ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΗΣ ΕΠΙΣΤΗΜΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΣΤΗΝ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΤΡΑΤΗΓΙΚΗ

ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΜΠΟΥΡΟΣ ΠΑΝΑΓΙΩΤΗΣ

Διπλωματική Εργασία υποβληθείσα στο Τμήμα Οικονομικών Επιστημών του Πανεπιστημίου Πειραιώς ως μέρους των απαιτήσεων για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης στην Οικονομική και Επιχειρησιακή Στρατηγική

Πειραιάς, Ιανουάριος 2023

UNIVERSITY OF PIRAEUS

DEPARTMENT OF ECONOMICS

MASTER PROGRAM IN ECONOMIC AND BUSINESS STRATEGY

SOCIAL NETWORKS AND PROTECTION OF PERSONAL DATA

BOUROS PANAGIOTIS

Master Thesis submitted to the Department of Economics of the University of Piraeus in partial fulfillment of the requirements for the degree of Master of Arts in Economic and Business Strategy

Piraeus, Greece, January 2023

Ευχαριστίες

Η ολοκλήρωση της παρούσας μεταπτυχιακής εργασίας θα ήταν αδύνατη χωρίς την στήριξη της επιβλέπων καθηγήτριάς μου Μαρία Ψυλλάκη. Θέλω να της εκφράσω ένα βαθύ ευχαριστώ για την βοήθεια που μου πρόσφερε. Επίσης ένα μεγάλο ευχαριστώ στον διευθυντή του μεταπτυχιακού προγράμματος Ιωάννη Πολλάλη για την άριστη συνεργασία όπως και για τον πολύτιμο χρόνο που διέθεσε δίνοντας μου χρήσιμες συμβουλές συμβάλλοντας σημαντικά στην ολοκλήρωση της εργασίας μου. Τέλος δεν μπορώ να αφήσω εκτός των ευχαριστιών την οικογένεια μου και συγκεκριμένα τον πατέρα μου ο οποίος αποτελεί για μένα ένα ανεκτίμητο στήριγμα και του οφείλω πολλά στη μέχρι τώρα πορεία μου.

Περίληψη

Μεταξύ των πολυτιμότερων αγαθών στις μέρες βρίσκεται και αυτό της πληροφορίας. Η παροχή πληροφοριών κατ' επιλογή των χρηστών μέσω του διαδικτύου και η εισαγωγή τους στον παγκόσμιο ιστό κατέστη δυνατή μέσω της πραγματοποιούμενης τεχνολογικής εξέλιξης. Για πλήθος οργανισμών και εταιρειών κάτι τέτοιο είναι ιδιαιτέρως σημαντικό στο πλαίσιο διαφήμισης και επίτευξης εμπορικών στόχων Υπάρχουν βέβαια περιπτώσεις κατά τις οποίες πραγματοποιείται ακούσια άντληση πληροφοριών κάτι που παραβιάζει την ιδιωτικότητα των πολιτών.

Βέβαια μετά την έναρξη εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων (GDPR), γίνεται προσπάθεια ώστε να προστατευτεί η ιδιωτική ζωή στο πλαίσιο επεξεργασίας των δεδομένων εντός των χωρών της ΕΕ αναγνωρίζοντας τον θεμελιώδη χαρακτήρα της προσωπικότητάς του. Ωστόσο, αν δε γίνει αποδοχή τους, μπορεί ο χρήστης να οδηγηθεί σε ένα μακροσκελές κείμενο που θα προσπαθήσει να τον πείσει να τα αποδεχτεί, ή ακόμα χειρότερα, να μη μπορέσει να ανοίξει καν τον ιστότοπο. Τελικά λαμβάνοντας υπόψη και το σύνολο των διαδικτυακών εφαρμογών κοινωνικών δικτύων θα ήταν δυνατόν να παραδεχτεί κανείς ότι μετά και τη θέσπιση του προαναφερθέντος κανονισμού, τα προσωπικά δεδομένα προστατεύονται πλήρως;

Abstract

Among the most valuable commodities today is information. The provision of information at the user's choice via the Internet and its introduction into the worldwide web has become possible due to technological development. For a number of organizations and companies, this is especially important in the context of advertising and achieving commercial goals. Of course, there are also cases when information is collected unintentionally, violating the privacy of citizens.

Of course, after the implementation of the General Data Protection Regulation (GDPR), attempts are made to protect privacy in the context of data processing in EU countries by recognizing the fundamental character of personality. However, if they are not accepted, the user may be led to a long text trying to convince him to accept them, or even worse, he may not even be able to open the website. Finally, taking into account all the online applications of social networks, could we admit that after the adoption of the aforementioned regulation, personal data is fully protected?

Πίνακας Περιεχομένων

Περίληψη **4**

Abstract **6**

ΚΕΦΑΛΑΙΟ Ι: Η ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ **12**

1.1 Τι ονομάζουμε «Κοινωνία της Πληροφορίας» 12

1.2 Ποιες αλλαγές έχουν έρθει με την Κοινωνία της Πληροφορίας 14

1.3 Η ιδιωτικότητα και η ανωνυμία στην σύγχρονη κοινωνία 15

ΚΕΦΑΛΑΙΟ ΙΙ: ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ **16**

2.1 Δημιουργία και εξέλιξη των μέσων κοινωνικής δικτύωσης 16

2.2 Το φαινόμενο Facebook 18

2.3 Προστασία της ιδιωτικότητας στην Ευρώπη 25

2.3.1 Επεξεργασία δεδομένων 27

2.3.2 Τα ευαίσθητα δεδομένα και η επεξεργασία δεδομένων μη μελών 30

2.4 Δικαιώματα των χρηστών 32

2.5 Η Ελληνική και η διεθνής νομοθεσία 33

2.6 Τα προσωπικά δεδομένα 37

2.7 Τα μέτρα για την προστασία των προσωπικών δεδομένων 39

2.8 Η ασφαλής περιήγηση στο διαδίκτυο 45

ΚΕΦΑΛΑΙΟ ΙΙΙ : SWOT ΑΝΑΛΥΣΗ ΤΟΥ FACEBOOK **47**

Επίλογος **54**

ΒΙΒΛΙΟΓΡΑΦΙΑ **56**

Ελληνική 56

Ξένη 57

Διαδίκτυο 59

Πίνακας Διαγραμμάτων

Γράφημα 1 Διακύμανση Εγγραφής Χρηστών Facebook, Πηγή: Statistica.com 47

Γράφημα 2 Διακύμανση Καθαρών Εσόδων Facebook, Πηγή: Statista.com 48

ΚΕΦΑΛΑΙΟ Ι: Η ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

1.1 Τι ονομάζουμε «Κοινωνία της Πληροφορίας»

Ο όρος «Κοινωνία της Πληροφορίας» χρησιμοποιείται περισσότερο στον ακαδημαϊκό λόγο και διευκρινίζει την παρουσία πληροφοριών. Ο όρος άρχισε να χρησιμοποιείται περίπου το 1970 και έπειτα άρχισε να αποκτά δημοτικότητα και ευρεία χρήση στην πολιτική και κοινωνική ζωή. Σε αυτό έχει συμβάλλει η επιταχυνόμενη ανάπτυξη και εξέλιξη των μέσων της τεχνολογίας καθώς και η εκπαίδευση (Κάλλας,2006).

Η διαρκής και επιταχυνόμενη ανάπτυξη των μέσων ενημέρωσης καθώς και της εκπαίδευσης και των νέων τεχνολογιών στον τομέα των επικοινωνιών και των ηλεκτρονικών υπολογιστών έχει οδηγήσει πολλούς να υποθέσουν ότι η συνακόλουθη έκρηξη πληροφοριών διακρίνει μια νέα εποχή. Η κοινωνία της πληροφορίας είναι μια κοινωνία στην οποία η ίδια η πληροφορία είναι το καθοριστικό χαρακτηριστικό της.

Στις μέρες μας χρησιμοποιούμε περισσότερες πληροφορίες στην καθημερινή μας ζωή. Ο όγκος των πληροφοριών που διατίθεται μέσω της τηλεόρασης, του διαδικτύου, των βιβλίων, των εφημερίδων και των περιοδικών έχει διευρυνθεί τόσο στις αναπτυσσόμενες όσο και στις ανεπτυγμένες χώρες (Κάλλας,2006).

Οι κοινωνίες της πληροφορίας έχουν τρία κύρια χαρακτηριστικά.

Α) Οι πληροφορίες χρησιμοποιούνται ως οικονομικός πόρος. Οι οργανισμοί κάνουν μεγαλύτερη χρήση των πληροφοριών για να αυξήσουν την αποτελεσματικότητά τους και την ανταγωνιστική τους θέση, συχνά μέσω της εξέλιξης στα αγαθά και τις υπηρεσίες που προσφέρουν (Bell The Coming of Post-Industrial Society, 1973).

Β) Είναι δυνατό να πραγματοποιηθεί μεγαλύτερη χρήση της ενημέρωσης του ευρύτερου κοινού. Οι άνθρωποι χρησιμοποιούν την πληροφόρηση εντατικότερα στις δραστηριότητές τους. Χρησιμοποιούν επίσης τις πληροφορίες ως πολίτες για να ασκήσουν τα

ατομικά τους δικαιώματα και τις υποχρεώσεις τους. Επιπλέον, αναπτύσσονται πληροφοριακά συστήματα που βοηθάνε στον τομέα του πολιτισμού και της γνώσης.

Γ) Είναι δυνατή η ανάπτυξη ενός τομέα πληροφοριών εντός μιας οικονομίας. Σημαντικό μέρος του κλάδου ασχολείται με την τεχνολογική υποδομή καθώς και τα δίκτυα τηλεπικοινωνιών και υπολογιστών. Σε όλες σχεδόν τις κοινωνίες της πληροφορίας, αυτός ο τομέας της πληροφορίας αναπτύσσεται τάχιστα (Bell The Coming of Post-Industrial Society (1973)).

1.2 Ποιες αλλαγές έχουν έρθει με την Κοινωνία της Πληροφορίας

Οι διαρθρωτικές αλλαγές που συνεχίζουν να συντελούνται, έχουν επίδραση στα πρότυπα απασχόλησης, φέρνοντας μαζί τους ανεργία και κοινωνική αναστάτωση. Παρατηρείται μια μετατόπιση του τρόπου απασχόλησης από τον πρωτογενή στον δευτερογενή τομέα και από τον δευτερογενή στον τριτογενή τομέα. (Bell The Coming of Post-Industrial Society,1973). Οι επενδύσεις επί των κεφαλαίων, σημαίνουν ότι η παραγωγή έχει παρουσιάσει αύξηση ενώ η εργασία μείωση. Στον πρωτογενή και δευτερογενή τομέα, η εργασία άλλαξε τρόπο και διεξάγεται μέσω των μηχανών. Το ίδιο συμβαίνει και στις κοινωνίες της πληροφόρησης. Αρκετοί εργαζόμενοι χάνουν την εργασία τους κάθε χρόνο εξαιτίας της εφαρμογής αυτοματοποιημένων διαδικασιών. Σε αναπτυγμένες-μεγάλες χώρες οι χρηματοοικονομικές αλλαγές πραγματοποιούνται ηλεκτρονικά, με αποτέλεσμα να μειωθούν τα άτομα που απασχολούνται στον τραπεζικό τομέα και να αναγκαστούν να βρουν αλλού εργασία (Κάλλας,2006).

Αυτές οι αλλαγές αλλάζουν την φύση της απασχόλησης. Αρκετές θέσεις εργασίας απαιτούν από τους εργαζόμενους περισσότερο χρόνο και γίνονται πιο εντατικές καθώς πρέπει να γίνει επεξεργασία μεγάλου όγκου πληροφοριών μέσω της τεχνολογίας.

Οι αλλαγές στον τρόπο εργασίας μέσω των πληροφοριών έχει πλεονεκτήματα καθώς και μειονεκτήματα. Οι εργαζόμενοι μπορούν να εργαστούν από το σπίτι, κάτι που πολλές φορές λειτουργεί αρνητικά για άτομα καθώς περνάνε αρκετό χρόνο στην οικεία τους, ενώ οι εργοδότες έχουν μεγαλύτερη εξουσία και ευελιξία για να απολύσουν και να προσλάβουν υπαλλήλους. Όλα τα παραπάνω δημιουργούν ένα αίσθημα ανασφάλειας στην αγορά εργασίας. Τα οφέλη από την κοινωνία της πληροφορίας, είναι ότι υπάρχει μεγαλύτερη αποτελεσματικότητα και παραγωγικότητα σε επιχειρήσεις και οργανισμούς, αυξημένες ευκαιρίες εκπαίδευσης, βελτίωση της υγειονομικής περίθαλψης και εφαρμογής τηλεϊατρικής, και αλλαγές στην διαχείριση του περιβάλλοντος (Κάλλας,2006).

1.3 Η ιδιωτικότητα και η ανωνυμία στην σύγχρονη κοινωνία

Η ιδιωτικότητα είναι δικαίωμα όλων. Αρκετοί όπως οι Warren και Brandeis[1], υποστήριξαν ότι οι πολιτικό-κοινωνικές και οικονομικές αλλαγές συμβαίνουν στην κοινωνία αρκετά συχνά και γι' αυτό τον λόγο ο νόμος πρέπει να αλλάζει και να δημιουργεί νέα δικαιώματα προκειμένου να ανταποκριθεί στις απαιτήσεις της νέας κοινωνίας και να εξασφαλίζεται η πλήρης προστασία των ατόμων. Η τεχνολογία αποτελεί απειλή για την ιδιωτικότητα. Λαμβάνοντας υπόψη αυτές τις αλλαγές, η κοινωνία έχει αρχίσει να αποζητά την αναγνώριση του δικαιώματος της ιδιωτικής ζωής. Η αρχή του δικαιώματος ήταν η απαραβίαστη προσωπικότητα. Η αναγνώριση αυτή οφείλεται στις κοινωνικές και τεχνολογικές αλλαγές που έκαναν την κοινή γνώμη υπέρ της αποδοχής της ιδιωτικής ζωής. Η Ευρώπη άρχισε να εξετάζει το δικαίωμα στην ιδιωτική ζωή πολύ αργότερα από τις ΗΠΑ και δημιούργησε ένα διαφορετικό είδος προστασίας (Warren, Brandeis).

