ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΡΑΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ
ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΘΕΜΑ

Η Συμβολή Των Μεγάλων Δεδομένων Στην Ανάπτυξη Τεχνητής Νοημοσύνης. Το Αδίκημα Του Σεξουαλικού Διαδικτυακού Εξαναγκασμού Και Εκβιασμού.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της **Καλώνη Σταυρούλας**

ΘΕΣΣΑΛΟΝΙΚΗ ΦΕΒΡΟΥΑΡΙΟΣ 2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΣΥΜΒΟΛΗ ΤΩΝ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΑΝΑΠΤΥΞΗ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ. ΤΟ ΑΔΙΚΗΜΑ ΤΟΥ ΣΕΞΟΥΑΛΙΚΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΞΑΝΑΓΚΑΣΜΟΥ ΚΑΙ ΕΚΒΙΑΣΜΟΥ

Διπλωματική Εργασία

της

Καλώνη Σταυρούλας

Θεσσαλονίκη, 02/2019

Η ΣΥΜΒΟΛΗ ΤΩΝ ΜΕΓΑΛΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΑΝΑΠΤΥΞΗ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ. ΤΟ ΑΔΙΚΗΜΑ ΤΟΥ ΣΕΞΟΥΑΛΙΚΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΞΑΝΑΓΚΑΣΜΟΥ ΚΑΙ ΕΚΒΙΑΣΜΟΥ

Καλώνη Σταυρούλα

Πτυχίο Εφαρμοσμένης Πληροφορικής, ΠΑΜΑΚ 2016

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ψάννης Ε. Κωνσταντίνος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28/02/2019

Ψάννης Ε. Κωνσταντίνος	Αλεξανδροπούλου Ευγενία	Ταμπούρης Ευθύμιος
.....	.....	.....

Καλώνη Σταυρούλα

Περίληψη

Η ραγδαία ανάπτυξη της τεχνολογίας σηματοδοτεί νέα δεδομένα για την καθημερινότητα των ατόμων και γενικότερα της ανθρωπότητας. Ένα πεδίο της επιστήμης της πληροφορικής που αποδεικνύεται ιδιαίτερα εξελίξιμο είναι αυτό της τεχνητής νοημοσύνης. Η επιστημονική κοινότητα δείχνει διχασμένη, καθότι μία μερίδα της υποστηρίζει τα πλεονεκτήματα και οφέλη που παρέχει η χρήση των επιτευγμάτων της, ενώ μία άλλη κρούει τον κώδωνα του κινδύνου για τις πολύπλευρες επιπτώσεις αυτής, στο εγγύς μέλλον. Σύμφωνα με ειδικούς επιστήμονες σε θέματα ασφαλείας, η τεχνητή νοημοσύνη έχει εξελιχθεί σε τέτοιο βαθμό που καθίσταται δυνατή η εκμετάλλευσή της από επιτήδειους, προβλέποντας πληθώρα εγκλημάτων που αναμένεται να αλλάξει άρδην τόσο τον παραδοσιακό τρόπο τέλεσής τους, όσο και αυτόν που, προς το παρόν, φαντάζει προοδευτικό.

Η διαρκώς αυξανόμενη χρήση των τεχνολογιών πληροφορικής, όπως μέσα κοινωνικής δικτύωσης και smartphones, έχει αλλάξει εν τάχει τη μορφή και των όγκο των δεδομένων, με αποτέλεσμα τη δημιουργία των λεγόμενων Big Data ή Δεδομένων Μεγάλης Κλίμακας. Πρόκειται για ένα φαινόμενο που απασχόλησε ιδιαιτέρως οργανισμούς και επιχειρήσεις ανά τον κόσμο, υποχρεώνοντάς τους να εναρμονιστούν με αυτό. Πέρα από τους επιχειρηματικούς κύκλους και τις επιχειρηματικές δραστηριότητες φαίνεται ότι τα Big Data λειτουργούν ωφέλιμα στην ανίχνευση και σύλληψη εγκληματιών. Το τελευταίο χρονικό διάστημα χρησιμοποιείται ώστε να προλαμβάνει την τέλεση κυβερνοεπιθέσεων, κυρίως μέσω των διαφόρων τεχνολογιών εξόρυξης δεδομένων αιχμής, όπως οι έξυπνοι πράκτορες, τα νευρωνικά δίκτυα, η μηχανική μάθηση κ.ά. Εντούτοις, τα πλεονεκτήματα που παρέχονται από τη χρήση των Big Data δύναται να χρησιμοποιηθούν και από τους εν δυνάμει δράστες. Ειδικότερα, συνιστούν αποτελεσματικό εργαλείο για την παραβίαση ασφαλείας και πρόκληση βλάβης των βάσεων δεδομένων.

Αντικείμενο της παρούσας εργασίας αποτελεί αφενός η αρωγή της τεχνητής νοημοσύνης και των δεδομένων μεγάλης κλίμακας στον τομέα της εγκληματολογίας, αφετέρου ο εντοπισμός των κινδύνων που εγκυμονεί η λανθασμένη χρήση τους.

Συνεπώς, μέσω της εργασίας επιδιώκεται η επισήμανση, υπό το πρίσμα της εγκληματολογίας, του δίπτυχου χαρακτήρα των δύο ορολογιών.

Λέξεις Κλειδιά: Τεχνητή νοημοσύνη, Μεγάλα δεδομένα, Νευρωνικά δίκτυα, instagram, Σεξουαλικός διαδικτυακός εξαναγκασμός και εκβιασμός

Abstract

The rapid development of technology signals new standards about the humans' routine. Artificial intelligence (AI) is a field of computer science that is particularly progressive (or sophisticated). Scientific community is divided as some support the benefits of using its achievements, while another point out the risk of its multifaceted impact in the near future. According to security experts, Artificial Intelligence has evolved to such an extent that it can be exploited by scammers predicting a multitude of crimes which are expected to change both their traditional way of doing and the one seems progressive now.

The constantly increasing use of information technologies, such as social networks and smartphones, has altered the form and the volume of data resulting in the creation of Big Data. This phenomenon has particularly affected organizations and businesses around the world, forcing them to be in harmony with it. Beyond circles of business, Big Data appear to be beneficial in detecting and capturing criminals. Recently, it has been used to prevent cyber-attacks notably through the use of various cutting-edge data mining technologies like intelligent agents, neural networks, machine learning etc. However, the benefits provided by the use of Big Data can also be used by potential criminals. In particular, Big Data is an effective tool for breaching security and damaging databases.

The aim of this thesis is to assist Artificial Intelligence and Big Data in forensic and to identify the risks of misuse. Therefore, through this thesis, is sought to note the double character of the two terminologies in the forensic field.

Keywords: Artificial Intelligence, Big Data, Neural Networks, Instagram, Sextortion

Ευχαριστίες

Προτού προχωρήσω στην ανάλυση και επεξήγηση του θέματος που πραγματεύεται η παρούσα διπλωματική εργασία θα ήθελα να ευχαριστώ θερμά, τον κ. Κ. Ε. Ψάννη που μου εμπιστεύθηκε και επέτρεψε την ανάλυση και επεξεργασία αυτού, καθώς και για την βοήθεια και καθοδήγησή του καθ'όλη τη διάρκεια της έρευνας και συγγραφής της παρούσας εργασίας. Τέλος, θα θεωρούσα παράλειψη να μην αναφερθώ στην οικογένειά μου για όλη την ψυχολογική υποστήριξη και υλική βοήθεια ώστε να φέρω εις πέρας το εν λόγω μεταπτυχιακό.

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος εικόνων

Εισαγωγή

Οι συζητήσεις που αφορούν τη τεχνητή νοημοσύνη και τα διάφορα επιτεύγματα αυτής τείνουν να ενδιαφέρουν ολοένα και περισσότερο το κοινωνικό σύνολο. Προσωπικότητες του χώρου τοποθετούνται σχετικά με το θέμα και κυρίως τις επιπτώσεις που θα επιφέρει στη κοινωνία και στην ύπαρξη της ανθρωπότητας. Τα σενάρια πληθαίνουν με πολλούς να τάσσονται κατά της τεχνητής νοημοσύνης εκφράζοντας τους προβληματισμούς τους για το μέλλον του ανθρώπου μεταξύ των οποίων και σημαίνουσες προσωπικότητες της επιστήμης όπως οι Elon Musk, Stephen Hawking και Sir Clive Sinclair, ενώ στο ίδιο μήκος κινούνται κινηματογραφικά, τηλεοπτικά ακόμα και λογοτεχνικά έργα ορμώμενα από τη τεχνητή νοημοσύνη και προτάσσοντας συνήθως την πιο απαισιόδοξη πλευρά αυτής, που πολλές φορές οραματίζεται το τέλος της ανθρωπότητας. Το πεσιμιστικό σενάριο, ωστόσο, είναι απόλυτα λογικό στα πλαίσια μίας κινηματογραφικής ταινίας ή ενός λογοτεχνικού βιβλίου καθώς είναι και αυτό που θα διεγείρει τη φαντασία των καταναλωτών, αυξάνοντας τα κέρδη. Η πραγματικότητα όμως είναι λίγο διαφορετική με τα σενάρια να αλλάζουν συνεχώς και να διαδέχονται το ένα το άλλο. Έτσι, για να ενστερνιστεί κάποιος τη θέση που υπερασπίζεται δημοσίως ένας άλλος άνθρωπος, θα πρέπει προηγουμένως να μελετήσει και ερευνήσει το όποιο θέμα. Η παρούσα εργασία αποσκοπεί στην αποσαφήνιση του όρου τεχνητή νοημοσύνη δίνοντας την ιστορική εξέλιξη και τη σημασία αυτής στη σημερινή εποχή, αλλά και του γεγονότος που συνετέλεσε στην πρόοδο της τεχνητής νοημοσύνης.

Εντούτοις, η τεχνητή νοημοσύνη δε θα μπορούσε να βρίσκεται σε αυτό το σημείο δίχως τη καταλυτική αρωγή των μεγάλων δεδομένων, με τη σύγκλιση των δύο πεδίων να αποτελεί εξέχων κομμάτι της εργασίας. Κατά μήκος του κειμένου γίνεται ιδιαίτερος λόγος για τη συμβολή των δεδομένων που κατακλύζουν τον κυβερνοχώρο στην ανάπτυξη της υπό συζήτηση επιστήμης, αλλά και των διαφόρων τεχνικών της δεύτερης στο χώρο των μεγάλων δεδομένων.

Πολλές φορές τεχνητή νοημοσύνη και μεγάλα δεδομένα κατηγορούνται για θέματα ασφάλειας και προστασίας προσωπικών δεδομένων στο χώρο του διαδικτύου, ενώ δε λείπει και η συσχέτισή τους με κάποιες μορφές ηλεκτρονικών εγκλημάτων. Χάριν τούτου, μελετάται η σχέση των δύο πεδίων με το ηλεκτρονικό έγκλημα και πιο συγκεκριμένα με το έγκλημα που τελείται στους κόλπους του διαδικτύου, στοχεύοντας στην απόδοση της συμβολής τεχνητής νοημοσύνης και μεγάλων δεδομένων σε θέματα που άπτονται του ηλεκτρονικού εγκλήματος

Τέλος, παρουσιάζεται ένα έγκλημα που διαπράττεται μέσω διαδικτύου και συνιστά παγκόσμιο φαινόμενο κυρίως λόγω της ιδιαίτερης απήχησης των μέσων κοινωνικής δικτύωσης. Έτσι, μέσω της εργασίας γίνεται προσπάθεια για διαλεύκανση του εγκλήματος και εύρεσης λύσης, που στη παρούσα στιγμή δίνεται με τη μορφή αλγορίθμου τεχνητής νοημοσύνης ικανό να εντοπίσει τέτοιες παράνομες ενέργειες. Ως εκ τούτου, η εργασία πέραν των άλλων στόχων, αποβλέπει στην αντιμετώπιση του συγκεκριμένου αδικήματος μέσω της σύγκλισης δύο αμφιλεγόμενων πεδίων.

Η παρούσα εργασία αποτελείται από δέκα κεφάλαια. Τα δύο πρώτα αφορούν την αποσαφήνιση των δύο κύριων εννοιών της εργασίας, καθώς και την ιστορική εξέλιξη αυτών. Το πρώτο κεφάλαιο αναφέρεται στη τεχνητή νοημοσύνη και το δεύτερο στα μεγάλα δεδομένα. Στο τρίτο κεφάλαιο παρουσιάζεται η σύγκλιση των δύο εννοιών. Το τέτατρο κεφάλαιο συνιστά εισαγωγή στο τομέα του ηλεκτρονικού εγκλήματος. Στο πέμπτο κεφάλαιο αναπτύσσεται η σχέση τη τεχνητής νοημοσύνης με το ηλεκτρονικό έγκλημα, ενώ στο έκτο των μεγάλων δεδομένων με το ηλεκτρονικό έγκλημα. Το έβδομο κεφάλαιο είναι η εισαγωγή στο αδίκημα του σεξουαλικού διαδικτυακού εξαναγκασμού και εκβιασμού. Στο όγδοο κεφάλαιο παρουσιάζεται ο ρόλος των κοινωνικών δικτύων, ενώ στο έννατο κεφάλαιο αναπτύσσονται οι αλγόριθοι τεχνητής νοημοσύνης. Στο δέκατο κεφάλαιο της εργασίας περιγράφεται ένας από τους κύριους στόχους της εργασίας, ο προτεινόμενος αλγόριθμος. Η εργασία ολοκληρώνεται με τη παράθεση των συμπερασμάτων και των μελλοντικών επεκτάσεων αυτής.

1. Εισαγωγή Στη Τεχνητή Νοημοσύνη

Το παρόν κεφάλαιο συνιστά μία πρώτη προσέγγιση της τεχνητής νοημοσύνης, διασαφηνίζοντας τι ονομάζεται τεχνητή νοημοσύνη καθώς επίσης και τον λόγο για τον οποίο θεωρείται ένας από τους πιο πολυσυζητημένους πληροφοριακούς κλάδους.

Από την αρχαιότητα ο άνθρωπος προσπαθούσε να κατανοήσει τον τρόπο με τον οποίο σκεπτόμαστε, που μάλιστα μας οδηγεί στην τέλεση συγκεκριμένων πράξεων. Σε αυτή τη λογική βασίζεται και η επιστήμη της τεχνητής νοημοσύνης, εξελίσσοντας ωστόσο τη παραπάνω σκέψη, καθώς πέρα από την κατανόηση, αποπειράται να κατασκευάσει νοήμονες οντότητας (Russell & Norvig, 2005).

Η ιστορία της τεχνητής νοημοσύνης χρονολογείται από την αρχαιότητα και εκτείνεται στο παρόν, με έντονες και σημαντικές προεκτάσεις για το μέλλον. Ο Αρχύτας ο Ταραντινός, θεωρείται ο παππούς της ρομποτικής κατασκευάζοντας το πρώτο ρομπότ στην ιστορία της ανθρωπότητας. Πρόκειται για την πρώτη αυτόνομη πτητική μηχανή, γνωστή με την ονομασία «η ιπτάμενη περιστερά του Αρχύτα». Ακόμη στους ελληνικούς μύθους του Ηφαιστίωνα και του Πυγμαλίωνα εμπεριέχεται η ιδέα του νοήμων ρομπότ, όπως ο Τάλως και των τεχνητών όντων, όπως η Γαλάτεια και η Πανδώρα. Φυσικά, ο Αριστοτέλης όντας ο πρώτος επιστήμονας περιέγραψε επίσημα το συλλογισμό της μηχανικής σκέψης. Προχωρώντας στη νεότερη ιστορία συναντάμε διάφορες προσωπικότητες που ασχολήθηκαν με την εν λόγω επιστήμη όπως ο Leonardo Da Vinci, ο Mark Rosheim, ο Isaac Asimov κ.α. Ωστόσο, η ουσιαστική εξέλιξη της τεχνητής νοημοσύνης τοποθετείται περί τον Δεύτερο Παγκόσμιο Πόλεμο, φτάνοντας σήμερα να απασχολεί ολοένα και περισσότερους, κυρίως λόγω της εκτεταμένης χρήσης της, αλλά και της αλληλεπίδρασής της με την ανθρώπινη καθημερινότητα.

1.1. Τι είναι τεχνητή νοημοσύνη

Σε αντίθεση με ορολογίες άλλων επιστημών, για τη τεχνητή νοημοσύνη δεν υπάρχει κάποιος γενικώς αποδεκτός ορισμός. Διάφοροι επιστήμονες διατύπωσαν ανά καιρούς τη δική τους ερμηνεία. Σε ένα γενικότερο πλαίσιο, θα μπορούσαμε να πούμε μία απλή και συγχρόνως περιεκτική διατύπωση είναι αυτή του J.McCarthy κατά τον οποίο τεχνητή νοημοσύνη είναι *η επιστήμη και μεθοδολογία της δημιουργίας νοούντων μηχανών*. Πρόκειται για τη μελέτη πρακτόρων που αντιλαμβάνονται το περιβάλλον και εν συνεχεία δρουν σύμφωνα με τις αντιλήψεις που έχουν λάβει. Στην επίσημη ορολογία αυτοί οι πράκτορες ονομάζονται intelligent agents, δηλαδή ευφυείς πράκτορες. Η έλλειψη ενιαίου ορισμού σχετικά με την τεχνητή νοημοσύνη έγκειται στην άγνοια των λόγων για τους οποίους οι άνθρωποι θεωρούμαστε νοήμονες και λογικά όντα.

1.2. Η ιστορική εξέλιξη της τεχνητής νοημοσύνης

Λέγεται ότι το 1943 είναι η χρονιά που δημοσιεύτηκε η πρώτη εργασία βασισμένη στη τεχνητή νοημοσύνη από τους Warren McCulloch και Walter Pitts, στην οποία προτάθηκε ένα μοντέλο τεχνητών νευρώνων με δύο δυνατές καταστάσεις. Κάθε νευρώνας μεταβαίνει σε μία εκ των δύο καταστάσεων εκτιμώντας τα αποτελέσματα που δέχεται από διάφορους γειτονικούς νευρώνες. Ωστόσο, το πρώτο ολοκληρωμένο όραμα για την τεχνητή νοημοσύνη ανήκει στο μαθηματικό Alan Turing που το 1950 στο άρθρο του "Computing Machinery and Intelligence" παρουσίασε μία σειρά «εργαλείων» που χρησιμοποιούνται μέχρι σήμερα όπως η μηχανική μάθηση, οι γενετικοί αλγόριθμοι και η ενισχυτική μάθηση. Παρά ταύτα αυτό που «μαγνήτισε τα βλέμματα» ήταν η δοκιμασία Turing που λειτούργησε ως ενδεικτική λίστα γνωρισμάτων, απαραίτητα για το χαρακτηρισμό της νοημοσύνης.

Στο πρώτο κεφάλαιο, «Το Παιχνίδι της Μίμησης (The Imitation Game)», του παραπάνω άρθρου περιγράφεται η διαδικασία της δοκιμασίας. Το παιχνίδι παίζεται με τρία άτομα, έναν άνδρα (Α), μία γυναίκα (Β) και έναν ανακριτή (Γ), που μπορεί να είναι είτε άνδρας είτε γυναίκα. Ο ανακριτής βρίσκεται σε ένα δωμάτιο χωριστά από

τους υπόλοιπους παίκτες και θέτοντας διάφορες ερωτήσεις στους δύο παίκτες προσπαθεί να προσδιορίσει την ταυτότητά τους. Μοναδική ένδειξη για αυτό είναι ο τρόπος με τον οποίο απαντούν στις ερωτήσεις που δέχονται. Ο ένας παίκτης, έστω ο Α προσπαθεί να ξεγελάσει τον ανακριτή, ενώ ο άλλος να τον βοηθήσει. Οι απαντήσεις δίνονται είτε γραπτώς είτε διαμέσου τηλετύπου, καθότι σε αντίθετη περίπτωση τα εξωτερικά χαρακτηριστικά και η φωνή ενδέχεται να συμβάλουν καθοριστικά στη λύση του προβλήματος. Ο Turing αναδιαμόρφωσε το παιχνίδι τοποθετώντας στη θέση του Α μία μηχανή. Σε αυτή τη περίπτωση, ο ανακριτής πρέπει να καταλάβει ποιος είναι ο άνθρωπος και ποια η μηχανή. Η μηχανή θεωρείται επιτυχής αν ο ανακριτής αδυνατίσει να τη διακρίνει από τον άνθρωπο. Αξίζει να σημειωθεί ότι η πρώτη μηχανή που κατάφερε να περάσει με επιτυχία τη δοκιμασία είναι η Eugene Goostman, το 2014, όπου και πέρασε τη πλήρη[1] δοκιμασία Turing στη Royal Society του Λονδίνου, μπερδεύοντας το 33% των κριτών[2]. Επομένως, η εν λόγω δοκιμασία έχει καταφέρει να διατηρήσει την ισχύ της ακόμη και σήμερα, ωστόσο δίχως να αποτελεί ισχυρή ένδειξη ευφυίας.

1.3. Βασικές αρχές της τεχνητής νοημοσύνης

Η τεχνητή νοημοσύνη, υπό μία έννοια, συνιστά ένα κράμα απόψεων, ιδεών και τεχνικών άλλων επιστημών, όπως η φιλοσοφία, τα μαθηματικά, η ψυχολογία, οι νευροεπιστήμες, τα οικονομικά, η τεχνολογία υπολογιστών, η θεωρία ελέγχου και κυβερνητική και τέλος η γλωσσολογία. Έπεται μία σύντομη αναφορά των χαρακτηριστικών, όπως επεσήμαναν οι Russell & Norvig το 2005, που έχει υιοθετήσει η τεχνητή νοημοσύνη από τις παραπάνω επιστήμες.

[1] Η πλήρης δοκιμασία Turing ή αλλιώς total Turing test περιλαμβάνει οπτικό σήμα. Ο ανακριτής δύναται να εξετάσει τις αντιληπτικές ικανότητες του συνομιλητή του, ενώ μπορεί να του παρέχει φυσικά αντικείμενα από την εσοχή. Συνεπώς, η μηχανή που λαμβάνει μέρος σε αυτή τη δοκιμασία εκτός των άλλων χρειάζεται να διαθέτει μηχανική όραση και ρομποτική, ώστε να βλέπει και να διατηρεί σωματική επαφή με τα φυσικά αντικείμενα. (Russel & Norvig, 2005)

[2] Σύμφωνα με τον Alan Turing για να στεφθεί με επιτυχία μία δοκιμασία και κατ' επέκταση να θεωρηθεί ευφυής μία μηχανή θα πρέπει να ξεγελάσει το 30% των κριτών.

1.3.1. Φιλοσοφία (από το 428 π.Χ.)

Η συνεισφορά της φιλοσοφίας έγκειται στην επεξεργασία των απόψεων διαφόρων φιλοσόφων σχετικά με τη νόηση. Αρχικά διατυπώνεται ένα σύνολο τυπικών κανόνων για την εξαγωγή έγκυρων συμπερασμάτων, περιγράφοντας το ορθολογικό μέρος της νόησης. Σειρά έχει η ανάλυση και επεξήγηση του τρόπου κατά τον οποίο προκύπτει η νόηση. Η πρώτη άποψη, υποστηρίζει τη θεωρία του *δυϊσμού*[3], σύμφωνα με την οποία ένα μέρος της νόησης δεν υπόκειται σε φυσικούς κανόνες. Στον αντίποδα, κάποιοι φιλόσοφοι είναι υποστηρικτές του *υλισμού*. Για αυτούς, νόηση είναι η λειτουργία του εγκεφάλου σύμφωνα με τους νόμους της φυσικής. Πέρα από τη νόηση, αυτό που ενδιαφέρει τη τεχνητή νοημοσύνη είναι η πηγή προέλευσης γνώσης. Εδώ ορθώνονται δύο κινήματα του εμπειρικισμού και της επαγωγής. Το πρώτο ξεκίνησε από μία αμφιλεγόμενη μορφή στην ιστορία της επιστήμης, τον Francis Bacon, προτείνοντας μία αναθεώρηση του έργου «Όργανον» του Αριστοτέλη, το Νέο Όργανο, θέτοντας στο κέντρο της νόησης την επιστήμη. Ωστόσο, την αποτυχία του Bacon να συστηματοποιήσει τον εμπειρισμό ως γνωσιολογική θεώρηση έρχεται να καλύψει ο John Locke, υποστηρίζοντας ότι «η ψυχή είναι άγραφος πίνακας, δέχεται ιδέες και γνώσεις από την εμπειρία». Με άλλα λόγια, πίστευε ότι η νόηση προέρχεται από τις πληροφορίες που παρέχουν οι αισθήσεις του ανθρώπου, ενώ διατύπωσε τη βάση του κλασσικού εμπειρικισμού, θεωρώντας ότι η επεξεργασία των δεδομένων που παρέχουν οι ανθρώπινες αισθήσεις δύναται να οδηγήσει την ανθρώπινη σκέψη σε αληθή συμπεράσματα. Ο David Hume, αν και εμπιστευόταν τα δεδομένα της εμπειρίας ήταν αντίθετος ως προς τις μεθόδους των Bacon και Locke, ενώ αγκάλιαζε τη θέση του George Berkeley ότι «δεν μπορεί να αποδεχθεί ότι δεν υπάρχει». Συνεπώς, στο σύγγραμμά του «Πραγματεία της Ανθρώπινης Φύσης» πρότεινε μία ενδιάμεση άποψη μεταξύ του ρεαλισμού και του ιδεαλισμού, γνωστή ως επαγωγή, σύμφωνα με την οποία είναι δυνατή η ύπαρξη υλικού κόσμου που δεν εξαρτάται από τις ανθρώπινες αισθήσεις, αντίθετα οι γενικοί κανόνες είναι απόρροια της έκθεσης σε επανειλημμένες συσχετίσεις. (Russel & Norvig, 2005)

Παρόλα αυτά το σημαντικότερο ερώτημα, για την τεχνητή νοημοσύνη, στο οποίο απαντά η φιλοσοφία είναι το πώς η γνώση οδηγεί στη δράση. Η κατανόηση

[3] Η θεωρία του δυϊσμού διατυπώθηκε από τον René Descartes τον 17ο αιώνα, παρόλο που η ιδέα ανάγεται στον Πλάτωνα.

μιας αιτιολογημένης ενέργειας μπορεί να οδηγήσει στη δημιουργία και κατασκευή των κατάλληλων πρακτόρων. Αρωγός σε αυτό είναι ο αλγόριθμος που πρότεινε ο Αριστοτέλης στα Ηθικά Νικομάχεια. Συγκεκριμένα υποστήριξε ότι η λογική σύνδεση μεταξύ των στόχων και του αποτελέσματος υποδεικνύουν τις απαραίτητες ενέργειες.

1.3.2. Μαθηματικά (περίπου από το 800 π.Χ.)

Οι θεμελιώδεις ιδέες για την τεχνητή νοημοσύνη απορροφήθηκαν από τη φιλοσοφική επιστήμη, εντούτοις η εκκίνηση της ξεχωριστής αυτής επιστήμης (σ.σ. τεχνητή νοημοσύνη) δόθηκε από τα μαθηματικά. Όλες οι ανωτέρω ιδέες και θεωρίες έπρεπε να γίνουν πράξη μέσω μαθηματικής τυποποίησης στη λογική, στη θεωρία υπολογισμού και στις πιθανότητες, που αποτελούν τους τρεις θεμελιώδεις τομείς. Συγκεκριμένα, η προσφορά των μαθηματικών στη τεχνητή νοημοσύνη ανάγεται πρώτον στους τυπικούς κανόνες που απαιτούνται για την εξαγωγή έγκυρων συμπερασμάτων, ιδέα που ξεκίνησε από τους Έλληνες φιλοσόφους αλλά αναπτύχθηκε αρχικά από τον George Boole με την προτασιακή λογική και εν συνεχεία από τον Gottlob Frege, δημιουργώντας τη λογική πρώτης τάξης. Δεύτερον, στο τι μπορεί να υπολογιστεί και τι όχι, περνώντας στο τομέα της θεωρίας υπολογισμού. Το 1931 ο Kurt Gödel διατύπωσε το θεώρημα της μη πληρότητας, υποδεικνύοντας ότι οποιαδήποτε γλώσσα μπορεί να περιγράψει τις ιδιότητες φυσικών αριθμών, έχει αληθείς προτάσεις, η αλήθεια των οποίων δεν μπορεί να επιβεβαιωθεί από κάποιον αλγόριθμο. Εξετάζοντας ενδελεχώς το θεώρημα της μη πληρότητας οδηγούμαστε στο συμπέρασμα ότι στο σύνολο των ακεραίων υπάρχουν συναρτήσεις για τις οποίες ο υπολογισμός είναι αδύνατος. Γεγονός που προέτρεψε τον Alan Turing να εντοπίσει τις συναρτήσεις που αφενός ανήκουν στο σύνολο των ακεραίων, αφετέρου μπορούν να υπολογιστούν με τη βοήθεια ενός αλγορίθμου. Κάπως έτσι ορίστηκε η θέση Church-Turing, κατά την οποία «η Turing- υπολογισιμότητα[4] περιλαμβάνει κάθε πιθανή αποτελεσματική διαδικασία υπολογισμών». Εκτός από τις υπολογίσιμες και μη υπολογίσιμες συναρτήσεις στη θεωρία υπολογισμού συναντά κανείς και την έννοια των δυσεπίλυτων προγραμμάτων, δηλαδή των προβλημάτων

[4] Με τον όρο Turing – υπολογισιμότητα ή αλλιώς Turing-computability αναφερόμαστε στην υπολογιστική διαδικασία μέσω των μηχανών Turing.

για τα οποία ο χρόνος επίλυσης αυξάνεται εκθετικά με το μέγεθος των στιγμιοτύπων. Η εκθετική αύξηση υποδηλώνει την μη επίλυση προβλημάτων ακόμη και μικρού ή μεσαίου μεγέθους σε λογικό χρόνο.

Τέλος, ο τομέας των πιθανοτήτων συνιστά σημαντική προσφορά στη τεχνητή νοημοσύνη, καθώς συμβάλλει στην αντιμετώπιση αβέβαιων συλλογιστικών, κυρίως μέσω της ανάλυσης Bayes, στα περισσότερα συστήματα τεχνητής νοημοσύνης.

1.3.3. Οικονομικά (από το 1776)

Η αρωγή της επιστήμης των οικονομικών εντοπίζεται κυρίως στη λήψη αποφάσεων. Οι πράκτορες συχνά καλούνται να λάβουν κατάλληλες αποφάσεις για την επόμενη κίνησή τους. Το ερώτημα, λοιπόν, που τίθεται είναι πως πρέπει να λάβουν τις αποφάσεις, ώστε να παρουσιάσουν τα καλύτερο δυνατό αποτέλεσμα. Απάντηση στην ερώτηση δίνει η θεωρία των αποφάσεων, συνδυάζοντας τη θεωρία των πιθανοτήτων με τη θεωρία των χρησιμοτήτων. Η θεωρία των αποφάσεων παρέχει λύσεις σε συνθήκες αβεβαιότητας, όπου το περιβάλλον δεν επηρεάζει τον πράκτορα. Αντίθετα, σε περιβάλλοντα που ο πράκτορας δύναται να επηρεαστεί από τις κινήσεις των υπόλοιπων πρακτόρων, είναι προτιμότερη η θεωρία των παιγνίων. Το παράδοξο με αυτή τη θεωρία έγκειται στη τυχαία λήψη αποφάσεων από έναν ορθολογικό πράκτορα ή τουλάχιστον στη λήψη αποφάσεων που φαντάζει τυχαία στους άλλους, καθώς ο πράκτορας δε γνωρίζει τον τρόπο με τον οποίο λαμβάνει αποφάσεις ο αντίπαλος. Τέλος, ένα πεδίο που ωφέλησε την τεχνητή νοημοσύνη είναι η επιχειρησιακή έρευνα και δει οι διαδικασίες αποφάσεων Markov του Bellman, για προβλήματα ακολουθιακών αποφάσεων.

1.3.4. Νευροεπιστήμες (από το 1861)

Η προσφορά των νευροεπιστημών στην τεχνητή νοημοσύνη είναι προφανής και έγκειται στον τρόπο με τον οποίο ο εγκέφαλος επεξεργάζεται τις πληροφορίες. Σύμφωνα με τους επιστήμονες, ο εγκέφαλος είναι το μέρος του σώματος που

εγκαθίσταται η συναίσθηση. Κατά τον J. Searle «μία συλλογή μεμονωμένων κυττάρων μπορεί να οδηγεί στη σκέψη, τη δράση και τη συναίσθηση», δηλαδή ότι ο εγκέφαλος δημιουργεί νόηση. Συχνά, ο τρόπος λειτουργίας των ηλεκτρονικών υπολογιστών παρομοιάζεται με τον τρόπο σκέψης και δράσης των ανθρώπων. Εντούτοις, οι διαφορές μεταξύ υπολογιστών και ανθρώπινων εγκεφάλων είναι αρκετές. Τα τσιπ των υπολογιστών είναι ικανά να εκτελούν τις εντολές σε εμφανώς μικρότερο χρονικό διάστημα από τους νευρώνες του ανθρώπινου εγκεφάλου, υπολογίζοντας τη διαφορά σε εκατομμύρια φορές. Ωστόσο, οι ανθρώπινοι νευρώνες είναι σχεδόν 1000 φορές περισσότεροι από τις λογικές πύλες της CPU, με αποτέλεσμα ο εγκέφαλος να είναι τελικά 100.000 φορές ταχύτερος από τους ηλεκτρονικούς υπολογιστές.

1.3.5.Ψυχολογία (από το 1879)

Η ψυχολογία είναι η επιστήμη που ερευνά τον τρόπο σκέψης και συμπεριφοράς κατ' αρχάς των ανθρώπων και σε δεύτερο στάδιο των ζώων. Το 1879 σηματοδοτεί την έναρξη της *πειραματικής ψυχολογίας*. Ο Wundt επιδιδόταν σε λεπτομερή πειράματα για τον έλεγχο διαφόρων ψυχολογικών θεωριών, με τη βοήθεια των συνεργατών του. Πλέον η πειραματική ψυχολογία ασχολείται με τη μελέτη διαφόρων ψυχικών φαινομένων και συμπεριφορών, μέσω της ενδοσκόπησης των ανθρώπων.

Από την εφαρμογή της μεθόδου μελέτης συμπεριφοράς των ζώων, στους ανθρώπους, δημιουργήθηκε το κίνημα του *συμπεριφορισμού*. Οι υποστηρικτές αυτού του κινήματος πίστευαν ότι η ενδοσκόπηση δεν μπορούσε να παρέχει αξιόπιστα αποτελέσματα και κατά συνέπεια θα έπρεπε να απορρίπτεται οποιαδήποτε θεωρία βασιζόμενη σε νοητικές διαδικασίες. Το κίνημα είχε πολλά αποτελέσματα στα ζώα, σε αντίθεση με τους ανθρώπους. Αρκετά χρόνια αργότερα, η ανάπτυξη της υπολογιστικής μοντελοποίησης, ώθησε στη δημιουργία της γνωστικής επιστήμης. Έρευνες έδειξαν ότι τα υπολογιστικά μοντέλα μπορούσαν να χρησιμοποιηθούν με επιτυχία στη μνήμη, τη γλώσσα και τη λογική σκέψη. Αξιοσημείωτος είναι ο παραλληλισμός, εκ μέρους του Aderson, της γνωστικής θεωρίας με το πρόγραμμα υπολογιστή.

