio/ (τελευταία πρόσβαση 11 Νοεμβρίου 2017).

* Dampali, S. (2011) Νομοθεσία στην κοινωνία της πληροφορίας https://www.dampali.gr/νομοθεσία-στην-κοινωνία-της-πληροφορίας (τελευταία πρόσβαση 9 Οκτωβρίου 2017).

* SAVAGEAUG, C. (2013) N.S.A. Said to Search Content of Messages to and From U.S. SAVAGEAUG.www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=2& (τελευταία πρόσβαση 19 Οκτωβρίου 2017).

* MADRIGAL, A. (2012) I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web, https://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/ (τελευταία πρόσβαση 23 Οκτωβρίου 2017).

* Koumentakis, L. (2017) Προστασία Προσωπικών Δεδομένων Και Επιχειρήσεις https://koumentakislaw.gr/prostasia-prosopikon-dedomenon-kai-epixeirhseis/ (τελευταία πρόσβαση 3 Οκτωβρίου 2017).

* Broumas, A. (2015) Facebook & Ιδιωτικότητα : Δικαιώματα Χρηστών και Έννομη Προστασία http://lawandtech.eu/2015/02/02/facebook-data-protection/ (τελευταία πρόσβαση 5 Οκτωβρίου 2017).

* Lawspot.gr (2014) Ηλεκτρονικό έγκλημα https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/ilektroniko-egklima (τελευταία πρόσβαση 1 Οκτωβρίου 2017).

* Γιαγκουδάκης, Γ. (2013) Τι θα Πρέπει να Ξέρεις για το Έγκλημα στο Διαδίκτυο; 8 Απαντήσεις που Λύνουν Κάθε Απορία (Μέρος Α΄), http://www.kavalapress.gr/ti-tha-prepi-na-xeris-gia-to-egklima-sto-diadiktio-8-apantisis-pou-linoun-kathe-aporia-meros-a΄/ (τελευταία πρόσβαση 1 Σεπτεμβρίου 2017).

* Ψαρά, Μ. (2016) Ασφαλής υπολογιστής είναι μόνο ο... κλειστός, http://cert.auth.gr/index.php/el/mnu-announce/101-interview-sfakianakis (τελευταία πρόσβαση 17 Σεπτεμβρίου 2017).

* ΜΠΟΛΑΡΗ, Τ. (2017) Δίωξη Ηλεκτρονικού Εγκλήματος: Οδηγίες προστασίας από δράστες που «ψαρεύουν» προσωπικά δεδομένα, http://www.cnn.gr/news/ellada/story/95802/dioxi-hlektronikoy-egklimatos-odigies-prostasias-apo-drastes-poy-psareyoyn-prosopika-dedomena (τελευταία πρόσβαση 29 Σεπτεμβρίου

2017).

* Γκαρτζώνη, Δ. (2017) Μ. Σφακιανάκης: «Μέσα από το διαδίκτυο θα πλάσουμε τις νέες γενιές», http://www.dimokratiki.gr/18-06-2017/m-sfakianakis-mesa-apo-diadiktyo-tha-plasoume-tis-nees-genies/ (τελευταία πρόσβαση 29 Ιανουαρίου 2018).

* Γιαννακοπούλου, Κ. (2017) Συνέντευξη από έναν κορυφαίο χάκερ: «Δεν υπάρχει καμία ασφάλεια στο διαδίκτυο» http://www.alphafreepress.gr/sinentefxi-apo-enan-korifeo-chaker-den-iparchi-kamia-asfalia-sto-diadiktio/ (τελευταία πρόσβαση 28 Ιανουαρίου 2018).

* Rouse, M. (2017) phishing http://searchsecurity.techtarget.com/definition/phishing, (τελευταία πρόσβαση 10 Ιανουαρίου 2018).

* Αυγουστάκη, Ε. (2010) Διαδικτυακό έγκλημα – Παιδική πορνογραφία στο διαδίκτυο (Μέρος 1ο), http://otyposnews.gr/archives/3916 (τελευταία πρόσβαση 10 Δεκεμβρίου 2017).