[1] https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

ΚΕΦΑΛΑΙΟ ΙΙ: ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ

2.1 Δημιουργία και εξέλιξη των μέσων κοινωνικής δικτύωσης

Η γέννηση του διαδικτύου ξεκίνησε την δεκαετία του 1950 από μια κατάσταση που ονομάστηκε «Phreaking». Πρόκειται για έναν όρο που χρησιμοποιήθηκε για να ορίσει τις δραστηριότητες που εκτελούσαν άνθρωποι πάνω σε θέματα τηλεπικοινωνιών. Οι άνθρωποι άρχισαν να εργάζονται πάνω στα συστήματα των τηλεπικοινωνιών, να τα τροποποιούν και να πειραματίζονται[2].

Η ανάπτυξη του όρου έγινε από την Engressia και την Draper και ακολούθησε η εξάπλωσή του γρήγορα και ευρέως, με βοήθεια από τα μέσα ενημέρωσης. Αρκετοί λάτρεις της τεχνολογίας άρχισαν να ακολουθούν τα βήματά τους, ενώ προσπάθησαν να φτιάξουν δικές τους συσκευές με επιτυχία. Μεταξύ αυτών ήταν ο Steve Wozniakand και ο Steve Jobs που ίδρυσαν την εταιρεία Apple. Οι Tapriyal & Kanwar προσδιορίζουν τους χάκερς από την εποχή του Phreaking ως τους πρώτους που προσπάθησαν να δημιουργήσουν μέσα κοινωνικής δικτύωσης, πειραματιζόμενοι με τις αυτοσχέδιες ηλεκτρονικές συσκευές, χωρίς περιορισμούς στην πρόσβαση στο σύστημα τηλεπικοινωνιών.

Το 1999 σημειώθηκε μια άλλη σημαντική εξέλιξη στον τομέα των μέσων κοινωνικής δικτύωσης και αυτή ήταν η «κοινή χρήση». Μέχρι τώρα, κυρίως μέσω της αλληλεπίδρασης μεταξύ των χρηστών αλλά και με την επιλογή της «κοινής χρήσης», οι άνθρωποι μπορούσαν να μοιράζονται επίσης αρχεία και έγγραφα, μπορούσαν να τα «ανεβάσουν» ή ακόμη και να τα κατεβάσουν από οπουδήποτε, εφόσον ήταν μέρος της πλατφόρμας ή του φόρουμ (Tapriyal & Kanwar,2012). Τον Ιούνιο του 1999 μια εταιρεία με το όνομα Napster κυκλοφόρησε μια πλατφόρμα για κοινή χρήση αρχείων, με την ονομασία Peer-To-Peer, ευρύτερα γνωστή ως P2P. Το P2P ήταν μια πλατφόρμα για τη μεταφόρτωση και τη λήψη αρχείων μουσικής. Καθώς οι χρήστες του μπορούσαν να κατεβάσουν όποιο τραγούδι ήθελαν και να το εγγράψουν σε CD,

[2] https://en-m-wikipedia-org.translate.goog/wiki/Phreaking?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

επιτρέποντας την εύκολη πρόσβαση. Αργότερα πλατφόρμες όπως το BitTorrent μπήκαν στο παιχνίδι. Το 2003 παρουσιάστηκαν το LinkedIn και το MySpace. Το 2004 το Facebook πήρε τη θέση του στον κόσμο των μέσων κοινωνικής δικτύωσης και άλλαξε για πάντα τον τρόπο με τον οποίο οι άνθρωποι αλληλοεπιδρούσαν εντός του διαδικτύου (Tapriyal & Kanwar,2012).

Το Facebook ιδρύθηκε στις 4 Φεβρουαρίου 2004, από τον Zuckerberg, ο οποίος ήταν μέλος του Πανεπιστημίου Χάρβαρντ. Δικαίωμα συμμετοχής σε αυτό είχαν όλοι οι φοιτητές του Πανεπιστημίου Χάρβαρντ ενώ από το 2015 επετράπη η πρόσβαση και σε μαθητές λυκείων. Το 2018, όταν ο Zuckerberg πουλούσε τις μετοχές του, η κοινότητα του Facebook μετρούσε πάνω από ένα δισεκατομμύριο χρήστες[3].

Επιπλέον όσον αφορά την εταιρεία Google, σημειώνεται ότι έχει δημιουργήσει δικό της ιστότοπο κοινωνικής δικτύωσής της με το όνομα Google+ (Google Plus). Με την άφιξη των ιστότοπων κοινωνικής δικτύωσης το επίπεδο της διαδικτυακής αλληλεπίδρασης αυξήθηκε κατακόρυφα. Έτσι, μετά το 2008 η μορφή της διαδικτυακής αλληλεπίδρασης ήταν περισσότερο άμεση. Αυτό επέτρεψε την εμφάνιση του Twitter (micro blogging) που επέτρεπε στους χρήστες να γράφουν οτιδήποτε θέλουν χρησιμοποιώντας 140 χαρακτήρες και να μοιράζονται εικόνες, εικόνες, αρχεία ήχου, βίντεο και άλλα αρχεία και έγγραφα αμέσως. Ήταν περισσότερο σαν μια υπηρεσία σύντομων μηνυμάτων (SMS) για το διαδίκτυο. Πλέον το όριο έχει αυξηθεί στους 280 χαρακτήρες

[3] https://en.wikipedia.org/wiki/Facebook

2.2 Το φαινόμενο Facebook

Επί του παρόντος, η συλλογή δεδομένων αποτελεί ύψιστη προτεραιότητα για την προώθηση καθεμίας εταιρείας. Πολλές από τις διαδικτυακές υπηρεσίες που χρησιμοποιούνται σήμερα αναγκάζουν τους χρήστες να δημιουργούν προφίλ και να μοιράζονται προσωπικά δεδομένα με σκοπό την αποφυγή πολλές φορές επιβολής σε αυτούς χρηματικών τελών. Τα κοινωνικά δίκτυα τα οποία αποτελούν έναν εκ των πολλών τύπων των παρεχόμενων υπηρεσιών του Διαδικτύου, επιτρέπει στους χρήστες να παρουσιάζουν τους εαυτούς τους και να αλληλεπιδρούν με άλλους. Αυτό βέβαια διευκολύνει το έργο των διαφημιστικών εταιρειών καθώς μπορούν εύκολα να συλλέξουν δεδομένα ώστε να απευθύνονται κάθε φορά στο κατάλληλο αγοραστικό κοινό(Determann, 2012) .

Υπάρχουν πολλά κοινωνικά δίκτυα, με το καθένα από αυτά να δελεάζει τους χρήστες υποσχόμενο μια μοναδική κοινωνική εμπειρία, παρέχοντας επιπλέον ορισμένες βοηθητικές υπηρεσίες. Ωστόσο, το επιχειρηματικό μοντέλο σε όλα αυτά τα κοινωνικά δίκτυα είναι το ίδιο και αφορά την αντιστοίχιση των χρηστών με διαφημιστικές εταιρείες με απώτερο πάντα στόχο το κέρδος.

Ο ανταγωνισμός μεταξύ των κοινωνικών δικτύων για την προσέλκυση και τη διατήρηση των διαφημιζόμενων, με καινοτόμες μεθόδους και εργαλεία, περιστρέφεται όχι μόνο γύρω από τον αριθμό των εγγεγραμμένων σε αυτά χρηστών αλλά και γύρω από τον βαθμό αλληλεπίδρασης στον οποίον υπόκεινται οι χρήστες, ωθούμενοι να μοιραστούν τα δεδομένα τους με αντάλλαγμα τη δημιουργία ενός εξατομικευμένου και εύχρηστου περιβάλλοντος (Borgatti, Mehra, 2009).

Το Facebook είναι ένα τέτοιο διαδικτυακό κοινωνικό δίκτυο με περισσότερους από 2 δισεκατομμύρια μηνιαίως ενεργούς χρήστες [2.934 δισεκατομμύρια (Ιούλιος 2022)] και εκατομμύρια εφαρμογές και διαφημιστές. Όταν άρχισε να λειτουργεί το 2004, είχε ονομαστεί «thefacebook.com».

Κατά τη στιγμή της εγγραφής, οι χρήστες υποβάλλουν τα προσωπικά τους δεδομένα και προσδιορίσουν την ταυτότητά τους. Οι χρήστες συμφωνούν με την πολιτική απορρήτου της πλατφόρμας και επιτρέπουν σε αυτήν να χρησιμοποιεί τα δεδομένα που δημιουργούν κατά τη διάρκεια της κοινωνικής τους αλληλεπίδρασης με άλλους χρήστες, τις εφαρμογές, καθώς και τις αλληλεπιδράσεις εκτός πλατφόρμας με υπηρεσίες/ιστοσελίδες που βασίζονται στο Facebook για έσοδα από διαφημίσεις(Lampe, Ellison,&Understanding 2012).

Η διαδικτυακή δραστηριότητα των χρηστών και οι κοινωνικές σχέσεις τους, δίνουν στο Facebook μια μοναδική εικόνα για αυτούς. Τα προσωπικά δεδομένα που παρέχονται άμεσα από τους χρήστες, μαζί με τα έμμεσα, μεταξύ των οποίων συγκαταλέγονται το αναγνωριστικό συσκευής, η τοποθεσία, η διεύθυνση IP, κλπ., χρησιμοποιούνται για τη δημιουργία φακέλων σχετικά με τους χρήστες και την ομαδοποίηση των εξατομικευμένων προφίλ. Για παράδειγμα, υπάρχουν χρήστες που είναι ενεργοί τις πρωινές ώρες και χρησιμοποιούν εφαρμογές για την αξιολόγηση της φυσικής τους κατάστασης. Τέτοια άτομα συσχετίζονται με πιο υγιεινές επιλογές τροφίμων, τις οποίες η πλατφόρμα μπορεί να ενισχύσει εάν ο χρήστης είτε ενδιαφέρεται για αναρτήσεις/σελίδες/εκδηλώσεις που έχουν σχέση με τον υγιεινό τρόπο ζωής, είτε παραγγέλνει φαγητό χρησιμοποιώντας κάποια εφαρμογή που σχετίζεται με την εν λόγω πλατφόρμα. Τα συμπεράσματα που προκύπτουν και η συσχέτιση χρήστη και προϊόντος βάσει του αλγορίθμου του Facebook, γίνονται χωρίς τη συγκατάθεση/γνώση αυτού και παρουσιάζονται ως μια διαδικτυακή εμπειρία προσαρμοσμένη στις επιθυμίες του(Lampe, Ellison,&Understanding 2012).

Οι εφαρμογές/υπηρεσίες/ιστοσελίδες λειτουργούν ως συνεργάτες της πλατφόρμας και δεν εξυπηρετούν μόνο τον χρήστη αλλά κοινοποιούν στο ίδιο το Facebook τα αναλυτικά στοιχεία της αλληλεπίδρασης των χρηστών με την πλατφόρμα. Η πλατφόρμα παρακολουθεί συνεχώς, συλλέγει, αποθηκεύει και επεξεργάζεται δεδομένα χρηστών προκειμένου να είναι άμεσα χρήσιμα σε τρίτους, δηλαδή διαφημιστικές εταιρείες.

Η Ευρωπαϊκή Ένωση μέσω του «Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR)» επιχείρησε να προβεί στη διαχείριση των προσωπικών δεδομένων των χρηστών [8]. Αυτός ο κανονισμός υποχρεώνει τον υπεύθυνο επεξεργασία δεδομένων, κατόπιν επιθυμίας του χρήστη/ να διαγράψει όλα τα προσωπικά δεδομένα και οποιαδήποτε άλλα δεδομένα σχετικά με αυτόν τον χρήστη, που θα μπορούσαν ενδεχομένως να επιτρέψουν την αναγνώρισή του στο μέλλον. Ωστόσο, σύμφωνα με αναφορές, οι χρήστες συνεχίζουν να γίνονται δέκτες σχεδόν παρόμοιων αναρτήσεων-κατ' επέκταση διαφημίσεων με αυτές που λάμβαναν στο παρελθόν, κάτι που έρχεται σε αντίθεση με την αρχή GDPR(Lampe, Ellison,&Understanding 2012).

Πριν από την εποχή των διαδικτυακών κοινωνικών δικτύων ή την εποχή της διαφήμισης, υπήρχαν ήδη διαδικτυακές οντότητες που διευκόλυναν τις ηλεκτρονικές συναλλαγές και είχαν πρόσβαση στα δεδομένα των χρηστών και τις δραστηριότητές τους. Για παράδειγμα, το DNS, τα email, οι ψηφιακές βιβλιοθήκες, οι ομάδες συζητήσεων (forums) κλπ. Αλλά τα δεδομένα που παράγονταν σε αυτού του είδους τις ψηφιακές πλατφόρμες χρησιμοποιούνταν μόνο για σκοπούς ελέγχου, εντοπισμού απάτης και παροχής υπηρεσιών.

Στην τρέχουσα εποχή, σχεδόν κάθε διαδικτυακή υπηρεσία συλλέγει δεδομένα χρηστών με το πρόσχημα της εξατομίκευσης ή/και της βελτίωσης των παρεχόμενων υπηρεσιών. Εξαιτίας της απουσίας Κανονισμού Προστασίας Προσωπικών Δεδομένων για τη συλλογή, αποθήκευση, επεξεργασία και χρήση των δεδομένων, η συλλογή δεδομένων άνθιζε στο παρελθόν και ο πολλαπλασιασμός τους συνεχιζόταν χωρίς έλεγχο. Ο όγκος συλλογής δεδομένων και η ποικιλομορφία τους αυξήθηκε με την εμφάνιση των κοινωνικών δικτύων, των κινητών τηλεφώνων και το ζήτημα του απορρήτου των χρηστών άρχισε να υπονομεύει την εμπιστοσύνη στο διαδικτυακό σύστημα δεδομένων.

Επισημαίνεται ότι τα κοινωνικά δίκτυα απαιτούν ιδιαίτερη προσοχή γιατί σε αυτές τις πλατφόρμες οι χρήστες αποκαλύπτουν οικειοθελώς τα προσωπικά τους δεδομένα χωρίς να το συνειδητοποιούν κάτι που έχει σοβαρές επιπτώσεις στην ιδιωτικότητά τους.

Το Facebook είναι η επιτομή των κοινωνικών δικτύων ως το πιο επιτυχημένο από αυτά, με τον μεγαλύτερο αριθμό εγγεγραμμένων χρηστών, που όχι μόνο τροφοδοτούνται από την πλατφόρμα κάθε αυτή για τις ανάγκες κοινωνικής επικοινωνίας αλλά και μέσω βοηθητικών και σχετιζόμενων υπηρεσιών. Οι χρήστες ταυτοποιούνται και ομαδοποιούνται σύμφωνα με τα ενδιαφέροντά τους. Αυτό συμβάλει στη δημιουργία εσόδων για το Facebook μέσω των διαφημίσεων, επιβραβεύοντας παράλληλα τους χρήστες με ένα εξατομικευμένο περιβάλλον που διευκολύνει τις κοινωνικές επικοινωνίες(Lampe, Ellison,&Understanding 2012).