1.3.6. Τεχνολογία υπολογιστών (από το 1940)

Ακούγοντας κάποιος τον όρο τεχνητή νοημοσύνη, θεωρεί ότι αναφερόμαστε σε ένα κλάδο της επιστήμης των υπολογιστών. Συνεπώς, πιστεύει ότι η μοναδική επιστήμη που σχετίζεται με τον όρο είναι αυτή της τεχνολογίας υπολογιστών, δίχως όμως να ισχύει όπως αναλύθηκε προηγουμένως. Παρά ταύτα η τεχνητή νοημοσύνη είναι άρρηκτα συνδεδεμένη με την εν λόγω επιστήμη, καθότι για την επίτευξή της απαιτείται πέρα από τη νοημοσύνη και η τεχνολογία. Η συνεισφορά της εστιάζεται στη κατασκευή αποδοτικών υπολογιστών. Η εκκίνηση αυτής της προσπάθειας δόθηκε στο δεύτερο μισό του 20^{ου} αιώνα, όταν η ομάδα του Alan Turing κατασκεύασε το Heath Robinson, το πρώτο λειτουργικό υπολογιστή[5]. Ακολούθησαν αρκετοί υπολογιστές, με αποκορύφωμα τον ENIAC που θεωρείται ο πιο σημαντικός πρόδρομος των σημερινών υπολογιστών. Κάθε γενιά υπολογιστών χαρακτηρίζεται από αύξηση ταχύτητας και χωρητικότητας, μεταβλητές ιδιαίτερα σημαντικές για την ανάπτυξη της τεχνητής νοημοσύνης.

1.3.7. Θεωρία ελέγχου και κυβερνητική (από το 1948)

Σε αυτή την επιστήμη, η τεχνητή νοημοσύνη, οφείλει την δυνατότητα των τεχνουργημάτων να δρουν υπό το δικό τους έλεγχο, με άλλα λόγια να είναι αυτοελεγχόμενα. Η θεωρία ελέγχου χρωστά πολλά στον Norbert Wiener, ο οποίος ασχολήθηκε με τη συμπεριφορά των δυναμικών συστημάτων. Σήμερα, ο κλάδος ασχολείται με τη σχεδίαση συστημάτων που μεγιστοποιούν μία αντικειμενική συνάρτηση μέσα στο χρόνο (Russell & Norvig, 2005). Θα αναρωτιόταν κανείς, για ποιο λόγο η θεωρία ελέγχου και η τεχνητή νοημοσύνη αποτελούν δύο ξεχωριστούς κλάδους. Η θεωρία ελέγχου βασίζεται στη χρήση μαθηματικού λογισμού και γραμμικής άλγεβρας. Στον αντίποδα, η τεχνητή νοημοσύνη σχετίζεται με τα διακριτά μαθηματικά. Η τεχνητή νοημοσύνη ξεπερνά τα όρια και τους περιορισμούς που θέτει

[5] Η κατασκευή του χρονολογείται το 1940, κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου στην Αγγλία. Σκοπός της μηχανής ήταν η αποκρυπτογράφηση της Γερμανικής μηχανής Enigma, που χρησιμοποιούταν από τη ναζιστική Γερμανία για τη κρυπτογράφηση των μηνυμάτων.

η θεωρία ελέγχου, προσφέροντας τη δυνατότητα στους ερευνητές της να ασχοληθούν με τομείς που η θεωρία ελέγχου αδυνατεί (Russell & Norvig, 2005).

1.3.8. Γλωσσολογία (από το 1957)

Η τελευταία επιστήμη με την οποία σχετίζεται η τεχνητή νοημοσύνη είναι η γλωσσολογία. Η γλωσσολογία προσπαθεί να απαντήσει μεταξύ των άλλων στο πώς η γλώσσα σχετίζεται με τη σκέψη. Η θεωρία του Noam Chomsky ήταν φιλική προς προγραμματισμό, αφού η τυπική της μορφή το επέτρεπε. Η υπολογιστική γλώσσα, συνιστά ένα πεδίο όπου «συναντιούνται» η σύγχρονη γλωσσολογία και η τεχνητή νοημοσύνη, με σκοπό την αξιοποίηση υπολογιστών για την επεξεργασία φυσικής γλώσσας. Πρόκειται για ένα αρκετά δύσκολο έργο, καθώς η κατανόηση της γλώσσας δε περιορίζεται στη κατανόηση της δομής των προτάσεων, αλλά αφορά κατανόηση του υπό συζήτηση θέματος και των συμφραζομένων του.

1.4. Ιστορική εξέλιξη

Όπως συνηθίζουν να λένε οι επιστήμονες της πληροφορικής ο ηλεκτρονικός υπολογιστής είναι ένα «χαζό» κουτί που κάνει ότι του προστάζει ο άνθρωπος, αξιοποιώντας πολλές φορές τις πληροφορίες που έχει αποθηκευμένες στο σκληρό δίσκο του σε δυαδική πάντα μορφή. Προσπαθώντας κάποιος να ορίσει τη σημασία της τεχνητής νοημοσύνης θα μπορούσε να υποστηρίξει ότι είναι η «τέχνη» να ορίζει κανείς τον υπολογιστή να βλέπει ότι και ένας άνθρωπος μέσα σε μία εικόνα (Κωνσταντίνος Δασκαλάκης). Επομένως, ο συνδυασμός των δύο προηγουμένων εννοιών συμβάλλει στην αρωγή ενός έξυπνου αλγορίθμου, που δεν είναι άλλη από τη βοήθειά του ώστε να μπορεί ένας υπολογιστής να μετατρέψει την παραπάνω πληροφορία σε κάτι που θα έχει νόημα. Στα πρώτα βήματα ανάπτυξης τεχνητής νοημοσύνης οι επιστήμονες προσπάθησαν να αντιγράψουν τον ανθρώπινο εγκέφαλο, σύντομα όμως αντιλήφθηκαν τη δυσκολία του εγχειρήματος τροποποιώντας το αρχικό σχέδιο και αποπειρώμενοι να κατασκευάσουν ένα άλλο κουτί, που παρά τις

τυχόν διαφορές του με το πρώτο, θα χαρακτηριζόταν από ενδιαφέρουσες λειτουργίες. Αυτή η προσέγγιση ονομάστηκε κλασική και όπως ήταν αναμενόμενο παρουσίασε μέτρια αποτελέσματα. Την κλασική προσέγγιση ακολούθησε η κλασική αλγοριθμική προσέγγιση του Alan Turing κατά τον οποίο «για να κάνει ο υπολογιστή κάτι, πρέπει να του ορίσουμε μία καλώς ορισμένη ακολουθία απλών υπολογισμών (πρόσθεση, αφαίρεση, αποθήκευση στη μνήμη, ανάκληση από τη μνήμη) που συνολικά έχουν το επιθυμητό αποτέλεσμα». Η φράση αυτή εσωκλείει το μαθηματικό πρόβλημα στα θεμέλια της τεχνητής νοημοσύνης. Έστω, ότι ο στόχος είναι η κατανόηση μίας εικόνας από τον υπολογιστή. Σύμφωνα με τη προσέγγιση του Alan Turing, πρέπει να οριστεί μία συνάρτηση που θα «κοιτάει» τα pixels της εικόνας και θα επιστρέφει ένα αποτέλεσμα σχετικά με το περιεχόμενο αυτής, π.χ. αν η εικόνα που έλαβε ως είσοδο αναπαρίσταται ένα δελφίνι ή όχι. Εντούτοις, πρόκειται για μαθηματικά ανέφικτο πρόβλημα, καθώς η κατανόηση μία εικόνας είναι τόσο περίπλοκη που δε μπορεί να περιγραφεί στον υπολογιστή με λεπτομέρεια η διαδικασία που θα πρέπει να ακολουθήσει ώστε να αναγνωρίσει το περιεχόμενό της.

Στη διαρκή προσπάθεια για εύρεση λύσης κατέληξαν στη χρήση *αντιπροσώπου*. Το σκεπτικό ήταν απλό. Αντί να περιγράφει ο άνθρωπος τον τρόπο με τον οποίο ο υπολογιστής θα επιλύσει μία περίπλοκη νοητική διεργασία όπως η αναγνώριση μίας εικόνας, θα χρησιμοποιηθεί ένας αλγόριθμος, που θα ψάχνει κάποιον άλλο αλγόριθμο ικανό να επιλύσει μία περίπλοκη λειτουργία. Έτσι, ο αρχικός αλγόριθμος χαρακτηρίζεται από μία απλή αρχιτεκτονική πολλών παραμέτρων που ορίζονται από τον ίδιο, βάση πολλών παραδειγμάτων της νοητικής διεργασίας που καλείται να επιλύσει. Αντιπαραβάλλοντας, το διαφορετικό αυτό «κουτί» με τον ανθρώπινο εγκέφαλο, οι αλγόριθμοι είναι όπως οι νευρώνες για τον ανθρώπινο εγκέφαλο. Κάθε αλγόριθμος αναλαμβάνει μία απλή διεργασία και όλοι πρέπει να συνδέονται με τέτοιο τρόπο ώστε να επιτυγχάνουν το στόχο τους.

Εφαρμόζοντας τη παραπάνω συλλογιστική, σημειώθηκε ραγδαία ανάπτυξη στην επιστήμη της τεχνητής νοημοσύνης. Αρωγός σε όλη τη προσπάθεια στάθηκε το διαδίκτυο. Από την αρχή της δημιουργίας του παγκόσμιου ιστού ο άνθρωπος έχει αποθηκεύσει ένα τεράστιο ηλεκτρονικό αποτύπωμα σε τεράστιους επεξεργαστές που λειτουργεί ως παράδειγμα στα συστήματα τεχνητής νοημοσύνης.

2. Εισαγωγή Στα Big Data

Στο παρόν κεφάλαιο αναμένεται να διασαφηνιστεί ο όρος big data και συνάμα να παρουσιαστεί η πορεία του μέχρι σήμερα παραθέτοντας τα κυριότερα σημεία και τις χρονολογίες σταθμούς.

Ο όρος Big Data ή αλλιώς Δεδομένα Μεγάλης Κλίμακας απασχολεί ολοένα και μεγαλύτερο τμήμα της ανθρωπότητας. Ειδικοί διαφόρων επιστημών ερευνούν τον όρο προσπαθώντας να συμβάλλουν στην ομαλή εξέλιξή του. Στο πρώτο άκουσμα πρόκειται για ένα αρκετά κατανοητό όρο, τουλάχιστον ευκολότερο της τεχνητή νοημοσύνης, που ωστόσο δε παύει να κρύβει κινδύνους. Πρόκειται για μία αφηρημένη έννοια και αυτό υποδεικνύεται από την έλλειψη ενός κοινώς αποδεκτού ορισμού.

2.1. Τι είναι big data

Έτσι λοιπόν, κατά καιρούς δόθηκαν αρκετοί ορισμοί. Οι Manyika et al. σε κοινό τους έργο το 2011 χαρακτήρισαν τα big data ως «ένα σύνολο στοιχείων δεδομένων τα οποία δεν μπορούν να συγκεντρωθούν, αποθηκευτούν και επεξεργαστούν από τα παραδοσιακά λογισμικά βάσεων δεδομένων». Οι Mayer-Schonberger & Cukier, τα όρισαν το 2013 ως «τεράστια σύνολα δεδομένων και πληροφοριών απ' όπου δύναται να εξαχθούν χρήσιμα συμπεράσματα, όπως ο μεγάλος όγκος, η ποικιλία, η ταχύτητα και η αξία τους». Την ίδια χρονιά ο Krasha, έδωσε μία διαφορετική απάντηση υποστηρίζοντας ότι τα big data είναι «η λύση όταν η κανονική εφαρμογή της τρέχουσας τεχνολογίας δεν επιτρέπει στους χρήστες να έχουν έγκαιρες, αποδοτικές και ποιοτικές απαντήσεις σε ερωτήσεις που βασίζονται σε δεδομένα». Τέλος, οι Chen et al, το 2014, έδωσαν τη δική τους ερμηνεία στον όρο,

αναφέροντάς τα ως «σύνολα δεδομένων τα οποία δεν μπορεί να αντιληφθεί και διαχειριστεί η παραδοσιακή πληροφορική και τα εργαλεία λογισμικού σε ένα ανεκτό επίπεδο χρόνου». Συνεπώς, αν προσπαθήσουμε να διατυπώσουμε ένα γενικότερο ορισμό θα λέγαμε ότι ως big data νοούνται τα *τεράστια σύνολα δεδομένων που βοηθούν στην λήψη χρήσιμων συμπερασμάτων και τα οποία είναι αδύνατο να αξιοποιηθούν και μελετηθούν από τα παραδοσιακά λογισμικά βάσεων δεδομένων*.

2.2. Ιστορική εξέλιξη των big data

Τα πρώτα δείγματα για τη γέννηση της ιδέας των big data δόθηκαν το 1941 όταν εμφανίστηκε ο όρος "information explosion" δηλαδή έκρηξη πληροφοριών. Στη συνέχεια έλαβαν χώρα διάφορα γεγονότα που συντέλεσαν στην εξέλιξή του. Παρά ταύτα η πρώτη εμφάνιση του όρου έγινε το 1997 από μία ομάδα επιστημών της NASA, δηλώνοντας ότι αντιμετωπίζουν πρόβλημα μεγάλων δεδομένων. Συγκεκριμένα, ήταν αδύνατο να αναπαραστήσουν γραφικά τα δεδομένα που κατείχαν, αφού το μέγεθός τους ήταν απαγορευτικό για αποθήκευση τόσο στη κύρια μνήμη όσο και στο τοπικό και εξωτερικό σκληρό δίσκο. Η εμφάνισή τους συνδέεται με την ραγδαία ανάπτυξη που σημειώθηκε εκείνη τη περίοδο στο χώρο του διαδικτύου και του παγκόσμιου ιστού.

Αυτή ήταν μόλις η αρχή, καθώς η ραγδαία εξέλιξη της τεχνολογίας και η υιοθέτησή της από όλα τα κοινωνικά στρώματα συνετέλεσε στην αύξηση της παραγόμενης πληροφορίας, με αποτέλεσμα όταν αναφερόμαστε σε big data να μιλάμε για δεδομένα της κλίμακας των μερικών terabytes έως και εκατοντάδων zetabytes, εκτιμώντας ότι το μέγεθος θα αυξηθεί (Khanduja et al., 2017). Λόγω της αλόγιστης πολλές φορές χρήσης του διαδικτύου, οι χρήστες πρόσθεσαν στην ιδιότητα του καταναλωτή και αυτή του παραγωγού δεδομένων και αυτό αφού κάθε άνθρωπος αφήνει καθημερινά το «ψηφιακό ίχνος» του. Χαρακτηριστικό είναι, μάλιστα, ότι το ποσοστό της ψηφιακής ανθρώπινης γνώσης ξεπερνούσε το 95% για το έτος 2008 σύμφωνα με αντίστοιχη μελέτη. Αξιοσημείωτη είναι η δήλωση του Αμερικανού επιχειρηματία Eric Schmidt το 2010 αναφορικά με το ρυθμό διόγκωσης των πληροφοριών «από την αρχή του ανθρώπινου πολιτισμού, η ανθρωπότητα

δημιούργησε 5 exabytes πληροφορίας μέχρι το 2003. Σήμερα δημιουργούμε τόση πληροφορία κάθε 2 μέρες και ο αριθμός αυξάνεται». Νωρίτερα, ο Buckminster Fuller εισήγαγε τη καμπύλη διπλασιασμού της γνώσης, επισημαίνοντας πως μέχρι το 1900 η ανθρώπινη γνώση διπλασιαζόταν περίπου κάθε εκατό χρόνια. Από τότε και μέχρι το 1945, δηλαδή το τέλος του Β΄ Παγκοσμίου Πολέμου η γνώση διπλασιαζόταν κάθε είκοσι πέντε χρόνια, ενώ στις μέρες μας υπολογίζεται ότι διπλασιάζεται κατά μέσο όρο κάθε 13 μήνες και αυτό οφείλεται στο διαφορετικό ρυθμό ανάπτυξης των διαφορετικών ειδών γνώσεων. Φυσικά σε ότι αφορά το μέλλον, ο χρόνος διπλασιασμού της ανθρώπινης γνώσης αναμένεται να μειωθεί κι άλλο.

Πολλοί άνθρωποι πιστεύουν λανθασμένα ότι το πρόβλημα σχετικά με όλες αυτές τις πληροφορίες έγκειται στο κόστος. Εντούτοις, στη πραγματικότητα το κόστος δεν είναι αυτό που απασχολεί την επιστήμη, καθώς είναι πολύ μικρό. Αντίθετα, η πρόκληση εντοπίζεται στο τρόπο ανάλυσης και επεξεργασίας των πληροφοριών και εν συνεχεία στην απόκτηση χρήσιμης γνώσης. Βέβαια, έχουν δοθεί απαντήσεις σχετικά με το παραπάνω ερώτημα που ταλάνιζε για χρόνια τους επιστήμονες. Πώς μπορούμε να επεξεργαστούμε τα big data σε σύντομο χρονικό διάστημα; Τη λύση στο πρόβλημα ήρθε να δώσει ο παραλληλισμός. Με άλλα λόγια, πολλοί υπολογιστές πραγματοποιούν ταυτόχρονα διεργασίες για τον ίδιο σκοπό. Η αρχή στην οποία βασίζεται ο παραλληλισμός είναι αυτή του διαίρει και βασίλευε κατά την οποία ένα μεγάλο πρόβλημα μπορεί να διαιρεθεί σε μικρότερα, υποπροβλήματα, τα οποία στη συνέχεια θα λυθούν παράλληλα. Με άλλα λόγια, αντί να χρησιμοποιείται ένας δίσκος, χρησιμοποιούνται χιλιάδες δίσκοι και επεξεργαστές. Το αποτέλεσμα όλων αυτών ήταν η δημιουργία των γνωστών πλέον data centers που αριθμούν περισσότερους από εκατό χιλιάδες υπολογιστές ανά τον κόσμο. Πέρα από αυτά όμως, υπάρχει και ένας ακόμη τρόπος που επιτρέπει την επεξεργασία των big data και ακούει στο όνομα cloud computing ή αλλιώς υπολογιστικό νέφος. Σε αυτό, είναι εφικτή η αποθήκευση και επεξεργασία υπό τη μορφή παρεχόμενης υπηρεσίας.

2.3. Το μοντέλο 3V

Το μοντέλο έχει πάρει το όνομά του από τις τρεις μεταβλητές Volume, Velocity και Variety, αποδίδοντας τις ιδιότητες σε κάθε σύνολο δεδομένων (Khanduja et al., 2017).

Volume – Όγκος

Αναφερόμαστε στον όγκο των δεδομένων που καλούμαστε να διαχειριστούμε. Η μέγεθος αυτών των δεδομένων αυξάνεται με εκθετικό ρυθμό. Σε αυτό συνετέλεσε και η πρόοδος της τεχνολογίας. Παλαιότερα, τα δεδομένα δημιουργούνταν από συγκεκριμένες ομάδες ατόμων, π.χ. για τα δεδομένα μίας εταιρίας δημιουργοί ήταν οι υπάλληλοι αυτής. Στις μέρες μας, τα δεδομένα προέρχονται από διάφορες ομάδες. στα πλαίσια μίας εταιρίας, υπεύθυνοι είναι οι υπάλληλοι, οι συνεργάτες αλλά και οι πελάτες. Εντούτοις, κάθε χρήστης έξυπνου κινητού θεωρείται ότι δημιουργεί δεδομένα, καθώς καθημερινά αποστέλλει πληροφορίες. Συνεπώς, κρίθηκε απαραίτητη η ανάγκη να δαμαστούν όλα αυτά τα δεδομένα[6], με αποτέλεσμα την εφεύρεση νέων τεχνικών και μεθόδων (Khanduja et al., 2017).

Velocity – Ταχύτητα

Πρόκειται για τη ταχύτητα με την οποία εισέρχονται νέα δεδομένα ή ανανεώνονται τα ήδη υπάρχοντα (Khanduja et al., 2017). Κατά το πρώιμο ή αρχικό στάδιο οι εταιρίες χρησιμοποιούσαν το λεγόμενο batch process, δηλαδή μία διαδικασία συνόλου παραγωγής. Σύμφωνα με αυτή, όταν υποβάλλεται μία εργασία στο server, ο ενδιαφερόμενος περιμένει για την απόκριση του αποτελέσματος. Ωστόσο, όπως είναι κατανοητό αυτό απαιτεί ο ρυθμός με τον οποίο εισέρχονται τα δεδομένα στο server να είναι μικρότερος από το ρυθμό με τον οποίο ο server τα επεξεργάζεται. Πλέον, η ανάπτυξη της τεχνολογίας και κυρίως των social media, επιτάσσει την ανάγκη ταχύτερων δικτύων, που μπορούν να επεξεργαστούν δεδομένα σε πραγματικό χρόνο. Κλειδί σε αυτό συνιστά η μείωση της καθυστέρησης.

[6] Αρκεί να αναφερθεί ότι ένα αρχείο κειμένου ανέρχεται σε μερικά kilo bytes, ένα αρχείο ήχου σε μερικά mega bytes και μία ταινία σε μερικά giga bytes.

Variety – Ποικιλία

Αναφερόμαστε στο εύρος πιθανών διαφορετικών τύπων δεδομένων που καλούμαστε να επεξεργαστούμε (Khanduja et al., 2017). Πριν από κάποια χρόνια η δομή μπορούσε να επιβληθεί, τώρα έχουν προστεθεί δεκάδες μορφές βάσεων δεδομένων από τις πιο απλές όπως είναι η φωτογραφία, το βίντεο, τα SMS, τα έγγραφα, έως τις πιο σύνθετες όπως το διαδίκτυο, τα δεδομένα GPS, οι σχεσιακές βάσεις δεδομένων, τα δεδομένα αισθητήρων. Σίγουρα όσο αυξάνεται και εξελίσσεται η τεχνολογία και ως εκ τούτου οι εφαρμογές, πρέπει να αναμένουμε την εμφάνιση νέων μορφών δεδομένων.

2.4. Η υλοποίηση των big data

Το πρώτο βήμα για την ύπαρξη των big data είναι η δημιουργία δεδομένων. Το βήμα αυτό είναι γνωστό και ως data generation. Οι πηγές δημιουργίας είναι πολλές και διάφορες. Τη μεγαλύτερη πηγή αποτελεί το διαδίκτυο. Οι εκατοντάδες χρήστες ανά τον κόσμο, παράγουν εν αγνοία τους τεράστιες ποσότητες δεδομένων μέσω των ενεργειών, όπως λόγου χάρη η αναζήτηση λέξεων-κλειδιών στις διάφορες μηχανές αναζήτησης, οι δημοσιεύσεις στα μέσα κοινωνικής δικτύωσης, οι σχολιασμοί σε ιστοσελίδες και blogs, το ανέβασμα φωτογραφιών ή βίντεο κ.ά.. Τα εν λόγω δεδομένα χρήζουν ιδιαίτερης αξίας, αφού είναι ενδεικτικά των ενδιαφερόντων, συνηθειών και αναγκών των χρηστών (Sapountzi & Spannis, 2016). Ως εκ τούτου, η επεξεργασία τους δύναται να προσφέρει μία εικόνα ανάλογη της προσωπικότητας του εκάστοτε χρήστη, αλλά και ένα ολοκληρωμένο προφίλ αυτού (Kersting & Meyer, 2018). Άλλες πηγές δεδομένων, εξίσου σημαντικές συνιστούν οι επιχειρήσεις, τα δεδομένα επιστημονικής έρευνας, το Internet of Things, τα βιοϊατρικά δεδομένα, οι εμπορικές συναλλαγές κ.ά. Όπως είναι φυσικό, η δημιουργία δεδομένων αποτελεί το θεμέλιο της έννοιας των big data και συνεπώς σημαντικό στοιχείο για τα επόμενα βήματα.

Τη δημιουργία δεδομένων έπεται η απόκτηση των δεδομένων, δηλαδή το data acquisition. Σε αυτό συγκαταλέγεται η συλλογή, η μετάδοση και η προ-επεξεργασία δεδομένων. Όπως γίνεται αντιληπτό τα δεδομένα συλλέγονται από τις διάφορες πηγές

που αναφέρθηκαν ανωτέρω (συλλογή) και μεταφέρονται σε ένα σύστημα διαχείρισης και αποθήκευσης (μετάδοση), για να υποστούν την πρώτη επεξεργασία (προ-επεξεργασία) ώστε να κρατηθούν τα χρήσιμα και να διαγραφούν τα άχρηστα δεδομένα. Έπειτα, τα αποθηκευμένα δεδομένα είναι έτοιμα προς επεξεργασία για οποιονδήποτε λόγο θεωρηθεί αναγκαίο.

3. Σύγκλιση Τεχνητής Νοημοσύνης Και Big Data

Το παρόν κεφάλαιο αποτελεί μία εισαγωγή στη σύγκλιση των δύο πεδίων. Ασχολείται με το πώς η τεχνητή νοημοσύνη σχετίζεται και επηρεάζει τη συλλογή και επεξεργασία των δεδομένων μεγάλης κλίμακας, αλλά και με τον τρόπου που τα δεδομένα συμβάλλουν στη ραγδαία ανάπτυξη και βελτιστοποίηση των συστημάτων τεχνητής νοημοσύνης.

Τα δύο πεδία παρόλο που παρουσιάζουν διαφορές ως προς το αντικείμενο ενασχόλησης, διακρίνονται από σχέση εξάρτησης και επηρεασμού. Η τεχνητή νοημοσύνη ως προγενέστερη έχει προσφέρει τις υπηρεσίες της στο πεδίο των big data, κυρίως με το τομέα της μηχανικής μάθησης αλλά και με μία πληθώρα τεχνολογιών. Από την άλλη, τα δεδομένα που έχουν κατακλύσει το διαδίκτυο, αλλά και αυτά που παράγονται καθημερινά αξιοποιούνται από τους επιστήμονες τεχνητής νοημοσύνης τόσο για τη δημιουργία νέων συστημάτων, όσο και για τη βελτιστοποίηση των ήδη υπαρχόντων.

3.1. Μηχανική μάθηση

Η μηχανική μάθηση ή ευρέως γνωστή ως machine learning συνιστά υποπεδίο της επιστήμης των υπολογιστών και απορρέει από την ανάγκη για ανάπτυξη και εξέλιξη της επιστήμης των υπολογιστών και απορρέει από την ανάγκη για ανάπτυξη και εξέλιξη της τεχνητής νοημοσύνης. Βασίζεται στη στατιστική και τη μαθηματική βελτιστοποίηση, υιοθετώντας μεθόδους και πεδία εφαρμογής. Χαρακτηριστική ιδιότητα των νοήμων όντων είναι η μάθηση, δηλαδή η απόκτηση γνώσεων συνήθως ως αποτέλεσμα διδασκαλίας. Επομένως, οι επιστήμονες της τεχνητής νοημοσύνης έπρεπε να δημιουργήσουν υπολογιστικά συστήματα που έχουν τη δυνατότητα να

μάθουν. Στο χώρο της πληροφορικής αυτό ονομάζεται μηχανική μάθηση. Ο Tom Mitchell πρότεινε ένα ορισμό που έτυχε κοινής αποδοχής.

«ένα πρόγραμμα υπολογιστή λέγεται ότι μαθαίνει από εμπειρία E ως προς μία κλάση εργασιών T και ένα μέτρο επίδοσης P, αν η επίδοσή του σε εργασίες της κλάσης T, όπως αποτιμάται από το μέτρο P, βελτιώνεται με την εμπειρία E»

Ο ανωτέρω ορισμός, μας παραπέμπει στα λόγια του Alan Turing, κατά τον οποίο αντί να αναρωτιόμαστε αν οι μηχανές μπορούν να σκεφθούν, πρέπει να αναρωτιόμαστε αν οι μηχανές μπορούν να επιτύχουν σε μία δοκιμασία ευφυούς συμπεριφοράς, δηλαδή να αντιγράψουν την ανθρώπινη συμπεριφορά (Turing, 1950).

Στην επιστήμη της τεχνητή νοημοσύνης, η μηχανική μάθηση ασχολείται με τη μελέτη και ανάπτυξη αλγορίθμων που βελτιώνουν τη συμπεριφορά τους βάσει της εμπειρίας τους. Συχνά οι διαδικασίες μάθησης κατηγοριοποιούνται σε επιβλεπόμενη, μη επιβλεπόμενη και ενισχυτική μάθηση (Russell & Norvig, 2005).

3.1.1 Επιβλεπόμενη μάθηση

Η επιβλεπόμενη μάθηση (supervised learning) αναφέρεται συχνά και ως μάθηση με επιτήρηση, καθώς υπάρχει ένας εκπαιδευτής με γνώση του περιβάλλοντος. Στόχος του αλγορίθμου επιβλεπόμενης μάθησης είναι η δημιουργία συνάρτησης με δεδομένες εισόδους σε γνωστές εξόδους, καθώς και η δημιουργία συνάρτησης για εισόδους με άγνωστη έξοδο (Lidong et al., 2015). Επομένως, αφορά την εκμάθηση μιας γενικής συνάρτησης ή γενικού κανόνα από διάφορα παραδείγματα εισόδου – εξόδου του πράκτορα (Russell & Norvig, 2005).

3.1.2. Μη επιβλεπόμενη μάθηση

Σε αντίθεση με τις συνθήκες που ισχύουν στην επιβλεπόμενη μάθηση, στη μη επιβλεπόμενη ή αλλιώς unsupervised learning δεν παρέχονται συγκεκριμένες τιμές εξόδου (Lidong et al., 2015). Αυτό σημαίνει ότι η μάθηση προτύπων εισόδου δε

περιλαμβάνει γνωστές τιμές εξόδου. Ο πράκτορας αναπτύσσει σταδιακά γνώση, λαμβάνοντας υπόψη του τις εκάστοτε περιπτώσεις. Συνεπώς, συχνά η μη επιβλεπόμενη μάθηση λειτουργεί στα πλαίσια της πιθανοτικής συλλογιστικής (Russell & Norvig, 2005).

3.1.3. Ενισχυτική μάθηση

Αρκετοί υποστηρίζουν ότι αποτελεί υποκατηγορία της μάθησης χωρίς εκπαιδευτή, ωστόσο στη παρούσα εργασία μελετάται ως ξεχωριστή περίπτωση του τομέα της μηχανική μάθησης. Στην ενισχυτική μάθηση ή reinforcement learning ο πράκτορας καλείται να μάθει μέσω της ενίσχυσης ή ανταμοιβής. Ειδικότερα, ο πράκτορας πρέπει να αλληλεπιδράσει με το περιβάλλον και να μάθει από αυτό, χωρίς τη πρόσθετη λήψη πληροφοριών από κάποιο δάσκαλο – όπως συμβαίνει στην επιβλεπόμενη. Κατά μία έννοια, το σύστημα μάθησης προσπαθεί να μάθει τον τρόπο λειτουργίας του δυναμικού περιβάλλοντος δράσης (Russell & Norvig, 2005). Ενδεικτικό παράδειγμα, συνιστά η εκμάθηση επιτραπέζιων παιχνιδιών, στην οποία ο πράκτορας οφείλει να μάθει τους κανόνες του παιχνιδιού, μελετώντας τις κινήσεις του αντιπάλου του, καθ'όση ώρα παίζει.

3.2. Εξόρυξη δεδομένων

Όπως ειπώθηκε σε προηγούμενο κεφάλαιο (σ.σ. 2. Εισαγωγή στα big data) η δημιουργία νέων δεδομένων αυξάνεται εκθετικά ως προς το χρόνο. Απόρροια αυτού είναι η αποθήκευση τεράστιου όγκου δεδομένων και επομένως η ανάγκη για διαχείριση και επεξεργασία αυτού. Έτσι γεννήθηκε ο όρος εξόρυξη δεδομένων (data mining), θέλοντας να περιγράψει τη διαδικασία ανακάλυψης γνώσης από βάσεις δεδομένων. Πρόκειται για την εξεύρεση έγκυρων, εν δυνάμει χρήσιμων και κατανοητών πληροφοριών ή προτύπων από μεγάλες βάσεις δεδομένων με τη βοήθεια ειδικών αλγορίθμων. Τα αποτελέσματα που προκύπτουν από αυτή τη διαδικασία μπορούν εύκολα να αξιολογηθούν και χρησιμοποιηθούν από τον άνθρωπο οδηγώντας

συχνά στη λήψη ορθών αποφάσεων. Η εξόρυξη δεδομένων συνιστά ένα από τα πέντε στάδια[7] της διαδικασίας ανακάλυψης γνώσης από βάσεις δεδομένων, χάριν συντομίας αναφέρεται και ως KDD, ακρωνύμιο των λέξεων Knowledge Discovery in Databases (Xu et al, 2017). Στη διεθνή βιβλιογραφία, συχνά, οι δύο όροι τείνουν να ταυτίζονται με αποτέλεσμα την ύπαρξη σύγχυσης τόσο στον ακαδημαϊκό κύκλο, όσο και στους αναγνώστες αυτής, ωστόσο κάτι τέτοιο αποτελεί λάθος. Για την εξόρυξη δεδομένων χρησιμοποιούνται μεταξύ άλλων και αρχές της στατιστικής, της τεχνητής νοημοσύνης, των νευρωνικών δικτύων και της μηχανικής μάθησης. Αυτό είναι και το πρώτο σημείο που διαπιστώνεται η σύγκλιση των δύο επιστημών (Russell & Norvig, 2005).

Η τεχνική της εξόρυξης δεδομένων είναι άρρηκτα συνδεδεμένη με το πεδίο των big data, αφού όπως αναφέρθηκε ανωτέρω συνιστά τη διαδικασία εξόρυξης χρήσιμων πληροφοριών από δεδομένα μεγάλης κλίμακας (Xu et al, 2017). Ωστόσο, η επιστήμη της τεχνητής νοημοσύνης έχει συντελέσει στην πραγμάτωση της εξόρυξης δεδομένων, μέσω της χρησιμοποίησης διαφόρων μεθόδων της.

Εικόνα 3.2.1. Διάφορα πεδία τεχνητής νοημοσύνης

[7] Τα πέντε στάδια της διαδικασίας ανακάλυψης γνώσης από βάσεις δεδομένων είναι οι συλλογή δεδομένων, προεπεξεργασία δεδομένων, μετασχηματισμός δεδομένων, εξόρυξη δεδομένων και τέλος διερμηνεία και αξιολόγηση αναφορών.