Υπολογίζεται ότι το σύνολο των εσόδων του σε τριμηνιαία βάση αγγίζει το ποσό των 2,6 δισεκατομμυρίων δολαρίων και η περιουσία του ιδρυτή του εκτιμάται στα 1,5 δισεκατομμύρια δολάρια. Καθημερινά, το σύνολο των χρηστών δημοσιεύει ένα πλήθος 15 εκατομμυρίων φωτογραφιών κατ' εκτίμηση.

Η πρόσβαση εντός της εν λόγω πλατφόρμας πραγματοποιείται μέσω της ιστοσελίδας www.facebook.com από Η/Υ και διαμέσου της m.facebook.com με τη χρήση κινητών συσκευών και σχετικών εφαρμογών.

Η υπόψη πλατφόρμα διακρίνεται για την πληθώρα επιλογών , το πλήθος των λειτουργιών, τις πολλαπλές δυνατές ρυθμίσεις που όμως, συχνά τη μετατρέπει σε αρκετά δύσχρηστη για την πλειοψηφία των χρηστών.

Προϋπόθεση για τη δημιουργία προφίλ αποτελεί η συμπλήρωση του 13^{ου} έτους ηλικιακά από τον υποψήφιο χρήστη, ο οποίος στη συνέχεια έχει τη δυνατότητα να πραγματοποιεί αλλαγές στις πληροφορίες και οπτικοακουστικά μέσα που έχει ο ίδιος παραθέσει/προσθέσει. Στη διακριτική ευχέρεια των χρηστών βρίσκεται το τι θα έχουν δυνατότητα οι λοιποί λογαριασμοί να βλέπουν όσον αφορά τα στοιχεία που δημοσιεύονται. Μάλιστα, διαμέσου της ξεχωριστής λειτουργίας των "Groups" και των "Events" δίνεται η δυνατότητα στο σύνολο των εγγεγραμμένων σε αυτά χρηστών να παρακολουθούν ξεχωριστά δημοσιεύσεις που σχετίζονται με τις ομάδες για τις οποίες έχουν δείξει ενδιαφέρον.

Όπως προαναφέρθηκε μια εκ των πιο πρόσφατων σχετικά δραστηριοτήτων του Facebook είναι οι παρεμβάσεις του στην καθημερινότητα μέσω των πληροφοριών που αντλεί από τους χρήστες για τις επιθυμίες τους, τα σημεία στα οποία βρίσκονται και το τι κάνουν μια δεδομένη στιγμή. Είναι επιπρόσθετα δυνατή η καταγραφή συνομιλιών των υπαλλήλων εταιρειών και πελατών για σκοπούς πωλήσεων και διαφημίσεων(Lampe, Ellison,&Understanding 2012).

Αδιαμφισβήτητα, στο διαδίκτυο υπάρχουν πολλές ιστοσελίδες και διαδικτυακές υπηρεσίες οι οποίες έφτασαν σε μια ορισμένη χρονική στιγμή τον μέγιστο πλήθος εγγεγραμμένων λογαριασμών και στη συνέχεια οδηγήθηκαν στην παρακμή αφού νέες ιστοσελίδες που παρουσίασαν περισσότερες καινοτομίες και εργονομία τις παραγκώνισαν. Κάτι τέτοιο έμοιαζε για το Facebook μέχρι πριν κάποια χρόνια ουτοπικό σενάριο αφού φάνταζε ως ταυτισμένο με την καθημερινότητα του μέσου χρήστη ο οποίος είχε προβεί σε ενσωμάτωση των τεχνολογιών στην ζωή του. Η εν λόγω πλατφόρμα είχε αναδειχθεί σε διεθνή κυρίαρχο και ταυτιζόταν με την έννοια της διαδικτυακής ταυτότητας κάθε ανθρώπου. Για την επίτευξη της κυριαρχίας του καθοριστικό ήταν ότι το Facebook φρόντιζε να εξαγοράζει κάθε πιθανή αντίπαλη ιστοσελίδα και να μην επιτρέπει σε αυτήν να αναδειχθεί.

Παρόλα αυτά, κανείς δεν μπορεί να αγνοήσει ότι κατά τη διάρκεια της πρόσφατης περιόδου το Facebook μοιάζει να απαξιώνεται από πλήθος χρηστών του οι οποίοι φαίνονται δυσαρεστημένοι. Αίτια αυτού είναι αφενός το ξέσπασμα πολιτικών σκανδάλων, το γεγονός ότι υπάρχει η φήμη ότι διαρρέουν προσωπικά δεδομένα για εκπλήρωση αθέμιτων στόχων καθώς και πλήθος φημών που αναφέρουν ότι το Facebook λειτουργεί ως μέσω χειραγώγησης των μαζών στον βωμό εξυπηρέτησης συμφερόντων. Άλλωστε ο εθισμός που προκαλεί η εν λόγω πλατφόρμα θα μπορούσε να βλάψει τόσο τους ίδιους τους χρήστες σε σωματικό και εγκεφαλικό επίπεδο όσο και το ίδιο το δημοκρατικό πολίτευμα (Kinast, Partner2014).

Μάλιστα είναι γνωστό, συμφώνως των παραδοχών του Facebook ότι πολλές φορές το σύστημα είχε χρησιμοποιηθεί από μερίδα ισχυρών για να εξυπηρετήσουν τα συμφέροντά τους. Κατά το 2016, Ρώσοι το είχαν χρησιμοποιήσει ώστε να συμβάλουν στο να εκλεγεί ο Donald Trump. Επιπλέον είχε λάβει χώρα διαρροή προσωπικών δεδομένων από 90 εκατομμύρια λογαριασμούς, ενέργεια η οποία δεν είχε εγκριθεί από τους χρήστες. Παράλληλα είναι αρκετές οι περιπτώσεις υποκλοπής δεδομένων από επιτήδειους (χάκερς). Τα εν λόγω γεγονότα ήταν καθοριστικά ώστε να λάβει χώρα ραγδαία υποχώρηση των μετοχών του Facebook.

Βέβαια το Facebook διακρίνεται αναμφίβολα για τη δύναμή του στον χώρο της διαφήμισης, εξαιτίας της τεράστιας απήχησής του σε πολλές και διαφορετικές ηλικίες ατόμων που ανήκουν σε πλήθος κοινωνικών ομάδων. Τα δεδομένα που έχει συλλέξει έχουν πολύ μεγάλο μέγεθος και το πιο σημαντικό είναι ότι έχουν έρθει στην κατοχή του κατόπιν έγκρισης των χρηστών. Επομένως έγινε εύκολο για το Facebook να προβαίνει σε εντοπισμό προτιμήσεων και στην διαμόρφωση της προσωποποιημένης διαφημιστικής στρατηγικής. Αδιαμφισβήτητα και συγκρινόμενο με τις λοιπές παραδοσιακές διαφημιστικές μεθόδους είναι φανερή η κυριαρχία του Facebook εξαιτίας, κατά κύριο λόγο, του πολύ χαμηλού κόστους για την παροχή της εν λόγω υπηρεσίας (Liu, Gummadi, &Krishnamurthy,2011).

Όσον αφορά το ξέσπασμα σκανδάλων που κατά καιρούς έχουν δημοσιευθεί για το Facebook σημειώνεται ότι είναι κάτι που έχει συμβεί στο παρελθόν προκαλώντας αναστάτωση στους εγγεγραμμένους χρήστες. Αξίζει να αναφερθεί το πρωταρχικό σκάνδαλο που αφορούσε τη φήμη κλοπής της ιδέας δημιουργίας του Facebook από τον Zuckerberg αν και αρχικά την είχαν επινοήσει άλλοι φοιτητές. Το δικαστήριο δεν οδηγήθηκε ποτέ σε λύση του μυστηρίου αφού οι δύο πλευρές συμβιβάστηκαν εξωδικαστικά. Άλλα σκάνδαλα αφορούν την κατά διαστήματα εκούσια παραγωγή ψευδών ειδήσεων, την υποκλοπή προσωπικών δεδομένων χρηστών με σκοπών την διαμόρφωση πολιτικής γνώμης και άποψης, την άσκηση επιρροής στην κριτική σκέψη των πολιτική και τελικά την εκλογή του Trump το 2016, την ηχογράφηση

συζητήσεων χρηστών από υπαλλήλους του Facebook καθώς και την εξαπάτησή τους από ψεύτικα προφίλ.

Επισημαίνεται ότι έχουν επιβληθεί χρηματικά πρόστιμα στο Facebook εξαιτίας των μη αποδεκτών πρακτικών που χρησιμοποιεί για τη συλλογή προσωπικών δεδομένων των χρηστών, οδηγούμενο κατ' επέκταση σε παραβάσεις. Άλλωστε το Facebook δεν προβαίνει μόνο στη συλλογή δεδομένων που εισάγονται από τον χρήστη. Αντίθετα προβαίνει σε καταγραφή των ιστοτόπων που επισκέπτονται οι χρήστες ακόμα και αν είναι αποσυνδεδεμένος από την πλατφόρμα.

2.3 Προστασία της ιδιωτικότητας στην Ευρώπη

Η Ευρωπαϊκή Ένωση αποτελείται από τα γνωστά κράτη μέλη, και ένα μέρος της κυριαρχίας της και ορισμένες εξουσίες της για την λήψη αποφάσεων τιςς έχει μεταβιβάσει στο Ευρωπαϊκό Συμβούλιο, το Ευρωπαϊκό Κοινοβούλιο και την Ευρωπαϊκή Επιτροπή. Η Ευρωπαϊκή Επιτροπή προτείνει νέους νόμους, το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο τους εγκρίνει και στη συνέχεια τα κράτη μέλη και η Ευρωπαϊκή Επιτροπή τα εφαρμόζουν. Οι κανονισμοί που εγκρίνονται είναι εφαρμοστέοι και δεσμευτικοί για όλα τα κράτη μέλη, ενώ κάποιοι νόμοι μπορεί να χρειαστεί να τροποποιηθούν. Η Ευρωπαϊκή Ένωση προσπαθεί να αποτελέσει παγκόσμιο πρότυπο για την ψηφιακή οικονομία και την διεθνή προώθηση των ψηφιακών προτύπων. Η ρύθμιση των μέσων κοινωνικής δικτύωσης συμβάλλει στη θέσπιση παγκόσμιων κανόνων (Αλεξανδροπούλου-Αιγυπτιάδου Ε,2007).

Στις 25 Μαΐου 2018, τέθηκε σε ισχύ ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)[4]. Έμοιαζε πολλά υποσχόμενος και ικανός να οδηγήσει στην περαιτέρω ανάπτυξη. Σκοπός του ήταν να εναρμονίσει τους νόμους περί απορρήτου και προστασίας δεδομένων σε όλη την Ευρώπη, βοηθώντας παράλληλα τους πολίτες της ΕΕ να κατανοήσουν καλύτερα τον τρόπο με τον οποίο χρησιμοποιούνται τα προσωπικά τους στοιχεία και ενθαρρύνοντάς τους να υποβάλουν καταγγελία σε περίπτωση παραβίασης των δικαιωμάτων τους. Ως νέο ρυθμιστικό πλαίσιο, ο GDPR αποτέλεσε την αναγνώριση ότι η ψηφιακή οικονομία —που τροφοδοτείται από (προσωπικές) πληροφορίες— πρέπει να λειτουργεί με την συγκατάθεση των χρηστών και με σαφείς κανόνες για εταιρείες που επιδιώκουν να δραστηριοποιηθούν στην Ευρωπαϊκή Ένωση[5].

Η πολιτική βούληση σε συνάρτηση με τα όσα προέβλεπε ο GDPR, οδηγούταν από την ανησυχία ότι τα προσωπικά στοιχεία των ατόμων υφίστανται εκμετάλλευση με τρόπους που

[4] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=el

[5] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=el

υπονόμευαν το απόρρητο και κατ' επέκταση, τη δημοκρατία. Ένας ιστότοπος απαιτείται σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) της ΕΕ να επιτρέπει στους χρήστες από την Ευρώπη να ελέγχουν την ενεργοποίηση των cookies και των ιχνηλατών που συλλέγουν τα προσωπικά τους δεδομένα.

Αξιοσημείωτο είναι ότι μετά την εφαρμογή του GDPR, αυξήθηκε ο αριθμός των ατόμων που άνθρωποι έκαναν κλικ στο «Συμφωνώ» και στο «Αποδέχομαι» σε σχέση με τα προηγούμενα χρόνια.Σύμφωνα με τις προβλέψεις της νέας νομοθεσίας τα κουμπιά αυτά ήταν οι βασικές μορφές αλληλεπιδράσειςστα μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούσαν συναίνεση. Η ειδοποίησης απορρήτου και η αποδοχή της από τους χρήστες ήταν οι κυρίαρχες προσεγγίσεις που ακολουθούσαν οι περισσότεροι οργανισμοί, ωστόσο η πράξη του γρήγορου κλικ σε ένα κουμπί για την συναίνεση εμφάνισε «κόπωση της συναίνεσης» μπροστά σε μια ατέλειωτη ροή αόριστα διατυπωμένων και συχνά αδιάβαστων ειδοποιήσεων έτσι ο τρόπος αυτός που χρησιμοποιείται από τους οργανισμούς ενδέχεται να μην είναι αποτελεσματικός(Μήτρου,2002).

Το νομοθετικό πλαίσιο του GDPR στην πραγματικότητα αποτελεί μια στην πολιτική ειδοποιήσεων που αφορούν την παραβίαση. Αυτή η πολιτική βασίζεται στην ιδέα ότι όταν συμβαίνει μια παραβίαση, η "εποπτική αρχή" πρέπει να ειδοποιείται εντός 72 ωρών, με απώτερο στόχο την ειδοποίηση των επηρεαζόμενων χρηστών, ώστε να μπορούν να αναλάβουν δράση για την προστασία του εαυτού τους (και των πληροφοριών τους). Σημειώθηκε τεράστια αύξηση στις αναφορές παραβάσεων (συμπεριλαμβανομένης της αυτοαναφοράς). Σύμφωνα με τη Διεθνή Ένωση Επαγγελματιών Προστασίας Προσωπικών Δεδομένων (IAPP), έχουν αναφερθεί περισσότερα από 89.000 περιστατικά — περίπου διπλάσιο από το προηγούμενο ποσοστό. Η υποχρέωση άμεσης και έγκαιρης ειδοποίησης ατόμων για δυνητικά επιζήμιες παραβιάσεις είναι ένα παράδειγμα του αναμφισβήτητα θετικού αντίκτυπου ενός ενοποιημένου

κανονισμού που διευρύνει τον ορισμό των προσωπικών δεδομένων και τα πρωτόκολλα γύρω από τη χρήση τους[6].

Υπάρχουν διατάξεις που σχετίζονται με το δικαίωμα των ατόμων να διατηρούν τα δεδομένα τους από το να υπόκεινται σε αποκλειστικά αυτοματοποιημένη λήψη αποφάσεων που έχει νομικές ή άλλες σημαντικές επιπτώσεις, όπως η δημιουργία προφίλ. Ωστόσο, η συνολική έλλειψη ακρίβειας στον τρόπο με τον οποίο ορίζονται τα δικαιώματα των υποκειμένων των δεδομένων σε σχέση με τεχνητά ευφυή αλγοριθμικά συστήματα καθιστά τον GDPR τρωτό σε αυτόν τον τομέα. Το πρόβλημα είναι ότι η αυτοματοποιημένη λήψη αποφάσεων εξακολουθεί να είναι σχετικά νέα και τα συστήματα για τον έλεγχο και την επίβλεψή τους γενικά δεν έχουν ακόμη τεθεί σε εφαρμογή[7].

2.3.1 Επεξεργασία δεδομένων

Τα δεδομένα στην ακατέργαστη μορφή τους δεν είναι χρήσιμα σε κανέναν οργανισμό. Η επεξεργασία δεδομένων είναι η μέθοδος συλλογής ακατέργαστων δεδομένων και μετατροπής τους σε πληροφορίες που μπορούν να χρησιμοποιηθούν. Συνήθως αυτό γίνεται μέσω μιας διαδικασίας, βήμα προς βήμα, από μια ομάδα επιστημόνων σε έναν οργανισμό, η οποία μελετά όλα τα διαθέσιμα δεδομένα. Τα ακατέργαστα δεδομένα συλλέγονται, φιλτράρονται, ταξινομούνται, επεξεργάζονται, αναλύονται, αποθηκεύονται και στη συνέχεια παρουσιάζονται σε αναγνώσιμη μορφή[8].

Η επεξεργασία δεδομένων είναι απαραίτητη για τους οργανισμούς, ώστε να δημιουργήσουν καλύτερες επιχειρηματικές στρατηγικές και να αυξήσουν το ανταγωνιστικό τους πλεονέκτημα. Μετατρέποντας τα δεδομένα σε αναγνώσιμες μορφές όπως γραφήματα και

[6] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=el

[7] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=el

[8] https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_el

έγγραφα, οι εργαζόμενοι σε όλο τον οργανισμό μπορούν να τα κατανοήσουν και να τα χρησιμοποιήσουν ανάλογα.

Η μέθοδος της μη αυτόματης επεξεργασίας δεδομένων είναι εκείνη κατά την οποία οι ειδικοί εισαγωγής δεδομένων καταγράφουν και επεξεργάζονται δεδομένα με μη αυτόματο τρόπο μέσω χειροκίνητων διαδικασιών. Αν και είναι μία από τις πρώτες μεθόδους επεξεργασίας δεδομένων, η χειροκίνητη εισαγωγή δεδομένων είναι δαπανηρή, χρονοβόρα, επιρρεπής σε σφάλματα και απαιτεί πολύωρη εργασία. Η μηχανική επεξεργασία δεδομένων επεξεργάζεται δεδομένα μέσω μηχανικών συσκευών όπως γραφομηχανές, μηχανικοί εκτυπωτές και άλλες συσκευές. Αν και είναι ταχύτερη από τη μέθοδο χειροκίνητης επεξεργασίας δεδομένων, άρχισε να εξασθενεί κατά τη διάρκεια των τεχνολογικών επιτευγμάτων που τη διαδέχθηκαν[9].

Η επεξεργασία σε πραγματικό χρόνο δημιουργήθηκε με την έλευση του Διαδικτύου. Με τη χρήση του διαδικτύου, αυτή η μέθοδος επεξεργασίας αφορά τη λήψη και επεξεργασία δεδομένων ταυτόχρονα. Με απλά λόγια, συλλέγει δεδομένα σε πραγματικό χρόνο και δημιουργεί γρήγορες ή αυτόματες αναφορές. Ως εκ τούτου, αυτή είναι μια από τις ταχύτερες μεθόδους επεξεργασίας δεδομένων. Η ηλεκτρονική επεξεργασία δεδομένων συχνά συγχέεται με την επεξεργασία δεδομένων σε πραγματικό χρόνο. Λαμβάνουν και επεξεργάζονται δεδομένα ταυτόχρονα, αλλά με την ηλεκτρονική επεξεργασία, ο χρήστης μπορεί να εξάγει δεδομένα οποτεδήποτε, οπουδήποτε. Το σύστημα γραμμικού κώδικα είναι το καλύτερο παράδειγμα ηλεκτρονικής επεξεργασίας. Ένα άλλο συγκεκριμένο παράδειγμα είναι οι κάρτες πρόσβασης. Οι σημερινοί νέοι εισέρχονται στη νέα εποχή της επεξεργασίας δεδομένων με την είσοδο της Τεχνητής Νοημοσύνης. Η επεξεργασία δεδομένων δεν μπορεί παρά να γίνει καλύτερη, περιορίζοντας την ανθρώπινη παρέμβαση, εισάγοντας δεδομένα σε πραγματικό

[9] https://texnologia.net/ti-einai-epexergasia-dedomenon-kai-se-ti-chrisimeuei/2018/10

χρόνο, χωρίς σφάλματα και με ασφάλεια περισσότερη από οποιαδήποτε μέθοδο επεξεργασίας (Κάτσικας).

2.3.2 Τα ευαίσθητα δεδομένα και η επεξεργασία δεδομένων μη μελών

Τα ευαίσθητα προσωπικά δεδομένα είναι δεδομένα που αποκαλύπτουν θρησκευτικές, πολιτικές απόψεις, φυλετική ή εθνική καταγωγή και φιλοσοφικές πεποιθήσεις. Επίσης η συμμετοχή σε ομάδες που έχουν να κάνουν με την σεξουαλική ζωή και υγεία θεωρούνται ευαίσθητα δεδομένα. Τα ευαίσθητα προσωπικά δεδομένα μπορούν να δημοσιεύονται στο Διαδίκτυο μόνο με τη ρητή συγκατάθεση. Σε ορισμένα κράτη μέλη της ΕΕ, οι εικόνες θεωρούνται ειδική κατηγορία προσωπικών δεδομένων, δεδομένου ότι μπορούν να χρησιμοποιηθούν για τη διάκριση μεταξύ φυλετικής/εθνοτικής καταγωγής ή μπορεί να χρησιμοποιηθούν για την εξαγωγή δεδομένων που σχετίζονται με την υγεία και τις θρησκευτικές πεποιθήσεις. Οι εικόνες στο διαδίκτυο δεν αποτελούν ευαίσθητα δεδομένα εκτός εάν αποκαλύπτουν ευαίσθητα δεδομένα για άτομα (Ιγγλεζάκης,2003).

Ως υπεύθυνοι επεξεργασίας δεδομένων, τα κοινωνικά δίκτυα δεν μπορούν να επεξεργάζονται ευαίσθητα δεδομένα σχετικά με μέλη ή μη μέλη κοινωνικών δικτύων χωρίς τη ρητή συγκατάθεσή τους. Εάν περιλαμβάνεται στη φόρμα προφίλ των χρηστών οποιεσδήποτε ερωτήσεις σχετικά με ευαίσθητα δεδομένα, τα κοινωνικά δίκτυα πρέπει να καθιστούν σαφές ότι οι απαντήσεις σε αυτές τις ερωτήσεις είναι εντελώς εθελοντικές. Πολλές κοινωνικών δικτύων επιτρέπουν στους χρήστες να συνεισφέρουν δεδομένα σχετικά με άλλα άτομα, όπως η προσθήκη ονόματος σε μια φωτογραφία ή βαθμολογία σε ένα άτομο και εκδηλώσεις γ αυτόν (Ιγγλεζάκης, 2003). Η επισήμανση αυτή μπορεί να προσδιορίσει σαφώς τα μη μέλη ωστόσο, η επεξεργασία τέτοιων δεδομένων σχετικά με τα μη μέλη εντός ενός κοινωνικού δικτύου, μπορεί να εκτελεστεί μόνο αν ισχύουν κάποια κριτήρια του άρθρου 7 περι επεξεργασίας προσωπικών δεδομένων.

Η δημιουργία προκατασκευασμένων προφίλ μη μελών μέσω της συγκέντρωσης δεδομένων που ανεξαρτήτων χρηστών SNS, συμπεριλαμβανομένων των δεδομένων σχέσεων που προέρχονται στερείται νομικής βάσης. Ακόμα κι αν το SNS είχε τα μέσα να επικοινωνήσει

με τον μη χρήστη και να ενημερώσει αυτόν για την ύπαρξη προσωπικών δεδομένων που τον αφορούν, πιθανή να λάβει πρόσκληση μέσω e-mail για συμμετοχή στο SNS προκειμένου να αποκτήσετε πρόσβαση σε αυτά τα προσωπικά δεδομένα και με αυτόν τον τρόπο παραβίαζε την απαγόρευση που ορίζεται στο άρθρο 13.4 για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες σχετικά με την αποστολή ηλεκτρονικών μηνυμάτων για άμεσο μάρκετινγκ.

2.4 Δικαιώματα των χρηστών

Ένα κοινωνικό δίκτυο θα πρέπει να σέβεται τα δικαιώματα των ατόμων των οποίων υπόκεινται σε επεξεργασία, σύμφωνα με τις διατάξεις που ορίζονται στα άρθρα 12 και 14 της οδηγίας για την προστασία των προσωπικών δεδομένων. Τα δικαιώματα αυτά δεν αφορούν μόνο τους χρήστες της υπηρεσίας αλλά και οποιοδήποτε φυσικό πρόσωπο του οποίου τα δεδομένα υποβάλλονται σε επεξεργασία.

Η αρχική σελίδα των τοποθεσιών θα πρέπει να αναφέρεται ξεκάθαρα στην ύπαρξη «γραφείου διεκπεραίωσης παραπόνων» που έχει συσταθεί πάροχος για την αντιμετώπιση ζητημάτων προστασίας δεδομένων και απορρήτου και καταγγελιών τόσο από μέλη όσο και από μη μέλη. Το άρθρο 6 παράγραφος 1 της Οδηγίας για την Προστασία Δεδομένων απαιτεί τα δεδομένα να είναι επαρκή σε σχέση με τους σκοπούς για τους οποίους συλλέγονται.

Σε αυτό το πλαίσιο, μπορεί να παρατηρηθεί ότι μπορεί να χρειαστεί να καταχωρίσει κάποιος ορισμένα στοιχεία για ταυτοποίηση δεδομένων σχετικά με τα μέλη, αλλά δεν χρειάζεται να εμφανίζεται το πραγματικό όνομα των μελών στο Διαδίκτυο. Επομένως θα πρέπει να εξεταστεί προσεκτικά εάν μπορεί να δικαιολογήσει τον εξαναγκασμό των χρηστών του να ενεργήσουν με την πραγματική τους ταυτότητα παρά με ψευδώνυμο. Το άρθρο 17 της οδηγίας για την προστασία δεδομένων απαιτεί από τον υπεύθυνο επεξεργασίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων. Ειδικότερα, τα μέτρα ασφαλείας περιλαμβάνουν μηχανισμούς ελέγχου πρόσβασης και επαλήθευσης ταυτότητας που μπορούν να ισχύσουν ακόμα και κάποιος χρησιμοποιεί ψευδώνυμο.

2.5 Η Ελληνική και η διεθνής νομοθεσία

Στις 23.09.2020 ο Ελληνικός Νόμος 4727/2020[10] « Ψηφιακή Διακυβέρνηση (Μεταφορά στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) – Ηλεκτρονικές Επικοινωνίες (Μεταφορά στην Ελληνική Οδηγία ΕΕ) 2018/1972) και άλλες διατάξεις » δημοσιεύτηκε στην Εφημερίδα της Κυβερνήσεως (Α' 184/23.09.2020).). Ο νόμος 4727/2020 ενσωματώνει στην ελληνική έννομη τάξη, μεταξύ άλλων, την Οδηγία (ΕΕ) 2018/1972 για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών («ΕΕCC»), καθώς και την Οδηγία (ΕΕ) 2016/2102 για την προσβασιμότητα των ιστοσελίδων. και κινητές εφαρμογές φορέων του δημόσιου τομέα και Οδηγία (ΕΕ) 2019/1024 για τα ανοιχτά δεδομένα και την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα.

Η εν λόγω νομοθεσία μεταρρυθμίζει και εκσυγχρονίζει το νομικό καθεστώς των τηλεπικοινωνιών στην Ελλάδα τόσο για τις υπηρεσίες όσο και για τα δίκτυα. Μεταξύ άλλων, περιλαμβάνει διατάξεις για Γενική Εξουσιοδότηση, Δίκτυα/Υπηρεσίες Ηλεκτρονικών Επικοινωνιών, Επιβολή, Διαδικασίες Εσωτερικής Αγοράς, Ασφάλεια, Πρόσβαση στην Αγορά και Ανάπτυξη, Υποχρεώσεις Καθολικής Υπηρεσίας, Πηγές Αρίθμησης, Δικαιώματα Τελικών Χρηστών κ.λπ. Επιπλέον, Ν. 4727 /2020 περιέχει διατάξεις για την ψηφιακή κατάσταση, η ηλεκτρονική επικοινωνία, οι αλληλεπιδράσεις και οι συναλλαγές με το κράτος μέσω της πληροφορικής, της ψηφιακής διακυβέρνησης, των ηλεκτρονικών εγγράφων και των ψηφιακών δημόσιων υπηρεσιών, των ανοιχτών δεδομένων[11]. Επιπλέον, ο Νόμος 4727/2020 περιλαμβάνει ένα κεφάλαιο για την ανάπτυξη του ψηφιακού οικοσυστήματος 5G στην Ελλάδα. Η Ελληνική Εθνική Στρατηγική Κυβερνοασφάλειας εφαρμόζεται από την 1η Σεπτεμβρίου 2017, καθορίζοντας τις βασικές αρχές και θέτει στρατηγικούς στόχους και το πλαίσιο δράσης μέσω

[10] https://www.kodiko.gr/nomothesia/document/640620/nomos-4727-2020

[11] https://www.kodiko.gr/nomothesia/document/640620/nomos-4727-2020

του οποίου θα επιτευχθούν. Την εφαρμογή του NCSS αναλαμβάνει η νεοσύστατη Εθνική Αρχή Κυβερνοασφάλειας[12].