3.3. Τεχνητή νοημοσύνη οδηγούμενη από τα δεδομένα

Στις αρχές της δεκαετίας του 2000 παρατηρείται μία σύγκλιση τεχνητής νοημοσύνης και big data, δημιουργώντας μία νέα γενιά που σήμερα ονομάζεται data driven AI ή αλλιώς τεχνητή νοημοσύνη οδηγούμενη από τα δεδομένα. Πηγή αυτού είναι αφενός οι αλγόριθμοι μηχανικής μάθησης και αφετέρου τα big data, δηλαδή των μεγάλων δεδομένων. Η data driven AI βασίζεται κατά κόρον στα δεδομένα που δημιουργούνται από τους εκατομμύρια χρήστες της τεχνολογίας. Τα διάφορα παραγόμενα δεδομένα χρησιμοποιούνται ως είσοδοι στη μηχανή. Κάθε φορά που ένα δεδομένο (δεδομένο μάθησης) εισέρχεται στη μηχανή, αυτή παράγει μία έξοδο ως αποτέλεσμα της επεξεργασίας του εισερχόμενου δεδομένου. Η έξοδος μπορεί να είναι είτε αληθής, ενισχύοντας την εσωτερική συνάρτηση, είτε ψευδής αναγκάζοντας το δίκτυο να τροποποιήσει τη συνάρτηση ώστε να παράγει σωστές εξόδους. Συνεπώς, η εισαγωγή νέων δεδομένων τροφοδοτεί το δίκτυο, βελτιστοποιώντας τη γενική συνάρτηση. Χαρακτηριστικό παράδειγμα αποτελούν οι αλγόριθμοι που χρησιμοποιούνται από τις μεγαλύτερες εταιρείες παγκοσμίως όπως είναι η Google, το Facebook και η Apple στοχεύοντας στη δημιουργίας μηχανών φωνητικής ή οπτικής αναγνώρισης.

Κατ’ αυτό τον τρόπο λειτουργεί οποιαδήποτε μηχανή επιθυμούμε να παρέχει ομαδοποιημένα δεδομένα. Στο χώρο της αστυνομίας, η νέα γενιά τεχνητής νοημοσύνης χρησιμοποιείται σε συστήματα αναγνώρισης προσώπων. Άλλα παραδείγματα συνιστούν οι μηχανές που παίζουν παιχνίδια, η αυτόματη μετάφραση, τα αυτό οδηγούμενα οχήματα, τα στρατιωτικά ρομπότ, οι μηχανές αναγνώρισης ομιλίας και ερμηνείας, οι μηχανές Eureka, τα συστήματα τεχνητής νοημοσύνης σε τομείς όπως η ιατρική και τα καλλιτεχνικά και τέλος τα συστήματα που αποσκοπούν στην εξυπηρέτηση των ανθρώπων.

Λαμβάνοντας υπόψη τα ανωτέρω στοιχεία, γίνεται κατανοητή η σημασία των δεδομένων στην ανάπτυξη και εξέλιξη της τεχνητής νοημοσύνης, τουλάχιστον στη τωρινή της μορφή. Τα σωστά και ποικίλα δεδομένα οδηγούν στην δημιουργία συστημάτων τεχνητής νοημοσύνης. Στον αντίποδα, τα ελλιπή και μη αντιπροσωπευτικά δεδομένα προάγουν την αναξιόπιστη τεχνητή νοημοσύνη. Αυτό οφείλεται στην αυτοαναφορικότητα που την χαρακτηρίζει. Σε αντίθεση με ότι

συνέβαινε τα προηγούμενα[8] χρόνια, στόχος των επιστημόνων είναι η δημιουργία «νοήμων» μηχανών, οι οποίες εκ σχεδιασμού θα επεξεργάζονται τα ερεθίσματα που θα λαμβάνουν από το περιβάλλον και θα προσαρμόζονται σε αυτά ώστε όποτε είναι αναγκαίο να αλλάζουν τη συμπεριφορά τους. Αυτό, βέβαια, προϋποθέτει κάποια μορφή σκέψης είτε απλής είτε πιο σύνθετης.

3.4. Παράδειγμα σύγκλισης

Συνεχώς αυξανόμενη ζήτηση σημειώνουν τα chatbots από επιχειρήσεις και οργανισμούς. Πρόκειται για τα ειδικά προγράμματα που φιλοξενούνται σε μία ιστοσελίδα με σκοπό να συνομιλούν με τους χρήστες της. Χρησιμοποιούν τη τεχνητή νοημοσύνη για να παρέχουν αυτόματες απαντήσεις, σχετικές με τον εκάστοτε διάλογο που έχει αναπτυχθεί μεταξύ μηχανής και ανθρώπου. Τα chatbots έχουν αντικαταστήσει ήδη τα live chat καθότι παρέχουν πληθώρα δυνατοτήτων και πλεονεκτημάτων. Η αξιοποίηση της τεχνητής νοημοσύνης τα εξοπλίζει με την ικανότητα να εκμηδενίζουν το χρόνο αναμονής, ανταποκρινόμενα ταυτόχρονα σε πολλές αιτήσεις. Σε αντίθεση με τους ανθρώπους τα chatbots παραμένουν φιλικά ακόμη και προς τους πιο θυμωμένους ή επιθετικούς πελάτες, διατηρώντας την υπομονή και την ψυχραιμία που υπό τις ίδιες καταστάσεις ένας άνθρωπος ίσως αδυνατούσε. Τέλος, δύναται να αυξήσουν τις πωλήσεις αναβαθμίζοντας τη στρατηγική μάρκετινγκ της επιχείρησης. Σε αυτό συμβάλλει η ικανότητά τους να παρακολουθούν τα πρότυπα αγοράς, λαμβάνοντας ερεθίσματα από το περιβάλλον και δημιουργώντας κατ' επέκταση εξατομικευμένα διαφημιστικά μηνύματα για τους χρήστες.

Το ερώτημα είναι πως λειτουργούν. Τα chatbots διαθέτουν τεχνολογία εκμάθησης, δηλαδή κάποιο είδος μηχανικής μάθησης που τα επιτρέπει να θυμούνται παλαιότερες συνομιλίες και να μαθαίνουν από καινούργιες. Έτσι, δημιουργούν μία βάση δεδομένων που τους επιτρέπει να απαντούν σε πολλές και διαφορετικές ερωτήσεις. Οι Microsoft και Facebook συνέβαλαν στη δημιουργία τέτοιων

[8] Παλαιότερα, μία μηχανή σχεδιαζόταν για να ακολουθήσει ένα συγκεκριμένο πρότυπο λειτουργίας που καθοριζόταν από το δημιουργό αυτής.

προγραμμάτων, προσφέροντας πληθώρα εργαλείων. Μάλιστα, μέσα σε πέντε μήνες δημιουργήθηκαν κατ'ελάχιστο 30.000 chatbots για το Messenger του Facebook. Δεν είναι τυχαία άλλωστε η τοποθέτηση των Satya Nadella και David Marcus αναφορικά με τα chatbots ως μία σημαντική διεπαφή ανθρώπου και μηχανής.

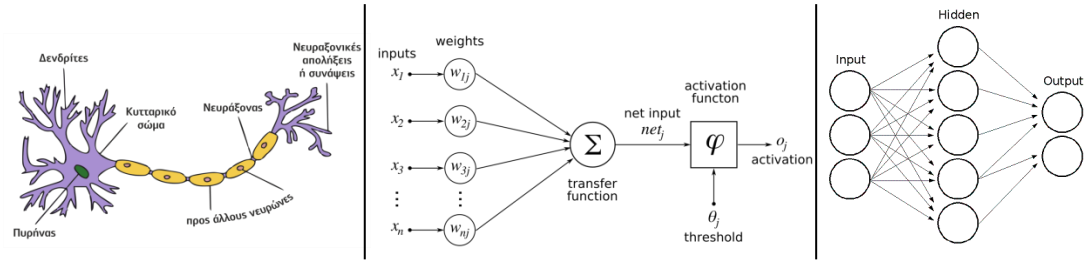
Ωστόσο, η τεχνολογία συνοδεύεται και από αρνητικές στιγμές. Μία από αυτές είναι η Tay, ένα chatbot που δημιούργησε η Microsoft με σκοπό την αλληλεπίδραση με τους χρήστες του Twitter. Η Tay, όπως και κάθε παράδειγμα της κατηγορίας της, δεχόταν ως δεδομένα της διάφορες συζητήσεις με τους υπόλοιπους χρήστες και μάθαινε από αυτές. Σύντομα, δέχθηκε επίθεση από χρήστες με ρατσιστική συμπεριφορά που την τροφοδότησαν με λάθος πληροφορίες ρατσιστικού και ναζιστικού περιεχομένου με αποτέλεσμα την υιοθέτηση αυτής της συμπεριφοράς και από την ίδια και τη δημοσίευση ανάλογων σχολίων. Όπως ήταν αναμενόμενο, η εταιρία προχώρησε στην καταστροφή της.

3.5. Νευρωνικά δίκτυα

Σε προηγούμενο κεφάλαιο έγινε λόγος για «αντιγραφή του ανθρώπινου εγκεφάλου»,δηλαδή για αντιγραφή του τρόπου με τον οποίο λειτουργεί ο ανθρώπινος εγκέφαλος. Κάτι τέτοιο συνιστά ιδιαίτερα δύσκολη υπόθεση καθότι ο εγκέφαλος είναι εξαιρετικά περίπλοκος και πολύπλοκος. Ωστόσο, τα επιτεύγματα της νευρολογικής επιστήμης έχουν συμβάλλει κατά τι στην ανάπτυξη της τεχνητής νοημοσύνης. Μετά το Β' Παγκόσμιο Πόλεμο, πραγματοποιήθηκαν αρκετές προσπάθειες για την άνθιση της τεχνητής νοημοσύνης, με τις πρώτες από αυτές να αφορούν τη μίμηση του νευρωνικού δικτύου[9]. Επομένως, οι επιστήμονες που μελέτησαν τη δομή και τη λειτουργία των ανθρώπινων νευρώνων, διαπίστωσαν πως αποτελούνται από πολλές εισόδους που ονόμασαν δενδρίτες, τον άξονα και τις απολήξεις δηλαδή τις εξόδους. Ακολούθως, οι επιστήμονες της τεχνητής νοημοσύνης θέλησαν να το προσεγγίσουν μαθηματικά, θέτοντας μία σειρά από εισόδους, οι οποίες πολλαπλασιάζονται με κάποια βάρη, αθροίζονται και αφού εισέλθουν σε μία τελική επεξεργασία εξέρχονται ενεργοποιώντας ή μη τον αντίστοιχο νευρώνα. Η προέκταση

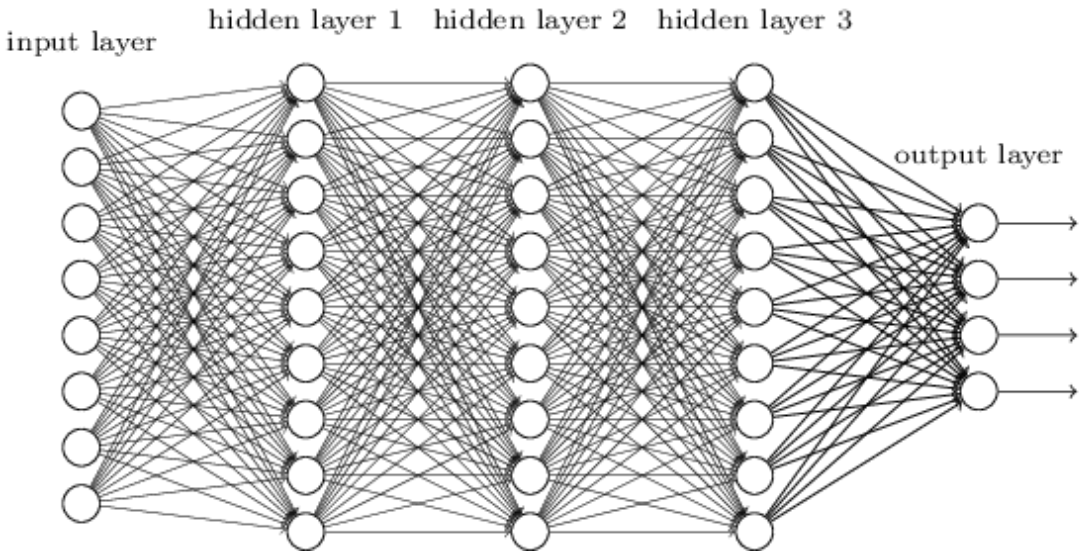
[9] Άλλωστε για αυτό το λόγο ονομάζονται για νευρωμορφικές προσπάθειες.

της μαθηματικής προσέγγισης οδηγεί στη δημιουργία δικτύων με συγκεκριμένες εισόδους και εξόδους, ώστε ένας συγκεκριμένος συνδυασμός από εισόδους να ενεργοποιεί κάποιους από τους νευρώνες εξόδου (Russell & Norvig, 2005).



Εικόνα 3.5.1. Νευρωνικά δίκτυα Πηγή: Google

Το πρώτο μοντέλο τεχνητού νευρώνα προτάθηκε το 1943 από τους McCulloch και Pitts κατά τη προσπάθειά τους να μοντελοποιήσουν τη λειτουργία του ανθρώπινου νευρώνα, εισάγοντας τη θεώρηση των νευρωνικών δικτύων ως μηχανές. Κάποια χρόνια αργότερα, το 1958, ο Rosenblatt πρότεινε το πρώτο νευρωνικό δίκτυο βασιζόμενο στο μοντέλο των McCulloch και Pitts. Το perceptron, όπως ονομάστηκε, συνιστά την απλούστερη δυνατή μορφή ενός γραμμικού ταξινομητή. Το 1969, οι Marvin Minsky και Seymour Papert δημοσίευσαν την εργασία τους αναφορικά με τα όρια των πρώτων διατάξεων των δικτύων perceprtons καταλήγοντας στην ανάγκη ύπαρξης πολλών επιπέδων. Έτσι, οδηγηθήκαμε στη δημιουργία των λεγόμενων deep neural networks, βαθιών νευρωνικών δικτύων, δηλαδή δικτύων που αποτελούνται από πληθώρα επιπέδων.



Εικόνα 3.5.2. Βαθύ νευρωνικό δίκτυο Πηγή: https://el.tipsandtrics.com/what-are-neural-networks-767559

Τα νευρωνικά δίκτυα που χρησιμοποιούνται σήμερα αποτελούνται από χιλιάδες τέτοια επίπεδα, με εκατομμύρια εισόδους και χιλιάδες εξόδους. Ωστόσο, παρά την εφεύρεση τους, εκείνη την εποχή υπήρχαν δύο σημαντικά προβλήματα, τροχοπέδη για την ανάπτυξη αυτής της τεχνολογίας. Το πρώτο ήταν η έλλειψη τεχνικών υποδομών, ικανών να τα χειριστούν και το δεύτερο η περιπλοκότητά τους. Το 1986 πραγματοποιήθηκε μία προσπάθεια από τους Hindon et al., ωστόσο χωρίς ιδιαίτερα αποτελέσματα. Η σημαντική πρόοδος σημειώθηκε από το 2012 κι έπειτα.

Αυτό που έχει ιδιαίτερη σημασία για τα βαθιά νευρωνικά δίκτυα είναι αλληλοσυσχέτισή τους με τα δεδομένα . Τα δίκτυα βασίζονται στην ύπαρξη πολλών δεδομένων, τα οποία δέχονται ως είσοδο. Τα δεδομένα είναι προ επεξεργασμένα και ταυτοποιημένα. Κατ' αυτό τον τρόπο λειτουργούν οι μεγάλες διαδικτυακές εταιρίες παγκοσμίως. Για κάθε χρήστη του διαδικτύου υπάρχει ένα τεράστιο νευρωνικό δίκτυο, που μελετά τα ενδιαφέροντά του. Ως εισόδους δέχεται τα διάφορα είδη διαφημίσεων και ανάλογα με τα ενδιαφέροντα του κάθε χρήστη ορίζει το πρόσωπο στο οποίο θα αντιστοιχίσει τη κάθε διαφήμιση. Συνεπώς είναι εύκολο να καταλάβουμε τη σημασία που έχει η υιοθέτηση και χρησιμοποίηση τέτοιων τεχνολογιών από τις μεγαλύτερες διαδικτυακές εταιρίες παγκοσμίως. Τα νευρωνικά δίκτυα συγκαταλέγονται στις πιο κερδοφόρες «εφαρμογές» και αυτό διότι, συνδράμουν στην εισροή εσόδων της επιχείρησης που τα χρησιμοποιεί

αποφασίζοντας μεταξύ άλλων, ποιες διαφημίσεις είναι κατάλληλες για ποιους χρήστες, τι υλικό από αυτό που βρίσκεται στο διαδίκτυο μπορεί να μας ενδιαφέρει, ποιες αναρτήσεις φίλων θα δούμε στο timeline του facebook και πολλά ακόμη με μοναδικό στόχο την αύξηση των εσόδων.

Εντούτοις, για κάποιες εφαρμογές τα δεδομένα δεν είναι απαραίτητα. Χαρακτηριστικό παράδειγμα αποτελεί το AlphaGo Zero, μία εφαρμογή που σχεδιάστηκε και αναπτύχθηκε με σκοπό να κερδίσει τον άνθρωπο στο αντίστοιχο παιχνίδι. Το AlphaGo Zero είναι μετεξέλιξη του AlphaGo της πρώτης εφαρμογής που νίκησε τον άνθρωπο στο Go, ένα ασιατικό παιχνίδι. Πρόκειται για ένα επιτραπέζιο παιχνίδι στρατηγικής, όπου οι δύο παίκτες τοποθετούν εναλλάξ άσπρες και μαύρες πέτρες αντίστοιχα στο ταμπλό, περικλείοντας μία περιοχή και προσπαθώντας να προστατέψουν τις πέτρες τους κυκλώνοντας αυτές του αντιπάλου. Η πρώτη έκδοση, λοιπόν, της εφαρμογής χρησιμοποιούσε δεδομένα. Συγκεκριμένα, της δίναμε ως εισόδους ήδη παιγμένα παραδείγματα, την εκπαιδεύαμε και στη συνέχεια τη βάζαμε να παίξει. Αντίθετα, για το AlphaGo Zero χρησιμοποιήθηκε μία άλλη λογική. Σκεπτόμενοι, λοιπόν, την απλότητα των κανόνων του παιχνιδιού οι δημιουργοί αποφάσισαν να μην αξιοποιήσουν τα δεδομένα, αλλά να θέσουν δύο τέτοια συστήματα αντιμέτωπα. Έτσι, το σύστημα θα εκπαιδευόταν από τον εαυτό του. Το αποτέλεσμα της όλης διαδικασίας ήταν η δημιουργία ενός ισχυρότερου συστήματος που αποδείχθηκε και πάλι καλύτερο από τον πρωταθλητή του εν λόγω παιχνιδιού.

4. Ζητήματα Ασφάλειας Και Κυβερνοέγκλημα

Στο παρόν κεφάλαιο θα παρουσιαστούν τα ζητήματα ασφαλείας που απασχολούν την επιστημονική κοινότητα ανά τον κόσμο, καθώς επίσης θα αναπτυχθούν και οι διάφορες μορφές του κυβερνοεγκλήματος.

Προτού ξεκινήσει η ανάλυση των κυβερνοεγκλημάτων αξίζει να διασαφηνιστεί ότι οι όροι κυβερνοέγκλημα και ηλεκτρονικό έγκλημα δεν είναι ταυτόσημοι. Το ηλεκτρονικό έγκλημα δύναται να πάρει δύο μορφές ανάλογα με τον τρόπο τέλεσής του. Ως ηλεκτρονικό έγκλημα (computer crime) νοείται οποιοδήποτε τελείται με τη χρήση ηλεκτρονικού υπολογιστή, αντίθετα ως κυβερνοέγκλημα (cyber crime) χαρακτηρίζεται αυτό που τελέσθηκε μέσω του διαδικτύου. Εντούτοις, δεν είναι δυνατός ο πλήρης διαχωρισμός, καθώς η έννοια του κυβερνοεγκλήματος εσωκλείει αυτή του ηλεκτρονικού εγκλήματος. Επομένως, δε νοείται κυβερνοέγκλημα δίχως τη τέλεση ηλεκτρονικού εγκλήματος, όμως το αντίθετο μπορεί να συμβεί. Παρά ταύτα δεν έχει στοιχειοθετηθεί κάποιος σαφής ορισμός που να διευκρινίζει τα σημεία στα οποία οι δύο ορισμοί διαφέρουν. Ωστόσο, υπάρχει μία γενική διάκριση σε ότι αφορά τα εγκλήματα που σχετίζονται με το διαδίκτυο. Γι αυτό στη πρώτη κατηγορία, *προηγμένο έγκλημα στο κυβερνοχώρο ή έγκλημα υψηλής τεχνολογίας συγκαταλέγονται οι εξελιγμένες επιθέσεις κατά υλικού ή λογισμικού ηλεκτρονικών υπολογιστών*, ενώ στη *δεύτερη cyber-enabled εγκλήματος κατατάσσονται τα παραδοσιακά εγκλήματα που έχουν πάρει νέα τροπή με την έλευση του διαδικτύου*, όπως είναι τα εγκλήματα κατά των παιδιών, τα οικονομικά εγκλήματα και η τρομοκρατία. Στη παρούσα εργασία, θα ασχοληθούμε περισσότερο με την έννοια του κυβερνοεγκλήματος, καθότι αυτό σχετίζεται περισσότερο με τα big data και με την τεχνητή νοημοσύνη. Οι κυριότερες και πιο συχνές μορφές ηλεκτρονικών εγκλημάτων συνοψίζονται στα: κακόβουλες εισβολές σε δίκτυα, ηλεκτρονικό

ψάρεμα, διασπορά κακόβουλου λογισμικού, ανεπιθύμητη αλληλογραφία, πειρατεία ονομάτων χώρου, κυβερνοεκφοβισμός και επιθέσεις άρνησης εξυπηρέτησης.

Η εταιρία PwC διεξήγαγε έρευνα για το οικονομικό έγκλημα και την απάτη το 2018 με τίτλο «2018 Global Economic Crime and Fraud Survey», στην οποία συμμετείχε μεταξύ άλλων χωρών και η Ελλάδα. Σε αυτή επισημαίνεται η αυξημένη πιθανότητα, η τεχνολογία να αποτελέσει τη πιο επιβλαβή μορφή απάτης κατά τη διάρκεια των επόμενων δύο ετών. Μάλιστα, οι δύο πιο συχνές μορφές επιθέσεων που σημειώθηκαν είναι το phishing και το malware με ποσοστά 44% και 41% αντίστοιχα. Ωστόσο, αξίζει να σημειωθεί πως η τεχνολογία πέρα από τους φόβους και τα προβλήματα που γεννά μπορεί να αποτελέσει τροχοπέδη για τους ίδιους της τους κινδύνους, μέσω των καινοτόμων τεχνολογιών όπως τα predictive analytics και η τεχνητή νοημοσύνη, καθώς η σωστή χρήση τους μπορεί να επιφέρει εξαιρετικά χρήσιμα αποτελέσματα.

4.1. Μορφές κυβερνοεγκλημάτων

Το ηλεκτρονικό έγκλημα δύναται να πάρει διάφορες μορφές επιθέσεων, που είτε αφορούν κοινά εγκλήματα που μεταφέρονται στο χώρο του Διαδικτύου είτε την εμφάνιση νέων μορφών εγκλημάτων που διαπράττονται εξ ολοκλήρου στο Διαδίκτυο. Οι κυριότερες από αυτές είναι οι απάτες μέσω Διαδικτύου, το hacking (και cracking), η παιδική πορνογραφία, η διασπορά κακόβουλου λογισμικού, η τροποποίηση και κλοπή δεδομένων και πολλά ακόμη. Παρακάτω αναλύονται κάποιες από τις ανωτέρω μορφές κυβερνοεγκλήματος.

4.1.1. Απάτες μέσω διαδικτύου

Σε αυτή τη κατηγορία ενδέχεται να παρουσιαστούν ποικίλοι τρόποι απάτης, από τις κοινές απάτες που συναντά κάποιος στη καθημερινότητα μέχρι νέες που δημιουργήθηκαν και αναπτύχθηκαν στο διαδικτυακό χώρο. Έτσι, για παράδειγμα, ο χρήστη θα μπορούσε να καταστεί θύμα οικονομικής απάτης, όπως η γνωστή πλέον σε

όλους Νιγηριανή απάτη, παραπλάνησης, κυρίως μέσω ψευδών ειδήσεων, απάτης μέσω διαγωνισμών που τελούνται στα μέσα κοινωνικής δικτύωσης αλλά και οποιασδήποτε άλλης μορφής. Σε ότι αφορά την Ελλάδα, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, μόνο για το έτος 2017 κλήθηκε να αντιμετωπίσει 3.120 νέες υποθέσεις. Οι 1.093 από αυτές αφορούσαν οικονομικές απάτες και νομιμοποίηση εσόδων, οι 547 περιπτώσεις απειλών, οι 347 προαναγγελίες αυτοκτονίας και οι λοιπές 164 κρούσματα παιδικής πορνογραφίας και άλλων εγκλημάτων κατά της γενετήσιας ελευθερίας, σύμφωνα με το αντίστοιχο δελτίο τύπου που αυτή εξέδωσε, μάλιστα κατά τον κ. Χαλκιά προϊστάμενο της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδος, η συχνότερη μορφή επίθεσης που σημειώνεται είναι το λεγόμενο man in the middle attack, σύμφωνα με την οποία στη συνομιλία δύο επικοινωνούντων παρεμβαίνει ένας τρίτος. Αυτός, ακολούθως παρουσιάζεται στο ένα μέλος της επικοινωνίας ως το άλλο και αντιστρόφως. Αξιοσημείωτο είναι το γεγονός ότι μόνο κατά το έτος 2017 κινδύνευσαν να χαθούν 3 εκατομμύρια ευρώ μέσω αυτής της απάτης. Άξιες αναφοράς είναι και οι εκτιμήσεις των Ηνωμένων Εθνών για το 2016, σύμφωνα με τις οποίες το 80% του κυβενροεγκλήματος προερχόταν από οργανωμένες εγκληματικές συμμορίες, που συγκαταλεγόταν στις μεγαλύτερες παράνομες οικονομίες στο κόσμο με τζίρο που έφτανε τα 445 δισεκατομμύρια δολάρια, ξεπερνώντας το ΑΕΠ 160 χωρών. Όπως είναι αναμενόμενο, στις μέρες μας τα διάφορα είδη απάτης στοχεύουν κυρίως στην οικονομική εξαπάτηση των θυμάτων τους, προσπαθώντας να τους αποσπάσουν οποιοδήποτε χρηματικό ποσό.

4.1.2.Παράνομη πρόσβαση σε σύστημα – Hacking

Πρόκειται ίσως για το πιο γνωστό είδος επίθεσης στο ευρύ κοινό, την παράνομη πρόσβαση σε ένα πληροφοριακό σύστημα όπως έχει συνηθίσει να αποκαλείται. Στην ιστορία της πληροφορικής το hacking αποδίδεται σε μικρά υπολογιστικά προγράμματα που ονομαζόταν hacks, ως εκ τούτου οι προγραμματιστές που επιδιδόταν σε αυτά ονομάστηκαν hackers. Ωστόσο στις ημέρες μας ο όρος hacker ηχεί σε ένα ιδιαίτερα έξυπνο άνθρωπο και πολύ καλό γνώστη των ηλεκτρονικών υπολογιστών που αποσκοπεί στη τέλεση παράνομων ενεργειών προς όφελος του

ιδίου ή άλλου προσώπου. Ο τρόπος με τον οποίο θα επιλέξει ο κάθε επιτιθέμενος να εξαπολύσει την επίθεσή του ποικίλει ανάλογα με το τι θέλει να προσβάλει. Έτσι, μπορεί να χρησιμοποιηθεί πληθώρα κακόβουλων λογισμικών όπως λόγου χάρη, ιοί, σκουλήκια, δούρειοι ίπποι, rootkits κ.ά., καθώς και χειροκίνητες επιθέσεις όπως SQL injections, cross side scripting, denial και distributed of service κ.ά.. Με τη τελευταία να αποτελεί τη πιο συνηθισμένη μέθοδο.

4.2. Επιθέσεις άρνησης εξυπηρέτησης – (Distributed) Denial of Service

Πρόκειται για κάποιες από τις πιο συχνές μορφές επιθέσεων που σημειώνονται τα τελευταία χρόνια παγκοσμίως. Συχνά αναφέρονται ως DDoS και DoS επιθέσεις, ακρωνύμια των φράσεων “Distributed Denial of Service” και “Denial of Service” που στα ελληνικά μεταφράζονται ως “Κατανεμημένη Επίθεση Άρνησης Εξυπηρέτησης” και “Επιθέσεις Άρνησης Εξυπηρέτησης”. Στόχος τους είναι η κατάρρευση ενός συστήματος. Πώς επιτυγχάνεται όμως μία τέτοια επίθεση; Συνήθως οι επιθέσεις DoS προσπαθούν να εκμεταλλευτούν είτε αδυναμίες του πρωτοκόλλου TCP/IP, είτε του IPv4, είτε προσπαθούν να εξαντλήσουν πόρους του συστήματος. Στη πρώτη της μορφή η εν λόγω επίθεση μετατρέπει κάποια από τα χαρακτηριστικά του πρωτοκόλλου TCP/IP σε αδυναμίες, τις οποίες εν συνεχεία και εκμεταλλεύεται. Κατά τη διάρκεια μίας επικοινωνίας, οι θύρες των υπολογιστών παραμένουν για ένα χρονικό διάστημα ανοιχτές μέχρι να δεχθούν την επόμενη απόκριση από το σύστημα. Τότε ο επιτιθέμενος βρίσκει έφορο έδαφος για να εξαπολύσει την επίθεσή του μέσω αποστολής πακέτων σε μεγάλο ρυθμό με αποτέλεσμα ο υπολογιστής-θύμα να αδυνατεί να απαντήσει στα μηνύματα που λαμβάνει και ως εκ τούτου να τεθεί εκτός λειτουργίας.

4.3. Ζητήματα ασφαλείας

Ένα από τα μεγαλύτερα ζητήματα που προσπαθεί να λύσει ο επιστημονικός κύκλος της πληροφορικής είναι αυτός της ασφάλειας. Στο σημείο αυτό αξίζει να σημειωθεί ότι η αναφορά στην ασφάλεια πληροφοριακών συστημάτων ουδεμία σχέση έχει με τη δημιουργία άτρωτων συστημάτων, καθώς κάτι τέτοιο όχι μόνο είναι δύσκολο, αλλά φαντάζει ουτοπικό. Στον αντίποδα, ο τομέας της ασφάλειας συμβάλλει στην επιτυχία της κάθε εταιρίας ή οργανισμού, μέσω της δημιουργίας ασφαλών δικτύων και συστημάτων. Ο τομέας της ασφάλειας συνιστά ένα από τα δυσκολότερα εγχειρήματα των ανθρώπων της πληροφορικής, αφού αποτελεί κράμα πολλών ενεργειών διαφόρων ανθρώπων από τον αναλυτή μέχρι τον προγραμματιστή ενός πληροφοριακού συστήματος. Έτσι, αυτό που στην πραγματικότητα προσπαθεί να πετύχει ένας ειδικός ασφαλείας είναι να προφυλάξει όσο το δυνατό περισσότερο το σύστημα από ενδεχόμενες επιθέσεις, επιδιδόμενος σε μία σειρά ελέγχων και υπολογισμών που θα προσδώσουν το επιθυμητό αποτέλεσμα. Φυσικά, η εμφάνιση ολοένα και περισσότερων τεχνολογιών συνδράμει στην εκθετική διεύρυνση του φάσματος πιθανόν επιθέσεων. Περιπτώσεις στις οποίες το θέμα της ασφάλειας δεν περιορίζεται σε αυτή των πληροφοριακών συστημάτων, αντιθέτως αφορά την ασφάλεια κρατών, πολιτών ακόμα και πολιτισμού. Αποδεικτικό αυτού είναι η κοινή έκθεση είκοσι έξι ειδικών σε θέματα ασφαλείας σχετικά με την ανάπτυξη και ποσό μάλλον χρήση νέων τεχνολογιών.

Οι ειδικοί εμφανίζονται ανήσυχοι για τη μελλοντική χρήση και αξιοποίηση των νέων τεχνολογιών και ιδιαίτερα της τεχνητής νοημοσύνης, σε περίπτωση κατάχρησής της από εγκληματίες και αυταρχικά κράτη. Προειδοποιούν για αύξηση τους κυβερνοεγκλήματος μέσω τεχνητής νοημοσύνης, κατευθυνόμενης προπαγάνδας (όπως fake news, bots κ.ά), χειραγώγησης αυτόνομων οχημάτων και drones και εισβολών σε δίκτυα υποδομών. Έτσι, αναμένεται να αυξηθούν συν της άλλης οι παραβιάσεις ιδιωτικότητας που οδηγούν σε παραβίαση προσωπικών δεδομένων. Η εκατοντασέλιδη έκθεση καταλήγει, με την πρόβλεψη για νέες πιο ισχυρές επιθέσεις, που θα δυσκολέψουν περισσότερο το έργο των ειδικών ασφαλείας, όπως αυτοματοποιημένες επιθέσεις, scam μηνύματα με φαινομενικά ορθές πληροφορίες, fake news, λογισμικά αυτόματης ομιλίας κ.ά.