Το NCSS προσδιορίζει 8 επιμέρους στόχους[13]:

1. Αναβάθμιση του επιπέδου πρόληψης, αξιολόγησης, ανάλυσης και αποτροπής απειλών κατά της ασφάλειας συστημάτων και υποδομών ΤΠΕ.
2. Βελτιωμένη ικανότητα των ενδιαφερομένων του δημόσιου και του ιδιωτικού τομέα να αποτρέπουν και να χειρίζονται περιστατικά ασφάλειας στον κυβερνοχώρο και να βελτιώνουν την ανθεκτικότητα και την ανακτησιμότητα των συστημάτων ΤΠΕ μετά από κυβερνοεπίθεση·
3. Δημιουργία ενός αποτελεσματικού πλαισίου συντονισμού και συνεργασίας με τον καθορισμό των επιμέρους αρμοδιοτήτων και ρόλων των διαφόρων φορέων του δημόσιου και του ιδιωτικού τομέα που εμπλέκονται στην εφαρμογή της Εθνικής Στρατηγικής για την Ασφάλεια στον Κυβερνοχώρο.
4. Εξασφάλιση της ενεργού συμμετοχής του Κράτους σε διεθνείς πρωτοβουλίες και δράσεις για την ασφάλεια στον κυβερνοχώρο από διεθνείς οργανισμούς, για την ενίσχυση της εθνικής ασφάλειας.
5. Ενημέρωση όλων των κοινωνικών ιδρυμάτων και ενημέρωση των χρηστών σχετικά με την ασφαλή χρήση του κυβερνοχώρου.
6. Συνεχής προσαρμογή του εθνικού θεσμικού πλαισίου στις νέες τεχνολογικές απαιτήσεις και στις κατευθύνσεις της ΕΕ για αποτελεσματικό χειρισμό παράνομων πράξεων που συνδέονται με τη δραστηριότητα στον κυβερνοχώρο.
7. Προώθηση της καινοτομίας, της έρευνας και της ανάπτυξης σε θέματα ασφάλειας και της συνεργασίας μεταξύ των εμπλεκόμενων φορέων.

[12] https://www.kodiko.gr/nomothesia/document/640620/nomos-4727-2020

[13] https://www-enisa-europa-eu.translate.goog/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece&_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

8. Αξιοποιήστε τις βέλτιστες διεθνείς πρακτικές[14].

Στην Ευρωπαϊκή Ένωση, στις 25 Νοεμβρίου 2009, μετά από δύο χρόνια νομοθετικής επεξεργασίας , τέθηκε σε ισχύ η Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Ευρωπαϊκού Συμβουλίου. Μεταξύ άλλων οδηγιών, η οδηγία του 2009 τροποποίησε την οδηγία 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών σχετικά με δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών. Η τροπολογία αντικατέστησε το άρθρο 4 της Οδηγίας του 2002, μέρος του οποίου έχει ως εξής[15]:

«Παροχή πρόσβασης σε σταθερή τοποθεσία και παροχή τηλεφωνικών υπηρεσιών

1. Τα κράτη μέλη διασφαλίζουν ότι όλα τα εύλογα αιτήματα για σύνδεση σε σταθερή τοποθεσία σε δημόσιο δίκτυο επικοινωνιών ικανοποιούνται από τουλάχιστον μία επιχείρηση
2. Η παρεχόμενη σύνδεση πρέπει να μπορεί να υποστηρίζει επικοινωνίες φωνής, φαξ και δεδομένων με ρυθμούς δεδομένων που είναι επαρκείς για να επιτρέπουν τη λειτουργική πρόσβαση στο Διαδίκτυο, λαμβάνοντας υπόψη τις επικρατούσες τεχνολογίες που χρησιμοποιούνται από την πλειοψηφία των συνδρομητών και την τεχνολογική σκοπιμότητα…».[16]Τα κράτη μέλη της ΕΕ είναι υποχρεωμένα να μεταφέρουν την Οδηγία στο εθνικό δίκαιο έως τις 25 Μαΐου 2011. Εν τω μεταξύ, στις 2 Μαρτίου 2010, η Ευρωπαϊκή Επιτροπή ξεκίνησε δημόσια διαβούλευση (η οποία ολοκληρώθηκε στις 7 Μαΐου 2010 αφού έλαβε σημαντικό αριθμό απαντήσεων), για να αναλυθεί εάν οι υποχρεώσεις καθολικής υπηρεσίας θα πρέπει να επεκταθούν στην ευρυζωνική πρόσβαση. Λίγες ημέρες αργότερα, η Ευρωπαϊκή Επιτροπή παρουσίασε το σχέδιο δράσης για την Ψηφιακή Ατζέντα για την Ευρώπη, σύμφωνα με τον οποίο

[14] https://www-enisa-europa-eu.translate.goog/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece&_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

[15] https://digital-strategy.ec.europa.eu/en

[16] https://digital-strategy.ec.europa.eu/en

ένας από τους στόχους είναι να «Διασφαλιστεί ότι έως το 2020 όλοι οι Ευρωπαίοι θα μπορούν να έχουν πρόσβαση σε πολύ πιο γρήγορο Διαδίκτυο, όπως ορίζεται στους στόχους της ΕΕ. Το 2010 η Ευρωπαϊκή Επιτροπή θα παρουσιάσει ανακοίνωση για τις ευρυζωνικές συνδέσεις, η οποία θα καθορίσει ένα κοινό πλαίσιο για δράσεις σε επίπεδο ΕΕ και κρατών μελών…»[17]

[17] https://digital-strategy.ec.europa.eu/en

2.6 Τα προσωπικά δεδομένα

Στα προσωπικά δεδομένα ανήκει οποιαδήποτε πληροφορία σχετικά με ένα ζωντανό άτομο, που θα μπορούσε να συμβάλει στην ταυτοποίηση ή στην αναγνώρισή του. Τα προσωπικά δεδομένα μπορούν να σχετίζονται με διάφορους τύπους πληροφοριών όπως όνομα, ημερομηνία γέννησης, αριθμό τηλεφώνου, διεύθυνση, διεύθυνση email, φυσικά χαρακτηριστικά ή δεδομένα τοποθεσίας (Μήτρου Λ, 2002)

Τα προσωπικά δεδομένα δεν χρειάζεται να έχουν απαραίτητα γραπτή μορφή. Μπορεί να περιέχουν πληροφορίες σχετικά με την εμφάνιση ενός υποκειμένου, για παράδειγμα να είναι φωτογραφίες ή εγγραφές ήχου ή βίντεο αλλά ο νόμος περί προστασίας δεδομένων ισχύει μόνο για εκείνες τις πληροφορίες που υποβάλλονται σε επεξεργασία από ηλεκτρονικά συστήματα (Determann,2012).

Τα προσωπικά δεδομένα μπορεί να είναι πληροφορίες όπου προσδιορίζεται το υποκείμενό τους (π.χ. «το αγαπημένο χρώμα η φαγητό του/της … είναι αυτό»). Ακόμη και όταν τα προσωπικά στοιχεία είναι εν μέρει ανώνυμα ή « ψευδώνυμα », αυτό θα μπορούσε να αντιστραφεί και το υποκείμενο των δεδομένων θα μπορούσε ενδεχομένως να εντοπιστεί χρησιμοποιώντας πρόσθετες πληροφορίες. Έτσι και αυτού του είδους τα δεδομένα απαιτείται να θεωρούνται προσωπικά δεδομένα . Ωστόσο, εάν οι πληροφορίες είναι πραγματικά ανώνυμες αμετάκλητα και δεν μπορούν να αντιστοιχηθούν σε αναγνωρισμένο πρόσωπο, δεν θεωρούνται προσωπικά δεδομένα (Kinast,Partner,2014).

Για να προσδιοριστεί εάν ένα άτομο είναι «αναγνωρίσιμο», ιδίως όταν οι πληροφορίες για αυτό το άτομο είναι ψευδώνυμα, πρέπει να ληφθούν υπόψη όλες οι μέθοδοι και οι πληροφορίες που είναι εύλογα πιθανό να χρησιμοποιηθούν από τον υπεύθυνο επεξεργασίας ή άλλο άτομο για την ταυτοποίηση είτε άμεσα είτε έμμεσα.

Ορισμένοι τύποι ευαίσθητων προσωπικών δεδομένων, που ονομάζονται «ειδικές κατηγορίες», υπόκεινται σε πρόσθετη προστασία βάσει του GDPR και η επεξεργασία τους

γενικά απαγορεύεται, εκτός από τις περιπτώσεις όπου πληρούνται συγκεκριμένες απαιτήσεις όπως ορίζεται λεπτομερώς στο Άρθρο 9 του GDPR . Οι ειδικές κατηγορίες είναι: προσωπικά δεδομένα που αποκαλύπτουν φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα, γενετικά δεδομένα, βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία για τη μοναδική ταυτοποίηση ενός ατόμου, δεδομένα σχετικά με την υγεία κάποιου και δεδομένα που αφορούν τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό ενός ατόμου (Αλεξανδροπούλου,Αιγυπτιάδου, 2007).

Η νομοθεσία περί προστασίας δεδομένων διέπει καταστάσεις όπου τα προσωπικά δεδομένα «υποβάλλονται σε επεξεργασία» . Η επεξεργασία σημαίνει βασικά χρήση προσωπικών δεδομένων με οποιονδήποτε τρόπο , συμπεριλαμβανομένης της συλλογής, της αποθήκευσης, της ανάκτησης, της συμβουλευτικής, της αποκάλυψης ή της κοινής χρήσης με κάποιον άλλο και της διαγραφής ή της καταστροφής προσωπικών δεδομένων. Ωστόσο, ο νόμος περί προστασίας δεδομένων δεν εφαρμόζεται όταν το αντικείμενο των δραστηριοτήτων είναι καθαρά προσωπικό/οικογενειακό.

2.7 Τα μέτρα για την προστασία των προσωπικών δεδομένων

Η προστασία δεδομένων και το απόρρητο είναι ένα ευρύ θέμα. Μια επιτυχημένη διαδικασία προστασίας δεδομένων μπορεί να αποτρέψει την απώλεια δεδομένων ή τη διαφθορά και να μειώσει τη ζημιά που προκαλείται σε περίπτωση παραβίασης. Οι μέθοδοι απορρήτου δεδομένων διασφαλίζουν ότι τα ευαίσθητα δεδομένα είναι προσβάσιμα μόνο σε εγκεκριμένα μέρη.

Η ευρεία χρήση προσωπικών και ευαίσθητων δεδομένων έχει αυξήσει τη σημασία της προστασίας αυτών των δεδομένων από απώλεια και διαφθορά. Οι παγκόσμιες αρχές έχουν παρέμβει με κανονιστική συμμόρφωση όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). Ο GDPR δίνει έμφαση στα δικαιώματα προσωπικών δεδομένων των κατοίκων της ΕΕ, συμπεριλαμβανομένου του δικαιώματος αλλαγής, πρόσβασης, διαγραφής ή μεταφοράς των δεδομένων τους. Τα προσωπικά δεδομένα αναφέρονται σε κάθε πληροφορία που σχετίζεται με ένα άτομο. Αυτό περιλαμβάνει ονόματα, φυσικά χαρακτηριστικά, διευθύνσεις, φυλετικά ή εθνοτικά χαρακτηριστικά και βιομετρικά δεδομένα όπως DNA και δακτυλικά αποτυπώματα (European Commission 2012).

Η προστασία δεδομένων είναι ένα σύνολο στρατηγικών και διαδικασιών που μπορείτε να χρησιμοποιήσετε για να εξασφαλίσετε το απόρρητο, τη διαθεσιμότητα και την ακεραιότητα των δεδομένων σας. Μερικές φορές ονομάζεται επίσης ασφάλεια δεδομένων.

Μια στρατηγική προστασίας δεδομένων είναι ζωτικής σημασίας για κάθε οργανισμό που συλλέγει, χειρίζεται ή αποθηκεύει ευαίσθητα δεδομένα. Μια επιτυχημένη στρατηγική μπορεί να βοηθήσει στην αποτροπή απώλειας δεδομένων, κλοπής ή διαφθοράς και μπορεί να βοηθήσει στην ελαχιστοποίηση της ζημίας που προκαλείται σε περίπτωση παραβίασης ή καταστροφής.

Οι αρχές προστασίας δεδομένων συμβάλλουν στην προστασία των δεδομένων και στη διάθεσή τους υπό οποιεσδήποτε συνθήκες. Καλύπτει τη δημιουργία αντιγράφων ασφαλείας

λειτουργικών δεδομένων και την ανάκτηση επιχειρηματικής συνέχειας/καταστροφών (BCDR) και περιλαμβάνει την υλοποίηση πτυχών της διαχείρισης δεδομένων και της διαθεσιμότητας δεδομένων. Το απόρρητο δεδομένων είναι μια κατευθυντήρια γραμμή για τον τρόπο συλλογής ή χειρισμού των δεδομένων, με βάση την ευαισθησία και τη σημασία τους. Το απόρρητο δεδομένων εφαρμόζεται συνήθως σε προσωπικές πληροφορίες υγείας (PHI) και προσωπικά αναγνωρίσιμες πληροφορίες (PII). Αυτό περιλαμβάνει οικονομικές πληροφορίες, ιατρικά αρχεία, αριθμούς κοινωνικής ασφάλισης ή ταυτότητας, ονόματα, ημερομηνίες γέννησης και στοιχεία επικοινωνίας (Determann, 2012).

Τα ζητήματα απορρήτου δεδομένων ισχύουν για όλες τις ευαίσθητες πληροφορίες που διαχειρίζονται οι οργανισμοί, συμπεριλαμβανομένων των πελατών, των μετόχων και των εργαζομένων. Συχνά, αυτές οι πληροφορίες διαδραματίζουν ζωτικό ρόλο στις επιχειρηματικές δραστηριότητες, την ανάπτυξη και τα οικονομικά.

Το απόρρητο δεδομένων βοηθά στη διασφάλιση ότι τα ευαίσθητα δεδομένα είναι προσβάσιμα μόνο σε εγκεκριμένα μέρη. Αποτρέπει τους εγκληματίες από το να μπορούν να χρησιμοποιούν κακόβουλα δεδομένα και διασφαλίζει ότι οι οργανισμοί πληρούν τις κανονιστικές απαιτήσεις. Οι κανονισμοί προστασίας δεδομένων διέπουν τον τρόπο με τον οποίο συλλέγονται, μεταδίδονται και χρησιμοποιούνται ορισμένοι τύποι δεδομένων. Τα προσωπικά δεδομένα περιλαμβάνουν διάφορους τύπους πληροφοριών, όπως ονόματα, φωτογραφίες, διευθύνσεις email, στοιχεία τραπεζικού λογαριασμού, διευθύνσεις IP προσωπικών υπολογιστών και βιομετρικά δεδομένα.

Οι κανονισμοί προστασίας δεδομένων και απορρήτου διαφέρουν μεταξύ χωρών, πολιτειών και βιομηχανιών. Για παράδειγμα, η Κίνα έχει δημιουργήσει έναν νόμο περί απορρήτου δεδομένων που τέθηκε σε ισχύ την 1η Ιουνίου 2017 και ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης (ΕΕ) τέθηκε σε ισχύ το 2018. Η μη συμμόρφωση μπορεί να οδηγήσει σε ζημιές στη φήμη και σε χρηματικές πρόστιμα,

ανάλογα με την παράβαση σύμφωνα με τις οδηγίες του κάθε νόμου και του εκάστοτε διοικητικού φορέα (European Commission – Eurostat0 .

Η συμμόρφωση με ένα σύνολο κανονισμών δεν εγγυάται τη συμμόρφωση με όλους τους νόμους. Επιπλέον, κάθε νόμος περιέχει πολλές ρήτρες που μπορεί να ισχύουν για μια περίπτωση αλλά όχι για μια άλλη, και όλοι οι κανονισμοί υπόκεινται σε αλλαγές. Αυτό το επίπεδο πολυπλοκότητας καθιστά δύσκολη τη συνεπή και κατάλληλη εφαρμογή της συμμόρφωσης. Το απόρρητο δεδομένων επικεντρώνεται στον καθορισμό του ποιος έχει πρόσβαση στα δεδομένα, ενώ η προστασία δεδομένων εστιάζει στην εφαρμογή αυτών των περιορισμών. Το απόρρητο δεδομένων καθορίζει τις πολιτικές που χρησιμοποιούν τα εργαλεία και οι διαδικασίες προστασίας δεδομένων.

Η δημιουργία οδηγιών απορρήτου δεδομένων δεν διασφαλίζει ότι οι μη εξουσιοδοτημένοι χρήστες δεν έχουν πρόσβαση. Ομοίως, μπορείτε να περιορίσετε την πρόσβαση μέσω προστασίας δεδομένων, ενώ εξακολουθείτε να αφήνετε ευάλωτα τα ευαίσθητα δεδομένα. Και τα δύο χρειάζονται για να διασφαλιστεί ότι τα δεδομένα παραμένουν ασφαλή. Όσον αφορά την προστασία των δεδομένων σας, υπάρχουν πολλές επιλογές αποθήκευσης και διαχείρισης από τις οποίες μπορείτε να διαλέξετε. Οι λύσεις μπορούν να σας βοηθήσουν να περιορίσετε την πρόσβαση, να παρακολουθείτε τη δραστηριότητα και να απαντάτε σε απειλές. Ακολουθούν μερικές από τις πιο συχνά χρησιμοποιούμενες πρακτικές και τεχνολογίες (European Commission – Eurostat) :

(α) Ανακάλυψη δεδομένων — ένα πρώτο βήμα για την προστασία δεδομένων. Περιλαμβάνει την ανακάλυψη του συνόλου των δεδομένων που υπάρχουν στον οργανισμό, το ποια από αυτά είναι κρίσιμα για τις επιχειρήσεις και το ποια από αυτά χαρακτηρίζονται ως ευαίσθητα και ενδέχεται να υπόκεινται σε κανονισμούς συμμόρφωσης.

Πρόληψη απώλειας δεδομένων (DLP) — ένα σύνολο στρατηγικών και εργαλείων που μπορείτε να χρησιμοποιήσετε για να αποτρέψετε την κλοπή, την απώλεια ή την κατά λάθος

διαγραφή δεδομένων. Οι λύσεις πρόληψης απώλειας δεδομένων συχνά περιλαμβάνουν πολλά εργαλεία για την προστασία και την ανάκτηση από την απώλεια δεδομένων.

(β) Αποθήκευση με ενσωματωμένη προστασία δεδομένων — ο σύγχρονος εξοπλισμός αποθήκευσης παρέχει ενσωματωμένη ομαδοποίηση δίσκων και πλεονασμό. Για παράδειγμα, το Hyperstore της Cloudian παρέχει έως και 14 εννέα αντοχής, χαμηλό κόστος που επιτρέπει την αποθήκευση μεγάλων όγκων δεδομένων και γρήγορη πρόσβαση για ελάχιστο RTO/RPO. Μάθετε περισσότερα στον οδηγό μας για την ασφαλή αποθήκευση δεδομένων .

(γ) Δημιουργία αντιγράφων ασφαλείας — δημιουργεί αντίγραφα δεδομένων και τα αποθηκεύει χωριστά, καθιστώντας δυνατή την επαναφορά των δεδομένων αργότερα σε περίπτωση απώλειας ή τροποποίησης. Τα αντίγραφα ασφαλείας είναι μια κρίσιμη στρατηγική για τη διασφάλιση της επιχειρηματικής συνέχειας όταν τα αρχικά δεδομένα χάνονται, καταστρέφονται ή καταστραφούν, είτε κατά λάθος είτε από κακόβουλο τρόπο. Μάθετε περισσότερα στον οδηγό μας για τη διαθεσιμότητα δεδομένων .

(δ) Στιγμιότυπα — ένα στιγμιότυπο είναι παρόμοιο με ένα αντίγραφο ασφαλείας, αλλά είναι μια πλήρης εικόνα ενός προστατευμένου συστήματος, συμπεριλαμβανομένων δεδομένων και αρχείων συστήματος. Ένα στιγμιότυπο μπορεί να χρησιμοποιηθεί για την επαναφορά ενός ολόκληρου συστήματος σε ένα συγκεκριμένο χρονικό σημείο.

(ε) Αντιγραφή — μια τεχνική για την αντιγραφή δεδομένων σε συνεχή βάση από ένα προστατευμένο σύστημα σε άλλη τοποθεσία. Αυτό παρέχει ένα ζωντανό, ενημερωμένο αντίγραφο των δεδομένων, επιτρέποντας όχι μόνο την ανάκτηση αλλά και την άμεση αποτυχία του αντιγράφου εάν το πρωτεύον σύστημα διακοπεί.

(στ) Τείχη προστασίας — βοηθητικά προγράμματα που σας επιτρέπουν να παρακολουθείτε και να φιλτράρετε την κυκλοφορία του δικτύου. Μπορείτε να

χρησιμοποιήσετε τείχη προστασίας για να διασφαλίσετε ότι μόνο εξουσιοδοτημένοι χρήστες επιτρέπεται να έχουν πρόσβαση ή να μεταφέρουν δεδομένα.

(ζ) Έλεγχος ταυτότητας και εξουσιοδότηση —Στοιχεία ελέγχου που σας βοηθούν να επαληθεύσετε τα διαπιστευτήρια και να διασφαλίσετε ότι τα δικαιώματα χρήστη εφαρμόζονται σωστά. Αυτά τα μέτρα χρησιμοποιούνται συνήθως ως μέρος μιας λύσης διαχείρισης ταυτότητας και πρόσβασης (IAM) και σε συνδυασμό με ελέγχους πρόσβασης βάσει ρόλου (RBAC).

(η) Κρυπτογράφηση —αλλάζει το περιεχόμενο δεδομένων σύμφωνα με έναν αλγόριθμο που μπορεί να αντιστραφεί μόνο με το σωστό κλειδί κρυπτογράφησης. Η κρυπτογράφηση προστατεύει τα δεδομένα σας από μη εξουσιοδοτημένη πρόσβαση, ακόμη και αν τα δεδομένα κλαπούν, καθιστώντας τα μη αναγνώσιμα. Μάθετε περισσότερα στον οδηγό για την κρυπτογράφηση d ata e .

(θ) Προστασία τελικού σημείου — προστατεύει τις πύλες στο δίκτυό σας, συμπεριλαμβανομένων των θυρών, των δρομολογητών και των συνδεδεμένων συσκευών. Το λογισμικό προστασίας τελικού σημείου σάς δίνει συνήθως τη δυνατότητα να παρακολουθείτε την περίμετρο του δικτύου σας και να φιλτράρετε την κίνηση όπως απαιτείται.

(ι) Διαγραφή δεδομένων —περιορίζει την ευθύνη διαγράφοντας δεδομένα που δεν χρειάζονται πλέον. Αυτό μπορεί να γίνει μετά την επεξεργασία και ανάλυση των δεδομένων ή περιοδικά όταν τα δεδομένα δεν είναι πλέον σχετικά. Η διαγραφή περιττών δεδομένων είναι απαίτηση πολλών κανονισμών συμμόρφωσης, όπως ο GDPR. Για περισσότερες πληροφορίες σχετικά με το GDPR, ανατρέξτε στον οδηγό μας: GDPR Data Protection .

(ια) Ανάκτηση καταστροφών — ένα σύνολο πρακτικών και τεχνολογιών που καθορίζουν τον τρόπο με τον οποίο ένας οργανισμός αντιμετωπίζει μια καταστροφή, όπως μια επίθεση στον κυβερνοχώρο, μια φυσική καταστροφή ή μεγάλης κλίμακας αστοχία

εξοπλισμού. Η διαδικασία αποκατάστασης από καταστροφή συνήθως περιλαμβάνει τη δημιουργία μιας απομακρυσμένης τοποθεσίας αποκατάστασης καταστροφών με αντίγραφα προστατευμένων συστημάτων και την εναλλαγή λειτουργιών σε αυτά τα συστήματα σε περίπτωση καταστροφής.

Η φορητότητα δεδομένων είναι μια σημαντική απαίτηση για πολλούς σύγχρονους οργανισμούς πληροφορικής. Σημαίνει τη δυνατότητα μεταφοράς δεδομένων μεταξύ διαφορετικών περιβαλλόντων και εφαρμογών λογισμικού. Πολύ συχνά, η φορητότητα δεδομένων σημαίνει τη δυνατότητα μεταφοράς δεδομένων μεταξύ κέντρων δεδομένων εσωτερικού χώρου και του δημόσιου νέφους και μεταξύ διαφορετικών παρόχων cloud.

Η φορητότητα δεδομένων έχει επίσης νομικές επιπτώσεις—όταν τα δεδομένα αποθηκεύονται σε διαφορετικές χώρες, υπόκεινται σε διαφορετικούς νόμους και κανονισμούς. Αυτό είναι γνωστό ως κυριαρχία δεδομένων.

2.8 Η ασφαλής περιήγηση στο διαδίκτυο

Το να είσαι ασφαλής στο διαδίκτυο είναι σημαντική υπόθεση, ωστόσο η χρήση αυτού δεν είναι πάντα αξιόπιστη. Το διαδίκτυο επιτρέπει τους χρήστες να συνδέονται άμεσα και ταυτόχρονα σε μια μεγάλη γκάμα δικτύων διαδικτυακών υπηρεσιών και πληροφοριών. Καθώς η τεχνολογία αλλάζει με γοργά βήματα και εξελίσσεται μαζί έρχεται και ο κίνδυνός από κακόβουλα λογισμικά. Οι χρήστες πρέπει να είναι σε εγρήγορση για τις ηλεκτρονικές απάτες για να μπορέσουν να τις αποφύγουν (Κάτσικας).

Κάθε φορά που επισκέπτεται κάποιος έναν ιστότοπο, χρειάζεται το URL του, το οποίο είναι η διεύθυνση ιστού που βοηθάει την συσκευή να βρει τον ιστότοπο. Ο χρήστης με την πληκτρολόγηση μιας URL στην γραμμή διευθύνσεων μεταφέρεται στον ιστότοπο.
Πληκτρολογώντας μια διεύθυνση URL απευθείας στη γραμμή διευθύνσεων ενός προγράμματος περιήγησης θα μεταφερθείτε σε μια συγκεκριμένη σελίδα. Δεν είναι όλοι οι σύνδεσμοι ασφαλής, ακόμη και αυτοί που βρίσκονται σε νόμιμους ιστότοπους. Οι επιτήδειοι χρησιμοποιούν κακόβουλες διευθύνσεις URL και ιστότοπους για να:

1. Κλέψουν διαπιστευτήριά χρηστών
2. Παραπλανούν τον χρήστη για κατεβάσει το κακόβουλο λογισμικό
3. Παρουσιάζουν ψευδείς πληροφορίες για νόμιμες

Στο παράδειγμα που ακολουθεί και οι δύο διευθύνσεις ισχυρίζονται ότι αντιστοιχούν στον ιστότοπο Τράπεζας.