4.4. Σκοτεινό διαδίκτυο

Συχνά γίνεται λόγος για μία άλλη σκοτεινή πλευρά του διαδικτύου που προκαλεί φόβο και ανησυχία στους ανθρώπους. Τι είναι όμως το σκοτεινό διαδίκτυο και τι πραγματικά συμβαίνει σε αυτό; Για την καλύτερη κατανόηση των εννοιών είναι σύνηθες η παρομοίωση του ιστού με ένα παγόβουνο, η επιφάνεια του οποίου αποτελεί τον επιφανειακό ιστό (surface web), αυτό που οι περισσότεροι αναγνωρίζουν ως διαδίκτυο. Κάτω από την επιφάνεια του νερού συναντά κανείς το βαθύ ιστό (deep web) και στη συνέχεια το σκοτεινό διαδίκτυο (dark web). Αξιοσημείωτο είναι ότι το surface web αποτελεί μόλις το 4%, ενώ τα deep web και dark web το 90% και 6% αντίστοιχα του συνόλου. Στο surface web πραγματοποιούνται οι καθημερινές δραστηριότητες όπως αναζήτηση ειδήσεων, παρακολούθηση εικόνων και βίντεο, έλεγχος μέσων κοινωνικής δικτύωσης και γενικότερα ότι μπορεί να συμπεριλαμβάνεται στην καθημερινότητα ενός μέσου χρήστη. Αντίθετα, στο deep web περιλαμβάνονται ιστοσελίδες που δεν είναι άμεσα προσβάσιμες από τις συμβατικές μηχανές αναζήτησης (βλ. Google, Bing, Yahoo!, Quora κ.ά.) και ο λόγος έγκειται στη μη κατάταξη του περιεχομένου των ιστοσελίδων από τους crawlers των μηχανών αναζήτησης. Κάθε μηχανή αναζήτησης χρησιμοποιεί ειδικούς αλγορίθμους, που ονομάζονται crawlers, δηλαδή αράχνες. Οι crawlers, ευρετηριάζουν τους διάφορους ιστοτόπους βάσει του περιεχομένου τους, με τη βοήθεια των web crawlers που σαρώνουν το διαδίκτυο. Όταν ο χρήστης πραγματοποιεί μία αναζήτηση πληκτρολογώντας μία λέξη-κλειδί ή μία φράση, η μηχανή αναζήτησης προσπαθεί να βρει το αντίστοιχο έγγραφο ή αρχείο. Για την διαδικασία αυτή χρησιμοποιούνται οι λεγόμενοι crawlers, ένα ειδικό λογισμικό που λαμβάνει το περιεχόμενο των ιστοτόπων και δημιουργεί λέξεις-κλειδιά, επιτρέποντας στους χρήστες να βρίσκουν αυτό που αναζητούν. Συχνά υπάρχουν κρυφοί πόροι που δεν μπορούν να εντοπιστούν, όπως το δυναμικό περιεχόμενο, το private και contextual web, το περιεχόμενο περιορισμένης πρόσβασης, το μη συνδεδεμένο περιεχόμενο, το κρυπτογραφημένο περιεχόμενο, το Non-HTML/text content και γενικώς ότι δεν ακολουθεί το HTTP/HTTPS πρότυπο. Βέβαια, αυτό δε συνεπάγεται την απόλυτη επικινδυνότητα του deep web, αφού ένα μεγάλο ποσοστό ανθρώπων έχει επωφεληθεί την ανωνυμία του συγκεκριμένου χώρου. Για παράδειγμα, κάτοικοι χωρών που κυβερνώνται από δικτατορικά ή καταπιεστικά καθεστώτα

εκμεταλλεύονται το deep web ως ένα «σχετικά ασφαλή τρόπο» για ενημέρωση και οποιοδήποτε άλλη δραστηριότητα. Επίσης, το deep web είναι μέρος συνάντησης υψηλόβαθμων στελεχών, κυβερνητικών υπαλλήλων, βουλευτών, στρατιωτικών για καταγγελία αδικημάτων και διαφθοράς στους αντίστοιχους χώρους. Επομένως, πρόκειται για μία καλή πηγή πληροφόρησης αποκλειστικών ειδήσεων δημοσιογράφων. Το deep web είναι θεωρητικά ασφαλές, αυτό σημαίνει ότι μέσω της περιήγησης σε αυτό δεν υπάρχει φόβος εξαπόλυσης επίθεσης ή μόλυνσης με ιούς. Σε αυτό περιέχονται ιδιαίτερα χρήσιμες πληροφορίες, όπως τα στοιχεία κρατικών εγγράφων (αστυνομικής ταυτότητας, διαβατηρίου, διπλώματος οδήγησης), το ΑΦΜ και το ΑΜΚΑ, οι φορολογικές δηλώσεις και ενημερώτητες, τα πιστοποιητικά γεννήσεως και οικογενειακής κατάστασης, η κινητή και ακίνητη περιουσία, τα συστήματα intranet σχολείων και πανεπιστημίων, οι ηλεκτρονικές βάσεις δεδομένων, ο προσωπικός λογαριασμός πρόσβασης σε μέσα κοινωνικής δικτύωσης, ηλεκτρονικό ταχυδρομείο, τραπεζικές υπηρεσίες, κ.λ.π. Ωστόσο, οι δραστηριότητες στο deep web δεν είναι απαραιτήτως παράνομες και οι πληροφορίες που βρίσκονται σε αυτό δεν είναι προς δημόσια κατανάλωση, γεγονός που αποδεικνύεται από τις προσπάθειες των ιδιοκτητών ώστε να τις καταστήσουν απρόσιτες.

Το deep web εκτός από όλες τις βάσεις δεδομένων των χρηστών, τις σελίδες webmail και web forum που απαιτούν εγγραφή χρήστη και τις ιστοσελίδες ασφαλών πληρωμών εμπεριέχει και το dark web ή αλλιώς σκοτεινό διαδίκτυο. Αυτό σημαίνει ότι για κάθε δράση που πραγματοποιείται στο surface web υπάρχει μια αντίδραση στο deep web που δεν είναι ορατή στο χρήστη εκτός κι αν αυτός διαθέτει τα απαραίτητα διαπιστευτήρια τα οποία σε συνδυασμό με τη χρήση κατάλληλου λογισμικού ανωνυμίας που συγκαλύπτει την IP address και την τεχνογνωσία μπορεί να προσπελαστεί. Σύμφωνα με τα στατιστικά στοιχεία του 2016 στο deep web περιέχονται 7500 terabytes πληροφοριών, ενώ στο surface web μόλις 19 terabytes πληροφοριών.

Το dark web συνιστά ένα μικρό υποσύνολο του deep web που περιέχει δίκτυα η πρόσβαση στα οποία απαιτεί την εφαρμογή ειδικού λογισμικού. Φυσικά, το εγχείρημα είναι κατά τι δυσκολότερο, αφού απαιτείται η γνώση και κατανόηση της δομής του ιστού. Βασική προϋπόθεση της περιήγησης στο dark web είναι η διατήρηση της ανωνυμίας του χρήστη. Συνήθως, πρωταρχικό μέλημα των

ενδιαφερομένων είναι η εγκατάσταση μίας εικονικής μηχανής, ώστε σε περίπτωση μόλυνσης από κάποιον ιό, να μείνει ανεπηρέαστος ο κεντρικός υπολογιστής. Το δεύτερο βήμα είναι η χρήση κάποιου προγράμματος VPN για την ενίσχυση της ασφάλειας και φυσικά η εγκατάσταση του προγράμματος Tor ή οποιουδήποτε άλλου λογισμικού ανωνυμίας. Αφού καταστεί δυνατή η είσοδος στο dark web ο περιηγητής δύναται να επισκεφτεί τόσο ασφαλείς σελίδες είτε για ανακάλυψη γνώσεων, είτε για αγορά αντικειμένων που στο surface web είναι απαγορευμένα εξαιτίας κάποιας μορφής λογοκρισίας, όσο και παράνομο υλικό, λόγου χάριν ψεύτικα διαβατήρια, κλεμμένους λογαριασμούς, διακίνηση ναρκωτικών ουσιών και φαρμάκων, εμπόριο όπλων και λευκής σαρκός, επί πληρωμής δολοφόνους, διακίνηση πορνογραφικού υλικού, αγορά πλαστών εγγράφων κ.λ.π. Οι διαδικτυακές αγορές στο σκοτεινό διαδίκτυο μοιάζουν με το Amazon ή το eBay. Πρόκειται για ηλεκτρονικά περιβάλλοντα που παρουσιάζουν τα προϊόντα ή τις υπηρεσίες τους, αναγράφοντας τις τιμές αυτών, ενώ παράσχουν πληροφορίες σχετικά με βαθμολογίες και αξιολογήσεις των αγαθών και υπηρεσιών. Γιατί όμως να υφίσταται αυτό στο dark web και όχι σε κάποιο άλλο επίπεδο; Η απάντηση βρίσκεται στο πολυεπίπεδο σύστημα κρυπτογράφησής του, εξαιτίας του οποίου παραμένουν άγνωστες τόσο οι τοποθεσίες όσο και οι ταυτότητες των χρηστών, με τους μεν να εκμεταλλεύονται την ανωνυμία για να αποφύγουν τη λογοκρισία και τους δε για να προχωρήσουν σε εγκληματικές ενέργειες, δυσχεραίνοντας το έργο των διωκτικών αρχών.

5. Τεχνητή Νοημοσύνη Και Κυβερνοέγκλημα

Στο παρόν κεφάλαιο θα αναλυθεί η σχέση της τεχνητής νοημοσύνης με τα ηλεκτρονικά εγκλήματα. Αναφέροντας αφενός τη συνδρομή της στην αύξηση αυτών των φαινομένων και αφετέρου στην καταπολέμησή τους.

Ο τομέας της τεχνητής νοημοσύνης έχει δείξει πολλά σημάδια ανάκαμψης με τη πάροδο των τελευταίων ετών, συνιστώντας ένα δυνατό χαρτί στα χέρια του εκάστοτε κατόχου του. Όπως κάθε τεχνολογία ενδέχεται να επιφέρει θετικά ή αρνητικά αποτελέσματα ανάλογα με τον τρόπο χρήσης της. Αναφορικά πάντα με το τομέα της εγκληματολογίας και δει των ηλεκτρονικών επιθέσεων, ο διττός χαρακτήρας της τεχνητής νοημοσύνης είναι εντονότερος. Αυτό οφείλεται αφενός στη χρησιμοποίησή της για τον εντοπισμό του κυβερνοεγκλήματος με απώτερο στόχο τη μείωση αυτού και αφετέρου στις ολοένα και συχνότερες περιπτώσεις αρωγής της στη τέλεση διαφόρων μεθόδων επιθέσεων.

Αξιοσημείωτη είναι έκθεση είκοσι έξι ειδικών[10] στα θέματα ασφαλείας, με τίτλο «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation» σχετικά με τους κινδύνους που ενέχουν οι νέες τεχνολογίες. Οι ειδικοί από όλο τον κόσμο κρούουν τον κώδωνα του κινδύνου ως επί το πλείστον για τις εφαρμογές της τεχνητής νοημοσύνης και το λανθασμένο τρόπο χρήση αυτών που πιθανό να οδηγήσει σε επισφαλή αποτελέσματα. Κατά τους ειδικούς, η τεχνητής νοημοσύνη συνιστά μία ακόμη τεχνολογία-Ιανό με διπλή χρήση, που μέσα στα επόμενα πέντε με δέκα χρόνια θα εκμεταλλεύεται κακόβουλα προς όφελος hackers, τρομοκρατών και αναρχικών κρατών και κυβερνήσεων. Τα κυριότερα ζητήματα που θέτει η εν λόγω έκθεση αφορούν, τη ραγδαία αύξηση του κυβερνοεγκλήματος με την

[10] Την έκθεση που παρουσιάστηκε το Φεβρουάριο του 2018 υπογράφουν οι Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersle,y Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, Dario Amodei.

ενίσχυση της τεχνητής νοημοσύνης, τη πρόκληση βλαβών σε ζωτικά δίκτυα μέσω της διείσδυσης σε αυτά, τη χειραγώγηση αυτόνομων οχημάτων και drones μετατρέποντάς τα σε φονικά εργαλεία και τέλος την εξάπλωση της κατευθυνόμενης προπαγάνδας είτε με τη χρήση bots και fake news είτε με οποιονδήποτε άλλο τρόπο.

5.1. Η αρωγή της τεχνητής νοημοσύνης στη τέλεση ηλεκτρονικών εγκλημάτων

Η τεχνητή νοημοσύνη συγκαταλέγεται στις «νέες τεχνολογίες» που εκμεταλλεύονται ώστε να αποτρέψουν το έγκλημα στο κυβερνοχώρο με τη χρήση αντιμέτρων ασφαλείας. Άλλωστε, σύμφωνα με τον διευθυντή της Ευρωπαϊκής Υπηρεσίας για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), Duo Helmbrecht, «η αναγνώριση των απειλών και η δυναμική τους στον κυβερνοχώρο είναι το κλειδί για την κατανόηση της έκθεσης και των κινδύνων». Επομένως, τα αποτελέσματα της όποιας μορφής έρευνας δείχνουν σημαντικά στοιχεία για την καταπολέμηση του εγκλήματος στο διαδίκτυο.

Η συνεχής ανάπτυξη της τεχνολογίας έχει οδηγήσει στην εκτεταμένη χρήση των λεγόμενων IoT συσκευών καθώς και των δικτυωμένων συστημάτων επισύροντας νέα δεδομένα στο χώρο της κυβερνοασφάλειας. Η εφαρμογή των παραδοσιακών μέτρων ασφαλείας δεν αποτελεί επαρκή λύση, αφού οι κυβερνοεγκληματίες επιστρατεύουν συνεχώς νέες μεθόδους εξαπόλυσης επιθέσεων. Στον αντίποδα, οι ομάδες αντιμετώπισης κυβερνοεγκλήματος και οι ερευνητές ασφαλείας δρουν προς την αντίθετη κατεύθυνση, καταβάλλοντας ιδιαίτερη προσπάθεια ώστε να αντιμετωπίσουν τις κακόβουλες ενέργειες και να ακολουθήσουν τις νέες τάσεις εποχής (Ganesh, 2017). Προσπάθεια στην οποία συμβάλλει τα μέγιστα η τεχνητή νοημοσύνη, εντοπίζοντας τα ίχνη των κακόβουλων χρηστών. Μέσω της ανίχνευσης ύποπτων patterns και μοτίβων, ενισχύει το έργο των ερευνητών παραχωρώντας τους χρόνο και ευκαιρία να υπακούσουν στα καινούργια δεδομένα.

Ο χώρος της κυβερνοασφάλειας έχει μετατραπεί σε πεδίο μάχης, όπου κυβερνοεγκληματίες και ομάδες αντιμετώπισης κυβερνοεγκλήματος παρατάσσουν τα όπλα τους σε ένα διαρκή πόλεμο εξουσίας ανάμεσα στο καλό και το κακό, το ηθικό

και το ανήθικο. Ένα πόλεμο στον οποίο, η τεχνητή νοημοσύνη συνιστά το ισχυρότερο όπλο των δύο αντιπάλων και συνάμα ένα πολύτιμο χαρτί που όποιος το αξιοποιήσει με τον καλύτερο τρόπο θα στεφθεί νικητής.

Όπως ειπώθηκε και σε προηγούμενο κεφάλαιο οι hackers είναι ιδιαίτερα ευφυείς και ταλαντούχοι άνθρωποι, ωστόσο η απόκρυψη των στοιχείων και κινήσεών τους οφείλεται σε μεγάλο ποσοστό και στη χρήση εξελιγμένων εργαλείων (Elazari, 2017). Εμπόδιο το οποίο καλούνται να ξεπεράσουν οι ειδικοί ασφαλείας και αντιμετώπισης κυβερνοεγκλήματος. Τα εργαλεία που στοχεύουν στην επίλυση αυτού του προβλήματος εφαρμόζουν τεχνικές μηχανικής μάθησης. Συγκεκριμένα, το είδος της μηχανικής μάθησης που χρησιμοποιείται είναι αυτό της μη εποπτευόμενης, αφού η αντιμετώπιση θεμάτων ασφαλείας συνεπάγεται την αδυναμία καθορισμού συμπεριφορών. Η εποπτευόμενη μηχανική μάθηση χαρακτηρίζεται από ύπαρξη πολλών ετικετών και γνώση του τι ακριβώς αναζητείται, αντίθετα στη μη εποπτευόμενη μηχανική μάθηση ερευνώνται συμπεριφορές που είναι πιο γενικές, όπως στη περίπτωση των hackers οι συμπεριφορές τους μπορεί να αλλάξουν, αλλά είναι συγκεκριμένες σε ένα πρωτόκολλο.

Η ενσωμάτωση αλγορίθμων μηχανικής μάθησης, μπορεί να βοηθήσει τα έξυπνα συστήματα να εξελίξουν τις δυνατότητές τους να εντοπίζουν και να αναλύουν ένα ελάττωμα ασφαλείας στο σύστημα (Elazari, 2017). Για παράδειγμα, ένα σύστημα που εσωκλείει αλγόριθμο μηχανικής μάθησης, εξετάζοντας συνεχώς μηνύματα ηλεκτρονικού «ψαρέματος», μπορεί να αναπτύξει την ικανότητα να ανιχνεύει το μήνυμα και το πειστικό ύφος ενός phisher.

Άλλοι τρόποι με τους οποίους η τεχνητή νοημοσύνη συμβάλλει στην ελαχιστοποίηση των ηλεκτρονικών εγκλημάτων είναι η παρακολούθηση των εγκληματιών στον κυβερνοχώρο, η ανάλυση των αποτελεσμάτων επίθεσης, αλλά και η άμεση αντίδραση σε μία επίθεση, δηλαδή τη στιγμή που αυτή λαμβάνει χώρα.

Τέλος, γνωρίζοντας τη σημασία άμεσης αντίδρασης στη τέλεση κυβερνοεπιθέσεων, η τεχνητή νοημοσύνη μπορεί να συμβάλλει στην αναβάθμιση των υπαρχουσών λογισμικών ανίχνευσης όχι μόνο με τον εντοπισμό των κακόβουλων λογισμικών αλλά με την ανάλυση των επιπτώσεων που θα έχει στο πληροφοριακό σύστημα.

Πλέον τα παραδοσιακά μέτρα ασφαλείας, όπως κωδικοί πρόσβασης και τείχη προστασίας δεν είναι επαρκεί, αφού οι hackers μπορούν εύκολα να βρουν την δίοδο μέσα από αυτά. Επομένως, απαιτείται η χρήση εξελιγμένων μεθόδων ικανών να εμποδίσουν την παράνομη πρόσβαση. Η μηχανική μάθηση δύναται να επιτρέψει την ανάλυση συμπεριφοράς του χρήστη αυξάνοντας το επίπεδο ασφαλείας. Συνεπώς, η τεχνητή νοημοσύνη με χρήση μηχανικής μάθησης φαντάζει ως η πολυπόθητη λύση στο πρόβλημα που ταλανίζει και λέγεται κυβερνοασφάλεια.

Το ερώτημα όμως είναι πως λειτουργεί ένα σύστημα τεχνητής νοημοσύνης και τι είναι αυτό που εν τέλει του επιτρέπει να αναγνωρίζει τις απειλές του διαδικτύου. Την απάντηση έρχεται να δώσει η γενική συλλογιστική που αφορά τα δημιουργήματα τεχνητής νοημοσύνης (Elazari, 2017). Τα σύγχρονα εργαλεία, λοιπόν, χρησιμοποιούν τεχνικές μηχανικής μάθησης προσδίδοντας τους τη δυνατότητα να μαθαίνουν από το περιβάλλον (Ganesh, 2017). Στη προκειμένη περίπτωση δέχονται ως ερεθίσματα-δεδομένα από το περιβάλλον τις επιθέσεις που δέχθηκε ένα σύστημα σε παρελθόντα χρόνο. Μελετώντας τις συνέπειες που είχαν οι επιθέσεις αυτές στο σύστημα, ένα λογισμικό τεχνητής νοημοσύνης μπορεί όχι μόνο να εντοπίσει, αλλά και να προβλέψει μία κυβερνοεπίθεση.

Αγκάθι στο χώρο της κυβερνοασφάλειας συνιστά μεταξύ άλλων ο αριθμός των ενεργών εργαζομένων παγκοσμίως. Υπολογίζεται ότι εν έτη 2018, οι εργαζόμενοι στο τομέα της κυβερνοασφάλειας εργάζονται 52 ώρες εβδομαδιαίως, χρόνος που υπερβαίνει κατά πολύ το νόμιμο ωράριο, πόσο μάλλον αν ληφθεί υπόψη η κατάσταση εργασίας, ο χώρος, η ευθύνη, οι ασταθείς απειλές. Συνθήκη που αναμένεται να αναιρέσει η εφαρμογή συστημάτων τεχνητής νοημοσύνης.

5.2. Η τεχνητή νοημοσύνη τροχοπέδη για την κυβερνοασφάλεια

Ολοένα και συχνότερα γινόμαστε παρατηρητές δυσοίωνων απόψεων αναφορικά με τη τύχη της ανθρωπότητας εξαιτίας της τεχνητής νοημοσύνης. Ειδικοί ασφαλείας, μηχανικοί, επιστήμονες, επιχειρηματίες, ευρωβουλευτές, δημιουργοί ταινιών επιστημονικής φαντασίας είναι μόνο μερικοί από αυτούς που συγκαταλέγονται στους απαισιόδοξους που ταυτίζουν την ανάπτυξη της τεχνητής

νοημοσύνης με το άνοιγμα του κουτιού της Πανδώρας, επισύροντας δεινά για την ανθρωπότητα.

Αυτό φυσικά έχει επιδράσει και στην αντίληψη των πολιτών για τα μύρια κακά που έπονται τη χρήση/εφαρμογή τεχνητής νοημοσύνης. Το τελευταίο χρονικό διάστημα τα φώτα στρέφονται ως επί το πλείστον στις νέες τεχνολογίες όπως είναι τα drones, τα όπλα που δρουν με γνώμονα τη τεχνητή νοημοσύνη , τη πρόκληση βλαβών από κακόβουλα λογισμικά και τις διάφορες μορφές προπαγάνδας (Brundage et al., 2018).

Πιστεύεται ότι η ραγδαία αυτή ανάπτυξη θα επιφέρει κινδύνους τόσο σε ατομικό επίπεδο, για παράδειγμα αύξηση της ανεργίας, όσο και σε συλλογικό, παραπληροφόρηση, χειραγώγηση κοινής γνώμης. Σφοδρή επίθεση δέχεται και ο χώρος της κυβερνοασφάλειας, με τους ειδικούς να κρούουν το κώδωνα του κινδύνου για τέλεση κυβερνοεγκλημάτων στο άμεσο μέλλον (Brundage et al., 2018). Μάλιστα το σενάριο αναφέρεται στη πιθανή εμπλοκή τόσο κυβερνήσεων όσο και αναρχικών κρατών. Με τους ειδικούς να επισημαίνουν την ανάγκη αναδιαμόρφωσης του νομικού πλαισίου παγκοσμίως ώστε να συμμορφωθεί με τις επικείμενες αλλαγές στο τεχνολογικό τομέα λόγω της ανάπτυξης τεχνητής νοημοσύνης.

Η ανωνυμία στο διαδίκτυο είναι μία ισχύουσα κατάσταση - ένα γεγονός που εξακολουθεί να διχάζει τόσο τους επιστήμονες όσο και το ευρύ κοινό. Συνάμα αποτελεί ένα στοιχείο που βοηθά τους εγκληματίες του διαδικτύου να συνεχίζουν το έργο τους. Γεγονός που δυσχεραίνει τη παρακολούθησή τους, αφού αυτή πραγματοποιείται χειρωνακτικά καθιστώντας συχνά αδύνατο το έργο τους. Συστήματα τεχνητής νοημοσύνης υποβοηθούμενα από big data και αναλυτικά στοιχεία ασφαλείας ίσως απλουστεύσουν και επιταχύνουν την όλη διαδικασία εντοπίζοντας τη πηγή προέλευσης εγκληματιών, αλλά προβλέποντας ταυτόχρονα επικείμενες επιθέσεις.

Παραταύτα, είναι ουτοπία η πεποίθηση πως μέσω ευφυών πρακτόρων μπορεί να προβλεφθεί πλήρως μία διαδικτυακή κίνηση. Πέρα από τη πρόβλεψη ιδιαίτερη σημασία κατέχει η θεραπεία του προβλήματος. Στη παρούσα περίπτωση το πρόβλημα έγκειται στις πολυάριθμες ηλεκτρονικές επιθέσεις και η θεραπεία θα μπορούσε να εντοπίζεται στην υιοθέτηση αυτοματοποιημένων αλγορίθμων έρευνας. Έτσι, οι

ομάδες υπεράσπισης κυβερνοασφάλειας λαμβάνοντας τα αποτελέσματα ερευνών μπορούν να λάβουν τις κατάλληλες αποφάσεις (Elazari, 2017).

Φυσικά, η εφαρμογή τεχνητής νοημοσύνης δεν αναφέρεται στη χρήση ρομπότ που θα δρουν προς όφελος των επιτιθεμένων. Εξεναντίας, αφορά την ενδυνάμωση - ισχυροποίηση με τεχνητή νοημοσύνη των υπαρχουσών μορφών κυβερνοεπιθέσεων, καθιστώντας αυτές αποτελεσματικότερες (Brundage et al., 2018). Αυτό μαρτυρά ότι οι υπάρχουσες μορφές επιθέσεων όπως το password cracking, δηλαδή το «σπάσιμο» κωδικού, οι επιθέσεις άρνησης εξυπηρέτησης, η υποκλοπή δεδομένων, η διασπορά κακόβουλου λογισμικού μπορούν να γίνουν αποτελεσματικότερες και πιο επικίνδυνες.

Ωστόσο, μέχρι στιγμής οι κυβερνοεπιθέσεις που λαμβάνουν χώρα τελούνται από τον άνθρωπο. Συνεπώς, είναι και αυτός που αναλαμβάνει όλα τα στάδια που απαιτούνται για την ολοκλήρωση του εκάστοτε ηλεκτρονικού εγκλήματος. Ωστόσο, ο άνθρωπος χαρακτηρίζεται από συγκεκριμένες ανάγκες και όρια. Ως εκ τούτου είναι αδύνατο να εργάζεται ασταμάτητα δίχως διάλειμμα ή ανάπαυλα για κάποιο χρονικό διάστημα. Η αυτοματοποίηση μπορεί να προσφέρει στους hackers χείρα βοηθείας, πραγματοποιώντας τις ίδιες επιθέσεις σε συντομότερο χρονικό διάστημα και με απόλυτη ακρίβεια, ακόμη και σε περιπτώσεις πολυπλοκότερων επιθέσεων.

Έως πρότινος, το μοναδικό κακόβουλο πρόγραμμα που αξιοποιούσε στοιχειώδεις ικανότητες τεχνητής νοημοσύνης ήταν οι ιοί, καθότι μπορούν να αυτοαναπαράγονται σε άλλους υπολογιστές. Συνεπώς, οι hackers στη προσπάθειά τους να εξελίξουν το ηλεκτρονικό έγκλημα, εκμεταλλεύτηκαν τις δυνατότητες των ιών, με αποτέλεσμα τη δημιουργία των λεγόμενων κατανεμημένων επιθέσεων (distributed attacks), όπως η επίθεση που σημειώθηκε τον Οκτώβριο του 2016 αποκόπτοντας την επικοινωνία με διάφορες διαδικτυακές περιοχές.

Η συμβολή της τεχνητής νοημοσύνης δε περιορίζεται στη τέλεση κυβερνοεπιθέσεων. Αντίθετα, τα συστήματα τεχνητής νοημοσύνης καθίστανται αρωγοί για το πρώιμο στάδιο της δημιουργίας και επεξεργασίας βάσεων δεδομένων, απαραίτητων για τη ταυτοποίηση πληροφοριών και στοιχείων των χρηστών. Συχνά χρησιμοποιούνται ως εργαλεία αυτόματης συλλογής πληροφοριών που ενδέχεται να προέρχονται από forum υποστήριξης, μέσα κοινωνικής δικτύωσης, αλλά και code repositories δηλαδή βάσεις που περιέχουν κωδικούς πρόσβασης. Επιπρόσθετα,

δύναται να παράσχει σημαντική βοήθεια στους hackers, για περιπτώσεις «σπάσιμου» κωδικών, λαμβάνοντας υπόψη τη γεωγραφική θέση, τα δημογραφικά στοιχεία κ.ά αμβλύνοντας το πλήθος πιθανών κωδικών. Έτσι, μειώνουν το φόρτο εργασίας των hackers επιτρέποντας τους να προβούν σε άλλες ενέργειες. Επίσης, η εφαρμογή τεχνητής νοημοσύνης δύναται να βοηθήσει σε περιπτώσεις που η επίθεση συναντήσει εμπόδιο ή αντίσταση, καθώς μπορεί να εντοπίσει νέους τρόπους επίτευξης ή ακόμη να ερευνήσει και εκμεταλλευτεί κάποια άλλη ευπάθεια του συστήματος. Ενδεχόμενο που θα προκαλέσει ανησυχία σε όσους υπερασπίζονται την ασφάλεια στο διαδίκτυο, αφού πιθανώς να καθυστερήσουν στη λήψη των απαραίτητων μέτρων ασφαλείας.

6. Μεγάλα Δεδομένα Και Κυβερνοέγκλημα

Στο παρόν κεφάλαιο αναλύεται λεπτομερώς η σχέση των μεγάλων δεδομένων με το ηλεκτρονικό έγκλημα και δη του εγκλήματος που λαμβάνει χώρα στο διαδίκτυο.

Όπως συμβαίνει στη περίπτωση της τεχνητής νοημοσύνης, τα μεγάλα δεδομένα ενδέχεται από τη μία να συνεισφέρουν στη πραγμάτωση εγκληματικών πράξεων και από την άλλη να ενισχύσουν τη προσπάθεια όσων ασχολούνται με την ασφάλεια συστημάτων και εφαρμογών στο κυβερνοχώρο έχοντας ως απόρροια την παρακώλυση ηλεκτρονικών εγκλημάτων.

6.1. Τα μεγάλα δεδομένα προς όφελος των κυβερνοεγκληματιών

Η τεχνολογία έχει γίνει κομμάτι της καθημερινής ζωής των περισσοτέρων ανθρώπων. Ο επικεφαλής της Europol, Rob Wainwright, εξέφρασε «τους προβληματισμούς σχετικά με το πώς η όλο και επεκτεινόμενη κοινότητα των κυβερνοεγκληματιών είναι σε θέση να εκμεταλλεύεται την ολοένα και μεγαλύτερη εξάρτηση των χρηστών από το διαδίκτυο και τη τεχνολογία γενικότερα». Ωστόσο, είναι ελάχιστοι όσοι γνωρίζουν τα παράγωγα της διαδικτυακής τους δραστηριότητας. Τα προγράμματα, οι εφαρμογές, οι μηχανές αναζήτησης και γενικότερα οι τεχνολογίες βρίσκονται υπό τον έλεγχο μεγάλων εταιρειών και παρέχονται προς χρήση στο ευρύ κοινό. Όμως όπως κάθε παρεχόμενη υπηρεσία έτσι κι αυτές χαρακτηρίζονται από κάποιο είδος ανταλλάγματος. Η μη καταβολή χρηματικού ποσού δε συνεπάγεται την απουσία ανταλλάγματος εκ μέρους του χρήστη. Αντιθέτως, σε τέτοιες περιπτώσεις, ο χρήστης «πληρώνει» την υπηρεσία που χρησιμοποιεί με τα δεδομένα που της παρέχει. Έτσι, η αξιοποίηση των μεγαλύτερων εφαρμογών παγκοσμίως, όπως Google, Gmail, Facebook, Instagram, Twitter, Bing

κ.ο.κ. έχει ως αντάλλαγμα την λήψη δεδομένων από τους χρήστες. Τα δεδομένα, λοιπόν, συνιστούν πολύτιμο εργαλείο στα χέρια των μεγαλύτερων κολοσσών παγκοσμίως, αξιοποιώντας τα για την εξέλιξη και ενίσχυση άλλων τεχνολογιών, μεταξύ των οποίων και η τεχνητή νοημοσύνη. Συνάμα, αποτελούν εφαλτήριο για τη πραγμάτωση εγκλημάτων στο χώρο του διαδικτύου, εξοπλίζοντας τους δράστες με χρήσιμες πληροφορίες. Οι κυβερνοεγκληματίες δύναται να αξιοποιήσουν τόσο τις πληροφορίες όσο και τις δυνατότητες που προσφέρουν τα μεγάλα δεδομένα, ώστε να ενισχύσουν τις επιθέσεις τους καθιστώντας τες επιτυχημένες σε τέτοιο βαθμό που μπορεί να είναι ιδιαίτερα δύσκολη αν όχι αδύνατη η όποια μορφή αντίδρασης. Πόσο μάλλον στη περίπτωση που τα μεγάλα δεδομένα χρησιμοποιηθούν σε συνδυασμό με τη τεχνητή νοημοσύνη (Porcedda, 2018).

6.2. Τα μεγάλα δεδομένα ενισχύουν την κυβερνοασφάλεια

Ο κλάδος των μεγάλων δεδομένων συνιστά έναν από τους πιο αναπτυσσόμενους και προσοδοφόρους, που μάλιστα αναμένεται να σημειώσει πρόοδο τα επόμενα χρόνια. Οι επιχειρήσεις παγκοσμίως έχουν υιοθετήσει την εν λόγω τεχνολογία για την επίτευξη των προσδοκιών τους. Παρά ταύτα, τα μεγάλα δεδομένα μπορούν να συνδράμουν σε πολλούς διαφορετικούς τομείς, μεταξύ των οποίων και αυτός της κυβερνοασφάλειας. Τα εργαλεία που χρησιμοποιούνται για την αξιοποίηση των μεγάλων δεδομένων δύναται να συνεισφέρουν στη καταπολέμηση των εγκλημάτων που διαπράττονται μέσω του διαδικτύου, είτε προλαμβάνοντας τις επιθέσεις, είτε αντιδρώντας ταχύτερα σε αυτές (Marr, 2016). Πώς επιτυγχάνεται, όμως, κάτι τέτοιο; Τα μεγάλα δεδομένα χρησιμοποιούνται κατά κόρον στη δημιουργία μέτρων ασφαλείας, τροφοδοτώντας τα ώστε να βελτιστοποιηθούν. Οι εταιρίες που ασχολούνται με την ανάπτυξη προγραμμάτων προστασίας από ιούς (antivirus) και τειχών προστασίας (firewall) κάνουν χρήση των μεγάλων δεδομένων αφενός για να ελέγξουν τα προϊόντα πριν την έναρξη στην αγορά και αφετέρου για να εκμηδενίσουν τις πιθανότητες μη ενδεδειγμένων αποτελεσμάτων. Βέβαια, σε περίπτωση που στόχος είναι η εξέλιξη των προγραμμάτων, η εκμετάλλευση των μεγάλων δεδομένων συνιστά αρωγό της εκπαίδευσης προγραμμάτων ικανών να αναγνωρίζουν τις συχνότερα τελούμενες επιθέσεις ή ακόμη της δημιουργίας

απαραίτητων θεμελίων για την πρόληψη μελλοντικών μορφών επιθέσεων που μπορεί ακόμη να μην έχουν εμφανιστεί.

Ήδη τα data centers αξιοποιούν τα μεγάλα δεδομένα για να καταστείλουν ενδεχόμενες ηλεκτρονικές επιθέσεις. Τα δεδομένα που χρησιμοποιούν αποτελούν απόρροια φυσικών κέντρων δεδομένων ή αποθήκευσης στο σύννεφο. Έτσι, μπορούν να παρακολουθούν τις διαδικτυακές κινήσεις και να ελέγχουν λεπτομερώς όσες θεωρούν ύποπτες, συνήθως με αυτόματο τρόπο.

7. Διαδικτυακός Σεξουαλικός Εκβιασμός

Στο παρόν κεφάλαιο θα αναλυθεί εκτενώς ένα φαινόμενο που έχει απλώσει τις ρίζες του σε όλο τον κόσμο αποτελώντας μάστιγα της εποχής. Εκτός από την κοινωνική ανάπτυξη του θέματος, αναμένονται και οι νομικές προεκτάσεις του.

Γνωστός παγκοσμίως με τον όρο sextortion, ο σεξουαλικός εξαναγκασμός και εκβιασμός είναι η μία από τις μάστιγες της εποχής που αφορά άτομα μικρότερης ή μεγαλύτερης ηλικίας, καθώς θύματά του είναι τόσο ανήλικοι όσο και ενήλικες. Ανάλογα με τη περίπτωση, ο εκβιασμός εξελίσσεται με διαφορετικό τρόπο. Ωστόσο οι κύριες μορφές είναι δύο και διακρίνονται στις διαπροσωπικές σχέσεις και στις διαδικτυακές σχέσεις. Οι Wolak & Finkelhor σε σχετική έρευνά τους με τίτλο "Sextortion: Findings From A Survey Of 1.631 Victims", το 2016, διαπίστωσαν ότι τα περιστατικά sextortion που προέρχονταν από διαπροσωπικές σχέσεις ανέρχονταν στο 60%, ενώ τα υπόλοιπα αφορούσαν τις σχέσεις που αναπτυσσόταν μέσω διαδικτύου. Οι ερευνητές σημείωσαν αρκετές διαφοροποιήσεις σε σημεία προεξέχοντος σημασίας, όπως η «δυναμική, η ταχύτητα με την οποία εκτυλίσσονται τα περιστατικά, η φύση των απειλών και ο τρόπος αντιμετώπισης ή όχι των καταστάσεων». Σύμφωνα με τα ευρήματα της ίδια έρευνα, τα περιστατικά σεξουαλικού εκβιασμού προερχόμενου από διαπροσωπικές σχέσεις χαρακτηριζόντουσαν από σεξουαλικές επιθυμίες των δραστών ή εκδικητικές πράξεις που πήγαζαν από φθόνο ή ζήλια μεταξύ φίλων ή κοινών γνωστών. Στον αντίποδα, τα θύματα που επικαλούνταν διαδικτυακό σεξουαλικό εκβιασμό περιέγραφαν «σκηνές» ερωτικών επαφών, ενώ δεν έλλειπαν και οι περιπτώσεις όπου ο θύτης εξανάγκαζε το θύμα να προβεί σε άσεμνες πράξεις με τη βοήθεια απειλών.

Όπως σημειώνεται στην ίδια έρευνα, στη περίπτωση εκβιασμού μέσω διαπροσωπικής σχέσης το 96% των δραστών επικοινωνούσε με τα θύματά του μέσω ηλεκτρονικών συσκευών και κυρίως μέσω κινητών τηλεφώνων και ηλεκτρονικών

υπολογιστών. Μόλις το 2% επέλεγε τη δια ζώσης επικοινωνία απειλώντας με ανάρτηση του επίμαχου υλικού στο διαδίκτυο ή διαμοίρασή του μέσω κινητών τηλεφώνων. Παρατηρείται, λοιπόν, η κατά κόρον χρήση της τεχνολογίας και κυρίως των μέσω κοινωνικής δικτύωσης. Χαρακτηριστικό αυτών είναι μεταξύ άλλων, η δυνατότητα παραπλάνησης των χρηστών. Επιτήδειοι δημιουργούν ψεύτικους λογαριασμούς παριστάνοντας κάποιον άλλο άνθρωπο, ώστε να αποκρύψουν τη πραγματική τους ταυτότητα και να προσεγγίσουν με μεγαλύτερη ευκολία το στόχο τους. Οι λογαριασμοί αφορούν είτε ηλεκτρονικό ταχυδρομείο, είτε κάποιο μέσω κοινωνικής δικτύωσης ή ακόμα και αριθμούς κινητού τηλεφώνου.

Όσον αφορά τα ποσοστά ανδρών και γυναικών που «πέφτουν» θύματα αυτών των ενεργειών για τις περιπτώσεις διαπροσωπικών σχέσεων οι γυναίκες δέχονται την επίθεση σε ποσοστό 87%, ενώ οι άντρες σε ποσοστό 11%. Αντίστοιχα, στις περιπτώσεις όπου η σχέση δράστη θύματος αναπτύσσεται μόνο μέσω διαδικτύου οι γυναίκες αποτελούν το 77% των θυμάτων, ενώ οι άντρες το 20%. Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα ευρήματα σχετικά με τα ποσοστά των ανηλίκων. Συγκεκριμένα, το 47% των θυμάτων ήταν ανήλικοι (κάτω των 18 ετών) όταν απειλήθηκαν από κάποιο γνωστό τους, ενώ το 43% άνηκε στη ηλικία τουλάχιστον των 17 ετών όταν δέχθηκε σεξουαλικό εκβιασμό από κάποιο χρήστη του διαδικτύου (Wolak & Finkelhor, 2016). Τέλος όσον αφορά το σεξουαλικό εκβιασμό προερχόμενο από άγνωστο οπτικά στο θύμα θύτη, αναφέρεται ότι η επικοινωνία μεταξύ των δύο ξείνησε από κάποια κοινωνική πλατφόρμα, όπως Facebook, Instagram, Tagged κ.λπ. ενώ στη συνέχεια μπορεί αν μετακινήθηκε σε άλλη εφαρμογή.

Παρόλο που είναι εξαιρετικά δύσκολο να θεωρηθεί ήσσονος σημασίας μία κατηγορία σεξουαλικού εξαναγκασμού και εκβιασμού, στη παρούσα εργασία θα δοθεί ιδιαίτερη σημασία στις περιπτώσεις όπου θύτης και θύμα είχαν τη πρώτη τους επικοινωνία μέσω διαδικτύου.

7.1. Παρουσίαση θέματος

Ο σεξουαλικός εκβιασμός είναι ένα φαινόμενο που υπάρχει στους κόλπους της ανθρώπινης κοινωνίας σχεδόν από τη γέννηση αυτής. Ωστόσο, η εμφάνιση και περισσότερο η ανάπτυξη του διαδικτύου συνετέλεσαν στην εξέλιξή του σε ένα σαφώς πιο ισχυρό και δύσκολο ως προς την εξιχνίαση αδίκημα. Αναφέρεται ως διαδικτυακός σεξουαλικός εξαναγκασμός και εκβιασμός ή sextortion, σύντμηση των λέξεων sex και extortion (δηλ. εκβιασμός) είτε ως σεξουαλικός εκβιασμός τελούμενος στο χώρο του διαδικτύου. Πλέον αποτελεί παγκόσμια μάστιγα που απειλεί την ανθρώπινη κοινωνία απαξιώνοντας για το φύλο, την ηλικιακή ομάδα πολλές φορές ακόμη και για την ζωή των θυμάτων. Η εν λόγω δραστηριότητα παρουσιάζει έντονες κοινωνικές, ψυχολογικές και νομικές προεκτάσεις.

Γυναίκες και άνδρες όλων των ηλικιών, με πρόφαση το διαδικτυακό φλερτ παγιδεύονται από επιτήδειους που χρησιμοποιούν αρχεία ερωτικού περιεχομένου που έχουν συλλέξει από τα θύματά τους ώστε να αποσπάσουν περισσότερο υλικό ή χρηματικά ποσά. Αυτό θα μπορούσε να αποτελεί έναν ορισμό του σεξουαλικού εκβιασμού που τελείται μέσω διαδικτύου. Πρόκειται για ένα από τα πιο συχνά φαινόμενα εγκληματικών ενεργειών παγκοσμίως. Προέρχεται από τη σύντμηση των λέξεων sex και extortion δηλαδή εκβιασμός. Η διαδικασία είναι απλή αρχικά ένα αίτημα φιλίας, μία πιο ιδιωτική συνομιλία, ανταλλαγή φωτογραφιών ερωτικού περιεχομένου ή και βίντεο και ο εκβιασμός έχει ήδη στηθεί. Ωστόσο, ο τρόπος προσέγγιση των υποψήφιων θυμάτων διαφέρει ανάλογα με το προφίλ του θύτη και ανάλογα με το θύμα.

Παράδειγμα με θύμα ενήλικα άντρα

«Ξεκινήσαμε μία συνομιλία. Αρχίσαμε να ερωτοτροπούμε. Μπήκαμε στο Skype. Τα πράγματα μεταξύ μας ξεφεύγουν και εγώ καταλήγω να γδυθώ.Έβγαλε και εκείνη τα ρούχα της και συνέχισε να μου γράφει. Έπειτα έκλεισε τη συνομιλία και γύρισε στο Facebook. Όπου κάνει copy-paste όλες μου τις απαντήσεις σε όλες μου τις επαφές. Μου λέει πως έχει βίντεο, με εμένα παντελώς εκτεθειμένο. Μετά συνεχίζει λέγοντάς μου πως θα πρέπει να πληρώσω 1.500$, ειδάλλως θα τα έστελνε όλα σε φίλους και οικογένεια.» (Πηγή: CNN)

Παράδειγμα με θύμα ανήλικη κοπέλα

«Έλαβα ένα μήνυμα στο προφίλ μου στο Facebook από έναν εικοσάχρονο άντρα. Τον αποδέχτηκα, αφού μου άρεσε και είπα ότι είναι μία καλή ευκαιρία για να μιλήσουμε. Μετά από κάποια ώρα μου ζήτησε να του στείλω μία φωτογραφία μου χωρίς ρούχα και αποδέχτηκα. Ακολούθησε μία περίοδος όπου στέλναμε φωτογραφίες. Όμως αποφάσισα να το σταματήσω γιατί δεν ήθελα άλλο. Τότε μου είπε ότι αν δεν του στείλω και άλλες φωτογραφίες μου θα στείλει όσες έχει στους φίλους μου. Είπα ότι δεν θέλω να με ξανά ενοχλήσει και τον έκανα μπλοκ. Μου έστειλε μήνυμα σε άλλη εφαρμογή από κάποιον άλλο λογαριασμό όπου και συνέχισε τις απειλές, λέγοντάς μου μάλιστα να τον βρω σε ένα ξενοδοχείο κοντά στο σπίτι μου.»

7.2. Η τεχνική του διαδικτυακού σεξουαλικού εκβιασμού

Οι τρόποι με τους οποίους οι δράστες επιδιώκουν να «παραπλανήσουν» το εκάστοτε θύμα τους ποικίλλουν, καθώς εξαρτώνται από παράγοντες όπως το υποβόσκον κίνητρο του δράστη και φυσικά η συμπεριφορά των υποψήφιων θυμάτων. Εντούτοις, ξεχωρίζουν τρία στοιχεία που διακρίνουν το εν λόγω φαινόμενο. Το πρώτο είναι το υλικό, δηλαδή το αρχείο με φωτογραφίες ή βίντεο ασελγούς περιεχομένου με πρωταγωνιστή το θύμα και το οποίο έχει στην ιδιοκτησία του ο δράστης. Ακολουθεί η απειλή. Ο δράστης εκβιάζει το θύμα με δημοσιοποίηση του αποκτηθέντος ευαίσθητου υλικού αν ο δεύτερος δεν ικανοποιήσεις τις επιθυμίες του. Τέλος, η αξία, δηλαδή τα ανταλλάγματα που ζητάει ο δράστης για να κρατήσει τη σιωπή του. Το 66% ζητά νέο υλικό σεξουαλικού περιεχομένου, το 39% ζητά από το θύμα να εκτελέσει ενέργειες που ικανοποιούν τις εκάστοτε επιθυμίες του, το 28% να βρεθούν πρόσωπο με πρόσωπο, το 23% να παραμείνει στη «σχέση», το 36% διαδικτυακό sex και το 14 χρήματα (Wolak & Finkelhor, 2016). Στη προσπάθεια αποκωδικοποίησης της δράσης των επιτηδείων, παρατηρούνται αρκετές διαφορές που ωστόσο διακρίνονται από κοινή τακτική αποτελούμενη από τρία ή τέσσερα στάδια.

GROOMING πρόκειται για την αποπλάνηση των θυμάτων. Ο δράστης προσπαθεί να κερδίσει την εμπιστοσύνη του θύματος με αρχικά αθώες ερωτήσεις, ιδιαιτέρως στη περίπτωση που το θύμα είναι ανήλικο.

[PRIVETE COMMUNICION η συζήτηση μεταφέρεται σε μία πιο ιδιωτική συνομιλία, πιθανόν και σε κάποιο άλλο δίκτυο, όπου θύτης και θύμα επικεντρώνονται σε θέματα ερωτική φύσεως. Στις περιπτώσεις παρενόχλησης ανηλίκων ο θύτης μπορεί να ζητήσει από το ανήλικο θύμα του κάποια πιο προσωπικά δεδομένα ή ακόμα και να τάξει κάποιο δώρο. Σε αυτό το στάδιο πιθανόν να υπάρξει ανταλλαγή φωτογραφιών μη απαγορευμένου περιεχομένου.**]**

SEXTING πρόκειται για την ανταλλαγή φωτογραφιών με σεξουαλικό περιεχόμενο. Ο θύτης ζητά από το θύμα με κάποια πρόφαση να του αποστείλει ανάλογες φωτογραφίες. Πολλές φορές, μάλιστα, η συνομιλία μετατρέπεται από γραπτή σε προφορική μέσω χρήσης της webcam, όπου ο θύτης ζητά από το θύμα να προβεί σε ασελγείς πράξεις ή ακόμα και cybersex τα οποία ο πρώτος καταγράφει.

SEXTORTION το «παιχνίδι» τελείωσε και ο θύτης αποκαλύπτεται. Απειλεί το θύμα με δημοσιοποίηση του αποκτηθέντος υλικού και διαδικτυακή διαπόμπευση του θύματος, αν δεν εκπληρώσει τις απαιτήσεις του. Η συνομιλία σταματά απότομα και ο θύτης ενημερώνει το θύμα με αποστολή σχετικών μηνυμάτων στο λογαριασμό του θύματος.

7.3. Το προφίλ των δραστών

Οι θύτες διακρίνονται από αντικοινωνικές τάσεις και συνήθως επηρεάζονται από κοινωνικό-συναισθηματικούς παράγοντες, για παράδειγμα έλλειψη στενών διαπροσωπικών σχέσεων και φυσικά βίαιη ή επιθετική συμπεριφορά. Η κατηγοριοποίηση των δραστών είναι ιδιαίτερα δύσκολη υπόθεση αφού τα κίνητρά τους είναι συνήθως πολυπαραγοντικά με τις σεξουαλικές ανάγκες να επικαλύπτονται με τις οικονομικές και αντιστρόφως. Εντούτοις τείνουν να ξεχωρίζουν δύο προφίλ θυτών με γνώμονα το υποβόσκον κίνητρο. Τα δύο προφίλ διακρίνονται από σημαντικές διαφορές τόσο ως προς τα χαρακτηριστικά των δραστών όσο και κατά τον τρόπο με τον οποίο δρουν.

7.3.1. Σεξουαλικό κίνητρο

Στόχος είναι η απόκτηση είτε περαιτέρω υλικού σεξουαλικού περιεχομένου, είτε συνάντηση με το θύτη με σκοπό την ερωτική αποπλάνηση. Ο δράστης αν και συνήθως δρα μόνος τους, συχνά μοιράζεται ή ανταλλάσσει το υλικό που κατέχει. Στη πλειοψηφία τους οι δράστες που ενεργούν με σεξουαλικό κίνητρο είναι άνδρες και το ηλικιακό εύρος είναι από τα δέκα τέσσερα έως τα εβδομήντα έτη, δίχως αυτό να είναι απόλυτο. Η δράση τους εκτείνεται από τοπικό μέχρι εθνικό ή και διεθνές επίπεδο. Αξιοσημείωτο είναι το γεγονός πως τα θύματα είναι κυρίως γυναίκες ή κορίτσια. Σε πολλές περιπτώσεις μάλιστα θύτης και θύμα γνωρίζονται πριν τη διαδικτυακή τους εμπειρία.

7.3.2. Οικονομικό κίνητρο

Πρωτεύων στόχος είναι η απόκτηση χρημάτων σε αντάλλαγμα για μη δημοσιοποίηση του αποκτηθέντος ευαίσθητου υλικού. Σε αντίθεση με τα ισχύοντα για τους δράστες με σεξουαλικό κίνητρο, οι δράστες με οικονομικό κίνητρο ανήκουν και στα δύο φύλα, όμως στη πλειοψηφία των περιπτώσεων οι θύτες προσποιούνται εμφανίσιμες γυναίκες. Ειδοποιό διαφορά συνιστά και ο τρόπος με τον οποίο ενεργούν. Οι επιτήδειοι δρουν ως μέλη οργανωμένου εγκλήματος, σε ομάδες, έχοντας για έδρα κάποια αναπτυσσόμενη συνήθως χώρα, ενώ στοχεύουν σε εθνικό ή διεθνές επίπεδο. Σε αυτή τη περίπτωση τα θύματα είναι συνήθως αγόρια, άγνωστα προς το θύτη και η όποια επαφή μεταξύ τους πραγματοποιείται μόνο μέσω διαδικτύου και ποτέ δια ζώσης.

7.4. Χρονική περίοδος δράσης

Η χρονική περίοδος δράσης, δηλαδή ο χρόνος που θύτης και θύμα αλληλεπιδρούν ποικίλλει σημαντικά ανάλογα με τον απώτερο στόχο του πρώτου και τη συμπεριφορά ή τις αντιστάσεις του δευτέρου. Έτσι, η περίοδος μπορεί να κυμανθεί

από λίγες ώρες μέχρι πολλούς μήνες. Γεγονός που υποστηρίζεται και από αντίστοιχη έρευνα όπου το 27% των ερωτηθέντων χρειάστηκε το πολύ 24 ώρες για να στείλει την πρώτη φωτογραφία, το 22% την έστειλε σε χρονική περίοδο μέχρι μιας εβδομάδας (>1 μέρας – 1 εβδομάδα). Το 14% προέβη σε αποστολή φωτογραφικού υλικού σε χρονική περίοδο μεγαλύτερη της μίας εβδομάδας αλλά μικρότερη των δύο εβδομάδων. Το 22% μιλούσε με το δράστη περισσότερες από δύο εβδομάδες έως τρεις μήνες, ενώ το 10% περισσότερους από τρεις μήνες (Wolak & Finkelhor, 2016). Η διαφορά αυτή έχει πολυσήμαντες συνέπειες τόσο ως προς τον τρόπο εξέλιξης της επαφής όσο και για τις επιπτώσεις προς το θύμα.

7.5. Τόπος τέλεσης

Όπως είναι επόμενο ο χώρος που επιλέγουν να ξεδιπλώνουν τις πρακτικές τους οι επιτήδειοι είναι τα μέσα κοινωνικής δικτύωσης, κοινώς γνωστά ως social networks, τα δωμάτια επικοινωνιών, chat rooms και στις περιπτώσεις «ψαρέματος» ανηλίκων τα διαδικτυακά παιχνίδια. Οι πλατφόρμες κοινωνικής δικτύωσης (Facebook, Tagged, Instagram, κλπ) συγκεντρώνουν τα υψηλότερα ποσοστά προσέγγισης θυμάτων. Ακολουθούν οι πλατφόρμες αποστολής μηνυμάτων και φωτογραφιών (Kik, Snapchat, κλπ), οι εφαρμογές που προσφέρουν οπτικοακουστικό θέαμα και βίντεο κλήσεις (Skype, Facetime, webcam sites κλπ) και πολλές άλλες εφαρμογές (Wolak & Finkelhor, 2016).

7.6. Νομική πλευρά

Το υποσυζήτηση φαινόμενο συνιστά μία ιδιαίτερη περίπτωση εγκληματικής ενέργειας που τείνει να διχάζει το ακροατήριο. Συχνά, ο τρόπος εξαπόλυσης της επίθεσης δεν γίνεται αντιληπτός με αποτέλεσμα οι εκάστοτε επιστήμονες που προσπαθούν να το αποδώσουν να συγκρούονται. Η ίδια σύγχυση υπάρχει και στο κλάδο της νομικής επιστήμης. Η περίπτωση του διαδικτυακού σεξουαλικού εκβιασμού και γενικότερα το αδίκημα του σεξουαλικού εκβιασμού τιμωρείται

σύμφωνα με τη διάταξη για το έγκλημα του απλού εκβιασμού, δηλαδή με το άρθρο 385 Π.Κ. περί εκβίασης. Εντούτοις, για τη στοιχειοθέτηση του εγκλήματος του διαδικτυακού σεξουαλικού εξαναγκασμού και εκβιασμού απαιτείται συχνά η τέλεση μίας σειρά άλλων αξιόποινων πράξεων που διαφέρουν ανάλογα με το τον τρόπο που εκτυλίσσεται η κάθε περίπτωση και την ηλικία του αποδέκτη της πράξης. Για παράδειγμα, στην τεχνική του διαδικτυακού σεξουαλικού εκβιασμού που παρουσιάστηκε προηγουμένως αναφέρθηκαν κάποια στάδια, τα οποία υπό περιπτώσεις εμπίπτουν σε συγκεκριμένες εγκληματικές ενέργειες. Έτσι, όταν αποδέκτης των πράξεων είναι ανήλικος, το grooming ή αλλιώς αποπλάνηση συνιστά το ποινικό αδίκημα της αποπλάνησης ανηλίκου που τιμωρείται σύμφωνα με τις διατάξεις του άρθρου 339 Π.Κ., ενώ το sexting δηλαδή η ανταλλαγή φωτογραφιών άσεμνου περιεχομένου μπορεί να κριθεί ως πορνογραφική παράσταση ανηλίκου και συνεπώς η διάθεση αυτού ως πορνογραφία ανηλίκου, ενώ προσβάλλεται βάναυσα και η αξιοπρέπεια του παθόντα στο πεδίο της γενετήσιας ζωής του, επομένως τελείται το έγκλημα προσβολής της γενετήσιας αξιοπρέπειας. Όπως προκύπτει από τη παράθεση των προηγούμενων στοιχείων η αντιμετώπιση ή έστω η προσπάθεια αντιμετώπισης του σεξουαλικού εκβιασμού κρίνεται αναγκαία, καθώς εκτός των άλλων μπορεί να συμβάλλει και στην αντιμετώπιση άλλων παράνομων ενεργειών.

7.7. Η ισχύουσα κατάσταση στο διαδίκτυο

Ο εκβιασμός μέσω διαδικτύου συγκαταλέγεται στα νεότερα αδικήματα, διαπίστωση που προκύπτει τόσο από το χρόνο εκκίνησης τέτοιων περιστατικών όσο και από την έλλειψη νομικού πλαισίου. Συγκεκριμένα, ο νόμος χαρακτηρίζεται από πολλές ασάφειες σχετικά με την εν λόγω εγκληματική ενέργεια, με συνέπεια οι δράστες να τιμωρούνται σύμφωνα με τις γενικές διατάξεις του Ποινικού Κώδικα. Έτσι, στη πλειονότητα των περιπτώσεων, το θύμα προχωρά σε ποινική δίωξη του δράστη. Συνήθως οι επαπειλούμενες ποινές περιορίζονται στα πλημμελήματα, με δυνατότητα αύξησης του πλαισίου ποινής σε κάθειρξη έως δέκα ετών, μόνο στις περιπτώσεις που διαπιστώνεται κακουργηματική πράξη, δηλαδή εδώ εκβιασμός. Εντούτοις, το θύμα έχει αξίωση καταβολής χρηματικής αποζημιώσεως, σύμφωνα με τις διατάξεις περί προσβολής προσωπικότητας, όταν η υπόθεση φτάσει στα αστικά

δικαστήρια, κάτι που συμβαίνει σπάνια τουλάχιστον στα περιστατικά παρενοχλήσεων. Για αυτά η νομολογία θεωρεί ότι διαπράττονται δύο αδικήματα, αυτό της παραβίασης ευαίσθητων προσωπικών δεδομένων και της κατ'εξακολούθηση δυσφήμησης του θύματος.

Τα ανωτέρω ενισχύουν την αναγκαιότητα εφαρμογής νέων διατάξεων που θα στοχεύουν στην κάλυψη περιπτώσεων διαδικτυακού σεξουαλικού εκβιασμού και εξαναγκασμού, καθώς και διαδικτυακής σεξουαλικής παρενοχλήσεως.

Στην Αγγλία, ήδη από το 2014 και παρά τις αντιρρήσεις μίας μερίδας βουλευτών που υποστήριζε την αντιμετώπιση του προβλήματος από τις ισχύουσες διατάξεις περί βωμολοχίας και εκβίασης, προβλέπεται η τιμωρία του sexting, δηλαδή της ανταλλαγής εικόνων σεξουαλικού περιεχομένου σε μέσα κοινωνικής δικτύωσης αλλά κα σε sms, όταν δεν υπάρχει προηγούμενη συγκατάθεση του ατόμου που αναπαρίσταται σε αυτές. Η διάταξη εφαρμόζεται τόσο σε περιπτώσεις online δημοσίευσης, όσο και σε έντυπη μορφή.

Ο σεξουαλικός διαδικτυακός εξαναγκασμός και εκβιασμός (sextortion) μπορεί να συμβεί ανά πάσα ώρα και στιγμή. Ο δράστης προσεγγίζει τα υποψήφια θύματά του μέσω διαδικτύου και κυρίως κοινωνικών δικτύων, χρησιμοποιώντας δόλιες μεθόδους. Η διαδικασία είναι συνήθως απλή. Αρχικά επιδιώκει να αποκτήσει την εμπιστοσύνη του θύματος, ώστε να ζητήσουν φωτογραφίες ή βίντεο του θύματος και στη συνέχεια νέο υλικό αυτή τη φορά με πορνογραφικό περιεχόμενο. Όταν το θύμα ενδώσει στις επιθυμίες του δράστη, ο δεύτερος αποκαλύπτει το κίνητρό του.

Ανεξάρτητα από τη πεποίθηση πολλών σχετικά με το σεξουαλικό διαδικτυακό εξαναγκασμό και εκφοβισμό, αυτός εμφανίζεται τόσο σε ανηλίκους όσο και σε ενηλίκους. Ωστόσο, ποινικά η ηλικιακή ομάδα του θύματος επηρεάζει τα εγκλήματα που στοιχειοθετούνται από την εν λόγω πράξη αλλά και το επαπειλούμενο πλαίσιο ποινής. Έτσι, στη περίπτωση που το θύμα είναι ενήλικος η πράξη περιορίζεται στο έγκλημα της εκβίασης επισύροντας την ανάλογη τιμωρία του δράστη. Αντίθετα, αν το θύμα είναι ανήλικος, ο δράστης αντιμετωπίζει βαρύτερες κατηγορίες, καθώς θεωρείται ότι έχει διαπράξει περισσότερα εγκλήματα πέραν της εκβίασης. Για παράδειγμα, στο πρώτο στάδιο της αποπλάνησης (grooming) τελείται το αδίκημα της αποπλάνησης ανηλίκου, ενώ η ανταλλαγή οπτικοακουστικού υλικού ευαίσθητου

περιεχομένου στοιχειοθετεί το αδίκημα της πορνογραφίας ανηλίκου. Οι βαρύτερες κατηγορίες, όπως είναι επόμενο επισύρουν μεγαλύτερες τιμωρίες για το θύτη.

Συνεπώς, η εξιχνίαση τέτοιων υποθέσεων κρίνεται απαραίτητη όχι μόνο για την παραδειγματική τιμωρία του δράστη, αλλά και για την ενδεχόμενη εξιχνίαση και άλλων αδικημάτων πιθανώς πιο σκληρών από αυτό της εκβίασης. Ωστόσο, για να είναι εφικτό αυτό θα πρέπει να καταγγελθούν τα περιστατικά σεξουαλικού διαδικτυακού εκβιασμού, καθώς δε συγκαταλέγεται στα αυτεπαγγέλτως διωκόμενα εγκλήματα. Γεγονός που δυσχεραίνει το έργο των διωκτικών και διευκολύνει αυτό των επιτήδειων. Οι στατιστικές για την Ελλάδα είναι απογοητευτικές, υποστηρίζοντας ότι μόλις το 1% των θυμάτων καταγγέλλουν περιστατικά διαδικτυακής κακοποίησης.

Πολλές φορές έχει γίνει λόγος για τη ραγδαία εξέλιξη που σημειώνει η τεχνολογία και για τις συνέπειες αυτής στη καθημερινότητα των ανθρώπων. Συχνά υπερτονίζονται οι αρνητικές επιπτώσεις αυτής, δίχως να γίνονται ιδιαίτερες προτάσεις για την αντιμετώπισή τους. Το ίδιο τοπίο επαναλαμβάνεται και στους κόλπους της νομικής επιστήμης. Το ηλεκτρονικό έγκλημα και οι εξειδικευμένες κατηγορίες αυτού, όπως το κυβερνοέγκλημα, αυξάνονται διαρκώς προβληματίζοντας τόσο τους ειδικούς όσο και το κοινωνικό σύνολο. Εντούτοις, ο ρυθμός με τον οποίο η νομοθεσία πολλών χωρών προσαρμόζεται στα νέα δεδομένα παρομοιάζεται με αυτόν της χελώνας. Το αποτέλεσμα είναι η ποινικοποίηση ενεργειών που διαπράττονται στο χώρο του διαδικτύου (κυρίως) να πραγματοποιείται με τέτοια καθυστέρηση που ενδεχομένως νέες μορφές και μέθοδοι να είναι προ των πυλών ή ακόμη και να εφαρμόζονται από μία μερίδα χρηστών. Σε καμία περίπτωση δεν υποστηρίζεται μέσω της παρούσας εργασίας ότι η θέσπιση νέων νόμων που προσανατολίζεται στη καταπολέμηση αυτών των εγκληματικών ενεργειών είναι ικανή να εμποδίσει την εμφάνιση και άλλων παρόμοιων περιστατικών, όμως μπορεί να συμβάλει στο αίσθημα δικαίωσης και ικανοποίησης των θυμάτων, αλλά και στη παραδειγματική τιμωρία των δραστών.

8. Ο Ρόλος Των Μέσων Κοινωνικής Δικτύωσης

Στο παρόν κεφάλαιο αναπτύσσεται ο ρόλος των δύο κοινωνικών δικτύων και κυρίως ο λόγος που το Instagram επιλέγθηκε ως η πλατφόρμα μελέτης της εν λόγω εργασίας.

8.1. Η περίπτωση του Instagram

Το Instagram, ιδρύθηκε το 2010 θέλοντας να «καταγράψει και μοιραστεί τις στιγμές του κόσμου» και συγκαταλέγεται στα μέσα κοινωνικής δικτύωσης κερδίζοντας ολοένα και περισσότερο τους χρήστες, ανεβάζοντας τη φήμη του. Ωστόσο λίγοι είναι αυτοί που γνωρίζουν την ιστορία του. Η αρχική σκέψη ήταν απλή. Οι ιδρυτές τους ήθελαν να φτιάξουν μία εφαρμογή κοινωνικής δικτύωσης για κινητές συσκευές που θα επέτρεπε τη λήψη, επεξεργασία καθώς και τη κοινή χρήση φωτογραφιών, όπως και έγινε. Στη συνέχεια, η εφαρμογή αναβαθμίστηκε με τη προσθήκη βίντεο. Το ενδιαφέρον των χρηστών ώθησε τους δημιουργούς, στη μεταφορά της εφαρμογής και σε άλλες συσκευές, έτσι πλέον διατίθεται και η web έκδοση, επιτρέποντας τη χρήση της και μέσω υπολογιστών, με μοναδική διαφορά τη δυνατότητα προβολής και όχι διαμοιρασμού του περιεχομένου των χρηστών. Σύμφωνα με πληροφορίες του Instagram ξεπέρασε το ένα δισεκατομμύριο ενεργούς χρήστες μηνιαίως, ενώ το 2017 αριθμούσε περίπου 800 εκατομμύρια χρήστες, γεγονός που αποδεικνύει την αύξηση της δημοσιότητάς του. Κάθε ένα λεπτό, υπολογίζεται ότι ανεβαίνουν 882 φωτογραφίες στη συγκεκριμένη μόνο εφαρμογή, ενώ ημερησίως ο αριθμός ανεβαίνει στις 80 εκατομμύρια φωτογραφίες. Το 2012 το Facebook εξαγόρασε το Instagram έναντι ενός δισεκατομμύριο δολαρίων. (είναι μία από τις τέσσερις πλατφόρμες του Facebook που ξεπέρασε τους ένα δισεκατομμύριο χρήστες μαζί με το ίδιο το Facebook, το WhatsApp και το Messenger)

Η χρήση του είναι απλή. Ο ενδιαφερόμενος αφού δημιουργήσει ένα λογαριασμό μπορεί να προβεί στις υπόλοιπες ενέργειες είτε ακολουθώντας άλλους

χρήστες είτε δημιουργώντας το δικό του περιεχόμενο είτε προβαίνοντας και στις δύο ενέργειες. Με άλλα λόγια, δύναται να δει φωτογραφίες και βίντεο άλλων χρηστών στην αρχική του σελίδα όσο και να δημοσιεύσει το δικό του υλικού που στη συνέχεια θα δουν οι άλλοι χρήστες. όπως και στα υπόλοιπα μέσα κοινωνικής δικτύωσης, οι χρήστες μπορούν να συνοδεύσουν τις αναρτήσεις τους με τις κατάλληλες ετικέτες (tags). Λόγω τις εξαγοράς του από το Facebook, οι χρήστες του Instagram μπορούν να μεταφέρουν ή να βρουν τους φίλους που διατηρούν στην άλλη εφαρμογή.

Πρόκειται για μία εφαρμογή που κερδίζει τους εφήβους και τα άτομα νεαρής ηλικίας κοινό στο οποίο δείχνει ότι στοχεύει και η ίδια. Μάλιστα, ανακοινώθηκε μία νέα κινητή εφαρμογή του Instagram, το IGTV, που αναμένεται να λειτουργεί όπως το YouTube. Συγκεκριμένα, κάθε χρήστης θα διαθέτει το δικό του «κανάλι» όπου θα μπορεί να ανεβάζει βίντεο μεγάλης χρονικής διάρκειας, που όμως δε θα ξεπερνά τα δέκα λεπτά και για τους χρήστες με πολλούς ακόλουθους η μέγιστη χρονική διάρκεια ανέρχεται στη μία ώρα. Αξίζει να σημειωθεί ότι, στη κανονική εφαρμογή τα βίντεο δε ξεπερνούν το ένα λεπτό. Ιδιαίτερο ενδιαφέρον παρουσιάζει η δήλωση του διευθύνοντα συμβούλου του Instagram, Kevin Systrom, σχετικά με τις οικονομικές απολαβές, καθώς στο μέλλον ενδέχεται οι δημιουργοί των πιο δημοφιλών βίντεο να λαμβάνουν κάποιο οικονομικό όφελος όπως συμβαίνει ήδη με το YouTube.

Θέλοντας να δείξει την ευαισθησία του προς τα φαινόμενα σεξουαλικής παρενόχλησης, αλλά και ρατσισμού, το Instagram θα απαγορεύει τη προβολή βίντεο με ρατσιστικό, βίαιο ή σεξουαλικό περιεχόμενο. Πρέπει να τονιστεί όμως ότι τα βίντεο θα ελέγχονται ως προς τη νομιμότητά τους μετά την ανάρτησή τους στην πλατφόρμα, αφού δεν θα υπάρχει μηχανισμός που θα το κάνει εκ των προτέρων.

Ωστόσο η περίπτωση του Instargam είναι ιδιαίτερα ενδιαφέρουσα για τη παρούσα εργασία. Αν αναλογιστεί κανείς τον όγκο των φωτογραφιών και των βίντεο που διακινούνται μέσω της εφαρμογής, θα κατανοήσει ότι συνιστά ένα «εργοστάσιο παραγωγής δεδομένων» και συνεπώς μία εξαιρετική πηγή γνώσης για την ανάπτυξη νοήμων συστημάτων. Γεγονός που αναγνωρίζει και ο CEO της εταιρίας Kevin Systrom επισημαίνοντας πως εκτός των άλλων θα συνιστά μία μεγάλη εταιρία δεδομένων. Οι αρμόδιοι της εν λόγω εφαρμογής έχουν δείξει ευαισθησία ως προς συγκεκριμένα αδικήματα που τελούνται στον κυβερνοχώρο, όπως παρενόχληση και εκφοβισμός. Το 2017 διεξήχθη μία έρευνα με τίτλο «The Annual Bulling Survey

2017» από το Ditch the Label σε περισσότερους από δέκα χιλιάδες (10.000) ανθρώπους ηλικίας δώδεκα με είκοσι πέντε (12-25) ετών στο Ηνωμένο Βασίλειο. Το 42% του δείγματος ανέφερε ότι στο Instagram σημειώθηκαν τα περισσότερα περιστατικά εκφοβισμού. Έτσι, οι υπάλληλοι της εφαρμογής προσπάθησαν να προστατεύσουν τους χρήστες μέσω της μηχανικής μάθησης. Ελέγχουν και χρησιμοποιούν τις τρέχουσες δημοσιεύσεις για να εκπαιδεύσουν περαιτέρω τον αλγόριθμο, ώστε να ανιχνεύει τα προσβλητικά σχόλια. Ο αλγόριθμος που εφαρμόζει, αναπτύχθηκε από την ομάδα FAIR του Facebook και φέρει την ονομασία DeepText, λόγω της τεχνικής βαθιά μάθησης και του κειμένου που διαβάζει.

8.2. Οι αλγόριθμοι ροών δεδομένων των Instagram και Facebook

Η εξαγορά της Instagram από την εταιρεία που διαθέτει την κοινωνική πλατφόρμα Facebook συνοδεύτηκε με κάποιες αλλαγές σχετικά με τον τρόπο που οι δύο εφαρμογές αξιοποιούν τα δεδομένα που λαμβάνουν και διακινούνται σε αυτές. Εντούτοις, Instagram και Facebook χαρακτηρίζονται από πολλές διαφορές ως προς τον τρόπο λειτουργίας. Χαρακτηριστικό είναι το παράδειγμα του αλγορίθμου ροών ειδήσεων που εφαρμόζει η κάθε εφαρμογή. Αν και οι δύο χρησιμοποιούν τον News Feed Algorithm – το Facebook από το 2006 και το Instagram από το 2016 – παρατηρούνται αρκετές διαφοροποιήσεις ως προς τη λειτουργία του που σχετίζεται ως επί το πλείστον με τη σημασία που αποδίδεται σε κάθε παράμετρο του συστήματος. Συνεπώς, οι παράμετροι που έχουν τεθεί από του ιθύνοντες κάθε εφαρμογής είναι και αυτές που επηρεάζουν τον τρόπο λειτουργίας του αλγορίθμου κάθε πλατφόρμας.

8.2.1. Ο αλγόριθμος του Facebook

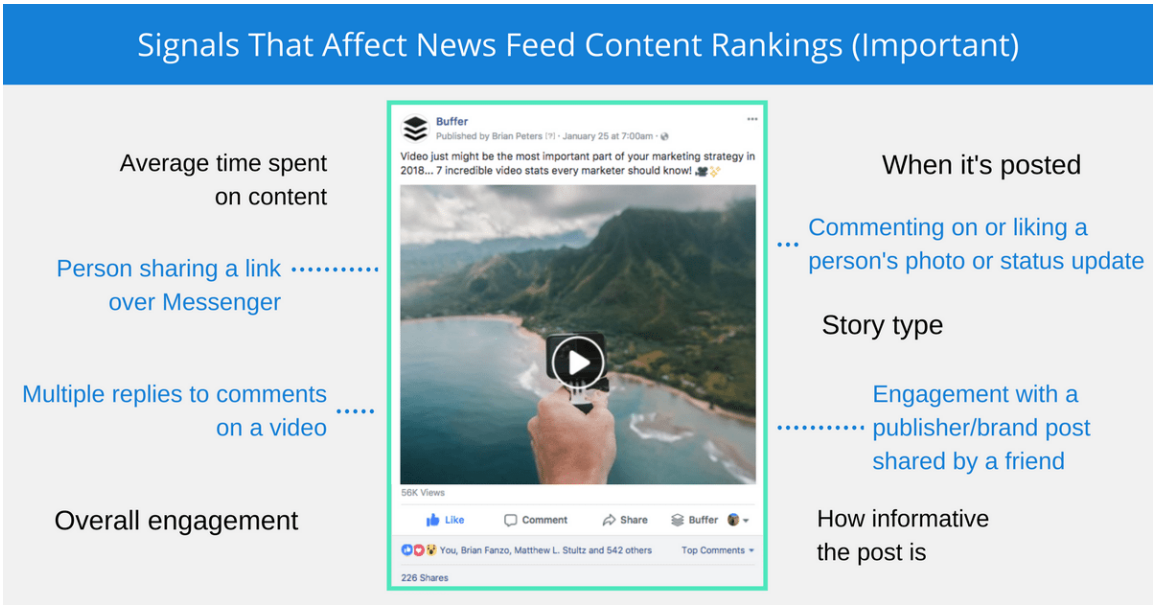
Τον Ιανουάριο του 2018 (11/1/2018) ο ιδρυτής της εταιρίας, Mark Zuckerberg, ανακοίνωσε τον νέο αλγόριθμο News Feed με τον οποίο θα λειτουργούσε εφεξής η πλατφόρμα κοινωνικής δικτύωσης, υιοθετώντας πιο

οικογενειακό προφίλ. Ο αλγόριθμος ευνοεί στις αναρτήσεις που προέρχονται από τους φίλους και την οικογένεια του χρήστη. Ταυτόχρονα υποβαθμίζονται οι δημοσιεύσεις που αφορούν επιχειρήσεις και μέσα μαζικής ενημέρωσης. Αφορμή στάθηκαν τα ολοένα και αυξανόμενα ποσοστά ψευδών ειδήσεων (fake news) που παρουσιάζονταν στην εφαρμογή. Οι ιθύνοντες προέβλεψαν, μάλιστα, τη μειωμένη παραμονή των χρηστών στην πλατφόρμα, όμως υποστήριξαν ότι ο χρόνο που θα διαθέτουν θα είναι πολυτιμότερος από ότι προηγουμένως διαβλέποντας μεγαλύτερα οφέλη στο μέλλον. Πάντως, όπως διαφαίνεται από τα μέχρι στιγμής στατιστικά στοιχεία οι χρήστες μείωσαν τη παραμονή τους στην εφαρμογή κατά 50 εκατ. ώρες ημερησίως.

Τα δεδομένα στο χώρο της τεχνολογία αλλάζουν συνεχώς, ανατρέποντας τα μέχρι πρότινος γνωστά. Το Facebook είναι ίσως το πιο γνωστό κοινωνικό δίκτυο, αφού περίπου το 1/5 του πλανήτη, δηλαδή σχεδόν 1,35 δισεκατομμύρια άνθρωποι παγκοσμίως, είναι χρήστες του. Το αξιοσημείωτο όμως εντοπίζεται στην επίδρασή του. Το Facebook διαχειρίζεται περίπου το 20% της διαδικτυακής κίνησης προς τις ειδησεογραφικές ιστοσελίδες. Η εφημερίδα New York Times παραλλήλισε τη σχέση δημοσιογραφίας και Facebook, με αυτή του Amazon και των εκδοτικών οίκων, οι οποίοι αν και διαφωνούν με την Amazon, επιθυμούν τα βιβλία τους να είναι διαθέσιμα προς πώληση από την εν λόγω εφαρμογή. Ομοίως, πολλοί δημοσιογράφοι και άνθρωποι του χώρου επικρίνουν το Facebook, ωστόσο οι πληθώρα αυτών το χρησιμοποιεί ως μέσο πληροφόρησης.

Ο αλγόριθμος που διαθέτει το Facebook και αποφασίζει το ποιες ειδήσεις και δημοσιεύσεις θα προβληθούν στον εκάστοτε χρήστη, επηρεάζει άμεσα τη προβολή και επισκεψιμότητα πολλών ιστοσελίδων ενημέρωσης. Έτσι, το κοινωνικό δίκτυο, αναβαθμίζεται καθορίζοντας τον τρόπο με τον οποίο οι άνθρωποι ενημερώνονται, καθώς και το περιεχόμενο αυτών, μέσω ενός αλγορίθμου που προβλέπει και πιθανολογεί το τι θα ήθελαν να διαβάσουν οι χρήστες. Κινούμενο στην ίδια λογική το Wired προέβλεψε ότι στο μέλλον το ειδησεογραφικό και μη περιεχόμενο δε θα κοινοποιείται τους χρήστες υπό τη μορφή συνδέσμων, αλλά απευθείας στα κοινωνικά δίκτυα. Τότε θα έχει ιδιαίτερο ενδιαφέρον η ανταπόκριση του κόσμου, το κατά πόσο δηλαδή οι χρήστες θα επιλέγουν ως αποκλειστική πηγή πληροφόρησης τις εν λόγω εφαρμογές.

Ο νέος αλγόριθμος δίνει προτεραιότητα στις λεγόμενες ενεργές αλληλεπιδράσεις, αφήνοντας σε δεύτερη μοίρα τις παθητικές, καθότι οι ιθύνοντες υποστηρίζουν ότι οι ενεργές αλληλεπιδράσεις είναι αυτές που συνδράμουν στην αύξηση του ποιοτικού χρόνου παραμονής. Σε αυτές συγκαταλέγονται ο σχολιασμός (commenting), η κοινή χρήση (sharing) και η διάδραση (reacting), ενώ τις παθητικές συνιστούν τα κλικ (clicking), η προβολή (watching) και η αιώρηση (viewing ή hovering). Οι ενέργειες που αποτελούν τις ενεργές αλληλεπιδράσεις αναφέρονται και ως signals δηλαδή σήματα.



Εικόνα 8.2.1 : Ο τρόπος που τα σήματα επηρεάζουν την θέση μίας δημοσίευσης Πηγή: https://blog.bufferapp.com/facebook-algorithm

Το σήμα, λοιπόν, στην κορυφή του αλγορίθμου ροών ειδήσεων είναι ο σχολιασμός. Ο σχολιασμός κάτω από μία ανάρτηση μπορεί να ανεβάσουν την ανάρτηση με αποτέλεσμα αυτή να εμφανιστεί πιο ψηλά στο σύνολο των ειδήσεων. Όπως σημείωσε και ο κ. Adam Mosseri, επικεφαλής της News Feed, «οι αναρτήσεις σελίδας που δημιουργούν συνομιλία μεταξύ ατόμων θα εμφανίζονται υψηλότερα στη ροή ειδήσεων. Για παράδειγμα, τα ζωντανά βίντεο συχνά οδηγούν σε συζήτηση μεταξύ των θεατών στο Facebook – στη πραγματικότητα τα ζωντανά βίντεο κατά μέσο όρο έχουν 6 φορές περισσότερες αλληλεπιδράσεις από τα συνηθισμένα βίντεο».

Το δεύτερο στη κατάταξη γραφήματος σήμα είναι η κοινή χρήση, δηλαδή ο διαμοιρασμός μίας δημοσίευσης. Αυτή μπορεί να γίνει ιδιωτικά ή δημόσια. Στη πρώτη περίπτωση ο χρήσης μοιράζεται μία δημοσίευση – που συχνά είναι σύνδεσμος – σε μία ιδιωτική συνομιλία στο Messenger, ενώ στη δεύτερη απλώς συμμετέχει σε μία δημοσίευση που κοινοποίησε προηγουμένως ένας φίλος του. Πρέπει να τονιστεί ότι το νέος αλγόριθμος δίνει ιδιαίτερη έμφαση στα post που κοινοποιήθηκαν και οδήγησαν σε συνομιλία μεταξύ των χρηστών. Εντούτοις, δεν είναι εφικτό όλοι οι χρήστες να προβούν στις παραπάνω ενέργειες, με αποτέλεσμα οι αντιδράσεις να αποτελούν το τρίτο σήμα του νέου αλγορίθμου. Έτσι, το περιεχόμενο κρίνεται (τριτογενώς) από τις αντιδράσεις που προκαλεί μία ανάρτηση, όπως είναι το like, ώστε να χαρακτηρισθεί ποιοτικό και να ανέλθει στις πρώτες θέσεις των ειδήσεων.

8.2.2 Ο αλγόριθμος του Instagram

Το 2018 η εταιρεία ανακοίνωσε την αναβάθμιση και τροποποίηση του αλγορίθμου τροφοδοσίας. Η νέα του έκδοση δίνει ιδιαίτερη βαρύτητα σε δύο κυρίως κριτήρια. Το πρώτο ονομάζεται engagement και όπως είναι φυσικό σχετίζεται με τη διάδραση. Κάτι που λίγοι γνωρίζουν είναι ότι τη στιγμή που ένας χρήστης αναρτά μία φωτογραφία του στην εφαρμογή, αυτή προβάλλεται σε ένα μικρό ποσοστό των ακολούθων του που συνήθως αντιστοιχεί στο 10% αυτού. Εν συνεχεία ο αλγόριθμος μπορεί να εμφανίσει την φωτογραφία σε περισσότερους ακολούθους, ανάλογα με την ανταπόκριση που θα έχει. Συνεπώς το κλειδί βρίσκεται στο τρόπο με τον οποίο δουλεύει ο αλγόριθμος.

Όπως αναφέρθηκε προηγουμένως η δημοσίευση μίας φωτογραφίας ή ενός βίντεο αρχικά προβάλλεται σε περιορισμένο αριθμό χρηστών. Σταδιακά ο αλγόριθμος καταμετρά το ρυθμό με το οποίο η δημοσίευση μαζεύει likes και σχόλια. Αν ο ρυθμός αυτός είναι μεγάλος, τότε ο αλγόριθμος θα την εμφανίσει σε περισσότερους ακολούθους, ενώ η συνεχώς αυξανόμενη διάδραση οδηγεί την ανάρτηση στη κορυφή της σελίδας τροφοδοσίας και κατά συνέπεια σε προσέγγιση ολοένα και περισσότερων ατόμων. Πιθανή είναι και η εμφάνιση της φωτογραφίας στις σελίδες του Chrome, Firefox κλπ. Αντιθέτως, αν η δημοσίευση δε στεφθεί από

επιτυχία, ο αλγόριθμος θα τη τοποθετήσει χαμηλότερα στη σελίδα τροφοδότησης με αποτέλεσμα να τη δουν λιγότεροι χρήστες.

Ένα ακόμα σημαντικό κεφάλαιο στο Instagram είναι τα λεγόμενα stories, δηλαδή οι ιστορίες που ανεβάζουν οι χρήστες και εμφανίζονται στη κορυφή της αρχικής σελίδας κάθε χρήστη. Ο αλγόριθμος μετρά τη διάδραση που δημιουργείται μέσω των ιστοριών. Έτσι, οι επόμενες δημοσιεύσεις ενός χρήστη έχουν περισσότερες πιθανότητες να εμφανιστούν στη ροή ειδήσεων ενός χρήστη που ανήρτησε μία ιστορία αν ο πρώτος τη σχολίασε ή τη κοινοποίησε, αν την είδε σε replay ή αν ψήφισε σε δημοσκόπηση που είχε προσθέσει ο δεύτερος στην ιστορία του.

Το δεύτερο κριτήριο συνιστά η σχέση (relationship) μεταξύ χρηστών. Για το καθορισμό της σχέσης μεταξύ δύο χρηστών, διακρίνονται πέντε παράγοντες, οι οποίοι καθορίζουν σε μεγάλο βαθμό τις αναρτήσεις που θα δει ο καθένας. Η πρώτη αφορά τη συχνότητα με την οποία ο χρήστης σχολιάζει ή εκδηλώνει την αγάπη του (like) προς τη δημοσίευση ενός συγκεκριμένου ατόμου. Τα likes και comments όμως αποτελούν και το δεύτερο παράγοντα, καθώς ο αλγόριθμος μετρά των αριθμό των likes και comments που λαμβάνει μία δημοσίευση. Ακολουθούν οι κοινοποιήσεις. Ο διαμοιρασμός μίας δημοσίευσης με κάποιο άλλο πρόσωπο υποδηλώνει την αρέσκεια του περιεχομένου. Έτσι ο αλγόριθμος θα ενημερώνει το χρήστη για παρόμοιες δημοσιεύσεις. Ο τέταρτος παράγοντας εντοπίζεται στις αναζητήσεις προφίλ, δηλαδή στα προφίλ που τείνει να αναζητά συχνότερα. Γεγονός που αποτελεί ένδειξη για τον αλγόριθμο ότι το άτομο θέλει να βλέπει τις δραστηριότητες του συγκεκριμένου χρήστη. Τέλος, τα ενδιαφέροντά του. Ο αλγόριθμος ελέγχει τα ενδιαφέροντα του χρήστη καθώς και το κατά πόσο έχει αλληλεπιδράσει με αυτά στο παρελθόν.

Επιπροσθέτως, ένα ακόμη σημαντικό κριτήριο για τον αλγόριθμο ροών ειδήσεων του Instagram είναι το timeliness ή αλλιώς η επικαιρότητα. Ο άνθρωπος ως επί το πλείστον ενδιαφέρεται για τα τρέχοντα γεγονότα και όχι για κάτι που έλαβαν χώρα σε παρελθόντα χρόνο. Έτσι ο αλγόριθμος πριμοδοτεί τις δημοσιεύσεις που αναρτήθηκαν πιο πρόσφατα, αυξάνοντας τη πιθανότητα τοποθέτησής τους σε υψηλότερη θέση στη ροή ειδήσεων.

9. Αλγόριθμοι Τεχνητής Νοημοσύνης

Στο εν λόγω κεφάλαιο παρουσιάζονται και αναλύονται δύο αλγόριθμοι τεχνητής νοημοσύνης, ένας κατανόησης κειμένου και ένας αναγνώρισης εικόνων, που είναι ιδιαιτέρως χρήσιμοι για την επίτευξη του σκοπού της παρούσας εργασίας, δηλαδή για την αντιμετώπιση των φαινομένων σεξουαλικού εκβιασμού τελούμενου στους κόλπους του διαδικτύου.

9.1. Ο αλγόριθμος DeepText της Facebook

Η ομάδα FAIR της Facebook, δημιούργησε έναν αλγόριθμο βαθέος νευρωνικού δικτύου με ικανότητα αναγνώρισης κοινόχρηστου κειμένου είτε αυτό αφορά περιεχόμενο δημοσίευσης είτε συνομιλιών. Ο αλγόριθμος διακρίνει και κατανοεί περισσότερες από είκοσι διαφορετικές γλώσσες με σχεδόν ανθρώπινη ακρίβεια. Το DeepText εκπαιδεύτηκε στο FBLearner Flow, μία μηχανή εκμάθησης της Facebook στη οποία εκπαιδεύονται τα περισσότερα μοντέλα της εταιρίας πριν προωθηθούν για χρήση. Ο αλγόριθμος βασίζεται στην ιδέα των Ronan Collobert και Yann LeCun σχετικά με τη βαθιά μάθηση. Προκειμένου να αντιληφθεί τη σημασιολογία της κάθε λέξης, ο αλγόριθμος χρησιμοποιεί τη τεχνική της βαθιάς μάθησης. Καθώς αδυνατεί να λειτουργήσει, όπως οι παραδοσιακοί επεξεργαστές φυσικής γλώσσας, ο αλγόριθμος συγκεντρώνει συνώνυμες ή λέξεις που σχετίζονται εννοιολογικά ώστε να αντιληφθεί με μεγαλύτερη ακρίβεια την ανθρώπινη συνομιλία.

Εικόνα 9.1: Ανάλυση φράσης με το DeepText. Πηγή: https://code.fb.com/core-data/introducing-deeptext-facebook-s-text-understanding-engine/

Ο DeepText σχεδιάστηκε ώστε να μιμείται τον τρόπο με τον οποίο το ανθρώπινο μυαλό αποκωδικοποιεί τη γλώσσα. Κάτι που για τον άνθρωπο είναι εξαιρετικά εύκολο, για τον υπολογιστή συνιστά πολύπλοκη διεργασία που απαιτεί πολλά στάδια. Κάθε λέξη έχει τη δική της σημασία, όμως η έννοια μπορεί να αλλάξει ανάλογα με τον τρόπο που χρησιμοποιείται η ίδια λέξη από το κάθε άνθρωπο. Οι άνθρωποι ερμηνεύουν τη λέξη σε σχέση με αυτές που τη περιβάλλουν, ώστε να εξάγουν συμπεράσματα. Με τον ίδιο τρόπο λειτουργεί και ο αλγόριθμος. Για παράδειγμα, το επίθετο λευκός, μπορεί να συνδυαστεί με διάφορα ουσιαστικά και να διαφοροποιεί το νόημά του, όπως λευκός πύργος, λευκό πουκάμισο, λευκό τοπίο, εμπόριο λευκής σαρκός κ.ά. Ο αλγόριθμος είναι σε θέση να συνδυάζει τις λέξεις μίας φράσης και να εξάγει τα δικά του συμπεράσματα, ώστε όπου είναι εφικτό να βοηθά το χρήστη (Abdulkader et al., 2016). Στη πρώτη περίπτωση, λόγου χάρη, ο χρήστης πιθανόν να θέλει να επισκεπτεί το λευκό πύργο, στη δεύτερη να αγοράσει ένα λευκό πουκάμισο, στη τρίτη να αναπολεί μία χιονισμένη ημέρα και στη τέταρτη να αναφέρεται σε εγκληματική δραστηριότητα. Επομένως, απαιτείται εκμάθηση του υπολογιστή ώστε να κατανοεί πολύπλοκες εκφράσεις, όπως ο ανθρώπινος νους.

Προκείμενου να προσεγγίσουν τέτοιες διεργασίες, οι αλγόριθμοι εφαρμόζουν αρχιτεκτονικές βαθέων νευρωνικών δικτύων, όπως τα συνελικτικά και επαναλαμβανόμενα νευρωνικά δίκτυα. Επίσης, είναι σε θέση να εκτελεί εκμάθηση

τόσο σε επίπεδο λέξεων όσο και χαρακτήρων. Προκειμένου να εκπαιδευτεί ο αλγόριθμος *χρησιμοποιούνται τα εργαλεία FbLearner Flow και Torch,* που αποτελούν επίσης συστήματα της εταιρίας. Ο DeepText παρέχει τη δυνατότητα δημιουργίας νέων μοντέλων μέσω της self-serve αρχιτεκτονικής που διαθέτει.

Η κατανόηση κειμένου απαιτεί την εκτέλεση διαφόρων διεργασιών μεταξύ των οποίων η γενική ταξινόμηση, μέσω της οποίας προσδιορίζεται αφενός το θέμα του post και αφετέρου οι υπόλοιπες οντότητες που σχετίζονται με αυτό και λοιπές σημαντικές πληροφορίες. Έστω μία ανάρτηση για τη διεξαγωγή σεμιναρίου. Το θέμα του post είναι η διεξαγωγή σεμιναρίου, ενώ η τοποθεσία, οι εισηγητές, τα επιμέρους θέματα ή ενότητες και ότι περιγράφει το θέμα αφορούν τις υπόλοιπες οντότητες (Abdulkader, 2016). Παρόλη την αναφορά στη βαθιά μάθηση, δεν έχει οριστεί ο λόγος για τον οποίο χρησιμοποιείται η τεχνική. Η απάντηση είναι πολύ απλή και έγκειται στην αδυναμία εύρεσης λύσης με τις παραδοσιακές τεχνικές NLP, καθώς οι προκλήσεις που καλείται - πρέπει να αντιμετωπίσει το σύστημα είναι πολλές και αφορούν τόσο την ποσότητα των δεδομένων(ετικέτες) όσο και τον αριθμό των γλωσσών που χρησιμοποιούνται στην εν λόγω εφαρμογή. Έτσι ο αλγόριθμος εξελίσσει την αρχική ιδέα των Ronan Collobert και Yann LeCun όπως αυτή διατυπώθηκε στο έγγραφό τους.

Το Facebook αποτελεί μία παγκόσμια εφαρμογή, που σημαίνει ότι άνθρωποι κάθε εθνικότητας βρίσκονται σε αυτό και μιλούν την μητρική τους γλώσσα, με αποτέλεσμα ο αλγόριθμος να πρέπει να αναγνωρίσει και κατανοήσει όσο το δυνατό καλύτερα και γρηγορότερα τη κάθε γλώσσα. Οι τεχνικές NLP βασίζονται στη γνώση που προέρχεται από τη γλώσσα μέσω πολύπλοκης τεχνολογίας, για τη διεξαγωγή της οποίας απαιτείται εκτεταμένη λογική επεξεργασίας. Σε αρκετές γλώσσες, οι άνθρωποι τείνουν να χρησιμοποιούν διάφορες διαλέκτους, όπως η επαγγελματική και το slang ή αλλιώς αργκό, ενώ δε λείπουν και τα διάφορα ορθογραφικά μέσα που βοηθούν στη παραγωγή του ίδιου συμπεράσματος. Επομένως, ο αλγόριθμος πρέπει να κατανοεί το νόημα κάθε φράσης είτε αυτή ακολουθεί τη κανονική μορφή και σύνταξη μίας γλώσσας είτε κάποια από τις διαλέκτους της. Επομένως, η βαθιά μάθηση κρίνεται απαραίτητη καθώς μπορεί να περιορίσει το βαθμό γνώσης κάθε γλώσσας μέσω τη εκμάθησης αυτής από το ίδιο το κείμενο είτε με κάποια ελάχιστη προεπεξεργασία είτε χωρίς. Έτσι διασχίζονται περισσότερες γλώσσες σε μικρότερο χρονικό διάστημα.

Σύμφωνα με τις παραδοσιακές τεχνικές NLP, κάθε λέξη μετατρέπεται σε μορφή κατανοητή προς τον αλγόριθμο. Για παράδειγμα η λέξη «κυρία» μπορεί να αναπαρασταθεί ως ο ακέραιος 8987, ενώ η συντομογραφία της «κα» να είναι ένας άλλος ακέραιος 879988. Η τήρηση αυτής της τεχνικής προϋποθέτει την σύνταξη κάθε λέξης κειμένου στα δεδομένα εκπαίδευσης με σωστή ορθογραφία. Στον αντίποδα, η βαθιά μάθηση εφαρμόζει τις λεγόμενες «word embeddings» ώστε να διατηρεί τη σημασιολογική σχέση των λέξεων. Στο προηγούμενο παράδειγμα, οι δύο λέξεις βρίσκονται σε κοντινή απόσταση, υποδηλώνοντας την εννοιολογική συσχέτιση των λέξεων. Με αυτό τον τρόπο το σύστημα κατανοεί το βαθύτερο νόημα των λέξεων. Η ίδια τεχνική χρησιμοποιείται και για τη κατανόηση φράσεων που χαρακτηρίζονται από κοινή σημασιολογία και διαφορετική γλώσσα.

Στη περίπτωση του Instagram, ο αλγόριθμος ξεκίνησε να χρησιμοποιείται ως λύση στην αντιμετώπιση των spam μηνυμάτων, όμως σύντομα η απόδοσή του οδήγησε στην εφαρμογή του σε ένα πιο περίπλοκο πρόβλημα που στόχευε στην *εξάλειψη* των σχολίων που παραβίαζαν τις Κοινοτικές Οδηγίες[11] της εταιρίας. Όπως και στη περίπτωση του spam ορίστηκε μία ομάδα ατόμων, ώστε να εξετάσει το περιεχόμενο των κειμένων. Τα μέλη της ομάδας έπρεπε να ελέγξουν κάθε σχόλιο ως προς τη καταλληλότητα του περιεχομένου. Όταν διαπιστωνόταν ακατάλληλο περιεχόμενο, ταξινομούνταν *σε μία κατηγορία verboten συμπεριφοράς* και η οποία υποδήλωνε περιπτώσεις ρατσισμού, (σεξουαλικής) παρενόχλησης και εκφοβισμού. Μέχρι στιγμής έχουν ελεγχθεί δύο εκατομμύρια σχόλια τουλάχιστον δύο φορές, με τις μηχανές να βαθμολογούν το κάθε σχόλιο σε μία κλίμακα εμπιστοσύνης 0-1, ως προς την ύπαρξη *προσβλητικού ή ακατάλληλου περιεχομένου*. Αν η βαθμολογία ενός σχολίου ξεπεράσει ένα συγκεκριμένο όριο, αυτό βαθμολογείται με zapped. Οι παράγοντες που επηρεάζουν τη βαθμολογία είναι η σημασιολογική ανάλυση του κειμένου, το ιστορικό του commenter (σχολιαστή) και η σχέση του με τον poster (χρήστης που ανήρτησε το κείμενο). Δηλαδή, ένα *σχόλιο που προέρχεται από άτομο που δεν γνωρίζει ο χρήστης, έχει περισσότερες πιθανότητες να βαθμολογηθεί άσχημα από ένα σχόλιο φίλου*. Πρέπει να τονιστεί ότι το προσβλητικό περιεχόμενο, όταν εντοπιστεί, εξαφανίζεται, με εξαίρεση το περιβάλλον του δράστη, όπου το μήνυμα

[11] Η εταιρία σε αντίστοιχη δημοσίευσή της εξέδωσε ένα έντυπο 1200 λέξεων, στο οποίο προέτρεπε τους χρήστες της εφαρμογής να ακολουθούν τους κανόνες ορθής συμπεριφοράς, όπως να σέβονται τους υπόλοιπους χρήστες, να είναι ευγενικοί, να μην αναρτούν γυμνές φωτογραφίες κ.ά.

συνεχίζει να υφίσταται. Με τον τρόπο αυτό η εταιρία επιθυμεί να δυσχεραίνει το έργο των επιτήδειων.

9.2. Ο αλγόριθμος Deep ConvNet

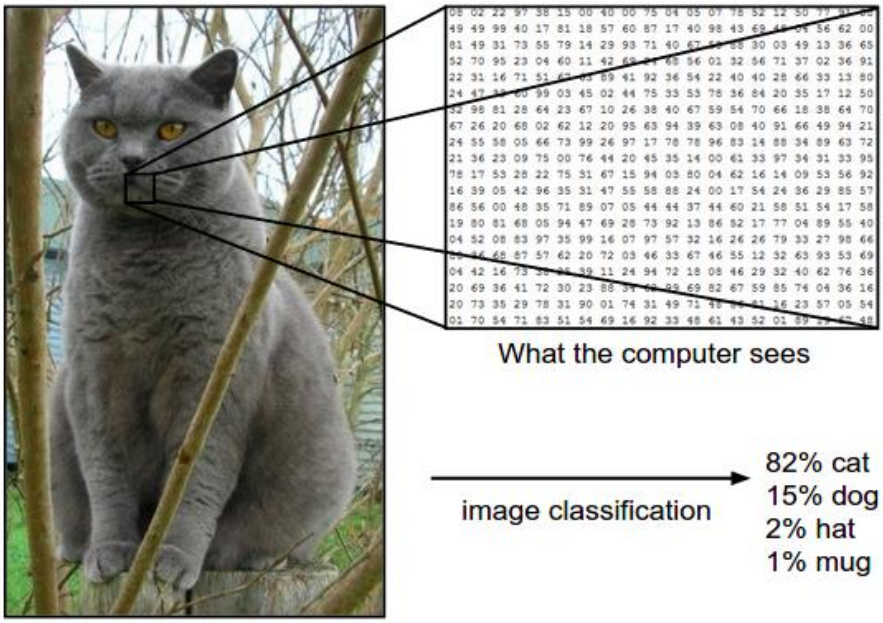
Πρόκειται για ένα σύστημα αναγνώρισης εικόνων που αναπτύχθηκε από την ομάδα FAIR του Facebook με σκοπό την αναγνώριση των εικόνων που αναρτούν οι χρήστες είτε στην ίδια εφαρμογή είτε σε κάποια άλλη εφαρμογή της εταιρίας. Κάθε ανάρτηση συνοδεύεται από tags, δηλαδή ετικέτες. Σε αυτές προστίθενται αυτόματα άλλες ετικέτες (alt tags), αντιπροσωπευτικές του περιεχομένου της εικόνας. Κάθε ετικέτα προστίθεται αυτομάτως στα big data της εταιρίας, αυξάνοντας τις γνώσεις και κατ'επέκταση τη δύναμή της. Ο αλγόριθμος βασίζεται στην αρχιτεκτονική των συνελικτικών νευρωνικών δικτύων (convolutional neural networks) στο εξής CNN, δηλαδή βαθιών νευρωνικών δικτύων ικανών να αναλύσουν μία εικόνα.

9.2.1. Συνεργατικά Νευρωνικά Δίκτυα - Convolutional Neural Networks

Η κατανόηση της λειτουργίας των CNN απαιτεί τη κατανόηση του τρόπου κατά τον οποίο ένα παιδί μαθαίνει να αναγνωρίζει τα αντικείμενα του περιβάλλοντος. Όταν βλέπει μία εικόνα προσπαθεί να την ερμηνεύσει αναλύοντας τα επιμέρους τμήματά της, τις περισσότερες φορές υποσυνείδητα. Αρχικά βλέπει, επισημαίνει και στη συνέχεια προβαίνει σε προβλέψεις για να αναγνωρίσει τελικά τα πρότυπα. Το σύστημα που επιτρέπει την κατανόηση του περιβάλλοντος είναι η συνεργασία ματιών και εγκεφάλου, καθώς στο πρώτο οφείλεται η όραση και στο δεύτερο η ερμηνεία. Με την ίδια λογική εργάζονται και τα εν λόγω δίκτυα (LeCun, 2015). Προς διευκόλυνση εφαρμόζεται ένας αλγόριθμος με πάρα πολλές εικόνες που δρουν ως παραδείγματα, ώστε να μπορεί να προβλέψει εικόνες που δεν έχει ξαναδεί.

Σε αντίθεση με τον άνθρωπο ο υπολογιστής δεν αντιλαμβάνεται λέξεις και εικόνες, παρά μόνο αριθμούς. Για τον κόσμο του κάθε εικόνα αναπαρίσταται ως μία διαφορετική εικονοστοιχεία, δηλαδή μία δισδιάστατη συστοιχία αριθμών. Οι

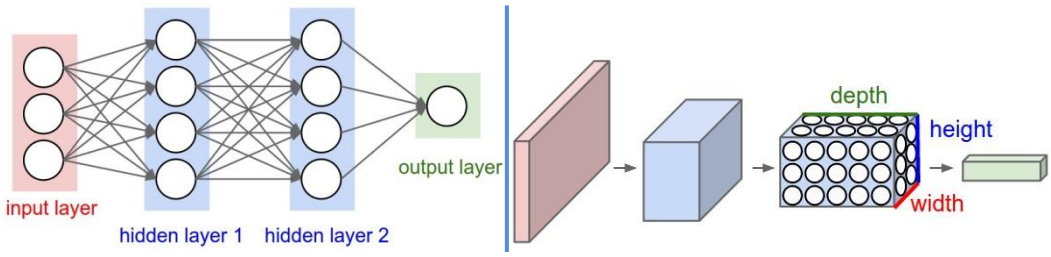
επιστήμονες κλήθηκαν να αναπαραστήσουν την εικόνα σε μία άλλη μορφή κατανοητή προς τον υπολογιστή. Έτσι, προκειμένου να διδάξουν έναν αλγόριθμο ικανό να αναγνωρίζει τις εικόνες που δέχεται ως είσοδο, χρησιμοποίησαν ένα είδος νευρωνικών δικτύων που ονομάστηκε συνεργατικό ή συνελικτικό.



Εικόνα 9.2.1.1: Ο τρόπος που ο υπολογιστής βλέπει και διαβάζει μία εικόνα. Πηγή: http://cs231n.github.io/convolutional-networks/

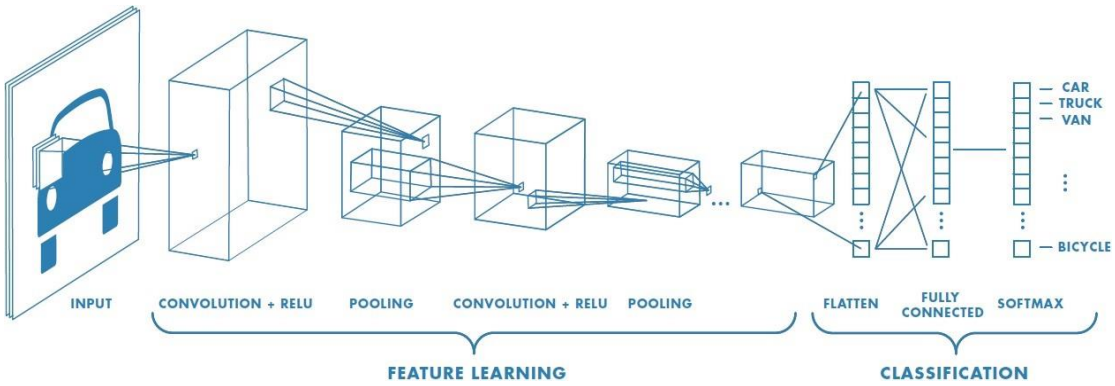
Τα CNN παρουσιάζουν αποκλείσεις ως προς την αρχιτεκτονική τους από τα κλασικά νευρωνικά δίκτυα. Τα κανονικά νευρωνικά δίκτυα μετασχηματίζουν μία είσοδο μέσω μίας σειράς κρυφών επιπέδων. Κάθε επίπεδο αποτελείται από ένα σύνολο νευρώνων. Κάθε επίπεδο του νευρώνα συνδέεται πλήρως με όλους τους νευρώνες του προηγούμενου επιπέδου, ενώ στο επίπεδο εξόδου, δηλαδή στο τελευταίο πλήρως συνδεδεμένο επίπεδο, αντιστοιχούν οι προβλέψεις.

Στον αντίποδα, τα επίπεδα στα CNN είναι οργανωμένα σε τρεις διαστάσεις, πλάτος, ύψος και βάθος (LeCun, 2015). Σε αντίθεση με τα κανονικά νευρωνικά δίκτυα, οι νευρώνες κάθε επιπέδου στα συνεργατικά νευρωνικά δίκτυα δε συνδέονται με όλους τους νευρώνες του επόμενου επιπέδου, αλλά με ένα μέρος αυτών. Τέλος, το δίκτυο θα παράγει έξοδο πιθανότητας ενός διανύσματος, οργανωμένη κατά μήκος της διάστασης βάθους.



Εικόνα 9.2.1.2: Δεξιά: Αρχιτεκτονική κανονικών Νευρωνικών Δικτύων τριών επιπέδων. Αριστερά: Διάταξη Συνεργατικών Νευρωνικών Δικτύων. Πηγή: http://cs231n.github.io/convolutional-networks/

Τα CNN διακρίνονται από δύο τμήματα. Το τμήμα κρυφών επιπέδων ή εξαγωγής χαρακτηριστικών και το τμήμα ταξινόμησης. Η εικόνα που έπεται παρακάτω συνιστά αναπαράσταση των τμημάτων και των επιμέρους επιπέδων των εν λόγω συνεργατικών νευρωνικών δικτύων.

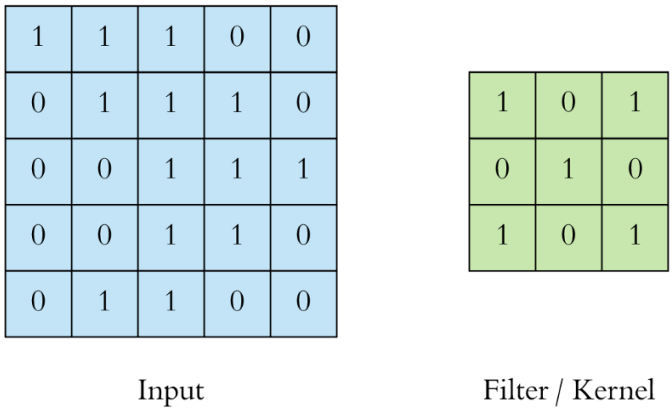


Εικόνα 9.2.1.3: Αναπαράσταση της αρχιτεκτονικής των Συνεργατικών Νευρωνικών Δικτύων. Πηγή: https://medium.com/@RaghavPrabhu/understanding-of-convolutional-neural-network-cnn-deep-learning-99760835f148

Τμήμα εξαγωγής χαρακτηριστικών

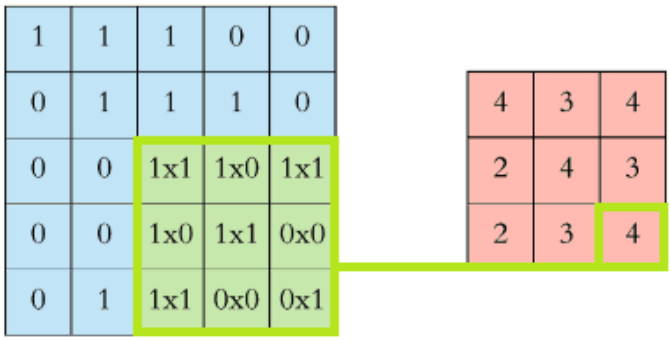
Το τμήμα είναι υπεύθυνο για τον εντοπισμό των χαρακτηριστικών μίας εικόνας, μέσω μίας σειράς συνελίξεων και συγκεντρώσεων. Ο όρος convolution δηλαδή συνέλιξη που χαρακτηρίζει τα CNN αναφέρεται σε μία μαθηματική

διαδικασία, ένα ολοκλήρωμα, που επιτρέπει τη σύνδεση δύο λειτουργιών για τη παραγωγή μίας τρίτης λειτουργίας. Στο παράδειγμα που ακολουθεί, η διαδικασία εφαρμόζεται στα δεδομένα εισόδου με τη χρήση ενός φίλτρου (ή αλλιώς πυρήνα) ώστε να παραχθεί ένας χάρτης χαρακτηριστικών, πρακτικά ένας νέος πινάκας μικρότερων διαστάσεων.



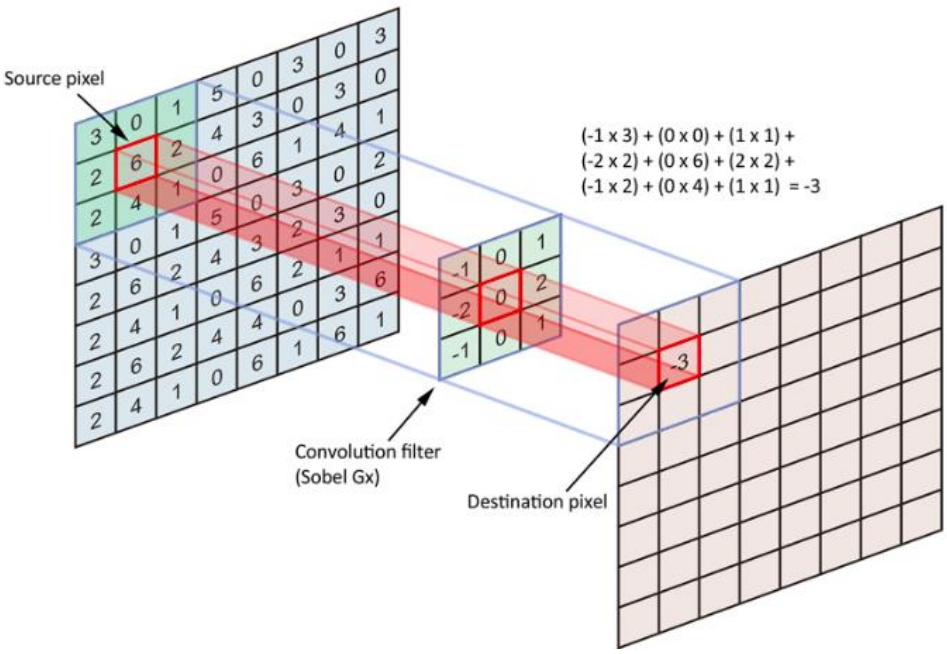
Εικόνα 9.2.1.4: Είσοδος και φίλτρο νευρωνικού δικτύου. . Πηγή: https://towardsdatascience.com/applied-deep-learning-part-4-convolutional-neural-networks-584bc134c1e2

Το φίλτρο μετακινείται πάνω από κάθε είσοδο του νευρώνα εκτελώντας μία περιέλιξη. Σε κάθε είσοδο πραγματοποιείται ένας πολλαπλασιασμός μήτρας, το αποτέλεσμα του οποίου προστίθεται στο χάρτη χαρακτηριστικών.



Εικόνα 9.2.1.5: Περιέλιξη φίλτρου στην είσοδο και προσθήκη αποτελέσματος στο χάρτη χαρακτηριστικών. Πηγή: https://towardsdatascience.com/applied-deep-learning-part-4-convolutional-neural-networks-584bc134c1e2

Στη πραγματικότητα, λόγω των τριών διαστάσεων η λειτουργία διαφέρει από την παραπάνω εικόνα. Η πραγματική λειτουργία περιγράφεται στην εικόνα που ακολουθεί παρακάτω.



Εικόνα 9.2.1.6: Περιέλιξη φίλτρου στις τιμές εισόδου για τη δημιουργία εξόδου στο επόμενο επίπεδο, σε μορφή τριών διαστάσεων. Πηγή: https://towardsdatascience.com/applied-deep-learning-part-4-convolutional-neural-networks-584bc134c1e2

Οι τέσσερις πυλώνες που αφορούν τα CNN και οφείλεται να καθοριστούν πριν τη λειτουργία του είναι το μέγεθος και ο αριθμός των φίλτρων, το μέγεθος του βήματος και τέλος το padding, ή αλλιώς η προσθήκη μηδενικών στην είσοδο.Στις εισόδους εκτελούνται πολλές συνελίξεις, με διαφορετικό φίλτρο για κάθε λειτουργία. Έτσι παράγονται διαφορετικοί χάρτες χαρακτηριστικών, οι οποίοι αποτελούν την τελική έξοδο του επιπέδου συνέλιξης. Στη συνέχεια, η έξοδος αυτή *εισέρχεται* στη λειτουργία ενεργοποίησης, ώστε το αποτέλεσμα να είναι μη γραμμικό. Στην εικόνα που έπεται η λειτουργία είναι η ReLU. Με τον όρο *stride* αναφέρεται το μέγεθος του βήματος με βάση το οποίο μετατοπίζεται το φίλτρο συνέλιξης. Αυτό συνήθως ισούται με τη μονάδα, για να είναι σε θέση να «διαβάσει» ένα-ένα τα pixels της εικόνας. Η αύξηση του βήματος, συνεπάγεται μεγαλύτερα διάστημα στη μετακίνηση του φίλτρου συνέλιξης και επομένως λιγότερη επικάλυψη των pixels.

Στη δημιουργία του χάρτη χαρακτηριστικών χρησιμοποιείται το λεγόμενο padding, δηλαδή ένα επίπεδο εικονοστοιχείων μηδενικής τιμής που προσθέτει μηδενικά στην είσοδο. Η διαδικασία επιτρέπει τη διατήρηση μεγέθους του χάρτη χαρακτηριστικών[12].

Συνήθως, το επίπεδο συνέλιξης ακολουθείται από το pooling layer, επίπεδο συγκέντρωσης. Εξαιτίας αυτού του επιπέδου μειώνεται σταδιακά η καταχώρηση σε διαστάσεις (διαστασιολόγηση) και κατά συνέπεια το πλήθος των παραμέτρων και ο υπολογισμός τους στο δίκτυο. Η διαδικασία μεταξύ άλλων στοχεύει στη ταχύτερη εκπαίδευση του νευρωνικού δικτύου καθώς και στην αποτροπή υπερφόρτωσης. Ως επί το πλείστων, στα CNN εκτελείται η μέγιστη συγκέντρωση, δηλαδή το max pooling, λαμβάνοντας τη μεγαλύτερη τιμή κάθε θέσης.

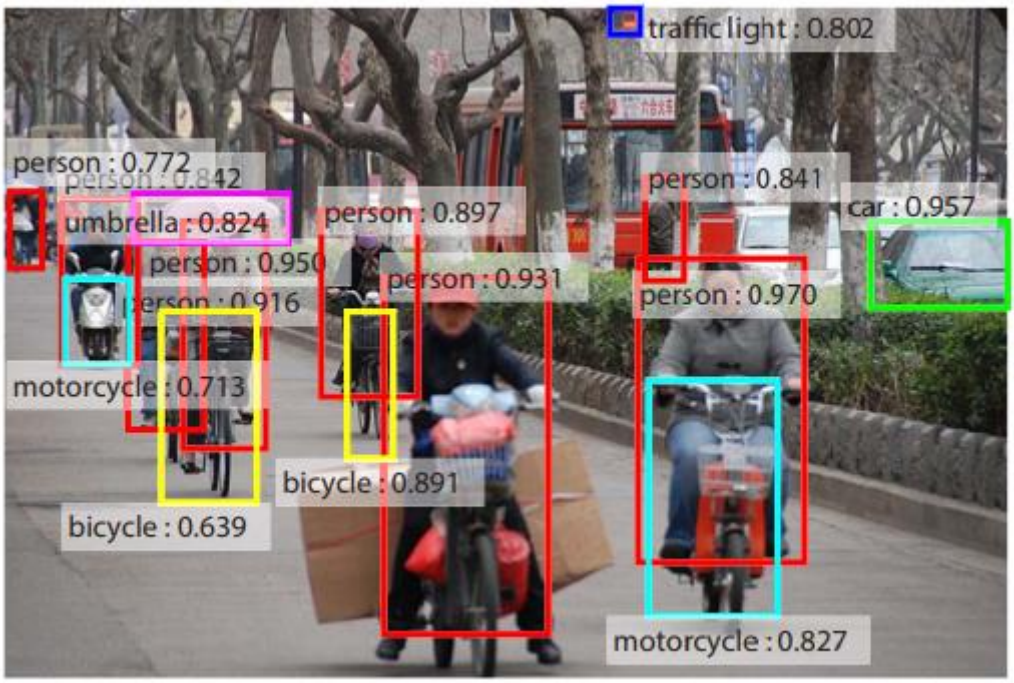
Τμήμα ταξινόμησης

Με την ολοκλήρωση του τμήματος εξαγωγής χαρακτηριστικών, το δίκτυο περνά στο τμήμα ταξινόμησης, αποτελούμενο από πλήρως συνδεδεμένα επίπεδα ταξινομεί τα εξαγόμενα χαρακτηριστικά του προηγούμενου τμήματος δίνοντας μία πιθανότητα στο υπό εξέταση αντικείμενο της εικόνας να ταυτίζεται με το αντικείμενο που προέβλεψε ο αλγόριθμος αναγνώρισης εικόνων.

[12] Ο χάρτης χαρακτηριστικών έχει πάντα μικρότερο μέγεθος από την είσοδο.

Σε αυτό όλα τα δεδομένα τριών διαστάσεων (3D) πρέπει να μετατραπούν σε δεδομένα μίας διάστασης (1D), καθότι τα επίπεδα αυτού του τμήματος δέχονται δεδομένα μόνο μίας διάστασης. Έπειτα, η διαδικασία ολοκληρώνεται με την ανάθεση πιθανοτήτων για κάθε περίπτωση.

Όπως είχε διατυπωθεί προηγουμένως, τα τελευταία επίπεδα του CNN είναι πλήρως συνδεδεμένα. Αυτό σημαίνει ότι οι νευρώνες κάθε επιπέδου έχουν πλήρη σύνδεση με όλες τις ενεργοποιήσεις του προηγούμενου επιπέδου. Αυτό το τμήμα των CNN ακολουθεί την αρχιτεκτονική των κανονικών νευρωνικών δικτύων.



Εικόνα 9.2.1.7: Παράδειγμα αποτελέσματος Συνεργατικού Νευρωνικού Δικτύου Πηγή: https://arxiv.org/pdf/1506.01497v3.pdf

Εκπαίδευση Συνεργατικών Νευρωνικών Δικτύων

Όσον αφορά την εκπαίδευση των συνεργατικών νευρωνικών δικτύων, αυτή ταυτίζεται με την εκπαίδευση των κανονικών νευρωνικών δικτύων. Χρησιμοποιείται η τεχνική του backpropagation ή αλλιώς όπως ονομάζεται στα ελληνικά της οπισθοδιάδοσης. Όπως είναι αναμενόμενο, η τεχνική χαρακτηρίζεται από μεγαλύτερη μαθηματική πολυπλοκότητα, στη περίπτωση των CNN, καθώς σε αυτά εσωκλείονται

οι διάφορες διαδικασίες συνέλιξης, κάτι που δε συμβαίνει στα υπόλοιπα νευρωνικά δίκτυα.

10. Προτεινόμενο Σχήμα

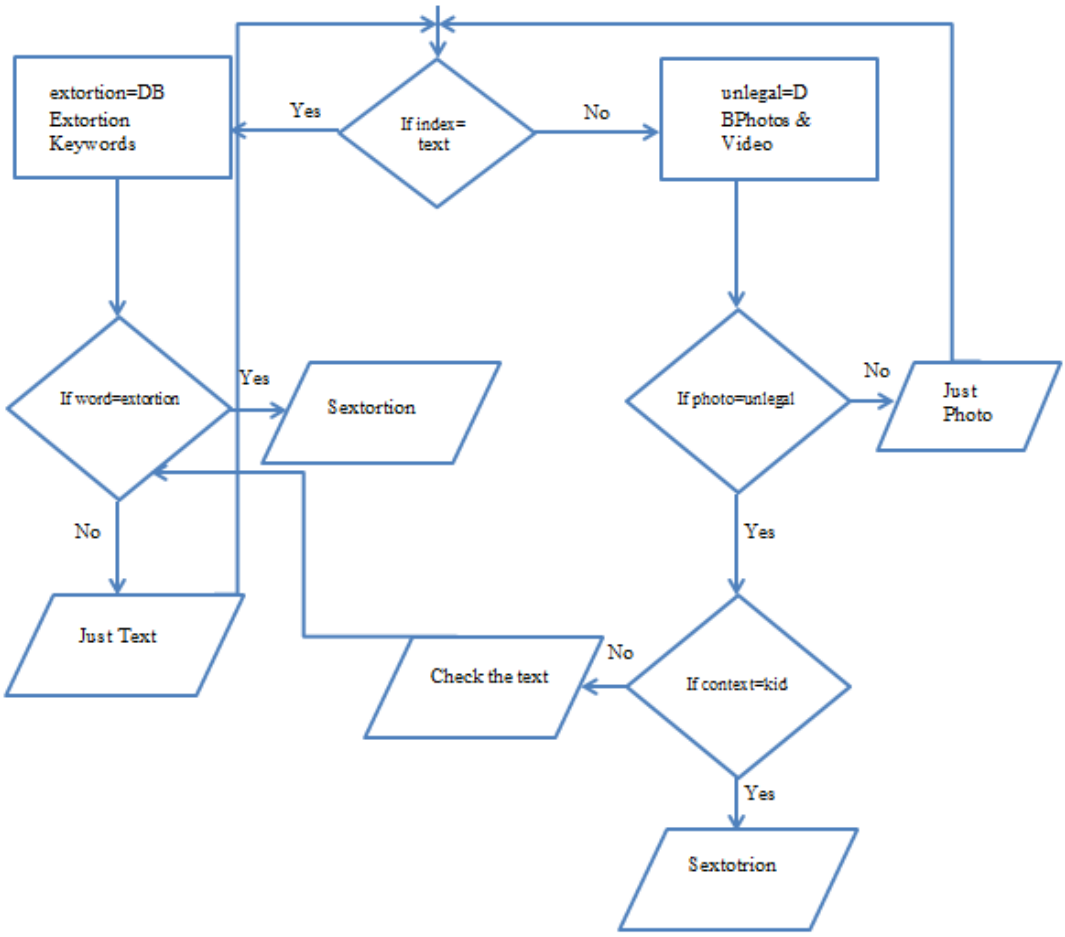
Στο παρόν κεφάλαιο θα παρουσιαστεί ο προτεινόμενος αλγόριθμος που στοχεύει στην προσπάθεια για δραστική αντιμετώπιση του φαινομένου του σεξουαλικού διαδικτυακού εξαναγκασμού και εκβιασμού.

Η επίταση του προβλήματος του σεξουαλικού διαδικτυακού εξαναγκασμού και εκβιασμού οδηγεί στην ανάγκη εύρεση λύσης, ώστε να εξαλειφθούν ή τουλάχιστον να αμβλυνθούν τέτοια γεγονότα. Λαμβάνοντας υπ'όψιν τα ανωτέρω στοιχεία που αναλύθηκαν στα προηγούμενα κεφάλαια (σς. Κεφάλαια 7 έως 9) η εύρεση ενός αλγορίθμου που θα χρησιμοποιείται της εφαρμογές που τείνουν να εκμεταλλεύονται οι επιτήδειοι ώστε να «ψαρεύουν» τα υποψήφια θύματά τους είναι επιβεβλημένη.

Ο αλγόριθμος βασίζεται στη λογική των αλγορίθμων τεχνητής νοημοσύνης. Πράγμα που σημαίνει ότι χαρακτηρίζεται από απλή αρχιτεκτονική με πολλές όμως παραμέτρους, τις οποίες και καθορίζει ο ίδιος. Προκειμένου να υλοποιήσει το αρχικό πρόβλημα, ο αλγόριθμος το διασπά σε μικρότερα υποπροβλήματα τα οποία και προσπαθεί να λύσει. Για να επιτευχθεί αυτό, καλεί άλλους αλγορίθμους που θα λύσουν τα επιμέρους προβλήματα, ώστε να οδηγηθεί στη λύση του αρχικού. Όπως και κάθε αλγόριθμος τεχνητής νοημοσύνης, τροφοδοτείται από πάρα πολλά παραδείγματα της νοητικής διεργασίας που καλείται να επιλύσει και με δεδομένα αυτά επιλέγει τις εκάστοτε παραμέτρους. Για τα δεδομένα της εργασίας ο αλγόριθμος τροφοδοτείται με παραδείγματα σεξουαλικού διαδικτυακού εξαναγκασμού και εκβιασμού. Τα παραδείγματα λαμβάνονται από το τεράστιο ηλεκτρονικό αποτύπωμα που αφήνει ο κάθε χρήστης το οποίο βρίσκεται διασκορπισμένο στο παγκόσμιο ιστό. Για την αποθήκευση των παραδειγμάτων χρειάζονται δύο βάσεις δεδομένων. Η πρώτη θα περιέχει οπτικοακουστικό υλικό άσεμνου ή προκλητικού περιεχομένου και η δεύτερη φράσεις και λέξεις – κλειδιά που υποδηλώνουν απειλή ή εκβιασμό προς

τον αποδέκτη. Για την ανάλυση των κειμένων, ο αλγόριθμος, καλεί τον αλγόριθμος τεχνητής νοημοσύνης που ανέπτυξε η ομάδα FAIR του Facebook, ενώ για την ανάλυση των εικόνων καλούνται τα συνεργατικά νευρωνικά δίκτυα.

Επιδιωκόμενος στόχος είναι η αξιοποίηση του αλγορίθμου από τις τεχνολογίες που συνιστούν στόχο των δραστών, όπως τα μέσα κοινωνικής δικτύωσης, τα εικονικά δωμάτια επικοινωνίας, τα διαδικτυακά παιχνίδια ακόμη και τα κινητά τηλέφωνα.



Εικόνα 10.1: Διάγραμμα ροής προτεινόμενου αλγορίθμου

Ο αλγόριθμος δέχεται σαν είσοδο ένα στοιχείο και ελέγχει αν αυτό είναι κείμενο ή οπτικοακουστικό μέσο. Για την πρώτη περίπτωση καλείται ο αλγόριθμος αναγνώρισης κειμένου που αναλύθηκε σε προηγούμενο κεφάλαιο. Για το σκοπό αυτό

χρησιμοποιείται και η αντίστοιχη βάση δεδομένων που παρέχει τα παραδείγματα εκβίασης με τα οποία τροφοδοτείται ο αλγόριθμος αναγνώρισης κειμένου ώστε να παρέχει τα κατάλληλα αποτελέσματα. Αν διαπιστωθεί ότι η μεταβλητή που δέχθηκε ως είσοδο ο αλγόριθμος αντιστοιχεί σε απειλή ή εκβιασμό, τότε το σύστημα αναφέρει την εν λόγω συνομιλία για σεξουαλικό εκβιασμό, αλλιώς περίπτωση καταγράφεται ως απλό κείμενο.

Όμως, στη περίπτωση που ο αλγόριθμος δέχεται ως είσοδο ένα οπτικοακουστικό υλικό, εικόνα ή βίντεο, αυτό ελέγχεται ως προς τη νομιμότητά του σύμφωνα με τα παραδείγματα που χρησιμοποιήθηκαν ώστε να εκπαιδευτεί ο αλγόριθμος και τα οποία περιέχονται στη δεύτερη βάση δεδομένων για παράνομο οπτικοακουστικό μέσο. Επομένως, αν το υλικό αναγνωριστεί ως νόμιμο ο αλγόριθμος επιστρέφει στην αρχή καθώς θεωρείται ότι είναι μία απλή εικόνα, αντίθετα αν ταυτοποιηθεί το παράνομο περιεχόμενο, ελέγχεται σε δεύτερο στάδιο η ηλικιακή ομάδα ένταξης του ανθρώπου που παρουσιάζεται σε αυτό. Αν ο άνθρωπος που απεικονίζεται είναι ανήλικος, ο αλγόριθμος τερματίζει αναφέροντας τη συνομιλία, καθώς παρόλο που δεν στοιχειοθετεί απαραίτητα το έγκλημα του σεξουαλικό διαδικτυακού εξαναγκασμού και εκβιασμού, τελείται το ιδιαίτερα σοβαρό αδίκημα της παιδικής πορνογραφίας,. Από τη άλλη, αν ο άνθρωπος αναγνωρίζεται ως ενήλικας, το σύστημα συνεχίζει την έρευνα μελετώντας τα κείμενα που ανταλλάσσονται στη αντίστοιχη συνομιλία, καλώντας τον αλγόριθμο κατανόησης κειμένου.

Επίλογος

Η καθημερινότητα κατακλύζεται από πολλές ειδήσεις και πολλά γεγονότα που συχνά προκαλούν την κοινή γνώμη. Τα μέσα μαζικής ενημέρωσης προβάλλουν ολοένα και περισσότερο εγκληματικές ενέργειες που σχετίζονται με τη γενετήσια και προσωπική ελευθερία των ανθρώπων. Τα περιστατικά παράνομων σεξουαλικών δράσεων πληθαίνουν με τον σεξουαλικό διαδικτυακό εξαναγκασμό και εκβιασμό να κατέχει σημαντική δράση, δίχως την ανάλογη αντιμετώπιση. Τα θύματα ως επί το πλείστον αρνούνται να καταγγείλουν το περιστατικό κυρίως λόγω φόβου για τη επίπτωση που μπορεί να έχει η πράξη τους, αλλά και ντροπής προς την οικογένεια και το γενικότερο κοινωνικό σύνολο με αποτέλεσμα την ενίσχυση του εγκλήματος. Καθώς η άνθιση αυτού οφείλεται στη εκτεταμένη και πολλές φορές αλόγιστη χρήση του διαδικτύου και δει των μέσων κοινωνικής δικτύωσης, η λύση στο πρόβλημα πρέπει να είναι κυρίως τεχνική. Εφαρμογές, όπως το Instagram, κινούνται προς αυτή την οδό, όμως χρειάζεται κάτι πιο δραστικό. Μία κοινή γραμμή. Στην εργασία προτάθηκε η δημιουργία ενός αλγορίθμου με βάση τη τεχνητή νοημοσύνη που θα αξιοποιηθεί από τις τεχνολογίες – ιανούς τέτοιων παράνομων ενεργειών. Εξ' ίσου χρήσιμη μπορεί να φανεί η ταυτοποίηση υποψήφιων χρηστών μίας πλατφόρμας κοινωνικής δικτύωσης ή εφαρμογής προτού την είσοδο σε αυτή. Η ταυτοποίηση μπορεί να γίνει με την επίδειξη ενός κρατικού εγγράφου ή κάποιου άλλου δεδομένου που θα λειτουργεί ως διαπιστευτήριο για την ορθότητα των λεγομένων του χρήστη, τουλάχιστον σε ότι αφορά την ταυτότητά του. Αρκετοί ίσως εκφράσουν τους ενδοιασμούς τους, καθώς αυτό πιθανόν να έρχεται σε σύγκρουση με την προστασία των προσωπικών δεδομένων του ατόμου, όμως πρέπει να γίνει στάθμιση των αγαθών ώστε να παρθεί η κατάλληλη απόφαση. Είναι πιο σημαντική η διασφάλιση των προσωπικών δεδομένων ή της γενετήσιας ελευθερίας και αξιοπρέπειας του ατόμου; Συνεπώς μέσω αυτής της ερώτησης δηλώνεται η αρωγή της νομικής επιστήμης. Αν η απάντηση στο παραπάνω ερώτημα συνηγορεί υπέρ της γενετήσιας ελευθερίας και αξιοπρέπειας του ανθρώπου τότε το νομικό οπλοστάσιο κάθε χώρα πρέπει να

ενισχυθεί θεσπίζοντας νέες ειδικές διατάξεις που θα καλύπτουν τις διάφορες μορφές του ηλεκτρονικού εγκλήματος.

Κατά καιρούς, η Ελλάδα, κλήθηκε να εναρμονιστεί με τις τεχνολογικές εξελίξεις ενισχύοντας το νομικό πλαίσιο της χώρας με νόμους και ειδικές διατάξεις για το κυβερνοέγκλημα. Ωστόσο πληροφορική και νομική συνιστούν δύο επιστήμες με διαφορετικούς ρυθμούς ανάπτυξης. Παρά τις προσπάθειες της νομικής να ακολουθήσει τις ραγδαίες εξελίξεις στο χώρο της πληροφορικής και τεχνολογίας, χρειάζεται ακόμα πολύς δρόμος ειδικότερα αν συνυπολογιστεί η σύγκλιση μεγάλων δεδομένων και τεχνητής νοημοσύνης.

Η ανάπτυξη της τεχνητής νοημοσύνης επέφερε νέα δεδομένα στο χώρο των επιστημών, ενώ συνάμα αποτέλεσε θέμα συζήτησης τόσο στην επιστημονική και ακαδημαϊκή κοινότητα όσο και στις καθημερινές συνομιλίες των ανθρώπων. Αφορμή πιθανόν στάθηκε το Παγκόσμιο Οικονομικό Forum του Νταβός, το 2016, όταν ακούστηκε για πρώτη φορά ο όρος «4^{η} Βιομηχανική Επανάσταση» με πολλούς να τον υιοθετούν και χρησιμοποιούν ακόμη και σήμερα. Ωστόσο κανείς δεν αναρωτήθηκε για ποιο λόγο αποδόθηκε αυτή η έννοια στο εν λόγω φαινόμενο της εποχής. Χαρακτηριστικό κάθε βιομηχανικής επαναστάσεως που προηγήθηκε ήταν η υιοθέτηση μίας νέας ανακάλυψης στο χώρο της τεχνολογίας. Έτσι η πρώτη βιομηχανική επανάσταση βασίστηκε στον ατμό, η δεύτερη στον ηλεκτρισμό και η τρίτη στην πληροφορική. Αν προσπαθήσει κανείς να αναγνωρίσει τη νέα τεχνολογία στην οποία βασίζεται η τέταρτη βιομηχανική επανάσταση θα αποτύχει, καθώς αυτή δε περιλαμβάνει κάποια νέα τεχνολογία αλλά ένα σύμπλεγμα ήδη υπαρχουσών τεχνολογιών. Συνεπώς ο λόγος για τον οποίο γίνεται δεκτή ως βιομηχανική επανάσταση δεν είναι η ύπαρξη μίας καινούργιας τεχνολογίας που αναμένεται να αλλάξει άρδην τον κόσμο, αλλά η από κοινού ανάπτυξη πολλών τεχνολογιών, όπως το διαδίκτυο, η βιντεοτεχνολογία, η ρομποτική, τα μεγάλα δεδομένα, το διαδίκτυο των πραγμάτων κ.ά. που επιταχύνουν τις εξελίξεις δημιουργώντας αλλαγές οι οποίες προκαλούν ανασφάλεια και φόβο στο κοινωνικό σύνολο. Η τεχνολογία - συνιστώσα που προκαλεί τη μεγαλύτερη ανησυχία είναι η τεχνητή νοημοσύνη.

Δεκάδες ερωτήσεις γεννήθηκαν από τα πρώτα κιόλας βήματα της τεχνητής νοημοσύνης, όταν ακόμη αυτή βρισκόταν σε θεωρητικό επίπεδο. Μπορούν να ενεργήσουν ευφυώς οι μηχανές; Μπορούν πράγματι να σκεφτούν; Μπορούν να

αισθανθούν; Μήπως πρέπει να σταματήσει η προσπάθεια δημιουργίας τέτοιων τεχνουργημάτων; Ποιοι είναι οι ηθικοί κίνδυνοι ανάπτυξης τεχνητής νοημοσύνης; Είναι μόνο κάποια από τα ερωτήματα που διατυπώθηκαν πολλά χρόνια πριν συνεχίζοντας όμως να βασανίζουν τις σκέψεις και των σημερινών ανθρώπων. Ασφαλώς η απάντηση σε αυτά είναι εξαιρετικά δύσκολη υπόθεση, καθώς πολλοί ήταν αυτοί που προσπάθησαν να αποκριθούν δίνοντας τις δικές τους προσεγγίσεις, ωστόσο μη τυγχάνοντας ευρείας αποδοχής. Στο ερώτημα περί ισχυρής τεχνητής νοημοσύνης, δηλαδή «αν πράγματι οι μηχανές μπορούν να σκεφτούν» προσπάθησε να απαντήσει ο Alan Turing, καθώς πρόκειται για μία ερώτηση που συνδέθηκε με τη ομώνυμη δοκιμασία του. Η απάντηση του ίδιου δόθηκε μέσω μίας ομιλία του Geoffrey Jefferson το 1949 σύμφωνα με τον οποίο «Μόνο όταν μία μηχανή θα γράψει ένα σονέτο ή θα συνθέσει ένα κονσέρτο λόγω των σκέψεων και των συναισθημάτων που νιώθει και όχι μέσω μίας τυχαίας καταγραφής συμβόλων, θα μπορέσουμε να συμφωνήσουμε ότι η μηχανή είναι ίση με τον εγκέφαλο. Με άλλα λόγια όχι όταν απλώς γράψει κάτι, αλλά και όταν γνωρίζει ότι το έγραψε». Με αυτή τη παράθεση ο Turing ήθελε να περάσει στους ανθρώπους τον τρόπο με τον οποίο ο ίδιος θεωρούσε τη τεχνητή νοημοσύνη. Χρειάστηκε μάλιστα να τοποθετηθεί και για την υπόθεση ύπαρξης μηχανών με συναίσθηση, θεωρώντας την το ίδιο ατυχή με την ερώτηση περί σκέψεως των μηχανών. Ανάγοντας το ερώτημα στην πραγματική ζωή, διαπιστώνει κανείς ότι κατά τη συνομιλία δύο ανθρώπων είναι σχεδόν αδύνατο να κατανοήσει ο ένας *τις εσωτερικές νοητικές καταστάσεις* του άλλου (Russell & Norvig, 2005). Συνεπώς, μπορεί η επικοινωνία με έναν «χαζό» άνθρωπο να στεφθεί με επιτυχία, ενώ με ένα ευφυή με αποτυχία. Ωστόσο η απάντηση του Turing δόθηκε και πάλι μέσω μίας απλής υπόθεσης «Αντί να διαφωνούμε συνεχώς για το θέμα αυτό, είναι σύνηθες να υιοθετούμε την *ευγενική σύμβαση* ότι όλοι σκέφτονται». Ωστόσο δεν παρέλειψε να απαντήσει και στο ερώτημα σχετικά με την ύπαρξη ή όχι συναίσθησης. Ο ίδιος αν και το θεωρεί ένα δύσκολο θέμα, υποστηρίζει ότι δεν έχει άμεση σχέση με την εφαρμογή της τεχνητής νοημοσύνης. Πράγματι η όλη προσπάθεια σχετίζεται με τη δημιουργία τεχνουργημάτων ικανών να συμπεριφέρονται κατά έξυπνο τρόπο. Όμως, τουλάχιστον σε αυτό το στάδιο, δεν ενδιαφέρει η προέλευση αυτής της ευφυούς συμπεριφοράς, δηλαδή αν είναι κάτι που πηγάζει όντως από την ίδια τη «μηχανή» ή πρόκειται απλώς για προσομοίωση σκέψης.

Η τεχνητή νοημοσύνη συνιστά μία τεχνολογία που όπως και κάθε άλλη έχει διττό χαρακτήρα. Μπορεί να χρησιμοποιηθεί με διαφόρους τρόπους. Η διαφορά αυτή της τεχνολογίας με τις άλλες είναι ότι αυτή σκέφτεται με κάποιον τρόπο, είτε απλό είτε πιο σύνθετο. Επομένως, οι κίνδυνοι που ελλοχεύουν από αυτή φαντάζουν πιο επικίνδυνοι. Ένα από τα θέματα που προκύπτουν από την πρόοδο της τεχνητής νοημοσύνης είναι σχετίζεται με την αξιοπιστία της. Η τεχνητή νοημοσύνη χαρακτηρίζεται από αυτοαναφορικότητα. Επομένως, τα δεδομένα εκπαίδευσης καθορίζουν εν πολλοίς το έργο που θα παράγει η τεχνητή νοημοσύνη. Αν τα δεδομένα είναι ελλιπή ή μη αντιπροσωπευτικά του δείγματος, η τεχνητή νοημοσύνη θα είναι αναξιόπιστη. Προς το παρόν αυτό σημαίνει ότι θα παράγει λανθασμένο ή μη επιτυχημένο έργο που ίσως προκαλεί γέλιο, ωστόσο όσο η επιστήμη προχωρά τα αποτελέσματα αυτής ίσως είναι πιο σημαντικά και εφιστούν την προσοχή του ανθρώπου. Τα δεδομένα που χρησιμοποιούνται για να εκπαιδεύσουν τη τεχνητή νοημοσύνη λαμβάνονται από το διαδίκτυο και πιο συγκεκριμένα από το τεράστιο ηλεκτρονικό αποτύπωμα του ανθρώπου. Επομένως, προκύπτουν θέματα ιδιωτικότητας.

Η τεχνητή νοημοσύνη μετρά αρκετούς πολέμιους, οι οποίοι εκτός από τη δυνατότητα ανάπτυξής της αναρωτιούνται και για το αν όντως πρέπει να προχωρήσει αυτό το έργο. Οι κίνδυνοι που ελλοχεύει η ραγδαία εξέλιξη της τεχνητής νοημοσύνης υπερβαίνουν συχνά τα κλασσικά ζητήματα που αντιμετωπίζουν οι μηχανικοί στη διάρκεια κατασκευής του έργου τους. Κίνδυνος απώλειας απορρήτου και μοναδικότητος του ανθρωπίνου είδους, αύξηση των ποσοστών ανεργίας, άπλετος ή ελάχιστος ελεύθερος χρόνος, ανεύθυνη χρήση συστημάτων τεχνητής νοημοσύνης, απειλή ανθρώπινου είδους είναι κάποια από τα ζητήματα που καλούνται να αντιμετωπίσουν και προβλέψουν οι επιστήμονες και μηχανικοί στην προσπάθεια εξέλιξης της τεχνητής νοημοσύνης. Ας προσπαθήσουμε όμως να μελετήσουμε όμως κάποια από τα πιο σημαντικά θέματα ξεχωριστά. Κατά τον Louis Brandeis (1890) «το ιδιωτικό απόρρητο είναι το πλέον περιεκτικό από όλα τα δικαιώματα… είναι το δικαίωμα του ατόμου στην προσωπικότητά του». Με αυτό συμφωνούν εκατοντάδες νομικοί υποστηρίζοντας μάλιστα ότι μέσω της τεχνητής νοημοσύνης επαπειλούνται κάποια από τα δικαιώματα απορρήτου του ατόμου. Για παράδειγμα, προκειμένου να αναπτυχθεί όσο το δυνατόν καλύτερα ένα νέο σύστημα, μπορεί να αξιοποιηθούν προσωπικά δεδομένα. Χαρακτηριστικό είναι το παράδειγμα της τεχνολογίας

αναγνώρισης ομιλίας, για την καλύτερη ανάπτυξη της οποίας είναι πιθανή η υποκλοπή διαλέξεων. Ωστόσο σε ένα κόσμο που καθένας δίνει απλόχερα πληροφορίες και δεδομένα για τη προσωπική του ζωή, η έννοια του απορρήτου είναι αμφιλεγόμενη κυρίως στο χώρο του διαδικτύου. Σύμφωνα με τον Scott McNealy, άλλωστε «Ούτως ή άλλως δεν έχετε ιδιωτική ζωή. Ξεπεράστε το αυτό», όμως αυτό μένει να αποδειχθεί.

Από τη 3^{η} Βιομηχανική Επανάσταση κι έπειτα ο κλάδος της βιομηχανίας έχει αλλάξει, με τα μηχανήματα να αντιγράφουν την ανθρώπινη δραστηριότητα αντικαθιστώντας πολλά από τα τότε επαγγέλματα. Εντούτοις, οι άνθρωποι απορροφήθηκαν σε νέες θέσεις εργασίας ίσως πιο ενδιαφέρουσες και υψηλότερα αμειβόμενες. Γιατί να μην συμβεί το ίδιο και με τα νέα τεχνουργήματα που παράγει η τεχνητή νοημοσύνη; Άλλωστε στόχος της είναι η προσφορά βοήθειας στον άνθρωπο. Μπορεί άραγε αυτή η προσφορά να μειώσει στο ελάχιστο το χρόνο εργασίας του ατόμου και αν ναι πόσο διαχειρίσιμο είναι αυτό από το ίδιο; Πράγματι οι ώρες εργασίας μειώθηκαν στο μισό κατά τον 19^{ο} αιώνα (Toffler, 1970), όμως μέχρι σήμερα αυτό παραμένει σταθερό ή τουλάχιστον δεν έχει μειωθεί σε τέτοιο βαθμό που ο άνθρωπος σταματά να παράγει έργο. Αντίθετα, για τους εργαζομένους στο κλάδο των βιομηχανιών τα νέα συστήματα επιφύλαξαν αλλαγές στο ωράριο εργασίας, καθώς πρέπει να δουλεύουν περισσότερο ώστε να συμβαδίσουν με τα νέα δεδομένα (Russell & Norvig, 2005). Οι περισσότερες εργατοώρες συνεπάγονται αύξηση μισθού, δηλαδή αύξηση εισοδήματος.

Τέλος ένα από τα ζητήματα που θα λάβει μεγαλύτερη έκταση εξαιτίας της ανάπτυξης της τεχνητής νοημοσύνης είναι ο λεγόμενος ψηφιακός αναλφαβητισμός. Ήδη διαπιστώνονται σημαντικές διακυμάνσεις ως προς τα ποσοστά ψηφιακού αλφαβητισμού. Η τεχνολογία και τα συστήματα που την υπηρετούν δεν είναι εύκολα διαχειρίσιμα από όλους τους ανθρώπους. Για παράδειγμα, οι άνθρωποι μεγαλύτερης ηλικίας δυσκολεύονται να χρησιμοποιήσουν προϊόντα νέας τεχνολογίας, ακόμα και τους κλασικούς πλέον υπολογιστές. Τα «μαραφέτια», όπως συχνά τείνουν να αποκαλούν, αποτελούν κάτι καινούργιου για τα δικά τους δεδομένα που απαιτεί πολλή δουλειά και θέληση τόσο από τους ίδιους όσο και από τα άτομα που θα κληθούν να τους τα μάθουν. Ως αποτέλεσμα, η πλειονότητα των μεγαλυτέρων ανθρώπων θεωρεί αδύνατη την ενασχόληση με αυτά, γεγονός που οδηγεί στον

ηλεκτρονικό και συνάμα κοινωνικό αποκλεισμό τους. Το φαινόμενο αναμένεται να λάβει μεγαλύτερες διαστάσεις με την ανάπτυξη της τεχνητής νοημοσύνης. Οι άνθρωποι θα πρέπει, εκτός από τη εκμάθηση των υπολογιστών και του διαδικτύου, να καταβάλλουν ιδιαίτερη προσπάθεια ώστε να κατανοήσουν τη νέα επιστήμη που θα κατακλύσει τη καθημερινότητά τους. Γεγονός που αυτή τη φορά θα αφορά και τους νεότερους, αν δεν θέλουν να παραγκωνιστούν. Ιδιαίτερη προσοχή απαιτείται και από τις υποανάπτυκτες και κάποιες αναπτυσσόμενες χώρες, καθώς η εξέλιξη της τεχνητής νοημοσύνης ίσως επισύρει τον πολιτιστικό και όχι μόνο αφανισμό τους. Η συσπείρωση δύναμης στα χέρια καπιταλιστικών και αυταρχικών κρατών ενδέχεται να προκαλέσει την αλλαγή κρατών που δεν προέβλεψαν σωστά την εξέλιξη της τεχνητής νοημοσύνης και το προνόμιο που αυτή μπορεί να δώσει σε όποιον φρόντισε να την κατέχει.

Τον κατάλογο τον κινδύνων συμπληρώνουν τα ηθικά διλήμματα που καλείται αντιμετωπίσει η ίδια η τεχνητή νοημοσύνη. Κλασικό είναι το παράδειγμα των αυτό-οδηγούμενων οχημάτων και η απόφαση που θα λάβουν στη περίπτωση αναπόφευκτου ατυχήματος. Κάθε αλγόριθμος σε μία περίπτωση διλήμματος αναλαμβάνει να πάρει μία απόφαση θέτοντας κάποιον σε προτεραιότητα και κάποιον άλλο ως δεύτερη ή τρίτη επιλογή. Κανείς δε μπορεί να απαντήσει όμως ποια είναι η σωστή και ποια η λάθος επιλογή. Πόσο μάλλον μία μηχανή.

Η μεγαλύτερη ανησυχία σχετικά με τη τεχνητή νοημοσύνη αφορά το μέλλον της ανθρωπότητας. Τα The Terminators, The Matrix, Metropolis, Ex Machina, Frankenstein, R.U.R κ.ά αποτελούν μερικά από τα έργα που παρουσίασαν την αρνητική διάσταση της τεχνητής νοημοσύνης με τα ρομπότ κατακτούν τον κόσμο. Ωστόσο, την ίδια άποψη εκφράζουν πέρα από τους συγγραφείς και σεναριογράφους κάποιες από τις σημαντικότερες προσωπικότητες. Όμως πόσο εφικτό είναι αυτό; ο καθηγητής Κωνσταντίνος Δασκαλάκης έσωσε τρία πιθανά σενάρια για την πρόοδο της τεχνητής νοημοσύνης και το μέλλον της ανθρωπότητας, ονομάζοντάς τα Wonderland, Pessiland και Stagnatia, δηλαδή το Αισιόδοξο σενάριο, το Απαισιόδοξο και το Τέλμα.

Το πρώτο σενάριο αποτελεί και τη πιο αισιόδοξη προοπτική, όπου επιστήμη και τεχνολογία κατακτούν τη γενική τεχνητή νοημοσύνη. Τα ρομπότ επαυξάνουν τις δυνατότητες των ανθρώπων, αναλαμβάνοντας τις χειρωνακτικές και μερικές από τις

πνευματικές εργασίες. Σε αυτό το σενάριο, ρομπότ και άνθρωποι συνυπάρχουν αρμονικά. Το βιοτικό επίπεδο ανεβαίνει, η κοινωνική ανισότητα μειώνεται, το ασφαλιστικό σύστημα σώζεται και ενισχύεται η παγκόσμια ειρήνη.

Στο δεύτερο σενάριο, πραγματοποιούνται τα όσο διαδραματίζονται στις κινηματογραφικές ταινίες. Επιστήμη και τεχνολογία κατακτούν και πάλι τη γενική τεχνητή νοημοσύνη, αυτή τη φορά προς όφελος καπιταλιστών και κυβερνήσεων, οι οποίοι και την κρατούν κρυφή για ιδίων όφελος και ιμπεριαλιστική επιβολή. Τα ρομπότ κυριαρχούν των ανθρώπων υποδουλώνοντάς τους και παραβιάζοντας την ιδιωτικότητά τους, ενώ υποκαθιστούν και την πνευματικότητά τους.

Το τρίτο και τελευταίο σενάριο, μοιάζει και το πιο πιθανό τουλάχιστον σε βάθος πέντε με δέκα ετών. Η γενική τεχνητή νοημοσύνη παραμένει ένα άπιαστο όνειρο. Συνεχώς περισσότερες ειδικές εφαρμογές τεχνητής νοημοσύνης εμφανίζονται στην επικαιρότητα, ενώ καπιταλιστές και κυβερνήσεις ετοιμάζονται (παίρνουν θέση) για το τέλος του «παιχνιδιού» (endgame) που θα μοιάζει είτε με το απαισιόδοξο είτε με το αισιόδοξο σενάριο και αυτό έγκειται στον τρόπο με τον οποίο ο άνθρωπος θα χειριστεί την τεχνολογία.

Καθώς πολλοί αναρωτιούνται σχετικά με τα θετικά και αρνητικά της τεχνητής νοημοσύνης, αλλά και με τις επιπτώσεις που ενδέχεται να έχει στη κοινωνική ισορροπία είναι εξαιρετικά σημαντική η κατανόηση της φύσης ενός τέτοιου τεχνουργήματος. Στη προσπάθεια διασαφήνισης της τεχνητής νοημοσύνης, ο Κωνσταντίνος Δασκαλάκης, τη παρομοίασε με ένα μωρό. Κάθε άνθρωπος, είπε, ερχόμενος στο κόσμο έχει εκ γενετής κάποια γενετικά χαρακτηριστικά, όχι όμως και δομημένο χαρακτήρα. Υπεύθυνοι για αυτό, δηλαδή για την προσωπικότητά του, είναι οι γονείς του. Από αυτούς δέχεται τα όποια ερεθίσματα και στόχους με τους οποίους αναμένεται να πορευθεί στην υπόλοιπη ζωή του. Έτσι ακριβώς συμβαίνει και με την τεχνητή νοημοσύνη. Πρόκειται για ένα μωρό που θα ενσωματωθεί στο πραγματικό κόσμο, αλληλεπιδρώντας με αυτόν. Όπως οι γονείς αποτελούν πρότυπο για τα παιδιά τους, οι άνθρωποι με τους οποίους θα αλληλεπιδράσει το σύστημα τεχνητής νοημοσύνης θα του δώσουν τα δεδομένα με τα οποία θα πορευτεί. Συνεπώς, οι θέσεις που περιέχουν τα δεδομένα θα υιοθετηθούν από το σύστημα. Αν τα δεδομένα περιέχουν ρατσιστικές προκαταλήψεις, είναι σχεδόν σίγουρο ότι αυτό θα προάγει και η τεχνητή νοημοσύνη. Επομένως, εν πολλοίς ο άνθρωπος είναι υπεύθυνος για την

εικόνα που προβάλλει προς τα έξω είτε μέσω της εξωτερικής του εμφάνισης και της κίνησής του στο χώρο είτε μέσω των ιδεολογιών και λεγομένων του, δηλαδή των δεδομένων που αφήνει καθημερινά στο διαδίκτυο και τα οποία θα αποτελέσουν τροφή σκέψης και συμπεριφοράς για τα εν γένει δημιουργήματα τεχνητής νοημοσύνης.

Η πλειονότητα των επιστημόνων αναλώνεται στην ανάπτυξη της τεχνητής νοημοσύνης χωρίς να εξετάζει την επίδραση της εκάστοτε δραστηριότητάς τους. Ένα ερώτημα που οφείλει να θέσει ο κάθε επιστήμονας στον εαυτό του κατά την διαδικασία ανάπτυξης της πρότασής τους σχετίζεται με τις όποιες συνέπειες που θα σημάνει η επιτυχής ολοκλήρωση του έργου τους. Άλλωστε, όπως υποστήριξε ο Alan Turing στην αντίστοιχη εργασία του μπορούμε να δούμε μόνο λίγο μπροστά, όμως μπορούμε να καταλάβουμε ότι πρέπει να γίνουν πολλά ακόμα, γεγονός που σίγουρα ακόμα ισχύει.

Κλείνοντας την εργασία αξίζει να επισημανθεί ότι όπως με κάθε νέα τεχνολογία έτσι και για την τεχνητή νοημοσύνη είναι δύσκολο έως και αδύνατο να ανακόψει κάποιος τη εξέλιξή της, ωστόσο μπορεί να της δώσει τη κατεύθυνση που επιθυμεί ή τουλάχιστον αυτή που θεωρεί ορθότερη. Όποιος πιστεύει ότι μπορεί να σταματήσει ένα ποτάμι που ρέει, μάλλον δεν έχει υπολογίσει σωστά την ορμή του. Ακόμα κι αν προσπαθήσει να κατασκευάσει φράγματα για να ανακόψει την πορεία του κάποια στιγμή το ποτάμι θα φουσκώσει ξεπερνώντας το εμπόδιο. Ο μοναδικός τρόπος με τον οποίο ο άνθρωπος δύναται να ελέγξει το ποτάμι είναι να το οδηγήσει προς εκεί που ο ίδιος θέλει. Σκεφτείτε τώρα ότι το ποτάμι είναι η τεχνητή νοημοσύνη. Ο άνθρωπος καλώς ή κακός δε μπορεί να σταματήσει την εξέλιξή της, όμως μπορεί να της δείξει το δρόμο κατευθύνοντάς την προς το σημείο που αυτός επιθυμεί. Μερικοί επιλέγουν να δουν την απαισιόδοξη οδό, ενώ κάποιοι άλλοι την αισιόδοξη. Κατά τις τρέχουσες ενδείξεις, η τεχνητή νοημοσύνη φαίνεται να ακολουθεί τη πορεία προηγούμενων τεχνολογιών, όπως τα κινητά τηλέφωνα, το διαδίκτυο, στα οποία τα αρνητικά χαρακτηριστικά αντισταθμίζονται με τα θετικά (Russell & Norvig, 2005). Το μόνο σίγουρο είναι ότι υπεύθυνος για την όποια πορεία τη τεχνητής νοημοσύνης είναι ο άνθρωπος.

Βιβλιογραφία

Διβράμης, Γιάννης., 2015. Deep Web – Το Ίντερνετ Που Δε Βλέπει η Google. *PAPARAMARKETING.GR* Διαθέσιμο στη: https://paramarketing.gr/deep-web-internet-vlepei-google/ [Πρόσβαση 9 Οκτωβρίου 2018]

Σπαθή, Θεώνη., 2017. Dark Web: Το Σκοτεινό Διαδίκτυο. *Crime Times.* [Online] Ιούλιος (3), Διαθέσιμο στη: http://www.crimetimes.gr/dark-web-το-σκοτεινό-διαδίκτυο/ [Πρόσβαση 9 Οκτωβρίου 2018]

Abdulkader, A., Lakshmiratan, A. & Zhang, J. (2016) Introducing DeepText: Facebook's text understanding engine. AI Resaerch. Διαθέσιμο στο: https://code.fb.com/core-data/introducing-deeptext-facebook-s-text-understanding-engine/

Anwar, A. & Syed, I. H. (2017) Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *IJCIR.* 13(5), 883-889 Διαθέσιμο στο: http://www.ripublication.com/ijcir17/ijcirv13n5_19.pdf

Arief, B., Adzmi, M. A. B., & Gross, T. (2015) Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1—Attackers. *IEEE Security & Privacy. 13*(1), 71-76

Athalye, A., Engstrom, L., Ilyas, A., & Kwok, K. (2018) Synthesizing Robust Adversarial Examples. *arXiv.* 1-19

Bara, S., et al. (2017) Data Analysis of Cybercrimes in Businesses *The Journal of Riga Technical University.*(20)1 Διαθέσιμο στο: https://www.degruyter.com/view/j/itms.2017.20.issue-1/itms-2017-0011/itms-2017-0011.xml

Bloem, J., Van Doorn, M., Duivestein, S., & Excoffier, D. (2014) The Fourth Industrial Revolution. *VINT.3*, 1-40

Bou-Harb, E. et al. (2017) Big Data Sanitization and Cyber Situational Awareness: A Network Telescope Perspective *IEEE Transactions on Big Data.* (PP)99, 1-16 Διαθέσιμο στο: http://ieeexplore.ieee.org/abstract/document/7968317/

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B. & Chon, S. (2014) An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology.8*(1), 1-20

Brown, C. S.D. (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology.9*(1), 55-119

Brundage, M. et all. (2018) The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation, Workshop in Oxford Διαθέσιμο και στο: https://maliciousaireport.com/

Chandler, Nathan., How the Deep Web Works. *Howstuffworks.* [Online] Διαθέσιμο στη:https://computer.howstuffworks.com/internet/basics/how-the-deep-web-works.htm [Πρόσβαση 10 Ιουλίου 2018]

Crowther, G. A. (2017) The Cyber Domain. *The Cyber Defense Review.2*(3), 63-78

Cung, V. (2018) "The Fourth Industrial Revolution : Its Security Implications" RSIS Commentaries, No. 086.RSIS Commentaries. Singapore : Nanyang Technological University

Curran, Dylan., 2018. My terrifying deep dive into one of Russia's largest hacking forums. *The Gaurdian.* [Online] Opinion (Hacking), Διαθέσιμο στη: https://www.theguardian.com/commentisfree/2018/jul/24/darknet-dark-web-hacking-forum-internet-safety [Πρόσβαση 17 Αυγούστου 2018]

Dilek, S., Cakir, H., & Aydim, M. (2015) APPLICATIONS OF ARTIFICIAL INTELLIGENCE TECHNIQUES TO COMBATING CYBER CRIMES: A REVIEW *International Journal of Artificial Intelligence & Applications (IJAIA).* (6)1, 21-39 Διαθέσιμο στο: https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf

Elazari, K. (2017) Hackers are on the brink of launching a wave of AI attacks: Artificial intelligence's ability to learn will be key in cyberdefence and attack. *WIRED* Διαθέσιμο στο: http://www.wired.co.uk/article/hackers-ai-cyberattack-offensive [Πρόσβαση 18 Μαρτίου 2018]

Feldman, R.C. (2018) ARTIFICIAL INTELLIGENCE: THE IMPORTANCE OF TRUST & DISTRUST *LEGAL STUDIES RESEARCH PAPER SERIES.* (268) 29 Διαθέσιμο στο: https://poseidon01.ssrn.com/delivery.php?ID=134094121066112086066065081090105120021087025040030006018105081106125082029071097023027001056044123040017070002077007115018089102008032018048089105097103127002088067086040078017090100083115103121006096086070084066095116120077001126105000110101105122096&EXT=pdf

Ganesh, V. (2017) Artificial Intelligence Applied to Computer Forensics. *IJARCSMS.* 5(5), 21-29 Διαθέσιμο στο: http://www.ijarcsms.com/docs/paper/volume5/issue5/V5I5-0001.pdf

Gavin, J. D., et al. (2017) The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*. *57* (2), 15

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2018) The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. *International Conference on Computer Networks and Communication Technologies.* 739-747

Ghanshyam, S., Himanshu, Y., & Anurag, J. (2017) An Approach to Detect Malicious URL through Selective Classification *International Journal of Scientific Research & Engineering Trends.* (3)4, 80-84 Διαθέσιμο στο: https://www.ijsret.com/paper/IJSRET_V3I4-179.PDF

Gupta, B. B., Nalin, A. G., & Psannis, K. E. (2017) Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. *Cryptography and Security*. Διαθέσιμο στη: https://arxiv.org/abs/1705.09819

Helbing, D., et al. (2017) Will Democracy Survive Big Data and Artificial Intelligence? *Scientific American.* 48 Διαθέσιμο στο: https://www.bsfrey.ch/articles/D_283_2017.pdf

Javed, Aisha., 2016. ARTIFICIAL INTELLIGENCE TECHNIQUES TO DETECT CYBER CRIMES. *Xorlogics.* [Online] Blogpost (August) Διαθέσιμο στη: http://www.xorlogics.com/2016/08/07/artificial-intelligence-techniques-to-detect-cyber-crimes/ [Πρόσβαση 20 Αυγούστου 2018]

Kersting, K., & Meyer, U. (2018) From Big Data to Big Artificial Intelligence? *Künstliche Intelligenz. 32*, 3-8

Khanduja, V., Arora, A., & Garg, S. (2017) Applications of big data in real world: It's not what you know. It's what you do with what you know *ICCCA.* ISBN: 978-1-5090-6471-7, 159-163 Διαθέσιμο στο: http://ieeexplore.ieee.org/abstract/document/8229792/?part=1

LeCun, Y. "Deep learning & convolutional networks," *2015 IEEE Hot Chips 27 Symposium (HCS)*, Cupertino, CA, USA, 2015, pp. 1-95. Διαθέσιμο στο:

Lidong, W., Guanghui, W., & Cheryl, A. A. (2016) Machine Learning in Big Data *International Journal of Advances in Applied Sciences (IJAAS).* (4)4, 117-123 Διαθέσιμοστο: http://www.iaescore.com/journals/index.php/IJAAS/article/view/868/5800

Lin, Z., Tong, L., & Zhijie, M., & Zhen, L. (2017) Research on Cyber Crime Threats and Countermeasures about Tor Anonymous Network Based on Meek Confusion Plug-in. *ICRIS.* Huaian, 15-16 October

Maher, D. (2017) Can artificial intelligence help in the war on cybercrime?. *Computer Fraud & Security. 2017*(8), 7-9

Mancini, P., & Jenkins, M., (2017) Ethics of Artificial Intelligence in the Legal Field. 1-6

Marr, B. (2016) How Big Data Is Used To Fight Cyber Crime And Hackers: Fascinating Use Case From BT. 3

Najafabadi, M. M., et al. (2015) Deep Learning Applications and Challenges in Big Data Analytics. *Journal of Big Data. 2*(1), 1-21

Oltsik, J. (2018) Artificial intelligence and cybersecurity: The real deal. *CSO* Διαθέσιμο στο:https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html

Parag, H. R. (2017) Artificial Intelligence Based Digital Forensics Framework. *IJARCS.* 8(8), 10-14

Patterson, Dan., 2018. How artificial intelligence is unleashing a new type of cybercrime. *TechRepublic*. [Online] Innovation (February), Διαθέσιμο στη: https://www.techrepublic.com/article/how-artificial-intelligence-is-unleashing-a-new-type-of-cybercrime/ [Πράσβαση 10 Σεπτεμβρίου 2018]

Pfeffer, A., et al. (2017) Artificial Intelligence Based Malware Analysis *Elsevier*. Διαθέσιμο στο: https://arxiv.org/pdf/1704.08716.pdf

Plageras, A.P., et al. (2018) Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. *Future Generation Computer Systems*. 82, 349-357

Porcedda, Maria Grazia and Wall, David S., Data Science, Data Crime and the Law (March 30, 2018). Porcedda, M.G. and Wall, D.S. (2018) 'Data Science, Data Crime and the Law', in V. M-ak, E. Tjong Tjin Tai & A. Berlee (eds) Research Handbook on Data Science & Law, London: Edward Elgar. . Διαθέσιμο στο SSRN: https://ssrn.com/abstract=3152946

Pramanik, M. I., et al (2017) Big data analytics for security and criminal investigations. *Wiley. 7*(4), 19

Ren, S., et al. (2016) Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. *Computer Vision And Pattern Recognition.* 1-14

Russell, S. & Norvig, P. (2004) *Τεχνητή Νοημοσύνη: Μία Σύγχρονη Προσέγγιση*. 2. Κλειδάριθμος.

Ruth, C. et al. (2018) Data Science: Big Data, Machine Learning, and Artificial Intelligence *Journal of the American College of Radiology*. (15)3, 2

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018) How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence. 76*, 130-157

Rasjeswari, C., et al. (2017) Survey of Cyber Crime in Big Data *IOP Conf. Series: Materials Science and Engineering.* (263) 7 Διαθέσιμο στο: http://iopscience.iop.org/article/10.1088/1757-899X/263/4/042053/meta

Sagiroglu, S., & Duygy, S. (2013) Big data: A review *Collaboration Technologies and Systems(CTS).* ISBN: 978-1-4673-6404-1, 42-47 Διαθέσιμο στο: http://ieeexplore.ieee.org/abstract/document/6567202/

Sapountzi, A. & Psannis, K.E., (2016) Social networking data analysis tools & challenges. *Future Generation Computer Systems*.

Sheils, Conor., 2018. Deep Web, Dark Web, Tor and More: The Hidden Internet Uncovered. *Digital.com.* [Online] July (Miscellaneous), Διαθέσιμο στη: https://digital.com/blog/deep-dark-web/ [Πρόσβαση 15 Νοεμβρίου 2018]

Srikanth, 2017. DIFFERENT WAYS ARTIFICIAL INTELLIGENCE COULD PREVENT HACKING. *TechJini.* [Online] Blog, Διαθέσιμο στη: https://www.techjini.com/blog/different-ways-artificial-intelligence-prevent-hacking/ [Πρόσβαση 22 Σεπτεμβρίου 2018]

Srivastava, S., et al. (2017) Safety and security in smart cities using artificial intelligence - A review *ICCCA.* ISBN: 978-1-5090-3519-9 Διαθέσιμο στο: http://ieeexplore.ieee.org/abstract/document/7943136/

Stergiou, C., Psannis, K. E., Kim, B., & Gupta, B. B. (2016) Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems 78*(3),964-975.

Suvansh, A., et al. (2017) INTERNET OF THINGS, ARTIFICIAL INTELLIGENCE, AUTOMATION,TECHNOLOGY. *World Journal of Technology, Engineering and Research.* (1)1 56-65 Διαθέσιμο στο:

http://wjter.com/Research%20Papers/November%202017/PDF/Internet%20of%20Things,%20Artificial%20Intelligence%20Automation%20Technology.pdf

Turing, A. M. (1950) Computing Machinery and Intelligence. *Mind. 59*(236), 433-460

Vaishnavi, G. (2017) Artificial Intelligence Applied to Computer Forensics. *International Journal of Advance Research in Computer Science and Management Studies.* 5 (5), 21-29

Villaronga, E. et al. (2017) Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten. *Computer Law & Security Review*. Διαθέσιμοστο: https://www.sciencedirect.com/science/article/pii/S0267364917302091

Williams, M. L., et al. (2016) Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns. *The British Journal of Criminology. 57* (2), 21

Wolak, J & Finkelhor, D. (2016) Sextortion: Findings From A Survey Of 1.631 Victims. *Thorn & Crimes Against Children Research Center.* 1-81

Xu, L., et al., (2014) Information Security in Big Data:Privacy and Data Mining. *IEEE.* 2,1149-1175

https://www.cnn.gr/ereynes/video/6309/sextortion-h-nea-apeili-toy-diadiktyoy

https://www.computer.org/csdl/proceedings/hcs/2015/8885/00/07477328-abs.html

http://cs231n.github.io/convolutional-networks/

https://medium.freecodecamp.org/an-intuitive-guide-to-convolutional-neural-networks-260c2de0a050

http://www.zdnet.com/article/how-ai-powered-cyberattacks-will-make-fighting-hackers-even-harder/

https://futurism.com/experts-warn-that-ai-enhanced-cyberattacks-are-an-imminent-threat/

https://www.wired.com/2016/04/mits-teaching-ai-help-analysts-stop-cyberattacks/

https://www.google.com/

www.lifo.gr