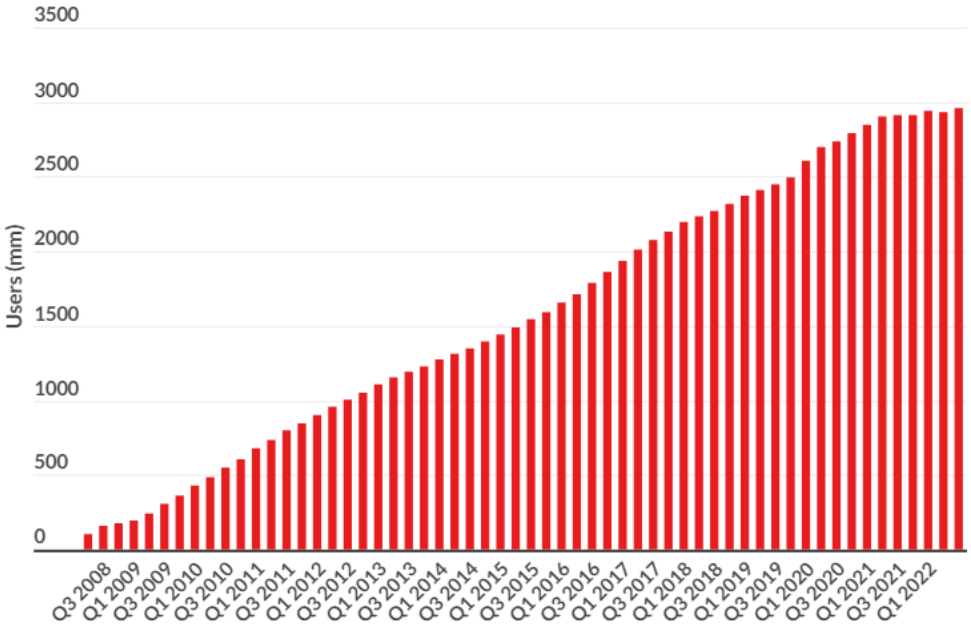
4. https://www.universitybank.com/account_login
5. https://www.universitybank-payment.com/login

Μπορεί οι διευθύνσεις URL να φαίνονται όμοιες αλλά έχουν διαφορές που θα μπορούσε να στοιχήσει αν κάποιος έκανε ένα κλικ. Αυτές οι διευθύνσεις URL οδηγούν σε διαφορετικούς ιστότοπους. Οι επιτήδειοι επιχειρούν με διάφορα τεχνάσματα να εξαπατήσουν τους χρήστες και να τους κάνουν να εισέλθουν σε κακόβουλους ιστότοπους.

Οι συντομευμένες διευθύνσεις URL είναι διευθύνσεις για μεγαλύτερους συνδέσμους. Οι εισβολείς μπορούν να χρησιμοποιήσουν εργαλεία συντόμευσης συνδέσμων στο διαδίκτυο, όπως προκειμένου να αποκρύψουν τον πραγματικό προορισμό ενός συνδέσμου. Οι περισσότερες εταιρείες χρησιμοποιούν λέξεις, όχι αριθμούς. Οι επιτήδειοι θα προσπαθήσουν να δημιουργήσουν μια διεύθυνση URL που να φαίνεται πανομοιότυπη με την νόμιμη τοποθεσία. Εάν έχετε τον ιστότοπο σελιδοδείκτη στο πρόγραμμα περιήγησής σας, χρησιμοποιήστε αυτόν αντί για τον σύνδεσμο. Εάν γνωρίζετε ήδη τη σωστή διεύθυνση ιστού, πληκτρολογήστε τη στη γραμμή διευθύνσεων αντί να κάνετε κλικ στον σύνδεσμο.

ΚΕΦΑΛΑΙΟ ΙΙΙ: SWOTΑΝΑΛΥΣΗ ΤΟΥ FACEBOOK

Το Facebook αδιαμφισβήτητα θεωρείται ο ηγέτης της αγοράς σε παγκόσμια κλίμακα στον τομέα της διαδικτυακής κοινωνικής δικτύωσης. Το Facebook έχει περίπου2,9 δισεκατομμύρια ενεργούς χρήστες ενώ 84,5 τοις εκατό των καθημερινών ενεργών χρηστών είναι εκτός των ΗΠΑ και του Καναδά. Ο αριθμός των ενεργών χρηστών όπως φαίνεται και στο παρακάτω διάγραμμα αυξάνεται σταθερά.

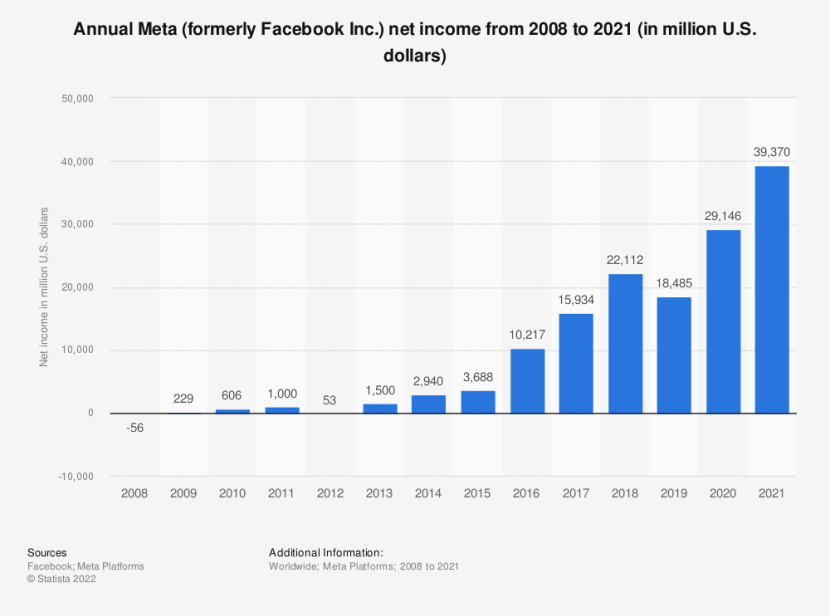


Γράφημα 1 Διακύμανση Εγγραφής Χρηστών Facebook, Πηγή: Statistica.com

Το Facebook γίνεται πηγή ειδήσεων για αυξανόμενους αριθμούς χρηστών σε παγκόσμια κλίμακα. Σύμφωνα με τα ευρήματα μιας μελέτης του Reuters Institute for the Study of Journalism, στην οποία συμμετείχαν 26 χώρες, οι άνθρωποι στρέφονται όλο και περισσότερο στα μέσα κοινωνικής δικτύωσης όπως το Facebook για ειδήσεις, γεγονός που καθιστά πιο δύσκολο για τους εκδότες να προσελκύσουν και να κερδίσουν χρήματα από τους αναγνώστες. Επιπλέον, έχει διαπιστωθεί ότι «το Facebook είναι μακράν η κυρίαρχη πηγή ειδήσεων μέσων κοινωνικής δικτύωσης με το 44% των ερωτηθέντων να το χρησιμοποιούν για να εντοπίσουν, να διαβάσουν, να παρακολουθήσουν, να μοιραστούν ή να σχολιάσουν ειδήσεις κάθε εβδομάδα». Αυξάνοντας τη δημοτικότητα του Facebook το οποίο χαρακτηρίζεται ως «Η

κύρια πηγή ειδήσεων στον πληθυσμό», με αποτέλεσμα να έχει τεράστιες θετικές επιπτώσεις στις μακροπρόθεσμες προοπτικές ανάπτυξής του (Sweney.2016).

Συνολικά, όσον αφορά το ύψος των καθαρών εσόδων, το Facebook σημειώνει αύξηση κάθε χρόνο, εκτός από το 2019, όταν μειώθηκαν κατά 4%., Το επόμενο έτος, δηλαδή το 2020, παρουσιάστηκε κατά 22%σε σχέση με το 2019, η οποία συνοδεύτηκε με αύξηση των διαφημιστικών εσόδων κατά 21%. Το 2021, τα καθαρά έσοδα της εταιρείας έφτασαν στο ύψος των 46,7 δισεκατομμυρίων δολαρίων. Συνολικά αυτή η αύξηση οφείλεται στο ότι αυξάνονται οι εγγεγραμμένοι χρήστες ενώ ταυτόχρονα αυξάνονται και οι διαφημίσεις.



Γράφημα 2 Διακύμανση Καθαρών Εσόδων Facebook, Πηγή: Statista.com

Συμφώνως της SWOT ανάλυσης του Facebook με δεδομένα ως το 2022 ισχύουν τα κάτωθι:

1. Δυνάμεις

1.1 Η ισχυρή εμπορική ταυτότητα είναι απαραίτητη για μακροπρόθεσμη σταθερότητα και βιωσιμότητα. Επί αυτού επισημαίνεται ότι το Forbes κατέταξε το Facebook ως μια από τις 5 πιο ισχυρές εταιρείες το 2019. Το Facebook αυτή τη στιγμή είναι το ισχυρότερο στον τομέα των μέσων κοινωνικής δικτύωσης, με την αξία του να υπολογίζεται στα 88,9 δισεκατομμύρια δολάρια.

1.2 Το επόμενο μεγαλύτερο πλεονέκτημα είναι η διαφοροποίηση και οι καινοτόμες ιδέες της εταιρείας, που βοηθούν στη βελτίωση της σταθερότητας της εταιρείας. Περιλαμβάνονται συσκευές εικονικής πραγματικότητας (Oculus), συστήματα ηλεκτρονικών πληρωμών (Calibra), επιχειρηματικά εργαλεία (Workplace) καθώς και το Instagram.Η αγορά του Instagram από τον κ. Zuckerberg το 2012 για το ποσό 1 δισεκατομμυρίου δολαρίων θεωρήθηκε από τους αναλυτές και επενδυτές ως αδικαιολόγητα επικίνδυνη κίνηση. Ωστόσο, το Instagram μετά από λίγα χρόνια αποτιμήθηκε σε 35 δισεκατομμύρια δολάρια και οι μετοχές του Facebook σχεδόν τριπλασιάστηκαν, ως απόδειξη της επιχειρηματικής οξυδέρκειας και της αποφασιστικότητας του Ζούκερμπεργκ (Sweney.2016). Ο αριθμός των μηνιαία ενεργών ατόμων σε αυτές τις πλατφόρμες είναι περίπου 2,89 εκατομμύρια.Ένας σημαντικός και συνεχώς αυξανόμενος αριθμός εξαιρετικά αφοσιωμένων πελατών λέει πολλά για τη δύναμη, τη βιωσιμότητα και τα επιτεύγματα μιας εταιρείας.

1.3 Το Facebook είναι διάσημο για την προσέλκυση και πρόσληψη κορυφαίων επαγγελματιών του κλάδου. Αυτό βοήθησε επίσης να μπει στη λίστα των 147 καλύτερων εργοδοτών του Forbes για το 2020.

1.4 Το Facebook είναι ένας από τους μεγαλύτερους επενδυτέςστον τομέα Έρευνας και Ανάπτυξης στον κόσμο, αφού αύξησε τις δαπάνες του για από 4,8 δισεκατομμύρια δολάρια το 2015 σε 13,6 δισεκατομμύρια δολάρια το 2019, αντιπροσωπεύοντας σχεδόν το 19% των ετήσιων εσόδων του. Εντός του έτους 2020, οι επενδύσεις της εταιρείας έφτασαν το ύψος των 16,7 δισεκατομμυρίων δολαρίων.

1.5 Η κύρια πηγή εσόδων της εταιρείας είναι η διαφήμιση...Από το 2015 έως το 2021, τα έσοδα από διαφημίσεις αυξήθηκαν με μέσο ετήσιο ρυθμό αύξησης 36,7%. Η μεγαλύτερη αύξηση από έτος σε έτος καταγράφηκε το 2016, όταν τα έσοδα από διαφημίσεις του Facebook αυξήθηκαν κατά 50%. Το 2020 σημειώθηκε η μικρότερη αύξηση, κατά 20,8% σε σχέση

με το 2019. Η αύξηση είναι συνεχής κάτι που αποτυπώνεται και στα δεδομένα του 2021 που έφτασε τα 114,9 δισεκατομμύρια δολάρια, ξεπερνώντας το όριο των 100 δισεκατομμυρίων δολαρίων για πρώτη φορά στην ιστορία.

1.6 Το μάρκετινγκ του Facebook είναι απλό. Το γεγονός ότι οι εφαρμογές τους χρησιμοποιούνται από πάνω από 2 δισεκατομμύρια άτομα καθημερινά, το καθιστά ένα πολύ ισχυρό και επιτυχημένο εργαλείο μάρκετινγκ.

1.7 Η εξαιρετική και καινοτόμα μορφή ηγεσίας που παρουσιάζει ο Mark Zuckerberg είναι κάτι που άλλες εταιρείες μπορούν μόνο να ονειρεύονται.Ο Zuckerberg επιδεικνύει εξαιρετική αποφασιστικότητα και αντιμετωπίζει όλα τα προβλήματα του Facebook. Αν και πολύ νεαρός σε ηλικία, συγκαταλέγεται μεταξύ των πιο αποτελεσματικών επιχειρηματικών ηγετών.Σε αντίθεση με άλλους οργανισμούς, το στρατηγικό όραμα του Zuckerberg είχε ως αποτέλεσμα την εταιρική βιωσιμότητα, την κουλτούρα, τα κέρδη, τη δημιουργικότητα και τη σταθερότητα, με ελάχιστες εσωτερικές διαφωνίες στα επίπεδα διοίκησης της εταιρείας.

2 Αδυναμίες

2.1 Το Facebook δέχεται αντιδράσεις για την αποτυχία του να προστατεύσει το απόρρητο των χρηστών και η εταιρεία χάνει δημοτικότητα σε ορισμένα μέρη του κόσμου. Εάν η εταιρεία δεν χειριστεί άμεσα και αποτελεσματικά τα ζητήματα απορρήτου των χρηστών, κινδυνεύει να χάσει τη δημοτικότητά της.

2.2 Το Facebook έχει τιμωρηθεί για τη διάδοση ψευδών και παραπλανητικών πληροφοριών. Η ανικανότητα του Fakebook να ελέγξει ψευδείς πληροφορίες μπορεί να είναι εξαιρετικά επιβλαβής για το κοινωνικό σύνολο.

2.3 Από την ίδρυση της εταιρείας, μια σειρά από σκάνδαλα διαβρώνει τις συμφωνίεςπου υπήρχαν στα ανώτατα επίπεδα διοίκησης. Κορυφαία στελέχη αποποιούνται των ευθυνών τους με σκοπό να μην κατηγορηθούν για το παραμικρό.

2.4 Τον Ιούνιο του 2020, η εικόνα του Facebook αμαυρώθηκε περαιτέρω όταν αποκαλύφθηκε ότι η εταιρεία είχε απολύσει έναν υπάλληλο που είχε επικρίνει τη σιωπή του Μαρκ Ζάκερμπεργκ απέναντι στις εμπρηστικές αναρτήσεις του Ντόναλντ Τραμπ.

2.5 Το Facebook σε πολλές περιπτώσεις έχει εκδηλώσει φυλετικές προκαταλήψεις. Έδωσε τη δυνατότητα στους επαγγελματίες του μάρκετινγκ να αρνηθούν ορισμένα δικαιώματα σε μειονοτικές ομάδες στην πλατφόρμα της. Πάνω από 750 εταιρείες έχουν σταματήσει να διαφημίζονται στο Facebook λόγω της αύξησης οργής των χρηστών..

2.6 Το οικονομικό μοντέλο του Facebook βασίζεται κυρίως στη διαφήμιση η οποία παραμένει σχεδόν η μοναδική πηγή εσόδων χωρίς να παρουσιάζεται μεγάλη ποικιλία.Ενδεικτικά αναφέρεται ότι τα έτη 2013, 2014,και 2015, οι διαφημίσεις αντιπροσώπευαν το 89% το 92% και 95%, αντίστοιχα των εσόδων της εταιρείας. Παράλληλα αυτό δημιουργεί δυσκολίες στη διατήρηση του ρυθμού αύξησης των εσόδων οι οποίες έγιναν αντιληπτές κατά τις περιόδους από το 2013 έως το 2014 όταν το ποσοστό έφτανε το 58% και από το 2014 έως το 2015 όταν αυτό μειώθηκε στο 44%. (Sweney.2016). Μια τέτοια εκτεταμένη εξάρτηση από τη διαφήμιση καθιστά την επιχείρηση ευάλωτη σε αλλαγές μάρκετινγκ των εταιρειών. Η μεγαλύτερη αδυναμία του Facebook είναι η απουσία δικών της προϊόντων, φυσικών ή ψηφιακών, ως πηγή εσόδων.

3 Ευκαιρίες

3.1 Με δισεκατομμύρια χρήστες, το Facebook μπορεί να επεκτείνει τις υπάρχουσες υπηρεσίες του, όπως η αγορά, η διαδικτυακή ροή βίντεο (streaming),οι διαδικτυακές γνωριμίες, τα επιχειρηματικά εργαλεία, το ηλεκτρονικό πορτοφόλι κ.λπ. για να ανταγωνιστεί εταιρείες όπως Amazon, Netflix, Apple, PayPal.

3.2 Καθώς η τεχνολογία βελτιώνεται, περισσότερες εφαρμογές και ιστότοποι ενσωματώνονται, επιτρέποντας στους καταναλωτές να συνδέονται σε διάφορες

πλατφόρμες. Η πλατφόρμα του Facebook μπορεί να διευρυνθεί ώστε να περιλαμβάνει, μεταξύ άλλων, ηλεκτρονικό εμπόριο, έρευνες, podcast, ταινίες και παιχνίδια.

3.3 Παρόλο που το Facebook χρησιμοποιείται ευρέως, οι χρήστες του είναι κυρίως άτομα νεότερης ηλικίας με κατάλληλες γνώσεις τεχνολογίας. Το Facebook μπορεί να προσελκύσει περισσότερα άτομα, είτε μεγαλύτερης ηλικίας είτε ακόμη και δίκτυα επιχειρήσεων όπως το LinkedIn, προσθέτοντας επιπλέον λειτουργίες.

3.4 Η πλειοψηφία των χρηστών του Facebook χρησιμοποιούν την εφαρμογή για κινητά για να έχουν πρόσβαση στους λογαριασμούς τους.Λαμβάνοντας υπόψη την αυξανόμενη μετατόπιση από υπολογιστές και φορητούς υπολογιστές σε φορητές συσκευές (κινητά) το Facebook συνεχίζει να επωφελείται. Με σκοπό την περαιτέρω αύξηση εσόδων εξαιτίας των διαφημίσεων, το Facebook θα μπορούσε να προσανατολιστεί στην εισαγωγή περισσότερων διαφημίσεων εντός της εφαρμογής για κινητά.

3.5 Η ανάγκη για λύσεις απομακρυσμένης εργασίας έχει αυξηθεί ως αποτέλεσμα των πρόσφατων γεγονότων (επιδημία Covid-19). Το Facebook επιχείρησε να εκμεταλλευτεί αυτήν την ευκαιρία, ανακοινώνοντας τον Ιούλιο του 2020 ότι τα Messenger Rooms και Facebook Live θα επεκταθούν ώστε να επιτρέπουν στους χρήστες να πραγματοποιούν ζωντανές βιντεοδιασκέψεις με έως και 50 άτομα ταυτόχρονα. Το Facebook είναι σε θέση να ανταγωνιστεί παρόχους υπηρεσιών όπως το Zoom και η Google που βασίζονται σε αυτές τις λειτουργίες.

4 Απειλές

4.1 Οι χρήστες του Facebook ενδέχεται να αρχίσουν να μειώνονται, ως αποτέλεσμα του ανταγωνισμού τόσο από παλιούς όσο και από νέους ιστότοπους. Το μέλλον του Facebook γίνεται όλο και πιο ζοφερό καθώς νέες εταιρείες στον κλάδο, όπως το TikTok, προσφέρουν πλατφόρμες που απευθύνονται στις νεότερες γενιές. Το Facebook δημιούργησε την έκδοση

της πλατφόρμας βίντεο «Lasso» σε μια προσπάθεια να ανταγωνιστεί το TikTok που όμως γρήγορα απέσυρε.

4.2 Ο αριθμός των κανονισμών που είναι αντίθετοι στο Facebook αυξάνεται με ανησυχητικό ρυθμό, ωθούμενος διάφορα σκάνδαλα. Επιπλέον, οι ανησυχίες σχετικά με την ασφάλεια των δεδομένων, το ακατάλληλο υλικό και την παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας έχουν αναγκάσει πολλούς ρυθμιστικούς φορείς να εφαρμόσουν κανονισμούς.

4.3 Το Facebook έχει πέσει θύμα πολλών παραβιάσεων δεδομένων που έχουν επηρεάσει εκατομμύρια χρήστες του. Για παράδειγμα, κατά τη διάρκεια μιας σημαντικής παραβίασης δεδομένων τον Δεκέμβριο του 2019, τα προσωπικά στοιχεία περισσότερων από 267 εκατομμυρίων χρηστών του Facebook εκτέθηκαν στον σκοτεινό ιστό.

4.4 Το Ηνωμένο Βασίλειο και η Ευρωπαϊκή Ένωση έχουν υιοθετήσει την εφαρμογή ενός φόρου για ψηφιακές υπηρεσίες με αποτέλεσμα την αύξηση της φορολογίας για το Facebook. Εάν και άλλες χώρες υιοθετήσουν αυτή τη μορφή ψηφιακής φορολογίας, ένα μεγάλο μέρος των εσόδων του Facebook θα χρησιμοποιηθεί για την πληρωμή φόρων με αποτέλεσμα τη συνολική συρρίκνωσή τους.

Επίλογος

Συμπερασματικά αναφέρεται ότι η εξέλιξη των διαδικτυακών κοινωνικών δικτύων αποτελεί απόδειξη των πραγματοποιούμενων τεχνολογικών βημάτων. Η κοινωνία πέρα από το ότι μπορεί να επωφεληθεί από αυτό, αναμφισβήτητα μπορεί και να ζημιωθεί.

Αναλυτικότερα επισημαίνεται ότι οι πληροφορίες που ανταλλάσσονται εμπεριέχουν πλήθος προσωπικών δεδομένων κάτι που δημιουργεί τις προϋποθέσεις για παραβίαση της προσωπικότητας των χρηστών και της ιδιωτικής τους ζωής.

Επιπλέον θα μπορούσε κανείς να σκεφτεί πως η ισχυροποίηση ορισμένων ιστοσελίδων που έχουν ως περιεχόμενο την κοινωνική δικτύωση θα ήταν δυνατό να περιορίσουν περαιτέρω ρηξικέλευθες ιδέες (Κάτι που ήδη γίνεται αφού το Facebook προβαίνει συνεχώς σε εξαγορά των ανταγωνιστών του). Η απουσία ιδιωτικότητας θα ήταν δυνατό να οδηγήσει στην ανάπτυξη ιδανικών συνθηκών ώστε οι πολίτες να χειραγωγηθούν εντός μιας καθημερινότητας που διακρίνεται για την κυριαρχία πλήθους περιορισμών και που διαρκώς θα μεριμνά ώστε οι πολίτες να επιτηρούνται.

Αναντίρρητα είναι χαρακτηριστικό γνώρισμα των νέων η συνεχής χρήση των διαδικτυακών υπηρεσιών κάτι που τελικά περιορίζει την ιδιωτική τους ζωή. Φυσικά πάντα είναι ορατό το ενδεχόμενο εκείνος που θα αρνηθεί να ακολουθήσει αυτόν τον τρόπο ζωής να αντιμετωπιστεί επικριτικά από τους άλλους.

Επιπρόσθετα αξίζει να αναφερθεί ο κλάδος των διαφημίσεων ο οποίος πλέον είναι άρρηκτα συνδεδεμένος το διαδίκτυο. Οι διαφημίσεις με αυτόν τον τρόπο εισβάλουν στην καθημερινότητα των ανθρώπων χωρίς να τους δίνουν το δικαίωμα της πληθώρας των επιλογών και ανάπτυξης της προσωπικότητας και της κριτικής τους σκέψης.

Τελικά αντιλαμβάνεται κανείς ότι το πλήθος των ανησυχιών είναι μεγάλο αλλά παρόλα αυτά υφίσταται περιθώριο αντιμετώπισης των κινδύνων, ώστε οι πολίτες να αισθάνονται προστατευμένοι. Απαιτείται να παραμένουν συνεχώς ενημερωμένοι αφενός για τους

κινδύνους και αφετέρου για το ισχύον νομοθετικό πλαίσιο το οποίο στόχο έχει να προστατεύει κάθε χρήστη αλλά και να προλαμβάνει την εξαπάτησή τους.

Άλλωστε τα τεχνολογικά επιτεύγματα αποτελούν δημιουργήματα της ανθρώπινης ύπαρξης και μόνο οι άνθρωποι μπορούν να επηρεάσουν την εξέλιξή της αξιοποιώντας τη θετική συνεισφορά τους και εκμηδενίζοντας τις αρνητικές τους επιπτώσεις.

Είναι κοινώς αποδεκτό ότι η ζωή αλλάζει με τον παράγοντα τεχνολογία να παίζει καθοριστικό ρόλο στην εξέλιξή της επιτρέποντας στον άνθρωπο να διατηρήσει τον ρόλο του ρυθμιστή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική

1. Αλεξανδροπούλου-Αιγυπτιάδου Ε.,(2007), *«Προσωπικά Δεδομένα»,* Εκδόσεις Σάκκουλα, Αθήνα –Κομοτηνή
2. Ιγγλεζάκης Ι., (2003), *«Ευαίσθητα Προσωπικά Δεδομένα»*, Εκδόσεις Σάκκουλα,
3. Αθήνα – Θεσσαλονίκη
4. Κάτσικας Σ, *«Προστασία και Ασφάλεια Συστημάτων Υπολογιστών»,*Ελληνικό Ανοιχτό Πανεπιστήμιο Διαθέσιμο στο https://lib.eap.gr/?page_id=1682 Πρόσβαση 17/11/22
5. Κάλλας Γ., (2006), *«Η Κοινωνία της Πληροφορίας και ο νέος Ρόλος των Κοινωνικών*
6. *Επιστημών»*. Αθήνα: Νεφέλη
7. Λαμπρινουδάκης Κ, Γκρίτζαλης Στ., Μήτρου Λ., Κάτσικας Σωκ.,(2010), «*Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών»*,Εκδόσεις Παπασωτηρίου Αθήνα.
8. Μήτρου Λ.,(1999), *«Η αρχή προστασίας προσωπικών δεδομένων»*, Εκδόσεις Σάκκουλα Αθήνα.
9. Μήτρου Λ., (2002), *«Το δίκαιο στην κοινωνία της πληροφορίας»,* Εκδόσεις Σάκκουλα, Αθήνα

Ξένη

1. Awad, N., Krishnan, M (2016), «*The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization.»* MIS quarterly
2. Brey, P.(2007), Ethical aspects of information security and privacy. In Petkovic, M., Jonker, W., Carey, M.J., Ceri, S., eds.: Security, Privacy, and Trust in Modern
3. Borgatti, S., Mehra, A., Brass, D., Labianca, G. (2009), *«Network analysis in the social*
4. *Sciences».* Science
5. Data Management. Data-Centric Systems and Applications. Springer Berlin Heidelberg
6. Determann, L.(2012), *«Social Media Privacy: A Dozen Myths and Facts*.» Stanford Technology Law Review
7. European Commission – Eurostat. ICT Security in Enterprises. International Journal on Information Technologies and Security (ijits-bg.com), 2 (vol. 3)
8. European Commission. (2012), How Will the Data Protection Reform Affect Social Networks. European Commission Review
9. Tapriyal, Varinder and Kanwar, Priya. (2012). *«Understanding Social Media»* Bookboon.com.
10. Kinast N., Partner H, (2014), *«Social Media and Data Protection»* kinast-partner
11. Kaplan, Andreas M., & Haenlein, Michael. (2009). *«The fairyland ofSecond Life: About virtual social worlds and how to use them»* Business Horizons
12. Lampe, C., Ellison, N. Understanding (2012), « *Facebook: Social Computing isn't 'Just' Social»* . Computer
13. Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A (2011), *«Analyzing facebook privacy settings: user expectations vs. reality.»* In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

14. Musial, K., Kazienko, P., (2013), *«Social networks on the internet».* World Wide
15. Rader, D. (2016) «How Facebook Turned a Big Risk into a Very Big Success»
16. Sweney, M. (2016) «Facebook's rise as news source hits publishers' revenues» The Guardian,
17. Wellman, B. (2001), *«Computer networks as social networks»*. Science

Διαδίκτυο

1. Ιστοσελίδα Εθνικό Μετσόβειο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών: www.medialab.ntua.gr/.../chap2d_1.htm Πρόσβαση 11/12/22
2. Αρχή Προστασίας Δεδομένων, Νόμος 2472/97, www.dpa.gr http://www.dpa.gr/portal/page?_pageid=33,23367&_dad=portal&_schema=PORTAL Πρόσβαση 08/12/22
3. Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), http://www.enisa.europa.eu/ Πρόσβαση 19/11/22
4. Αρχή Προστασίας Προσωπικών Δεδομένων, Μέτρα Προστασίας Προσωπικών Δεδομένων www.dpa.gr Πρόσβαση 19/11/22
5. Οδηγία Ευρωπαϊκής Νομοθεσίας από ιστοσελίδα http://ec.europa.eu/justice/policies/privacy/docs/guide/guide-greece_el.pdf με θέμα: «Προστασία Δεδομένων στην Ευρωπαϊκή Ένωση» Πρόσβαση 11/12/22
6. Shaping Europe's digital future https://digital-strategy.ec.europa.eu/en Πρόσβαση 06/11/22
7. Αρχή Προστασίας Δεδομένων,http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/2472_97_APR_10_FINAL.PDF Πρόσβαση 04/11/22
8. Opinion 5/2009 on online social networking https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf