ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

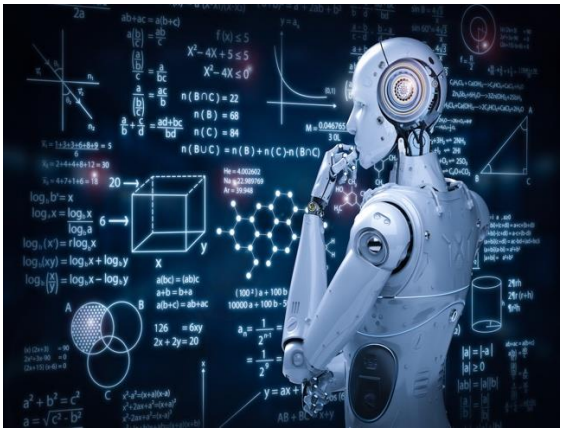
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Της Λήδας-Εμμανουέλας Βεντούρα (ΑΜ: ΜΔΙ2004)

«ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ»



<u>Επιβλέπουσα</u>

Κα Λίλιαν Μήτρου

Πειραιάς, Μάιος 2022

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ

Μέσα σε μια εποχή, όπου οι νέες τεχνολογίες όχι απλώς κατέχουν κυρίαρχο ρόλο αλλά και πρωταγωνιστούν στην καθημερινότητά μας, η τεχνητή νοημοσύνη έχει αναλάβει έναν πολύ κομβικό και σημαντικό ρόλο. Συναντάται σε όλες τις εκφάνσεις της ζωής των ανθρώπων και φιλοδοξεί να βελτιώσει την ποιότητά της, εισάγοντας τους ανθρώπους σε έναν κόσμο που μπορεί επί του παρόντος να φαντάζει ξένος και αλλόκοτος , στο μέλλον όμως θα κυριαρχεί. Η τεχνητή νοημοσύνη, μια σπουδαία εφεύρεση της επιστήμης και όσων δουλεύουν γι' αυτήν, δεν παράγει μόνο θετικό έργο, αλλά μπορεί να χρησιμοποιηθεί και προς όφελος των εγκληματιών.

Μια από τις εγκληματικές ενέργειες στις οποίες παρατηρείται ανάμειξη της τεχνητής νοημοσύνης είναι το κυβερνοέγκλημα. Αυτό αποτέλεσε και πηγή έμπνευσης της συγκεκριμένης εργασίας, η επαφή μιας καινοτόμου τεχνολογίας με τους επιτιθέμενους στο διαδίκτυο και η ανάγκη για εμβάθυνση στο ακανθώδες αυτό ζήτημα.

Στο πρώτο κεφάλαιο της παρούσας εργασίας, αναλύεται εκτενώς το κυβερνοέγκλημα, οι μορφές του, το νομοθετικό πλαίσιο σε ευρωπαϊκό, διεθνές και εθνικό επίπεδο καθώς και προτάσεις αντιμετώπισής του.

Στο δεύτερο κεφάλαιο αναλύεται η τεχνολογία της τεχνητής νοημοσύνης, οι νομοθετικές της προβλέψεις και σε ποιες περιπτώσεις συναντάμε το κυβερνοέγκλημα, αφενός ως θύμα των μηχανών της τεχνητής νοημοσύνης, αφετέρου ως θύτη.

Τέλος, γίνεται μια προσπάθεια προσέγγισης του ζητήματος από την πλευρά της αντιμετώπισης των εγκλημάτων στον κυβερνοχώρο μέσω συστημάτων τεχνητής νοημοσύνης αλλά και προτάσεων για μεθόδους πρόληψης για ενδεχόμενες επιθέσεις.

Λέξεις κλειδιά: Τεχνητή Νοημοσύνη, Κυβερνοέγκλημα

ABSTRACT

In an era, where new technologies not only dominate but also play a leading role in our daily lives, Artificial Intelligence plays a very significant and important role. It is found in all aspects of people's lives and aspires to improve its quality, introducing people to a world that may seem strange now, but in the future will dominate. Artificial intelligence, a great knowledge of science and those who work for it, not only produces positive work, but can also be used for the benefit of criminals-users.

One of the criminal activities in which Artificial Intelligence is involved, is cybercrime. This was also the source of inspiration for this paper, the contact of an innovative technology with the inspectors on the Internet and the need to delve into this thorny issue.

In the first chapter of this paper, cybercrime is analyzed in detail, its forms, the legal framework at European, international and national level, as well as proposals for tackling it.

The second chapter analyzes the technology of Artificial Intelligence, its legislative provisions and in which cases we encounter cybercrime on the one hand as a victim of the machines of Artificial Intelligence, on the other hand as a perpetrator.

Finally, an attempt is made to approach the issue in terms of tackling cybercrime through Artificial Intelligence systems and proposals for prevention methods for possible attacks.

Keywords: Artificial Intelligence (AI), Cyber-crime

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΔΑΕ: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΔΙΔΗΕ: Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

ΔΕΥ: (Συμβούλιο) Δικαιοσύνης και Εσωτερικών Υποθέσεων

ΕΕ: Ευρωπαϊκή Ένωση

ΕΕΤΤ: Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΝΝ: Νευρωνικά Δίκτυα

Ν: Νόμος

ΟΗΕ: Οργανισμός Ηνωμένων Εθνών

ΟΟΣΑ: Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης

ΤΝ: Τεχνητή Νοημοσύνη

ΤΠΕ: Τεχνολογίες Πληροφοριών και Επικοινωνιών

AI: Artificial Intelligence

GCC: Greek Cybercrime Center

IOCTA: Internet Organised Crime Threat Assessment

IP: Internet Protocol

UNICRI: United Nations Interregional Crime and Justice Research Institute

ΕΙΣΑΓΩΓΗ-ΠΡΟΛΟΓΟΣ

Η τεχνητή νοημοσύνη έχει γίνει πλέον αναπόσπαστο κομμάτι της ζωής μας, καθώς έχει πολύ σημαντικό και ουσιαστικό πλέον αντίκτυπο σε αυτή. Αποτελεί μια αναπτυσσόμενη επιστήμη σε πολλές πτυχές, σύμφωνα και με τις σύγχρονες προκλήσεις του 21ου αιώνα που διανύουμε. Παρά τις πολυάριθμες θετικές τις διαστάσεις, η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί και για αντίθετους σκοπούς, όπως για την παραβίαση των ανθρωπίνων δικαιωμάτων και να θέσει σε κίνδυνο ολόκληρη την ανθρωπότητα.

Το έγκλημα που διαπράττεται στον κυβερνοχώρο και βασίζεται στην τεχνητή νοημοσύνη αποτελεί προϊόν της τεχνολογικής ανάπτυξης και θέτει απειλές για την δημόσια και εθνική ασφάλεια καθώς και για την προστασία των θεμελιωδών δικαιωμάτων των χρηστών του Διαδικτύου. Δεν πρόκειται για ένα πρόβλημα που διαπιστώνεται μόνο σε ένα κράτος, αλλά αποτελεί παγκόσμιο φαινόμενο. Το ίδιο ισχύει και για υπόλοιπα υποκειμενικά χαρακτηριστικά (ηλικία, φύλο) καθώς δεν παρατηρούνται μεμονωμένα περιστατικά, αλλά θύματα μπορούν εν δυνάμει να είναι όλοι ανεξαρτήτως γένους και ηλικιακής ομάδας. Αυτό το οποίο θα πρέπει να διασφαλίσουμε σε μεγάλο βαθμό, είναι η εφαρμογή ισχυρών μέτρων ασφάλειας στον κυβερνοχώρο έτσι ώστε να εφαρμοστεί ο νομικός ορθολογισμός στην εποχή της τεχνολογικής ανάπτυξης. Σε αυτό το πλαίσιο καταβάλλεται προσπάθεια κατανόησης των βασικών ζητημάτων που άπτονται της τεχνητής νοημοσύνης και του εγκλήματος στον κυβερνοχώρο, αλλά και το πως οι μηχανές τεχνητής νοημοσύνης εκτός από όργανο των εγκληματιών, δύνανται να χρησιμοποιούνται για την επίλυση και την εξακρίβωση του ακανθώδους και ευαίσθητου αυτού θέματος.

ΚΕΦΑΛΑΙΟ Ι

1. ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

1.1.ΟΡΙΣΜΟΣ

Η έννοια του κυβερνοεγκλήματος θα μας απασχολήσει αρκετά στην παρούσα εργασία, επομένως χρήσιμο θα ήταν να προχωρήσουμε στον ορισμό της. Ως κυβερνοέγκλημα ή αλλιώς έγκλημα στον κυβερνοχώρο, ονομάζεται το έγκλημα εκείνο το οποίο συνίσταται σε εγκληματικές πράξεις που διαπράττονται διαδικτυακά με την χρήση δικτύων ηλεκτρονικών επικοινωνιών και συστημάτων πληροφοριών. Με δύο λόγια, γίνεται με την χρήση ενός υπολογιστή ως εργαλείο για τους περαιτέρω παράνομους σκοπούς, όπως η διάπραξη απάτης, η εμπορία παιδικής πορνογραφίας και πνευματικής ιδιοκτησίας, η κλοπή ταυτοτήτων ή η παραβίαση της ιδιωτικής ζωής.[1]

Υπό στενή έννοια (*computer crime*), το κυβερνοέγκλημα ορίζεται ως μια παράνομη δραστηριότητα όπου ο υπολογιστής είναι το εργαλείο ή ο τόπος της εγκληματικής δραστηριότητας ή ο στόχος είναι η ασφάλεια των συστημάτων υπολογιστών και των δεδομένων τους.[2] Από την άλλη πλευρά, υπό ευρεία έννοια (*computer related crime*) κυβερνοέγκλημα αποτελεί το έγκλημα εκείνο όπου η παράνομη δραστηριότητα διαπράττεται μέσω του υπολογιστή ή σε σχέση με αυτό.[3]

Αξίζει να σημειωθεί, πως το κυβερνοέγκλημα έχει συνώνυμη έννοια με το ηλεκτρονικό έγκλημα, το οποίο δεν έχει κάποιον κοινό νομικό ή επιστημονικό ορισμό, μπορεί όμως να προσδιοριστεί ως «*κάθε πράξη ή παράλειψη που διαπράττεται σε παγκόσμιο πληροφοριακό*

---

[1] Ορισμός του κυβερνοεγκλήματος από την Britannica δημοσιευμένος στην ιστοσελίδα https://www.britannica.com/topic/cybercrime ανευρεθέν στην ιστοσελίδα στις 21/11/2021 (τελευταία πρόσβαση: 26/2/2022)

[2] *The Convention on Cybercrime*, Margaret Killerby, Head of Department of Crime of Problems DGI, Council of Europe, Strasbourg δημοσιευμένο στην ιστοσελίδα https://www.itu.int/osg/spu/cybersecurity/2006/presentations/killerby-15-may-2006.pdf ανευρεθέν στις 22/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[3] Μελέτη του καθηγητή Dr. Marco Gercke με τίτλο «*Understanding Cybercrime: Phenomena, Challenges and Legal Response*», δημοσιευμένη τον Σεπτέμβριο του 2012 στην ιστοσελίδα https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf ανευρεθείσα στις 22/1/2022 (τελευταία πρόσβαση: 26/2/2022)

επίπεδο με την βοήθεια του διαδικτύου»[4] καθώς και σαν *«μια εγκληματική πράξη στην οποία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της».*[5]

Δεν υπάρχει αμφιβολία πως το έγκλημα στον κυβερνοχώρο θεωρείται από τα πιο επικίνδυνα εγκλήματα στην ανθρωπότητα, μετά την κυβερνητική διαφθορά και την διακίνηση των ναρκωτικών και γι' αυτό και χρήζει ιδιαίτερης νομοθετικής και ουσιαστικής αντιμετώπισης.[6]

1.2. Χαρακτηριστικά Εγκλημάτων

Αναμφίβολα, υπάρχουν πολλοί λόγοι οι οποίοι συνέβαλαν στην ανάπτυξη και εξάπλωση του εγκλήματος στον κυβερνοχώρο.[7] Τα κυβερνοεγκλήματα, ως ειδικότερη έκφανση των ηλεκτρονικών εγκλημάτων χαρακτηρίζονται από ορισμένες ιδιαιτερότητες, οι οποίες τα ξεχωρίζουν από τα κοινά εγκλήματα και καθιστούν κάπως δυσχερέστερη την ποινική τους αντιμετώπιση. Αρχικώς, τα κυβερνοεγκλήματα χαρακτηρίζονται από **ταχύτητα.** Η διάπραξή τους γίνεται σε πολύ σύντομο χρονικό διάστημα και τις περισσότερες φορές δεν προλαβαίνει το θύμα να το αντιληφθεί για να το προλάβει και να το σταματήσει. *Για παράδειγμα*, η παραβίαση των προσωπικών κωδικών e-banking και η πρόσβαση στον λογαριασμό του θύματος μπορεί να συμβεί σε δευτερόλεπτα και μέχρι να το αντιληφθεί το θύμα, ο δράστης να έχει ήδη εισχωρήσει στον λογαριασμό του τελευταίου. Λόγω της φύσης του Διαδικτύου, το οποίο επιτρέπει την εύκολη και άμεση πρόσβαση σε κάθε είδους υλικού σε όλον τον κόσμο και ανά πάσα ώρα και στιγμή, ευνοείται επίσης η **ανωνυμία,** η οποία ενισχύει την δράση των θυτών και την εκμεταλλεύονται για την ανάπτυξη των παράνομων δραστηριοτήτων τους και την δημιουργία μυστικών κύκλων μεταξύ τους, οι οποίοι επικοινωνούν και ανταλλάσσουν παράνομο περιεχόμενο. Επιπλέον, η τεράστια εξάπλωση

---

[4] Άρθρο της Θεώνης Γ.Σπαθή με τίτλο *«Νέες τεχνολογίες και έγκλημα»* δημοσιευμένο τον Οκτώβριο του 2016 στην ιστοσελίδα http://www.indeepanalysis.gr/nomika-themata/nees-technologies-kai-egklhma ανευρεθέν στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[5] Άρθρο με τίτλο *«Τι είναι το ηλεκτρονικό έγκλημα»* δημοσιευμένο στην ιστοσελίδα https://sites.google.com/site/elektronikoenklema2012/ti-einai-elektroniko-enklema ανευρεθέν στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[6] Επιστημονική μελέτη του James Andrew Lewis με τίτλο *«Economic Impact of Cybercrime»* δημοσιευμένο στις 21/2/2018 στην ιστοσελίδα https://www.csis.org/analysis/economic-impact-cybercrime ανευρεθείσα στις 10/1/2021 (τελευταία πρόσβαση: 26/2/2022)

[7] Μελέτη του XiaoLing Wang με τίτλο *«Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime»* δημοσιευμένη το 2020 στην ιστοσελίδα https://iopscience.iop.org/article/10.1088/1742-6596/1533/3/032014/pdf?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc ανευρεθείσα στις 28/1/2022 (τελευταία πρόσβαση: 26/2/2022)

του Διαδικτύου παγκοσμίως, δημιουργεί **δυσχέρεια στην διερεύνηση** και στην εξιχνίαση των εγκλημάτων, καθώς ο διασυνοριακός χαρακτήρας των κυβερνοεγκλημάτων καθιστά εξαιρετικά δύσκολη την αναζήτηση του δράστη αλλά και του τόπου και χρόνου τέλεσης του εγκλήματος.

1.3. Διακρίσεις Κυβερνοεγκλημάτων

Πιο συγκεκριμένα, το έγκλημα τον κυβερνοχώρο μπορεί να ταξινομηθεί σε τρείς γενικούς ορισμούς:

- Εγλήματα ειδικά για το Διαδίκτυο, όπως οι επιθέσεις εναντίον συστημάτων πληροφοριών ή phishing (π.χ. ψεύτικοι ιστότοποι τραπεζών για την αναζήτηση κωδικών πρόσβασης που επιτρέπουν την πρόσβαση στους τραπεζικούς λογαριασμούς των θυμάτων)
- Διαδικτυακή απάτη και πλαστογραφία : όπως κλοπή ταυτότητας, ηλεκτρονικό ψάρεμα, ανεπιθύμητη αλληλογραφία και κακόβουλος κώδικας
- Παράνομο διαδικτυακό περιεχόμενο , συμπεριλαμβανομένου υλικού σεξουαλικής κακοποίησης παιδιών, υποκίνησης σε φυλετικό μίσος, υποκίνησης τρομοκρατικών ενεργειών και εξύμνησης της βίας, της τρομοκρατίας, του ρατσισμού και της ξενοφοβίας.

Πολλά είδη εγκλημάτων, συμπεριλαμβανομένης της τρομοκρατίας, της εμπορίας ανθρώπων, της σεξουαλικής κακοποίησης παιδιών και της διακίνησης ναρκωτικών, έχουν μετακινηθεί στο Διαδίκτυο ή διευκολύνονται στο Διαδίκτυο. Κατά συνέπεια, οι περισσότερες ποινικές έρευνες έχουν ψηφιακό στοιχείο.[8]

Ειδικότερα:

- Ηλεκτρονικό Ψάρεμα||Phishing: Το phishing αποτελεί μια προσπάθεια απόκτησης ευαίσθητων προσωπικών πληροφοριών όπως είναι τα ονόματα χρήστη, οι κωδικοί πρόσβασης κ.ά., μέσω της εξαπάτησης των χρηστών του διαδικτύου. Για να πετύχει τον στόχο του, ο θύτης, υποδύεται πως είναι ένας αξιόπιστος άνθρωπος και εκμεταλλευόμενος την άγνοια του θύματος όσο και τις ελλιπείς προστατευτικές

[8] Ορισμός του κυβερνοεγκλήματος δημοσιευμένος στην ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en ανευρεθέν στις 21/11/2021 (τελευταία πρόσβαση: 26/2/2022)

ηλεκτρονικές δικλείδες προσπαθεί να εισχωρήσει αθέμιτα στα προσωπικά δεδομένα του θύματος. Ο όρος phising ανήκει στον διάσημο χάκερ και σπάμερ Khan C Smith, ο οποίος έγινε γνωστός την δεκαετία του 1990[9] και στην συνέχεια υιοθετήθηκε από όλους του χάκερς. Η τακτική του phishing γίνεται με την χρήση emails, όπου το θύμα ανοίγει ένα ηλεκτρονικό μήνυμα το οποίο έχει όλα τα εξωτερικά χαρακτηριστικά γνωρίσματα ενός έγκυρου και αξιόπιστου μηνύματος, με αποτέλεσμα να επιτυγχάνεται η εγκατάσταση ενός κακόβουλου λογισμικού το οποίο θα οδηγήσει τον χρήστη σε μια πλαστή ιστοσελίδα και μετά θα του υποκλέψει τα προσωπικά, ιδιωτικά του στοιχεία.

- Ηλεκτρονικό Ψάρεμα||Pharming: Μια άλλη μορφή ηλεκτρονικού ψαρέματος είναι και το pharming. Στην περίπτωση του pharming, ο επιτιθέμενος, εκμεταλλευόμενος κάποιο τρωτό ηλεκτρονικό πρόγραμμα ενός συστήματος ονομάτων χώρου (DNS-Domain Name), επεμβαίνει στο σύστημα αυτό και ανακατευθύνει τους επισκέπτες μιας ιστοσελίδας σε μια άλλη. Έτσι, όταν ο χρήστης πληκτρολογήσει μια γνωστή σε αυτόν ηλεκτρονική διεύθυνση, θα μεταφερθεί εν αγνοία του σε έναν κακόβουλο ιστότοπο[10], ο οποίος θα έχει ως στόχο να του αποσπάσει προσωπικά στοιχεία (π.χ. όνομα χρήστη, κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας ή τραπεζικού λογαριασμού κ.ά.) Η μέθοδος ηλεκτρονικού ψαρέματος pharming έχει ομοιότητες με το phishing, καθώς και στις δύο περιπτώσεις ο δράστης μέσα από την αποστολή παραπλανητικών ηλεκτρονικών emails προσπαθεί να αποσπάσει εμπιστευτικές πληροφορίες του θύματος ώστε να τις εκμεταλλευτεί.

- Vishing11: Αυτού του είδους η επίθεση μοιάζει αρκετά με το phishing, ως προς τον τρόπο λειτουργίας του. Πρόκειται για το λεγόμενο «φωνητικό ψάρεμα», μια περίπτωση ηλεκτρονικής απάτης, όπου οι χρήστες εξαπατώνται και παραχωρούν

[9] Άρθρο της Helga George με τίτλο «*Phising Emails are Homeland Security's Most Feared Cyber Threat*» δημοσιευμένο στις 29/4/2021 στην ιστοσελίδα https://www.homelandsecurityedu.org/2017/01/phishing-emails-are-homeland-securitys-most-feared-cyber-threat/ ανευρεθέν στις 23/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[10] Συνήθως ο κακόβουλος ιστότοπος είναι μια «πλαστή/ψεύτικη» ιστοσελίδα, όπου η ηλεκτρονική διεύθυνση είναι παρόμοια με την αυθεντική έτσι ώστε να παραπλανάται ο χρήστης και να πιστεύει πως έχει επισκεφθεί την ιστοσελίδα που γνώριζε.

[11] Voice, VoIP phising

σημαντικά προσωπικά τους δεδομένα σε μη εξουσιοδοτημένους φορείς. Το μέσο τέλεσης δεν είναι μόνο το διαδίκτυο, αλλά και ο τηλέφωνο και το ηχογραφημένο μήνυμα.[12]

- Smishing:[13] Κατ' αντιστοιχία με το phishing και το vishing, πρόκειται για μια μορφή ηλεκτρονικής απάτης, η οποία συντελείται μέσω μηνυμάτων. Δεν πρόκειται για ηλεκτρονικό μήνυμα ή ανεπιθύμητο email, αλλά για ένα απλό μήνυμα κειμένου (SMS) στο κινητό τηλέφωνο. Συνήθως το μήνυμα θα περιλαμβάνει έναν σύνδεσμο που με το που τον πατήσει ο χρήστης, ο δράστης θα υποκλέψει προσωπικά στοιχεία του χρήστη ή θα εισέλθει παράνομα στο κινητό του.

- Πλαστές διευθύνσεις||IP Spoofing: Στην συγκεκριμένη επίθεση, ο επιτιθέμενος παρεμβαίνει στην αριθμητική διεύθυνση (IP address) ενός πακέτου πληροφοριών που διακινείται σε ένα δίκτυο και την τροποποιεί έτσι ώστε να φαίνεται ότι πρόκειται για μία αξιόπιστη και ήδη γνωστή στους υπολογιστές του συστήματος διεύθυνση. Πιο συγκεκριμένα, αντιγράφει την συγκεκριμένη αλληλουχία αριθμών που συνιστούν μια έγκυρη και αξιόπιστη διεύθυνση IP μιας ηλεκτρονικής συσκευής που συνδέεται στο δίκτυο, και στη συνέχεια αποστέλλει ένα κακόβουλο μήνυμα στους υπόλοιπους υπολογιστές ενός δικτύου, το οποίο όμως φαίνεται ότι προέρχεται από την παραπάνω αξιόπιστη διεύθυνση IP.

  Με την απομίμηση (spoofing) μιας ήδη γνωστής διεύθυνσης IP και εκμεταλλευόμενος τη σχέση εμπιστοσύνης μεταξύ των υπολογιστών ενός δικτύου ο επιτιθέμενος αποκτά χωρίς δικαίωμα πρόσβαση σε έναν υπολογιστή ή σε ένα σύστημα υπολογιστών.

  Ο χρήστης του δικτύου που θα πληκτρολογεί το συγκεκριμένο όνομα χώρου θα οδηγείται αυτόματα στην πλαστή διεύθυνση που έχει επιλέξει ο επιτιθέμενος και θα παραχωρεί προσωπικές του πληροφορίες νομίζοντας πως βρίσκονται στον αυθεντικό δικτυακό τόπο.

---

[12] Άρθρο της Jennifer van der Kleut με τίτλο «*What is vishing? Tips for spotting and avoiding voice scams*» δημοσιευμένο στην ιστοσελίδα https://us.norton.com/internetsecurity-online-scams-vishing.html ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[13] Άρθρο του David Nield με τίτλο «*How to Guard Against Smishing Attacks on Your Phone*» δημοσιευμένο στις 12/12/2021 στην ιστοσελίδα https://www.wired.com/story/smishing-sms-phishing-attack-phone/ ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

- Πρόγραμμα «Καταγραφής πλήκτρων»||Key logger/Key stroke logging: Πρόκειται για ένα κακόβουλο λογισμικό παρακολούθησης και καταγραφής (logging) μέσω των πλήκτρων ενός πληκτρολογίου όλων των πληροφοριών που πληκτρολογεί ο χρήστης στον υπολογιστή του (όπως οι διάφορες ιστοσελίδες που έχει επισκεφτεί, οι κωδικοί πρόσβασης του σε αυτές). Όλες αυτές οι ενέργειες καταγράφονται από το πληκτρολόγιο μέσω του κακόβουλου λογισμικού παρακολούθησης, χωρίς να αφήνει ίχνη έτσι ώστε να υποψιαστεί για την παράνομη ενέργεια ο χρήστης. [14]Οι πληροφορίες που καταγράφονται αποστέλλονται στον χάκερ μέσω ηλεκτρονικού μηνύματος, έτσι ώστε να προχωρήσει στην παράνομη ενέργειά του.

- Hacking: Στην συγκεκριμένη μορφή επίθεσης, η οποία είναι από τις παλαιότερες και τις πιο διαδεδομένες, οι επιτιθέμενοι-χάκερς εισβάλουν στα υπολογιστικά συστήματα και έχοντας τις κατάλληλες γνώσεις και ικανότητες τα διαχειρίζονται και τα τροποποιούν. Πρόκειται για μια μη εξουσιοδοτημένη πρόσβαση σε συστήματα ηλεκτρονικών υπολογιστών,[15] η οποία μπορεί να μην γίνεται πάντα για κακόβουλους σκοπούς, ωστόσο τις περισσότερες φορές πρόκειται για μια παράνομη δραστηριότητα από εγκληματίες του κυβερνοχώρου, με στόχο το οικονομικό όφελος, την συλλογή πληροφοριών και την αλλοίωση του υπάρχοντος περιεχομένου.[16] Εκτός από τους hackers υπάρχουν και οι crackers, οι οποίοι έχουν ως στόχο να προκαλέσουν ζημιά σε δίκτυα υπολογιστών, να εισβάλουν χωρίς νόμιμη εξουσιοδότηση και παραβιάζοντας κωδικούς πρόσβασης σε υπολογιστές ξένων χρηστών, να δημιουργήσουν ιούς και να καταστρέψουν υπάρχον οπτικό ή άλλο υλικό.[17]

[14] Άρθρο με τίτλο «*What is Keystroke Logging and Keyloggers?*» δημοσιευμένο στην ιστοσελίδα https://www.kaspersky.com/resource-center/definitions/keylogger ανευρεθέν στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)
[15] Μελέτη του Κέντρου ΠΛΗ.ΝΕ.Τ.Ν. ΦΛΩΡΙΝΑΣ με τίτλο «*Οι Hackers και οι Crackers*» δημοσιευμένη στην ιστοσελίδα http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html ανευρεθείσα στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)
[16] Άρθρο με τίτλο «Hacking definition: What is hacking» δημοσιευμένο στην ιστοσελίδα https://www.malwarebytes.com/hacker ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)
[17] Άρθρο με τίτλο «*Difference between Hackers and Crackers*» δημοσιευμένο στην ιστοσελίδα https://www.geeksforgeeks.org/difference-between-hackers-and-crackers/ ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

- Ανεπιθύμητη Αλληλογραφία||Spamming: Η τακτική του spamming υφίσταται με την μαζική αποστολή μεγάλου αριθμού ηλεκτρονικών μηνυμάτων (e-mails) τα οποία απευθύνονται σε ένα μεγάλο σύνολο χρηστών του διαδικτύου χωρίς να τα έχουν ζητήσει ή να βρίσκονται σε κάποια λίστα αποστολής τέτοιου είδους μηνυμάτων. Τα συγκεκριμένα μηνύματα συνήθως αποστέλλονται για διαφημιστικούς ή ενημερωτικούς λόγους.[18]

- Διασπορά κακόβουλου λογισμικού: Αποτελεί από τα πιο διαδεδομένα εγκλήματα στον κυβερνοχώρο και αφορά σε προγράμματα τα οποία προκαλούν ζημιά σε έναν ξένο υπολογιστή, αλλοιώνουν στοιχεία και υποκλέβουν προσωπικά δεδομένα των χρηστών. Οι πιο ευρέως γνωστοί τρόποι διασποράς κακόβουλου λογισμικού είναι οι εξής:

    - Ιοί||Viruses: Οι ιοί περιλαμβάνονται σε ένα πρόγραμμα, το οποίο επισυνάπτει τον εαυτό του σε αρχεία τα οποία υπάρχουν ήδη στον υπολογιστή, μια διαδικασία δηλαδή που είναι γνωστή και ως «μόλυνση». Αφού «μολυνθεί» το υπολογιστικό περιβάλλον, ο ιός ζει παρασιτικά, το αρχείο πλέον τροποποιείται και ανάλογα με την θέληση του επιτιθέμενου, επισυνάπτονται στον εαυτό του αρχεία τα οποία υπάρχουν στον υπολογιστή. Για να μεταδοθεί ο ιός συνήθως χρειάζεται ανθρώπινη παρέμβαση και πραγματοποιείται από υπολογιστή σε υπολογιστή κυρίως μέσω του διαδικτύου ή μέσω της ανταλλαγής αρχείων. Οι ιοί μπορεί να είναι και ακίνδυνοι αλλά και επικίνδυνοι και να στοχεύουν στο να διαγράψουν προσωπικά στοιχεία των χρηστών, να υποκλέψουν άλλα και να καταστρέψουν ορισμένο υλικό.[19]
    - Δούρειοι Ίπποι||Trojan horses: Πρόκειται για προγράμματα, τα οποία φορτώνονται στον σκληρό δίσκο του ηλεκτρονικού υπολογιστή και εκτελούνται κανονικά μαζί με τα υπόλοιπα προγράμματα. Ο «Δούρειος

[18] Άρθρο με τίτλο «*What is Spam: The Essential Guide to Detecting and Preventing Spam*» δημοσιευμένο στην ιστοσελίδα https://www.avast.com/c-spam ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[19] Άρθρο με τίτλο «*What is a computer virus?*» δημοσιευμένο στην ιστοσελίδα https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Ίππος» εμφανίζεται υπό την μορφή ενός άλλου, συνήθως γνωστού αρχείου, που φαίνεται να κρύβει κάποιο χρήσιμο και καλό σκοπό, ώστε να οδηγήσει τον χρήστη στην εγκατάσταση του συγκεκριμένου προγράμματος, αλλά στην ουσία καλύπτει κάποιο Με το που εγκατασταθεί το πρόγραμμα στον υπολογιστή του θύματος, ο επιτιθέμενος αποκτά πρόσβαση στο σύστημα πληροφοριών, στις πληροφορίες του σκληρού δίσκου ή στο e-mail του χρήστη και οι χρήστες μη έχοντας αντιληφθεί τι έχει συμβεί, παρέχουν τα στοιχεία εισόδου τους (όνομα χρήστη και κωδικό πρόσβασης). [20]Μάλιστα, μέσω αυτής της εγκατάστασης, ο επιτιθέμενος μπορεί να παρακολουθεί ενέργειες, να εκτελεί εντολές, να στέλνει αρχεία στον επιτιθέμενο, να καταγράφει κινήσεις πληκτρολογίου.

- Λογισμικό κατασκοπείας||Spyware: Πρόκειται για ένα κατασκοπευτικό λογισμικό που εγκαθίσταται σε έναν υπολογιστή χωρίς την γνώση του χρήστη, προκειμένου να επιτηρείται η δραστηριότητά του και να διαβιβάζεται η πληροφορία σε ένα τρίτο μέρος.[21] Είναι ένα κατεξοχήν κακόβουλο λογισμικό, όπου ο επιτιθέμενος έχει στόχο και καταφέρνει να υποκλέπτει προσωπικά στοιχεία του χρήστη.
- Λογικές βόμβες||Logic bombs: Πρόκειται για ένα είδος κακόβουλου προγράμματος, το οποίο έχει την ιδιότητα να εγκαθίσταται και να παραμένει ανενεργό στην μνήμη μιας συσκευής και να ενεργοποιείται είτε σε μια συγκεκριμένη ημερομηνία, είτε μετά το πέρας ενός συγκεκριμένου χρονικού διαστήματος, είτε μετά από μια ορισμένη ενέργεια στην οποία προβαίνει ο χρήστης της συσκευής.[22] Όταν ενεργοποιηθεί η «λογική βόμβα» απελευθερώνεται κάποιος ιός, ο οποίος είτε δημιουργεί λειτουργικές βλάβες στο σύστημα, είτε διαγράφει αρχεία είτε καταστρέφει τελείως το σύστημα του υπολογιστή.

[20] Άρθρο με τίτλο «*What is a Trojan horse and what damage can it do?*» δημοσιευμένο στην ιστοσελίδα https://www.kaspersky.com/resource-center/threats/trojans ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[21] Άρθρο με τίτλο «*Τι είναι το Spyware? Οδηγός άμυνας*» δημοσιευμένο στην ιστοσελίδα https://el.safetydetectives.com/blog/τι-είναι-το-spyware-οδηγός-άμυνας/ ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[22] Άρθρο με τίτλο «*Τι είναι το κακόβουλο λογισμικό Logic Bomb και πώς μπορείτε να το αποτρέψετε;*» δημοσιευμένο στην ιστοσελίδα https://el.denizatm.com/pages/46845-what-is-logic-bomb-malware-and-how-can-you-prevent-it ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

- Ανιχνευτές διαδικτυακών πακέτων||Packet sniffers: Πρόκειται για εφαρμογές λογισμικού, οι οποίες μπορούν να εντοπίζουν όλα τα «πακέτα» πληροφοριών που κυκλοφορούν στο διαδίκτυο. Ο επιτιθέμενος που έχει στην κατοχή του αυτό το λογισμικό έχει την δυνατότητα να παρεισφρήσει και να αποκτήσει πακέτα πληροφοριών τα οποία δεν είναι κρυπτογραφημένα και έτσι είναι «ευάλωτα» σε επιθέσεις.[23]

- SQL Injection[24]: Πρόκειται για μια τεχνική έγχυσης κώδικα που επιτίθεται σε συστήματα που χρησιμοποιούν την γλώσσα SQL (τέτοια συστήματα είναι οι βάσεις δεδομένων και online εφαρμογές που είναι συνδεδεμένες με μια βάση δεδομένων). Στην συγκεκριμένη περίπτωση, οι επιτιθέμενοι εκμεταλλευόμενοι κάποιες ευπάθειες στην ασφάλεια μιας ιστοσελίδας ή μιας εφαρμογής αποκτούν πρόσβαση και επεμβαίνουν ακόμα και σε μία ολόκληρη βάση δεδομένων.

- Τεχνική Joomla Bugs: Η συγκεκριμένη τεχνική χρησιμοποιείται ευρέως τα τελευταία χρόνια κυρίως σε υποθέσεις phishing και ηλεκτρονικής απάτης, ενώ πλέον είναι και βασικό όπλο των επιθέσεων με την δημιουργία ιστοσελίδων Botnet. Ο επιτιθέμενος εκμεταλλεύεται το σύστημα διαχείρισης ιστοσελίδων (*Joomla)* και τοποθετεί μέσω αυτού, κακόβουλα λογισμικά (*bugs*) σε μια ιστοσελίδα-παγίδα για τον χρήστη, η οποία είτε εγκαθιστά κακόβουλο λογισμικό στην συσκευή του, ή πραγματοποιεί τεχνικές phishing και αποσπά από τον χρήστη προσωπικά του στοιχεία.

- Διακίνηση παιδικού πορνογραφικού υλικού: Η διαδικτυακή παιδική πορνογραφία, αποτελεί μια από τις μορφές του ηλεκτρονικού εγκλήματος, καθώς η αξιόποινη πράξη συντελείται με την χρήση ηλεκτρονικού υπολογιστή και συστημάτων επεξεργασίας δεδομένων. Στο άρθρο 2 περ. γ του Πρόσθετου

[23] Άρθρο με τίτλο «*What is Sniffer?*» δημοσιευμένο στην ιστοσελίδα https://www.netscout.com/what-is/sniffer ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)
[24] Επιστημονική μελέτη του Xue Ping-Chen με τίτλο «*SQL injection attack and guard technical research*» δημοσιευμένη στις 6/12/2011 στην ιστοσελίδα https://www.sciencedirect.com/science/article/pii/S1877705811022764?via%3Dihub ανευρεθείσα στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Πρωτοκόλλου της Σύμβασης του ΟΗΕ για τα δικαιώματα του παιδιού[25], ως παιδική πορνογραφία ορίζεται: «*κάθε αναπαράσταση, με οποιοδήποτε μέσο, ενός παιδιού που εμπλέκεται σε πραγματικές ή προσομοιωμένες γενετήσιες δραστηριότητες, ή οποιαδήποτε αναπαράσταση των γεννητικών οργάνων ενός παιδιού πρωταρχικά για γενετήσιους σκοπούς*».

[25] Νομοθετικό κείμενο του Ν.3625/2007, δημοσιευμένο στην ιστοσελίδα https://www.e-nomothesia.gr/kat-anilikoi/n-3625-2007.html ανευρεθέν στις 23/1/2022 (τελευταία πρόσβαση: 26/2/2022)

2. ΔΡΑΣΗ ΤΗΣ ΕΥΡΩΠΑΙΚΗΣ ΕΝΩΣΗΣ, ΤΟΥ ΔΙΕΘΝΟΥΣ ΤΟΠΙΟΥ ΚΑΙ ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΕΝΝΟΜΗΣ ΤΑΞΗΣ ΓΙΑ ΤΟ ΕΓΚΛΗΜΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Έχοντας ως δεδομένο τον παγκόσμιο και διασυνοριακό χαρακτήρα του κυβερνοεγκλήματος απαιτείται ένας βαθμός εναρμόνισης για να επιτευχθεί ένας προσδιορισμός του αξιοποίνου και απονομή της δικαιοσύνης. Προς αυτόν τον σκοπό τόσο οι θεσμοί και οι αρχές της Ευρωπαϊκής Ένωσης και Κοινότητας όσο και η διεθνής και ελληνική έννομη τάξη, συνασπίζονται και συνεργάζονται ώστε να αναζητηθούν και να εφαρμοστούν αρμοστές λύσεις οι οποίες θα οδηγήσουν στην αντιμετώπιση του κυβερνοεγκλήματος και στην θέσπιση ενός ισχυρού νομικού πλαισίου, το οποίο θα είναι ικανό να επιλύσει αυτό το περίπλοκο ζήτημα.

2.1. ΕΥΡΩΠΑΙΚΟ ΠΛΑΙΣΙΟ

Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.)[26]

Το 1983 έγινε για πρώτη φορά προσπάθεια να αντιμετωπιστεί το ζήτημα της ηλεκτρονικής εγκληματικότητας από μια ομάδα εμπειρογνωμόνων του ΟΟΣΑ, η οποία ανέλαβε αυτή την πρωτοβουλία στην προσπάθειά της να πετύχει την εναρμόνιση της ευρωπαϊκής νομοθεσίας με το κυβερνοέγκλημα. Εκεί ορίστηκε ως «*πληροφορικό έγκλημα*» αυτό που «*συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή και μετάδοση δεδομένων*».[27]

Ο ΟΟΣΑ μάλιστα προχώρησε στην πραγματοποίηση μιας μελέτης σχετικά με την δυνατότητα να εφαρμοστούν διεθνώς και να εναρμονιστούν οι ποινικοί νόμοι προς τον σκοπό της αντιμετώπισης του εγκλήματος στον κυβερνοχώρο αλλά και της κατάχρησης.[28] Η

[26] Πρόκειται για έναν διεθνή οργανισμό από ανεπτυγμένες χώρες, οι οποίες υποστηρίζουν τις αρχές της αντιπροσωπευτικής δημοκρατίας και της οικονομίας της ελεύθερης αγοράς, διαθέσιμο σε https://el.wikipedia.org/wiki/Οργανισμός_Οικονομικής_Συνεργασίας_και_Ανάπτυξης (τελευταία πρόσβαση: 26/2/2022)

[27] Μελέτη του Stein Schjolberg με τίτλο «*The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva*» δημοαπό ανσιευμένη τον Δεκέμβριο του 2008 στην ιστοσελίδα https://cybercrimelaw.net/documents/cybercrime_history.pdf ανευρεθείσα στις 22/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[28] Άρθρο με τίτλο «Cyber Crime Legislation» του Tala Tafazzoli, δημοσιευμένο τον Μάιο του 2018 στην ιστοσελίδα https://www.itu.int/en/ITU-D/Regional-

μελέτη αυτή κατέληξε σε μια έκθεση το 1986 με τίτλο *Computer Related Crime: Analysis of Legal Policy*, η οποία εξέταζε τους ήδη ιστάμενους νόμους και συνιστούσε μια λίστα από καταχρήσεις και επιθέσεις, τις οποίες οι χώρες θα πρέπει να εξετάζουν για να τις τιμωρούν με το ποινικό τους δίκαιο.[29]

Τον Ιούλιο του 2002, ο ΟΟΣΑ ενέκρινε ορισμένες κατευθυντήριες γραμμές σχετικά με την ασφάλεια των συστημάτων πληροφοριών, καλώντας τις κυβερνήσεις να το θέσουν ως προτεραιότητα και να προωθήσουν μια «κουλτούρα ασφαλείας» μεταξύ όλων των συμμετεχόντων. Οι κατευθυντήριες γραμμές καθιέρωσαν τις αρχές της ευαισθητοποίησης, της ευθύνης, της ηθικής, της δημοκρατίας, της διαχείρισης ασφάλειας και της αξιολόγησης κινδύνου.[30]

Σύμβαση για το έγκλημα στον κυβερνοχώρο (Convention of Cybercrime)

Μια πολύ σημαντική νομοθετική πρωτοβουλία για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και την χάραξη αντεγκληματικής πολιτικής αποτελεί η σύμβαση του Συμβουλίου της Ευρώπης ή όπως είναι γνωστή η Σύμβαση της Βουδαπέστης. Υπογράφτηκε στην Βουδαπέστη στις 23 Νοεμβρίου 2001 από 26 κράτη-μέλη του Συμβουλίου της Ευρώπης[31]. Στην Ελλάδα κυρώθηκε με τον Ν.4411/2016, με τον οποίο γίνεται πλέον επικαιροποίηση της ποινικής νομοθεσίας στον τομέα της «κυβερνοεγκληματικότητας» («cybercriminality»). Αποτελεί μάλιστα την πρώτη διεθνή συνθήκη[32] η οποία αποσκοπεί στην αντιμετώπιση του

Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf ανευρεθέν στις 10/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[29] Μελέτη του M.Chawki με τίτλο «*A Critical Look at the Regulation of Cybercrime*» δημοσιευμένη στην ιστοσελίδα https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiU8rT6t_X1AhUoRvEDHdotCXMQFnoECBMQAQ&url=https%3A%2F%2Fwww.ie-ei.eu%2FIE-EI%2FRessources%2Ffile%2Fbiblio%2FCriticalLookattheRegulationofCybercrime.doc&usg=AOvVaw2j24pxOk_-l2IE9cZbelYn ανευρεθείσα στις 10/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[30] Μελέτη του Xingan Li, με τίτλο «*International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene*» δημοσιευμένο στις 26/9/2007 στην ιστοσελίδα https://www.webology.org/2007/v4n3/a45.html#13 ανευρεθέν στις 10/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[31] Στην πραγματικότητα την υπέγραψαν 30 χώρες, από τις οποίες οι 26 ανήκαν ως μέλη στο Ευρωπαϊκό Συμβούλιο και οι 4 ήταν παρατηρητές-μη μέλη (Η.Π.Α, Καναδάς, Ιαπωνία, Νότια Αφρική)

[32]Γιαννόπουλος Γ. «*Εισαγωγή στην Νομική Πληροφορική*», εκδόσεις Νομική Βιβλιοθήκη, 2018 σελ. 154-155

Ηλεκτρονικού Εγκλήματος μέσω της εναρμόνισης των εθνικών νομοθεσιών, της βελτίωσης των διερευνητικών τεχνικών και την αύξηση της συνεργασίας μεταξύ των κρατών. Η σύμβαση περιλαμβάνει διατάξεις ουσιαστικού ποινικού δικαίου, ποινικού δικονομικού δικαίου και διεθνούς δικαστικής συνεργασίας. [33] Πιο συγκεκριμένα, οι διατάξεις ουσιαστικού ποινικού δικαίου αφορούν: διατάξεις που αναφέρονται σε εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας[34] των δεδομένων και των συστημάτων ηλεκτρονικού υπολογιστή[35], όπως είναι η παράνομη πρόσβαση και υποκλοπή, η επέμβαση σε δεδομένα, η επέμβαση σε συστήματα και η κακή χρήση συσκευών, διατάξεις για εγκλήματα σχετιζόμενα με υπολογιστές , όπως η απάτη μέσω Η/Υ και η πλαστογραφία, διατάξεις για εγκλήματα σχετικά με το περιεχόμενο[36], όπως το αδίκημα της παιδικής πορνογραφίας και διατάξεις για αδικήματα σχετικά με παραβιάσεις πνευματικών και συγγενικών δικαιωμάτων[37].

Οι διατάξεις ποινικού δικονομικού δικαίου αναφέρονται σε θέματα: ταχείας διαφύλαξης δεδομένων αποθηκευμένων σε σύστημα υπολογιστή, ταχείας διαφύλαξης και γνωστοποίησης διακινουμένων δεδομένων, εντολής παροχής πληροφοριών , έρευνας και κατάσχεσης αποθηκευμένων στοιχείων σε ηλεκτρονικό υπολογιστή ,πραγματικού χρόνου συλλογής διακινουμένων δεδομένων και παγίδευσης – υποκλοπής περιεχομένου δεδομένων. Οι διατάξεις διεθνούς δικαστικής συνεργασίας αναφέρονται :στην έκδοση, σε γενικές αρχές σχετικές με την αμοιβαία συνδρομή, σε παροχή αυθόρμητων πληροφοριών, στην ταχεία διαφύλαξη δεδομένων αποθηκευμένων σε σύστημα υπολογιστών, στην ταχεία γνωστοποίηση των διαφυλαγμένων διακινούμενων δεδομένων. [38] Αποτελεί πρότυπο και πηγή έμπνευσης ακόμα και για τις χώρες που δεν την έχουν υπογράψει.

---

[33] Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (ελληνικά) δημοσιευμένη στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0?lspt_destination=upgrade ανευρεθείσα στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[34] «*Confidentiality, integrity, availability*»

[35] «*Computer related offences*»

[36] «*Content related offences*»

[37] «*Offences related to infringement of copyright and related rights*»

[38] Άρθρο με τίτλο «Κινητοποιήσεις Ευρωπαϊκής Ένωσης σχετικά με το Ηλεκτρονικό Έγκλημα» δημοσιευμένο στις 17/9/2010 στην ιστοσελίδα https://electroniccrime.wordpress.com ανευρεθέν στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Πρόσθετο Πρωτόκολλο της Σύμβασης για το έγκλημα στον κυβερνοχώρο[39]

Δύο χρόνια μετά την Σύμβαση της Βουδαπέστης, στις 28 Ιανουαρίου του 2003 στο Στρασβούργο, η Σύμβαση συμπληρώνεται από το Πρόσθετο Πρωτόκολλο, το οποίο αφορούσε στην ποινικοποίηση της εξάπλωσης του ρατσισμού και της ξενοφοβίας μέσω του Διαδικτύου. Συγκεκριμένα, προτάθηκε η ποινικοποίηση της: 1) Διάδοσης ρατσιστικού και ξενοφοβικού υλικού μέσω της χρήσης ηλεκτρονικών υπολογιστών, 2) Διάδοσης ρατσιστικών και ξενοφοβικών απειλών και υβριστικών συνθημάτων, 3) Την χρησιμοποίηση συστημάτων ηλεκτρονικών υπολογιστών για την διάδοση υλικού σχετικού με την προώθηση εγκληματικών πράξεων.

Συμβούλιο της Ευρώπης (The Council of Europe Convention on Cybercrime)

Στα πλαίσια του Συμβουλίου του Συνεδρίου της Ευρώπης για το ηλεκτρονικό έγκλημα, εκδόθηκαν οι παρακάτω συστάσεις[40], οι οποίες συνέβαλαν στην προώθηση της συνεργασίας των κρατών-μελών με κοινό στόχο την ενημέρωση των χρηστών για τις αξιόποινες πράξεις του διαδικτύου και με την λήψη μέτρων προς την καταστολή του φαινομένου.

- Σύσταση No R (1989) 941:_Υιοθετήθηκε στις 13 Σεπτεμβρίου 1989 και αφορά εγκλήματα που διαπράττονται με ηλεκτρονικό υπολογιστή. Στόχος της συγκεκριμένης σύστασης ήταν να προτρέψει τα κράτη-μέλη και τους κυβερνώντες, να προάγουν την συνεργασία μεταξύ τους έτσι ώστε να αντιμετωπίσουν μαζικά και οργανωμένα ζητήματα που αφορούν στα ηλεκτρονικά αδικήματα, έχοντας ως σημαντικό γνώμονα και τον παγκόσμιο και διασυνοριακό χαρακτήρα των ηλεκτρονικών εγκλημάτων.

[39] Πρόσθετο Πρωτόκολλο της Σύμβασης για το έγκλημα στον κυβερνοχώρο, δημοσιευμένο στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/prostheto-protokollo-tis-symvasis-gia-egklima-ston?lspt_destination=upgrade ανευρεθέν στις 7/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[40] Δεν είναι υποχρεωτικές, ούτε έχουν αναγκαστική ισχύ, χρησιμοποιούνται ως πρόταση και βάση για την αντιμετώπιση των ηλεκτρονικών αδικημάτων σε ευρωπαϊκό επίπεδο.

[41] Recommendation No. R (89) 9, on computer-related crime, Council of Europe, Committee of Ministers, δημοσιευμένο στις 13/09/1989 στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f1094 ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

- Σύσταση No R (1995) 1342:_Υιοθετήθηκε στις 11 Σεπτεμβρίου 1995 και αφορούσε ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών. Για πρώτη φορά με αυτήν την σύσταση, παρέχονται οι βασικές ποινικές δικονομικές αρχές με βάση τις οποίες πρέπει να λειτουργεί η έρευνα σχετικά με τα ηλεκτρονικά εγκλήματα, όπως για παράδειγμα οι όροι τήρησης και αποθήκευσης των προσωπικών δεδομένων.
- Σύσταση No R (2001) 843:_Υιοθετήθηκε στις 5 Σεπτεμβρίου 2001 και αφορούσε την αυτορρύθμιση σε θέματα σχετικά με το περιεχόμενο του διαδικτύου. Μέσα στην σύμβαση τονίζεται η ανάγκη της ελεύθερης χρήσης του διαδικτύου και η προστασία των δικαιωμάτων του ανθρώπων, ωστόσο τα κράτη-μέλη και οι κυβερνήσεις θα πρέπει να συνασπίζονται ώστε να ενημερώνουν τους χρήστες για τους κινδύνους που ελλοχεύουν αλλά και να προσπαθούν να βρουν λύσεις στα προβλήματα που προκύπτουν.
- Σύσταση CM/Rec (2001) 8:44_Όλες οι αναφερθείσες συστάσεις θα πρέπει να εφαρμόζονται με κεντρικό γνώμονα τον σεβασμό του δικαιώματος ελεύθερης χρήσης στο διαδίκτυο αλλά και την προστασία των δικαιωμάτων των ανθρώπων σε αυτό και προς τον σκοπό αυτό υιοθετήθηκε στις 21 Σεπτεμβρίου 2011 η εν λόγω σύσταση. Στόχος της είναι η προστασία του ανοιχτού και οικουμενικού χαρακτήρα του διαδικτύου, καθώς και η συνεργασία των κρατών-μελών προς επίρρωση του παραπάνω σκοπού.
- Απόφαση Πλαίσιο 2001/413/ΔΕΥ για την καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν μέσα πληρωμής (πλην μετρητών)45-Απάτη με υπολογιστή ως πρώτο από τα σχετικά εγκλήματα που εντοπίστηκε

[42] Recommendation No. R (95) 13, Concerning Problems of Criminal Procedural Law connected with Information Technology, Council of Europe Committee of Ministers δημοσιευμένο στις 11/9/1995 στην ιστοσελίδα https://rm.coe.int/16804f6e76 ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[43] Recommendation No. R (2001) 8, on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), Council of Europe, Committee of Ministers δημοσιευμένο στις 5/9/2001 στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5105 ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[44] Recommendation CM/Rec (2011) 8, on the protection and promotion of the universality, integrity and openness of the Internet, Council of Europe Committee of Ministers δημοσιευμένο στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8 ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[45] Απόφαση-πλαίσιο 2001/413/ΔΕΥ- Καταπολέμηση της απάτης και της πλαστογραφίας που αφορούν τα μέσα πληρωμής πλην των μετρητών δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=CELEX:3

- Απόφαση Πλαίσιο 2004/68/ΔΕΥ για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας[46]-Για πρώτη φορά πραγματοποιείται ορισμός του ηλεκτρονικού εγκλήματος και προσδιορισμός ως μέσο τέλεσης του αδικήματος της παιδικής πορνογραφίας
- Απόφαση Πλαίσιο 2005/222/ΔΕΥ για τις επιθέσεις κατά συστημάτων πληροφοριών47- Με την εν λόγω απόφαση η βαρύτητα δίνεται στο αδίκημα της παράνομης πρόσβασης σε σύστημα πληροφοριών. Τυποποίηση γνήσιων πληροφοριακών εγκλημάτων. Η απόφαση αυτή καταργήθηκε με την υιοθέτηση της Οδηγίας 2013/40.

Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος-EC3 (European Cybercrime Center)[48]

Στις αρχές του 2013 η Europol ίδρυσε το Ευρωπαϊκό Κέντρο για το Έγκλημα στον κυβερνοχώρο, το οποίο αποτελεί σημείο αναφοράς για την αντιμετώπιση του ηλεκτρονικού εγκλήματος και παρέχει ένα πλήθος υπηρεσιών, έχοντας ως στόχο να βοηθήσει στην ενίσχυση και την προστασία των ευρωπαίων πολιτών και επιχειρήσεων από το διαδικτυακό έγκλημα. Από την ίδρυσή του, το κέντρο έχει συμβάλει αποτελεσματικά στην αντιμετώπιση του αναφερθέντος προβλήματος και στην εξάρθρωση εγκληματικών δικτύων και η δράση του διαρθρώνεται σε τρία σκέλη, σε αυτό της εγκληματολογίας, της στρατηγικής και των επιχειρήσεων. Το EC3 εστιάζει κυρίως στην αντιμετώπιση εγκλημάτων που εξαρτώνται από τον κυβερνοχώρο (κακόβουλο λογισμικό, hacking κλπ.), στην διαδικτυακή σεξουαλική εκμετάλλευση των παιδιών και στην απάτη πληρωμών.

F0413 ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[46] Απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου της 22ας Δεκεμβρίου 2003 για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33138 ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[47] Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:32005F0222 ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[48] European Cybercrime Centre-EC3, Combating crime in a digital age δημοσιευμένο και αναθεωρημένο στις 19/11/2021 στην επίσημη ιστοσελίδα της Europol https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Europol: Έκθεση αξιολόγησης απειλών από το σοβαρό και οργανωμένο έγκλημα στον κυβερνοχώρο [49]

Το IOCTA (*Internet Organised Crime Threat Assessment*) είναι μια πρωτοβουλία της Europol, εκδίδεται σε ετήσια βάση και έχει ως αποστολή την ανάδειξη των απειλών από το έγκλημα στον κυβερνοχώρο αλλά και την αξιολόγηση των προκλήσεων και τον εξελίξεων σε αυτόν. Η ομάδα εργασίας της Europol συλλέγει δεδομένα από όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης και με βάση τα χαρακτηριστικά των απειλών που έχουν σημειωθεί στο διαδίκτυο το τελευταίο διάστημα επικεντρώνονται στους τρόπους επικράτησης του εγκλήματος στον Κυβερνοχώρο και στην δυνατότητα αντιμετώπισής του. Στο πεδίο δραστηριοτήτων της IOCTA περιλαμβάνονται εγκληματικές πράξεις οι οποίες δεν είναι εγγενώς εγκληματικοί αλλά μπορούν να εμπλέκονται σε περισσότερους τομείς εγκληματικότητας. Συγκεκριμένα αυτές οι πράξεις είναι οι εξής: phishing/smishing/vishing, επιχειρηματικός ηλεκτρονικός συμβιβασμός (business e-mail compromise), αλεξίσφαιρη φιλοξενία (bulletproof hosting), εργαλεία ανωμυμοποίησης (anonymization tools), ποινική κατάχρηση κρυπτοσυχνοτήτων (criminal abuse of cryptocurrencies) και money mulling[50].

Κέντρο Τεχνητής Νοημοσύνης και Ρομποτικής του Διαπεριφερειακού Ινστιτούτου Έρευνας του ΟΗΕ για το έγκλημα και την δικαιοσύνη

Πρόκειται για ένα ερευνητικό τμήμα των Ηνωμένων Εθνών, το οποίο είναι ενεργό στην επιχείρηση οργάνωσης και ενημέρωσης του κοινού σχετικά με την ρομποτική και την τεχνητή νοημοσύνη, καθώς και συμβάλλει στην κατανόηση και εμβάθυνση των απειλών στο κυβερνοχώρο αλλά και στην χάραξη πολιτικής και επιβολής του νόμου.[51] Μάλιστα, κάθε χρόνο η UNICRI διοργανώνει την Παγκόσμια Συνάντηση για την Τεχνητή Νοημοσύνη για την Επιβολή του Νόμου[52], μια εκδήλωση στην οποία συμμετέχουν εμπειρογνώμονες και επιστήμονες από διάφορους τομείς και από διαφορετικές χώρες και αναπτύσσει θέματα

[49] Αξιολόγηση απειλών για το οργανωμένο έγκλημα στο Διαδίκτυο (IOCTA)- Στρατηγικές, πολιτικές και τακτικές ενημερώσεις για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, δημοσιευμένη στις 7/12/2021 στην ιστοσελίδα https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[50] Πρόκειται για ένα είδους ξεπλύματος βρώμικου χρήματος.

[51] Δημοσίευση με τίτλο *Artificial Intelligence and Robotics for Law*, διαθέσιμη στην ιστοσελίδα http://www.unicri.it/artificial-intelligence-and-robotics-law-enforcement ανευρεθείσα στις 28/2/2022 (τελευταία πρόσβαση: 28/2/2022)

[52] Global Meeting 23-27 Nov, διαθέσιμο στην ιστοσελίδα http://www.unicri.it/News/AI-UNICRI-INTERPOL-Lawenforcement ανευρεθέν στις 28/2/2022 (τελευταία πρόσβαση: 28/2/2022)

σχετικά με την τεχνητή νοημοσύνη και τις προκλήσεις της, με στόχο την αντιμετώπιση των υπηρεσιών επιβολής νόμου και την ορθή απονομή δικαιοσύνης.

Europol,UNICRI, Trend Micro: Έκθεση για τις τρέχουσες και προβλεπόμενες εγκληματικές χρήσεις της τεχνητής νοημοσύνης[53]

Μέσα από την παρούσα έκθεση παρέχεται στους φορείς επιβολής του νόμου, στους υπεύθυνους χάραξης πολιτικής καθώς και σε άλλους οργανισμούς σημαντικές πληροφορίες για επιθέσεις (υπάρχουσες ή και πιθανές) που αξιοποιούν την τεχνητή νοημοσύνη και προτάσεις για το πως θα μειωθούν αυτές οι απειλές και αυτοί οι κίνδυνοι. Ο επικεφαλής του Ευρωπαϊκού Κέντρου για την Καταπολέμηση του Κυβερνοεγκλήματος της Europol Edvardas Sileris ανέφερε πως: *«Η τεχνητή νοημοσύνη υπόσχεται στον κόσμο μεγαλύτερη αποτελεσματικότητα, αυτοματοποίηση και αυτονομία. Σε μια εποχή όπου το κοινό ανησυχεί όλο και περισσότερο για την πιθανή κατάχρηση της τεχνητής νοημοσύνης, πρέπει να είμαστε διαφανείς σχετικά με τις απειλές, αλλά και να εξετάσουμε τα πιθανά οφέλη από την τεχνολογία AI. Αυτή η αναφορά θα μας βοηθήσει όχι μόνο να προβλέψουμε πιθανές κακόβουλες χρήσεις και καταχρήσεις της τεχνητής νοημοσύνης, αλλά και να προλάβουμε και να μετριάζουμε αυτές τις απειλές προληπτικά. Αυτός είναι ο τρόπος με τον οποίο μπορούμε να ξεκλειδώσουμε τις πιθανές δυνατότητες AI και να επωφεληθούμε από τη θετική χρήση των συστημάτων AI».*

Η έκθεση καταλήγει στο συμπέρασμα πως αφενός οι εγκληματίες του κυβερνοχώρου θα αξιοποιήσουν την τεχνητή νοημοσύνη τόσο ως φορέα επίθεσης όσο και ως τρόπο επίθεσης, αφετέρου στο μέλλον θα χρειαστεί μια να τεχνολογία ελέγχου ώστε να σταματήσει όσο γίνεται ο κίνδυνος παραπληροφόρησης αλλά και απειλές που στρέφονται κατά δεδομένων τεχνητής νοημοσύνης.

[53] Έκθεση της Europol με τίτλο «*New report finds that criminals leverage AI for malicious use-and it's not just deep fakes*» δημοσιευμένο στην ιστοσελίδα https://www.europol.europa.eu/media-press/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-–-and-it's-not-just-deep-fakes ανευρεθέν στις 3/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Οι τρεις οργανισμοί προέβησαν σε ορισμένες συστάσεις στο τέλος της έκθεσης για την αντιμετώπιση του παραπάνω προβλημάτων:

- Οι τεχνολογίες AI να αξιοποιηθούν ως εργαλεία καταπολέμησης του εγκλήματος για την προστασία του μέλλοντος της βιομηχανίας και της αστυνόμευσης στον κυβερνοχώρο.
- Να προχωρήσει η έρευνα για την ανάπτυξη της αμυντικής τεχνολογίας
- Να προωθηθεί και να αναπτυχθεί ασφαλές πλαίσιο σχεδίασης AI
- Να αποκλιμακωθεί η ρητορική σχετικά με τη χρήση της τεχνητής νοημοσύνης για σκοπούς κυβερνοασφάλειας
- Να δημιουργηθούν πολυεπιστημονικές ομάδες εμπειρογνωμόνων και να συμπράξει ο δημόσιος με τον ιδιωτικό τομέα

Οδηγία 2013/40/ΕΕ για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου[54]

Με την εν λόγω Οδηγία τίθεται το ευρωπαϊκό πλαίσιο με ενιαίους κανόνες για αδικήματα και επιθέσεις που στρέφονται κατά των συστημάτων πληροφοριών. Πηγή έμπνευσης της Οδηγίας υπήρξε η Σύμβαση για το Έγκλημα στον Κυβερνοχώρο, η οποία είναι το νομικό πλαίσιο αναφοράς για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων κατά συστημάτων πληροφοριών (αιτιολογική σκέψη 15) και αντικατέστησε την Απόφαση-Πλαίσιο 2013/40/ΕΕ. Ως νομοθετικό κείμενο δεν συνιστά ριζική τροποποίηση, αντίθετα το πεδίο εφαρμογής του είναι στενότερο από αυτού της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο. Σκοπός της Οδηγίας είναι η εναρμόνιση της κείμενης νομοθεσίας των κρατών μελών της Ευρωπαϊκής Ένωσης, ως προς τα θέματα επιθέσεων κατά πληροφοριακών συστημάτων, μέσω της θέσπισης κανόνων και κυρώσεων και συνεργασίας με εξειδικευμένους φορείς, όπως η Europol και ο ENISA.[55] Η συνεργασία

[54] Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32013L0040 ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση:)

[55] Σκέψη 1 της Οδηγίας 2013/40/ΕΕ «*Οι στόχοι της παρούσας οδηγίας είναι η προσέγγιση του ποινικού δικαίου των κρατών μελών στον τομέα των επιθέσεων κατά συστημάτων πληροφοριών, καθιερώνοντας ελάχιστους κανόνες σχετικά με τον ορισμό των ποινικών αδικημάτων και των σχετικών κυρώσεων, και η βελτίωση της συνεργασίας μεταξύ των αρμόδιων αρχών, συμπεριλαμβανομένης της αστυνομίας και άλλων εξειδικευμένων υπηρεσιών επιφορτισμένων με την επιβολή του νόμου στα κράτη μέλη, καθώς και των αρμόδιων ειδικευμένων οργανισμών της Ένωσης και*

διεθνώς μεταξύ των δικαστικών αρχών και των αρχών επιβολής νόμου, θα συμβάλει στην αποτελεσματικότερη καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

Ειδικότερα:

Το άρθρο 2 περιέχει τον ορισμό του συστήματος πληροφοριών. Ως τέτοιο σύστημα νοείται «*η συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μια ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ηλεκτρονικών δεδομένων, καθώς και τα ηλεκτρονικά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρησή τους*».

Το άρθρο 3, στο οποίο αναφέρεται στο έγκλημα της παράνομης πρόσβασης σε σύστημα πληροφοριών «*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι, η απόκτηση πρόσβασης εκ προθέσεως και χωρίς δικαίωμα, στο σύνολο ή σε μέρος του συστήματος πληροφοριών, τιμωρείται ως ποινικό αδίκημα, οσάκις διαπράττεται παραβιάζοντας μέτρο ασφαλείας, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις*», τίθεται ως προϋπόθεση η παραβίαση μέτρου ασφαλείας[56]. Το έννομο αγαθό το οποίο χρήζει προστασίας από την διάταξη είναι η εμπιστευτικότητα.

Το άρθρο 4, αναφέρεται στην παράνομη παρεμβολή σε σύστημα «*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η σοβαρή παρεμπόδιση ή διακοπή της λειτουργίας συστήματος πληροφοριών, με την εισαγωγή ηλεκτρονικών δεδομένων, διαβίβαση, ζημία, διαγραφή, φθορά, αλλοίωση ή εξάλειψη αυτών των δεδομένων ή με τον αποκλεισμό της πρόσβασης στα δεδομένα αυτά, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις*», όπου ρητώς γίνεται η αναφορά στην τέλεση της πράξης από τον δράστη, χωρίς ο τελευταίος να έχει αυτό το δικαίωμα. Προστατευτέο έννομο αγαθό είναι η ακεραιότητα και η διαθεσιμότητα των συστημάτων πληροφοριών και των δεδομένων τους.

φορέων της Ένωσης, όπως η Eurojust, η Ευρωπόλ και το Ευρωπαϊκό Κέντρο Ηλεκτρονικού Εγκλήματος, καθώς και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια δικτύων και Πληροφοριών (ENISA)».

[56] Ως παραβίαση ασφαλείας νοείται κάθε μέτρο παράκαμψης της ασφάλειας, για παράδειγμα η χρήση στοιχείων ταυτοποίησης άλλου νόμιμου χρήστη.

Το άρθρο 5, αναφέρεται στην παράνομη παρεμβολή σε δεδομένα «*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η διαγραφή, ζημία, φθορά, αλλοίωση ή εξάλειψη ηλεκτρονικών δεδομένων ενός συστήματος πληροφοριών ή ο αποκλεισμός της πρόσβασης στα δεδομένα αυτά εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις*», η οποία ποινικοποιείται μόνο όταν τελείται εκ προθέσεως και χωρίς δικαίωμα. Προστατευτέο αγαθό είναι η πληροφορία και η χρήση ή η αξιοποίησή της.

Στο άρθρο 6 περί της παράνομης υποκλοπής, ισχύουν τα παρακάτω «*Τα κράτη μέλη λαμβάνουν τα αναγκαία μέτρα για να εξασφαλίσουν ότι η υποκλοπή με τεχνικά μέσα, μη δημόσιων διαβιβάσεων ηλεκτρονικών δεδομένων από, προς ή μέσα σε ένα σύστημα πληροφοριών, συμπεριλαμβανομένων των ηλεκτρομαγνητικών εκπομπών από ένα σύστημα πληροφοριών που περιέχει τέτοια ηλεκτρονικά δεδομένα, εκ προθέσεως και χωρίς δικαίωμα, τιμωρείται ως ποινικό αδίκημα, τουλάχιστον όταν δεν πρόκειται για ήσσονος σημασίας περιπτώσεις*». Στην διάταξη προστατεύεται η εμπιστευτικότητα της ηλεκτρονικής επικοινωνίας. Αξίζει να αναφερθεί ότι σύμφωνα με την αιτιολογική σκέψη 9, «*Η υποκλοπή περιλαμβάνει, ενδεικτικά και όχι εξαντλητικά, την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και την παροχή του περιεχομένου των δεδομένων είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα*».

Συνοπτικά, σε κάθε προβλεπόμενη περίπτωση της Οδηγίας, η πράξη επίθεσης θα πρέπει να τελείται με πρόθεση από τον δράστη.[57] Με βάση την αιτιολογική σκέψη 17, η οδηγία δεν αποδίδει ποινική ευθύνη όταν πληρούνται τα αντικειμενικά κριτήρια των αδικημάτων που ορίζονται στην παρούσα οδηγία, αλλά οι πράξεις διαπράττονται χωρίς εγκληματική πρόθεση, παραδείγματος χάριν όταν το πρόσωπο δεν γνωρίζει ότι απαγορεύεται η πρόσβαση ή στην περίπτωση εξουσιοδοτημένης δοκιμής ή προστασίας συστημάτων

[57] Άρθρο του Lawspot με τίτλο «*Το ευρωπαϊκό πλαίσιο για τις επιθέσεις κατά των συστημάτων πληροφοριών*», δημοσιευμένο στις 16/11/2017 στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/eyropaiko-plaisio-gia-tis-epitheseis-kata-ton-systimaton?lspt_destination=upgrade ανευρεθέν στις 9/2/2022 (τελευταία πρόσβαση: 26/2/2022)

πληροφοριών, όπως όταν μια εταιρεία ή ένας πωλητής αναθέτει σε ένα πρόσωπο να ελέγξει την ισχύ του συστήματος ασφαλείας του.

Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA)

Ο ENISA (*European Network and Information Security Agency*) είναι ένα ευρωπαϊκό κέντρο για την ασφάλεια στον κυβερνοχώρο, το οποίο παρέχει συμβουλές σε φορείς δημοσίου και ιδιωτικού δικαίου των χωρών της Ευρωπαϊκής Ένωσης και βοηθάει στην ενίσχυση της πολιτικής και της νομοθεσίας της ΕΕ σχετικά με την ασφάλεια δικτύων και πληροφοριών. Κεντρικός στόχος είναι η διασφάλιση ενός υψηλού κοινού επιπέδου κυβερνοασφάλειας σε όλη την Ευρώπη.[58]

Κοινή ομάδα δράσης για το έγκλημα στον Κυβερνοχώρο-(J-CAT)[59]

Η πρωτοβουλία της δημιουργίας κοινών ομάδων δράσης για το κυβερνοέγκλημα, η οποία ξεκίνησε τον Σεπτέμβριο του 2014, αποτελεί σημαντική εξέλιξη με σκοπό την συντονισμένη δράση απέναντι στις απειλές που υπάρχουν στο διαδίκτυο και στην αντιμετώπισή τους εντός και εκτός της Ευρωπαϊκής Ένωσης. Η ομάδα αποτελείται από αξιωματικούς συνδέσμους της Ευρωπαϊκής Ένωσης αλλά και από εταίρους εκτός αυτής, οι οποίοι εργάζονται στο ίδιο γραφείο για να διασφαλίζεται η ομαλή και άμεση επικοινωνία μεταξύ των.

Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο

Στις 7.2.2013 η Ευρωπαϊκή Επιτροπή, παράλληλα με την Οδηγία, προχώρησε στην δημοσίευση της στρατηγικής για την ασφάλεια στον κυβερνοχώρο και στην πρόταση οδηγίας με κεντρικό στόχο την διασφάλιση ενός ασφαλούς δικτύου πληροφοριών στην

[58] Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) ανευρεθέν στην επίσημη ιστοσελίδα της Ευρωπαϊκής Ένωσης https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el

[59] Joint Cybercrime Action Taskforce (J-CAT), Fighting cybercrime around the world, δημοσιευμένο στις 14/12/2021 στην επίσημη ιστοσελίδα της Europol https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Ευρωπαϊκή Ένωση.[60] Η νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια έχει ως σκοπό την διαφύλαξη και προστασία ενός παγκόσμιου και ανοιχτού διαδικτύου αλλά και την προστασία των ευρωπαϊκών αξιών και των θεμελιωδών δικαιωμάτων. Οι τρεις τομείς δράσης της ΕΕ στοχεύουν στην *Ανθεκτικότητα, την τεχνολογική κυριαρχία και ηγετική θέση*, στην *Ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντιμετώπισης* και στην *Προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου μέσω αυξημένης συνεργασίας.*[61]

Βασικός στόχος των δράσεων της Ευρωπαϊκής Ένωσης είναι να ενισχυθεί η ασφάλεια στον κυβερνοχώρο αλλά και να προληφθούν και να αντιμετωπιστούν συνθήκες οι οποίες θα οδηγούσαν σε επιθέσεις σε αυτόν, πάντοτε με γνώμονα την προώθηση της δημοκρατίας και της ανάπτυξης του ψηφιακού κόσμου με ασφάλεια.[62]

2.2.ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ

Ν.4411/2016[63]

Ο νόμος 4411/2016[64], αποτελείται από δύο μέρη. Στο πρώτο μέρος κυρώνεται η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλό της. Στο δεύτερο μέρος γίνεται μεταφορά στο Ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του

---

[60] ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ, Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο, Βρυξέλλες, 7.2.2014 JOIN (2013) 1 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαικής Επιτροπής https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 ανευρεθέν στις 9/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[61] Άρθρο από adminlaw με τίτλο «*Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια*» δημοσιευμένο στις 16/12/2020 στην ιστοσελίδα https://lawnet.gr/law-news/nea-stratigiki-tis-ee-gia-tin-kyvernoasfaleia/ ανευρεθέν στις 9/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[62] Άρθρο του Ιγγλεζάκη με τίτλο «Επιθέσεις κατά συστημάτων πληροφοριών» δημοσιευμένο στις 9/10/2015 στο περιοδικό Δίκαιο και Νέες Τεχνολογίες, ανευρεθέν στην ιστοσελίδα http://www.cybercc.gr/m/filer_public/2015/10/09/igglezakhs_epitheseis_kata_systimatwn_pliroforiwn.pdf στις 9/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[63] Νόμος 4411/2016:Κύρωση της Σύμβασης για το έγκλημα στον Κυβερνοχώρο δημοσιευμένος στην ιστοσελίδα https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html ανευρεθείς στις 12/1/2021 (τελευταία πρόσβαση: 26/2/2022)

[64] Δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως στις 3/8/2016 (ΦΕΚ 142/Α΄/3.8.2016).

Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις Επιθέσεις κατά Συστημάτων Πληροφοριών.

-Άρθρο 13 ΠΚ- Πληροφοριακά συστήματα και Ψηφιακά Δεδομένα

Εισάγονται δύο πρόσθετοι ορισμοί σχετικά με το τι είναι πληροφοριακό σύστημα αλλά και ψηφιακά δεδομένα, καθώς είναι απαραίτητοι για την ερμηνεία των νέων διατάξεων.

« Στο άρθρο 13 του Ποινικού Κώδικα προστίθενται περιπτώσεις η' και θ' ως εξής: «η) Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

θ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία».

-Άρθρο 292Β &Γ- Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

Σύμφωνα με όσα ορίζονται και στην Οδηγία (άρθρο 4) προβλέπονται αυστηρότερες ποινές όταν προκαλείται ζημιά σε σημαντικό αριθμών πληροφοριακών συστημάτων μέσω εργαλείων που έχουν σχεδιαστεί ειδικά γι' αυτό. Με την συγκεκριμένη διάταξη καλύπτεται ένα μεγάλο νομοθετικό κενό το οποίο υπήρχε σχετικά με την ανάγκη αυτοτελούς αντιμετώπισης των τεχνολογικών επιθέσεων κατά των πληροφοριακών συστημάτων.

«Παρακώλυση λειτουργίας πληροφοριακών συστημάτων

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

2.Η πράξη της πρώτης παραγράφου τιμωρείται:

α) με φυλάκιση από ένα (1) έως τρία (3) έτη, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων

που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον ενός (1) έτους, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον ενός (1) έτους, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.
3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.
4.Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

-Άρθρο 348Β-Πορνογραφία ανηλίκων

Εισάγεται τροποποίηση ως προς τον όρο του πληροφοριακού συστήματος. Με την εν λόγω διάταξη γίνεται θεσμική αποτύπωση του γνωστού και ως «grooming», δηλαδή του φαινομένου της διαδικτυακής αποπλάνησης ανηλίκου, όπου συνιστά και μια από τις πιο σοβαρές εγκληματικές στο διαδίκτυο. Συγκεκριμένα εδώ, ο ενήλικας μπορεί διαδικτυακά να δημιουργήσει μια χρόνια σχέση οικειότητας με τον ανήλικο, ώστε να του εμπιστευτεί δεδομένα της προσωπικής του ζωής όπως είναι φωτογραφίες και οπτικοακουστικό υλικό. Στην συνέχεια, ο ενήλικος-δράστης με αυτό το υλικό μπορεί να προβεί σε παραγωγή, διάδοση, χρήση πορνογραφίας..[65]

«Προσέλκυση παιδιών για γενετήσιους λόγους
Όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται

[65] Άρθρο των Craven S./Brown S./Gilchrist E.με τίτλο «*Sexual grooming of children: Review of literature and theoretical considerations*» δημοσιευμένο στην ιστοσελίδα https://psycnet.apa.org/record/2006-23335-007 στις 20/2/2007 , ανευρεθέν στις 15/4/2022 (τελευταία πρόσβαση: 8/5/2022)

με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ».

-Άρθρο 370 Α-Ε ΠΚ- Παρεμβολές σε δεδομένα- Παράνομη Υποκλοπή Ψηφιακών Δεδομένων

Στο άρθρο 370Γ τιμωρείται και η χωρίς δικαίωμα πρόσβαση στο σύνολο ή σε τμήμα ενός πληροφοριακού συστήματος, δηλαδή το λεγόμενο hacking.

«Παράνομη πρόσβαση σε πληροφοριακό σύστημα

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

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

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

4.Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση».

Στο 370Δ τιμωρείται αυτοτελώς η παραβίαση του απορρήτου των επικοινωνιών μέσω πληροφοριακών συστημάτων και η χρήση των πληροφοριών.

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

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

3.Αν οι πράξεις των παραγράφων 1 και 2 συνεπάγονται παραβίαση στρατιωτικού ή διπλωματικού απορρήτου ή αφορούν απόρρητο που αναφέρεται στην ασφάλεια του Κράτους σε καιρό πολέμου τιμωρούνται κατά το άρθρο 146».

Στο 370Ε τιμωρείται αυτοτελώς η εισαγωγή, διανομή κατοχή και διάθεση προγραμμάτων, συσκευών ή τεχνικών μέσων, με τα οποία θα ήταν δυνατή η πρόσβαση σε πληροφοριακό σύστημα.

«Με φυλάκιση μέχρι δύο (2) ετών τιμωρείται όποιος χωρίς δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ παράγραφοι 2 και 3 και 370Δ παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει, διανέμει ή με άλλο τρόπο διακινεί: α) συσκευές ή προγράμματα υπολογιστή, σχεδιασμένα ή προσαρμοσμένα κυρίως για το σκοπό της διάπραξης κάποιου από τα εγκλήματα των άρθρων 370Β, 370Γ και 370Δ, β) συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τη χρήση των οποίων είναι δυνατόν να αποκτηθεί πρόσβαση στο σύνολο ή μέρος ενός πληροφοριακού συστήματος».

-Άρθρο 381Α-Φθορά ηλεκτρονικών δεδομένων

Προβλέπεται η ποινική ευθύνη των προσώπων που αγοράζουν, πωλούν, προμηθεύον, κατέχουν κλπ. προγράμματα και έτσι παρανόμως παρεμβαίνουν σε ψηφιακά δεδομένα. Το άρθρο 381Α ενσωμάτωσε το άρθρο 7 της οδηγίας 2013/40/ΕΕ.

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

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

3.Αν οι πράξεις των προηγούμενων παραγράφων τελέστηκαν στο πλαίσιο δομημένης και με διαρκή δράση ομάδας τριών ή περισσότερων προσώπων, που επιδιώκει την τέλεση περισσότερων εγκλημάτων του παρόντος άρθρου, ο υπαίτιος τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών.
4.Για την ποινική δίωξη της πράξης της παραγράφου 1 απαιτείται έγκληση».

-Άρθρο 386Α-Απάτη με υπολογιστές

Στο συγκεκριμένο άρθρο περιλαμβάνεται κάθε μορφή απάτης με την διαφορά όμως, πως ως μέσο για την τέλεσή της απαιτείται η χρήση του ηλεκτρονικού υπολογιστή. Στην διάταξη καλύπτονται και οι πιο σύγχρονες μορφές εγκληματικότητας όπως το phishing, η χρήση πλαστών πιστωτικών καρτών κ.ά.

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

Ελληνικό Κέντρο για το Κυβερνοέγκλημα (GCC)

Το GCC(*Greek Cybercrime Center*) είναι αποτελεί μέρος μιας συντονισμένης προσπάθειας[66] για την αντιμετώπιση του κυβενροεγκλήματος. Στόχος του κέντρου είναι η προσπάθεια κατάρτισης και εκπαίδευσης σε θέματα εγκλημάτων στον κυβερνοχώρο, η επέκταση της έρευνας σε συγκεκριμένες περιοχές και η αφύπνιση της περιφέρειας και η συνεργασία με παρόμοιους φορείς για την αποτελεσματικότερη αντιμετώπιση του ζητήματος. Μέσω της εκπαίδευσης και της έρευνας το GCC προωθεί μια καινοτόμα έρευνα ως προς το κυβερνοέγκλημα.[67]

[66] Διαχειριστής του έργου είναι το Ίδρυμα Τεχνολογίας και Έρευνας, ενώ τα λοιπά μέλη της κοινοπραξίας είναι το Safenet, το ΑΠΘ και το Κέντρο Μελετών Ασφάλειας (ΚΕ.ΜΕ.Α) του Υπουργείου Δημοσίας Τάξης και Προστασίας του Πολίτη.
[67] Ελληνικό Κέντρο για το Κυβερνοέγκλημα, δημοσιευμένο στην ιστοσελίδα του Κέντρου Μελετών Ασφαλείας http://www.kemea.gr/el/epikairotita/153-elliniko-kentro-gia-to-kyvernoegklima ανευρεθέν στις 9/2/2022 (τελευταία πρόσβαση: 26/2/2022)

Περιορισμός πρόσβασης χρηστών μόνο για παράνομο περιεχόμενο στο Διαδίκτυο

Από την ισχύουσα εθνική νομοθεσία μέχρι στιγμής προβλέπεται μόνο σε τρεις περιπτώσεις ο περιορισμός πρόσβασης χρηστών μόνο για παράνομο περιεχόμενο στο Διαδίκτυο:

- Ν.4002/2011 για την «Ρύθμιση της αγοράς παιγνίων»[68]- προβλέπεται φραγή πρόσβασης ημεδαπών σε ιστοσελίδες στοιχημάτων και τυχερών παιγνίων που δεν έχουν αδειοδοτηθεί από την Επιτροπή Εποπτείας και Ελέγχου Παιγνίων, σε συνεργασία με τις εταιρείες παροχής υπηρεσιών διαδικτύου (Internet Service Providers- ISPs) που λειτουργούν στην Ελλάδα.
- Ν.4267/2014- άρθρο 18 για την «Καταπολέμηση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις»[69]- φραγή πρόσβασης ημεδαπών σε υλικό πορνογραφίας ανηλίκων στο Διαδίκτυο σε συνεργασία με τους ISPs.
- Ν.4481/2017-άρθρο 52 για τις «Κυρώσεις για προσβολές δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων στο Διαδίκτυο»[70]-ταχεία διοικητική διαδικασία για την διακοπή πρόσβασης σε ιστοτόπους που φιλοξενούν παρανόμως προστατευόμενα πνευματικά έργα.

3. Το πρόβλημα της δικαιοδοσίας στο Διαδίκτυο

Λόγω του παγκόσμιου χαρακτήρα του Διαδικτύου και του γεγονότος ότι οποιοσδήποτε μπορεί να έχει πρόσβαση σε όποια πληροφορία θέλει, η δικαιοδοσία στο Διαδίκτυο δεν είναι μια απλή υπόθεση. Τα περισσότερα νομοθετικά και μη κείμενα, υποστηρίζουν πως με τις διαστάσεις που έχει πάρει πλέον η εγκληματικότητα στο διαδίκτυο, για να μπορέσει να υπάρξει ουσιαστική αντιμετώπιση των κυβερνοεγκλημάτων θα πρέπει να υπάρξει

[68] Ν.4002/2011 (ΦΕΚ Α'180/22-08-2011) ΜΕΡΟΣ Δ- ΡΥΘΜΙΣΗ ΤΗΣ ΑΓΟΡΑΣ ΠΑΙΓΝΙΩΝ ΚΑΙ ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ δημοσιευμένος στην ιστοσελίδα https://www.taxheaven.gr/law/4002/2011 ανευρεθέν στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[69] Ν.4267/2014- ΦΕΚ 137/Α/12-6-2014 Καταπολέμησης της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις, δημοσιευμένος στην ιστοσελίδα https://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.html ανευρεθείς στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[70] Ν.4481/2017- ΦΕΚ Α'100/20.07.2017 Συλλογική διαχείριση δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων, χορήγηση πολυεδαφικών αδειών για επιγραμμικές χρήσεις μουσικών έργων και άλλα θέματα αρμοδιότητας Υπουργείου Πολιτισμού και Αθλητισμού δημοσιευμένος στην ιστοσελίδα https://www.kodiko.gr/nomothesia/document/272968/nomos-4481-2017 ανευρεθείς στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

διακρατική συνεργασία και όλα τα κράτη να τάσσονται προς αυτόν τον σκοπό. Για να ανευρεθεί η αρμοδιότητα του δικαστηρίου θα πρέπει να καθοριστεί πρώτα ο τόπος τέλεσης του αδικήματος, και προς αυτόν τον σκοπό υποστηρίζονται τέσσερις θεωρίες[71]:

Η θεωρία του τόπου ενέργειας[72]: Σε αυτή την θεωρία, τόπος τέλεσης του εγκλήματος θεωρείται ο τόπος όπου έλαβε χώρα η εγκληματική πράξη. Ακόμα και αν το έγκλημα έγινε σε περισσότερα του ενός κράτη, ο τόπος που αυτό ολοκληρώθηκε θεωρείται ο τόπος τέλεσής του.

Η θεωρία του τόπου του αποτελέσματος: Τόπος τέλεσης εδώ θεωρείται ο τόπος που έλαβε χώρα το αποτέλεσμα που επέφερε την ζημιά.

Η μικτή θεωρία: Σε αυτή την θεωρία υπάρχει συνδυασμός των δύο παραπάνω θεωριών, καθώς ως τόπος τέλεσης του αδικήματος θεωρείται τόσο ο τόπος που έλαβε χώρα η εγκληματική ενέργεια όσο και ο τόπος που επήλθε το αποτέλεσμα και ο αδικηθείς έχει δικαίωμα επιλογής.

Η θεωρία του βαρύνοντος τόπου: Με βάση αυτή την θεωρία, ο τόπος του αδικήματος βρίσκεται στο κράτος που το έγκλημα πραγματοποιήθηκε κατά το περισσότερο. Είναι αρκετά δύσκολο να προσδιοριστεί ο τόπος που το έγκλημα συντελέστηκε περισσότερο και αποτελεί τον βαρύνοντα τόπο, ωστόσο και για την Ελλάδα και για την Ευρώπη αποτελεί την κρατούσα θεωρία.

4. Αντιμετώπιση Κυβερνοεγκλημάτων

Χαρακτηριστικό γνώρισμα των κυβερνοεγκλημάτων, όπως είδαμε και παραπάνω, είναι ο απρόσωπος και διεθνής χαρακτήρας τους. Όταν τα εγκλήματα αυτά μπορούν να λάβουν χώρα ανά πάσα ώρα και στιγμή, σε οποιοδήποτε μέρος και από οποιαδήποτε συσκευή, είναι αρκετά δύσκολο να μπορέσει κανείς να συλλάβει τον εγκληματία και να σταματήσει την εγκληματική δράση του. Σύμφωνα με μια μελέτη της McAfee το έγκλημα στον κυβερνοχώρο ευθύνεται για απώλειες περίπου 600 δισεκατομμυρίων δολαρίων στις Ηνωμένες Πολιτείες

[71] Άρθρο με τίτλο «*Δικαιοδοσία στο Διαδίκτυο*» δημοσιευμένο στις 17/9/2010 στην ιστοσελίδα https://electroniccrime.wordpress.com/2010/09/17/δικαιοδοσία-στο-διαδίκτυο/ ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[72] Μελέτη του Prashant Mali με τίτλο «*TEXT BOOK OF CYBERCRIME AND PENALTIES {AS PER ITA A 2008 AND IPC}(DRAFT VERSION)*» δημοσιευμένη το 2008 στην ιστοσελίδα https://ia600709.us.archive.org/21/items/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali.pdf ανευρεθείσα στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

της Αμερικής, σχεδόν δηλαδή το 1% του παγκόσμιου ΑΕΠ.[73] Για να μπορέσει λοιπόν να αντιμετωπιστεί σε παγκόσμιο επίπεδο αυτό το ακανθώδες φαινόμενο, θα πρέπει να υπάρξει συνεργασία μεταξύ των κρατών και ανάλογα τον τόπο τέλεσης των εγκλημάτων να προσδιοριστεί και η αρμοδιότητα του δικαστηρίου.

4.1. Αρχές που εποπτεύουν την προστασία του Διαδικτύου στην Ελλάδα

Στην Ελλάδα υπάρχουν τρεις ανεξάρτητες αρχές στις οποίες μπορεί να απευθυνθεί κάποιος για ζητήματα ασφάλειας και προστασίας στο διαδίκτυο. Και οι τρεις αρχές μπορούν να επιβάλλουν ιδιαίτερους όρους σχετικά με την τήρηση τόσο του απορρήτου όσο και των επικοινωνιών στις εταιρείες εκείνες, οι οποίες έχουν άδεια χρήσης τηλεπικοινωνιών δραστηριοτήτων όπου σε αυτές υπάγονται και οι Πάροχοι Υπηρεσιών Διαδικτύου.[74]

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)[75]

Η ΑΠΔΠΧ[76] έχει ως στόχο την εποπτεία της τήρησης του προσωπικού απορρήτου και στο Διαδίκτυο. Με βάση το νόμο για την «*Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα*», ν.2774/1999, οι ιστοσελίδες που περιλαμβάνουν προσωπικά στοιχεία των επισκεπτών, υπέχουν την νομική υποχρέωση να ενημερώνουν τους επισκέπτες τους για την συλλογή αυτών των στοιχείων, αλλά και για τον σκοπό που τα κρατούν.

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)[77]

Σκοπός της Αρχής[78] είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλον τρόπο καθώς και ο έλεγχος τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

---

[73] Άρθρο του Gabriel Olano με τίτλο «Artificial intelligence a valuable tool in combating cybercrime» δημοσιευμένο στις 11/2/2021 στην ιστοσελίδα https://www.insurancebusinessmag.com/us/risk-management/cyber/artificial-intelligence-a-valuable-tool-in-combating-cybercrime-246315.aspx ανευρεθέν στις 20/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[74] Άρθρο με τίτλο «*Αρχές που Εποπτεύον την Προστασία του Διαδικτύου στην Ελλάδα*» δημοσιευμένη στην ιστοσελίδα https://sites.google.com/site/elektronikoenklema2012/arches-pou-epopteuoun-ten-prostasia-tou-diadiktyou-sten-ellada ανευρεθέν στις 16/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[75] Επίσημη ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων https://www.dpa.gr/el

[76] Λειτουργεί από το 1977 σύμφωνα με τις διατάξεις του ν.2472/1997 και είναι συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια αρχή.

[77] Επίσημη ιστοσελίδα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών http://www.adae.gr

[78] Λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του ν.3115/2003.

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.)[79]

Η ΕΕΤΤ[80] αποτελεί την ανεξάρτητη εθνική ρυθμιστική αρχή σε θέματα επικοινωνιών. Συγκεκριμένα ρυθμίζει, εποπτεύει και ελέγχει την αγορά ηλεκτρονικών επικοινωνιών και την ταχυδρομική αγορά.

Λειτουργούν επίσης προς τον σκοπό της προάσπισης των πολιτών:

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΙ.Δ.Η.Ε.)[81]

Η Διεύθυνση[82] αποτελεί αυτοτελή κεντρική υπηρεσία της Ελληνικής Αστυνομίας και δίνει συμβουλές και οδηγίες σε πολίτες, οι οποίοι απευθύνονται σε εκείνη για να καταγγείλουν κάποιο περιστατικό που έχουν πέσει θύματα ή τους προστατεύουν από απάτες του Διαδικτύου. Βασικός της στόχος είναι η διερεύνηση εγκλημάτων που λαμβάνουν χώρος το διαδίκτυο.

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου- υπό την αιγίδα του Ιδρύματος Τεχνολογίας και Έρευνας[83]

Το εν λόγω κέντρο[84], μέσω τριών δράσεων, βοηθάει στην ενημέρωση μικρών και μεγάλων σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο. Αρχικά μέσω στην ιστοσελίδας **SafeInternet4Kids.gr,** όπου οι χρήστες ενημερώνονται σχετικά με τους κινδύνους που υπάρχουν για τα παιδιά στο διαδίκτυο και τις ασφαλιστικές δικλείδες οι οποίες θα τα προστατέψουν, μέσω της συμβουλευτικής γραμμής βοήθειας **Help-line** καθώς και της ιστοσελίδας της[85], όπου ψυχολόγοι ειδικοί σε θέματα διαδικτύου δίνουν συμβουλές στα παιδιά και στις οικογένειές τους, σχετικά με τον διαδικτυακό εκφοβισμό, το ακατάλληλο περιεχόμενο του διαδικτύου, την παρενόχληση, τα μη ασφαλή παιχνίδια κ.ά., και τέλος μέσω της **SafeLine[86],** της μοναδικής ανοιχτής γραμμής καταγγελιών παρανόμου περιεχομένου στο Διαδίκτυο, όπου υποβάλλονται καταγγελίες σχετικά με την παιδική κακοποίηση και την

[79] Επίσημη ιστοσελίδα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων https://www.eett.gr/opencms/opencms/EETT/EETT

[80] Ιδρύθηκε το 1992 με τον ν.2075/1992.

[81] Επίσημη ιστοσελίδα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος https://cyberalert.gr/

[82] Δημιουργήθηκε το 2004.

[83] Επίσημη ιστοσελίδα του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου https://saferinternet4kids.gr

[84] Λειτουργεί από τον Ιούλιο του 2016 υπό την αιγίδα του Ιδρύματος Τεχνολογίας και Έρευνας και συγκεκριμένα του Ινστιτούτου Πληροφορικής.

[85] Επίσημη ιστοσελίδα της helpline http://www.help-line.gr

[86] Ξεκίνησε την λειτουργία της στις 14 Απριλίου 2003 και είναι επίσημο μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοιχτών Γραμμών Διαδικτύου) από τις 18 Οκτωβρίου 2005.

παρενόχληση και γίνεται προσπάθεια διασφάλισης του δικαιώματος ασφαλούς πλοήγησης των παιδιών στο Διαδίκτυο.

ΚΕΦΑΛΑΙΟ ΙΙ

1. ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Η τεχνητή νοημοσύνη (Artificial Intelligence) αποτελεί βασικό πυλώνα και μοχλό της τέταρτης βιομηχανικής επανάστασης (web 2.0) και εξελίσσεται με τόσο μεγάλη ταχύτητα με αποτέλεσμα να τίθενται ουσιαστικά ηθικά, νομικά και κοινωνικά ζητήματα. Αποτελεί μια από τις πιο σύγχρονες καινοτομίες της εποχής μας και αναμένεται να επηρεάσει και να διαμορφώσει στο μέλλον τόσο τον επαγγελματικό τομέα όσο και την ανθρωπότητα. Ο συνδυασμός των εργαλείων της αυτοματοποίησης και των τεχνικών μηχανικής μάθησης, δίνει την δυνατότητα στα υπολογιστικά συστήματα να μπορούν να προσομοιώσουν την ανθρώπινη φύση και τις αισθήσεις και να λαμβάνουν αποφάσεις σαν να επρόκειτο για φυσικά πρόσωπα.

Εκτός του ότι έχει παρατηρηθεί πως η τεχνητή νοημοσύνη χρησιμοποιείται για την ανίχνευση εγκλημάτων και την αποκάλυψη απάτης μέσω διαδικτύου, για την πρόληψη και καταστολή εγκλημάτων, υπάρχουν πολλοί εγκληματίες οι οποίοι χρησιμοποιούν τις μηχανές της τεχνητής νοημοσύνης για να πραγματοποιήσουν τις εγκληματικές τους ενέργειες. Επομένως πρόκειται για ένα εύρος καταστάσεων, όπου η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί και ως «όργανο» τέλεσης εγκλημάτων αλλά και ως «μέσο» καταστολής και αντιμετώπισης αυτών.

1.1. <u>Ιστορία</u>

Οι απαρχές της τεχνητής νοημοσύνης βρίσκονται ήδη στους «συλλογισμούς» του Αριστοτέλη (384-322π.Χ.)[87] και στην θεωρία του περί συλλογιστικής, την μέθοδο της επίσημης μηχανικής σκέψης. Διατύπωσε ένα σύστημα συλλογισμών όπου θεωρητικά μπορούσε κάποιος να καταλήγει σε μηχανικά συμπεράσματα έχοντας ως δεδομένα κάποιες αρχικές υποθέσεις. Η πρώτη πρακτική εφαρμογή της τεχνητής νοημοσύνης

[87] Επιστημονική μελέτη της Laura Steele από το Queen's Management School με τίτλο «*From Aristotle to Artificial Intelligence Can Ancient Theories be Applied to Modern Ethical Challenges?*» δημοσιευμένη στην ιστοσελίδα https://www.qub.ac.uk/schools/QueensManagementSchool/Ethics/FileUpload/Filetoupload,895822,en.pdf ανευρεθείσα στις 12/1/2022 (τελευταία πρόσβαση: 26/2/2022)

πραγματοποιήθηκε την δεκαετία του 1950 από τον διάσημο Βρετανό μαθηματικό Alan Turing, ο οποίος έθεσε τις βάσεις γι' αυτό που σήμερα ονομάζουμε τεχνητή νοημοσύνη, με το ερώτημα αν μια μηχανή μπορεί να μιμηθεί την ανθρώπινη σκέψη: «I propose to consider the question, "Can machines think?"». Ο Turing θεωρώντας πως το ερώτημά του ήταν αρκετά γενικό και αόριστο πρότεινε ένα παιχνίδι μίμησης, το γνωστό και ως τεστ Τούρινγκ (Turing test).[88] Το τεστ Τούρινγκ βασίζεται στην εξής απλή υπόθεση: Τρεις άνθρωποι ένας εξεταστής και δύο ερωτώμενοι, βρίσκονται σε διαφορετικά δωμάτια και ο εξεταστής τους απευθύνει ερωτήσεις. Οι ερωτώμενοι απαντούν γραπτώς με στόχο να μην αποκαλυφθεί η φωνή τους και ο εξεταστής προσπαθεί να αναγνωρίσει το φύλο του κάθε ερωτώμενου. Εάν ένας άνθρωπος μπορεί να συμμετέχει σε μια συζήτηση για πέντε λεπτά χωρίς να καταλάβει ότι μιλάει σε μια μηχανή, τότε ο υπολογιστής περνάει το τεστ. Η μηχανή χαρακτηρίζεται ευφυής όταν επιτυχώς ο εξεταστής δεν μπορεί να μαντέψει σωστά εάν οι απαντήσεις προέρχονται από άνθρωπο ή από μηχανή. Για να επιτύχει την δοκιμασία ο υπολογιστής θα πρέπει να μπορεί να επεξεργάζεται την φυσική γλώσσα (natural language processing), να αναπαριστά την γνώστη που λαμβάνει (knowledge representation), να λειτουργεί με αυτοματοποιημένη συλλογιστική (automated reasoning), με μηχανική μάθηση και όραση (machine learning, computer vision) και να μπορεί να λειτουργεί ως ρομπότ (robotics). Αυτό που εγείρει το ενδιαφέρον είναι ότι πολλά από αυτά τα μηχανικά συστήματα έχουν καταφέρει να πείσουν κάποιον ότι μιλάει σε ένα άτομο όχι μέσα από μια πραγματική συνομιλία, αλλά λόγω ορθογραφικών λαθών[89].

1.2. Ορισμός

Με τον όρο τεχνητή νοημοσύνη αναφερόμαστε στην ικανότητα που έχει μια μηχανή να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα. Οι μηχανές αποκτούν την ικανότητα να αντιλαμβάνονται το περιβάλλον τους, να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου. Ο υπολογιστής λαμβάνει δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων, π.χ. κάμερας), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών. Τα

[88] Άρθρο των Graham Oppy και David Dowe με τίτλο «*The Turing Test*» δημοσιευμένο στις 9/4/2003 (αναθεωρημένο στις 4/10/2021) στην ιστοσελίδα https://plato.stanford.edu/entries/turing-test/ ανευρεθέν στις 12/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[89] Επιστημονικό άρθρο με τίτλο «Τεστ Τούρινγκ» δημοσιευμένο στην ιστοσελίδα https://atozofai.withgoogle.com/intl/el/turing-test/ ανευρεθέν στις 8/12/2021 (τελευταία πρόσβαση: 26/2/2022)

συστήματα τεχνητής νοημοσύνης είναι ικανά να προσαρμόζουν τη συμπεριφορά τους, σε ένα ορισμένα βαθμό, αναλύοντας τις συνέπειες προηγούμενων δράσεων και επιλύοντας προβλήματα με αυτονομία.[90]

Σύμφωνα με την ανακοίνωση της Ευρωπαϊκής Επιτροπής παρουσιάζεται ένας πρώτος ορισμός για την τεχνητή νοημοσύνη: « *Η τεχνητή νοημοσύνη (ΤΝ) αναφέρεται σε συστήματα που χαρακτηρίζονται από ευφυή συμπεριφορά, αναλύοντας το περιβάλλον τους και ενεργώντας- με κάποιο βαθμό αυτονομίας- για την επίτευξη συγκεκριμένων στόχων. Τα συστήματα που λειτουργούν βάσει τεχνητής νοημοσύνης μπορούν να βασίζονται αποκλειστικά σε λογισμικό, ενεργώντας στον εικονικό κόσμο (π.χ. βοηθοί φωνής, λογισμικό ανάλυσης εικόνας, μηχανές αναζήτησης, συστήματα αναγνώρισης ομιλίας και προσώπου) ή η τεχνητή νοημοσύνη μπορεί να ενσωματωθεί σε συσκευές υλισμικού (π.χ. προηγμένα ρομπότ, αυτόνομα αυτοκίνητα, δρόμοι ή εφαρμογές του Διαδικτύου των Πραγμάτων).»*[91]

Ο διάσημος μαθηματικός επιστήμονας John McCarthy[92] ορίζει το 1955 ότι «*Η Τεχνητή Νοημοσύνη είναι η επιστήμη και η τεχνική κατασκευής ευφυών μηχανών, ιδιαίτερα ευφυών προγραμμάτων για υπολογιστές. Σχετίζεται με την αντίστοιχη ιδέα της χρήσης υπολογιστών για την κατανόηση της ανθρώπινης νοημοσύνης, αλλά η ΤΝ δεν οφείλει να περιορίζεται σε μεθόδους που παρατηρούνται στη βιολογία*».

Ως «ευφυές» υπολογιστικό σύστημα ορίζεται το σύστημα εκείνο που αναδεικνύει τα χαρακτηριστικά μιας ανθρώπινης συμπεριφοράς που διακρίνονται από ευφυία, όπως είναι η μάθηση, η δυνατότητα επίλυσης των προβλημάτων, η σκέψη και η οργανωτικότητα.

---

[90] Επιστημονικό άρθρο του Ευρωπαϊκού Κοινοβουλίου με τίτλο «Τι είναι η τεχνητή νοημοσύνη και πως χρησιμοποιείται» δημοσιευμένο στην ιστοσελίδα https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai ανευρεθέν στις 7/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[91] Ανακοίνωση της Ευρωπαϊκής Επιτροπής-Τεχνητή νοημοσύνη για την Ευρώπη, Βρυξέλλες, 25.4.2018 COM (2018) 237 final, ανευρεθείσα στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52018DC0237&from=MT στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

[92] Το 1971 έλαβε το βραβείο Turing για τις σημαντικές του συνεισφορές στον τομέα της τεχνητής νοημοσύνης. Απόσπασμα ανευρεθέν στην ιστοσελίδα https://www.youtube.com/watch?v=Ozipf13jRr4 στις 8/12/2021 (τελευταία πρόσβαση: 26/2/2022)

Παρόλα αυτά, κανείς ορισμός δεν είναι καθολικά αποδεκτός, καθώς η τεχνητή νοημοσύνη είναι μια διεπιστημονική επιστήμη αποτελούμενη από πολλά πεδία μελέτης όπως τα μαθηματικά και η κοινωνιολογία.

1.3. Βαθιά μάθηση-Deep Learning

Αξίζει να σημειωθεί πως και το Deep Learning (βαθιά μάθηση) αποτελεί σημαντική ανακάλυψη στον τομέα της τεχνητής νοημοσύνης, καθώς είναι εμπνευσμένο από την δομή και την λειτουργία του εγκεφάλου και επιτρέπει στις μηχανές να επιλύουν πολύπλοκα προβλήματα ακόμα και όταν χρησιμοποιούν ένα σύνολο δεδομένων.[93] Η επίλυση των προβλημάτων αυτών και η εξαγωγή συμπερασμάτων και προβλέψεων πραγματοποιείται με τεχνητά νευρωνικά δίκτυα και αλγορίθμους, οι οποίοι αφενός επεξεργάζονται έναν μεγάλο όγκο δεδομένων και αφετέρου μιμούνται τον ανθρώπινο εγκέφαλο σε όλες του τις μορφές.

1.4. Μηχανική μάθηση-Machine learning

Σε κάθε αναφορά στην τεχνητή νοημοσύνη χρήσιμο είναι να αναφερόμαστε και στην μηχανική μάθηση. Στην μηχανική μάθηση (machine learning) χρησιμοποιούνται στατιστικές μέθοδοι, οι οποίες έχουν ως σκοπό την ενίσχυση και εκπαίδευση των μηχανών, ώστε να μπορούν να μάθουν να επιλύουν συγκεκριμένα προβλήματα με την χρήση πλήθους δεδομένων, χωρίς να προγραμματιστούν ρητώς. Η μηχανική μάθηση, η οποία βασίζεται στην δημιουργία αλγορίθμων οι οποίοι βασίζονται σε δεδομένα και μαθαίνουν να κάνουν προβλέψεις, αυτοματοποιεί την δημιουργία αναλυτικών μοντέλων. Στα ίδια πλαίσια πραγματοποιείται και εκμάθηση των αλγορίθμων από τα δεδομένα που παρέχονται. Ο λόγος που αναφερόμαστε στην μηχανική μάθηση είναι γιατί η τεχνητή νοημοσύνη εφαρμόζεται με βάση το machine learning.[94]

---

[93] Άρθρο του Bernard Marr με τίτλο «*What is Deep Learning AI? A Simple Guide With 8 Practical Examples*» δημοσιευμένο στις 1/10/2018 στην ιστοσελίδα https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/?sh=77f0dce08d4b ανευρεθείσα στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[94] Άρθρο του SecNews με τίτλο «*Σύνδεση μεταξύ data science, machine learning and artificial intelligence*» δημοσιευμένο στις 30/11/2019 στην ιστοσελίδα https://www.secnews.gr/205498/syndesi-metaksi-data-science-machine-learning-artificial-intelligence/ ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

2. Ευρωπαϊκή Ένωση και Τεχνητή Νοημοσύνη

Η Ευρωπαϊκή ένωση έλαβε ορισμένες πρωτοβουλίες προκειμένου να αναπτυχθεί η τεχνητή νοημοσύνη με κύριο γνώμονα την ηθική αξιοπιστία και τον σεβασμό των δικαιωμάτων, ακολουθώντας την ίδια γραμμή με την ψηφιοποίηση που οδήγησε στον Γενικό Κανονισμό για τα Προσωπικά Δεδομένα (GDPR).

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου (Φεβρουάριος 2017)[95] για τις ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής

Το εν λόγω ψήφισμα έκανε συστάσεις προς την Ευρωπαϊκή Επιτροπή σχετικά με τους κανόνες αστικού δικαίου για τα ρομπότ. Το να αναγνωριστούν τα ρομπότ ως «ηλεκτρονικά πρόσωπα» αντιμετωπίστηκε ποικιλοτρόπως, κυρίως από τον βιομηχανικό τομέα καθώς κάτι τέτοιο θα οδηγούσε στην αύξηση του κόστους των μηχανών. Χαρακτηριστικά αναφέρεται πως «*η ανθρωπότητα βρίσκεται πλέον στο κατώφλι μιας εποχής, κατά την οποία όλο και πιο εξελιγμένα ρομπότ, bots, ανδροειδή και άλλες εκφάνσεις της τεχνητής νοημοσύνης, αναμένεται να πυροδοτήσουν μια νέα βιομηχανική επανάσταση*». Επιπλέον, το ψήφισμα αναφέρει σχετικά με την αστική ευθύνη για ζημιές που προκαλούνται από ρομπότ, όπου προτείνεται η εφαρμογή της αστικής ευθύνης σε επίπεδο Ευρωπαϊκής Ένωσης, πως «*Λαμβάνοντας υπόψη ότι, αν υποτεθεί ότι ένα ρομπότ μπορεί να λαμβάνει αυτόνομα αποφάσεις, οι συμβατικοί κανόνες δεν θα επαρκούν για την στοιχειοθέτηση της νομικής ευθύνης για ζημιές που προκάλεσε ένα ρομπότ, καθώς δεν επιτρέπουν να οριστεί ο υπεύθυνος προς αποζημίωση και να απαιτηθεί από αυτόν η αποκατάσταση της ζημίας που προκάλεσε*».[96]

[95] Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)) δημοσιευμένο στην επίσημη ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EL.html ανευρεθέν στις 12/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[96] Μελέτη του Σταύρου Κιτσάκη με τίτλο «*Τεχνητή νοημοσύνη και συμβατική διαδικασία, Εισαγωγή στα βασικά προβλήματα*», δημοσιευμένη στις «Εφαρμογές ΑΣΤΙΚΟΥ ΔΙΚΑΙΟΥ & ΠΟΛΙΤΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ» Τεύχος 6/ Έτος 2018 ανευρεθείσα στην ιστοσελίδα https://www.researchgate.net/publication/326711736_Technete_noemosyne_kai_symbatike_diadikasia_Artificial_Intelligence_and_contract_law_An_introduction στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των περιφερειών- Τεχνητή Νοημοσύνη για την Ευρώπη[97]

Με την υπ' αριθμ. COM (2018) 237 ανακοίνωση της Ευρωπαϊκής Επιτροπής, παρουσιάστηκαν μια σειρά από μέτρα έτσι ώστε η τεχνητή νοημοσύνη να τεθεί στην υπηρεσία των Ευρωπαίων πολιτών και τα κράτη-μέλη να ενθαρρυνθούν και να προχωρήσουν σε επενδύσεις και στην έρευνα. Στόχος είναι όλοι οι Ευρωπαίοι πολίτες να συμμετέχουν στον ψηφιακό μετασχηματισμό, να προωθηθεί η καινοτομία και η δημιουργία μιας ψηφιακής ενιαίας αγοράς, αλλά να τηρούνται όλα τα ηθικά πλαίσια και οι αξίες στην εφαρμογή της τεχνητής νοημοσύνης. Η Ευρωπαϊκή Επιτροπή έθεσε έναν τριπλό στόχο, την ανάπτυξη της τεχνητής νοημοσύνης, την κοινωνικο-οικονομική προετοιμασία των ευρωπαϊκών κοινωνιών και την προετοιμασία ηθικού και νομικού πλαισίου.

Συμβούλιο της Ευρώπης (CAHAI)

Στις 11 Σεπτεμβρίου του 2019, συστάθηκε η ad-hoc επιτροπή για την Τεχνητή Νοημοσύνη του Συμβουλίου της Ευρώπης, όπου καθήκον της είναι «*η ολοκλήρωση της μελέτης σκοπιμότητας και η παραγωγή των πιθανών στοιχείων βάσει ευρειών διαβουλεύσεων με πολλούς ενδιαφερόμενους, ενός νομικού πλαισίου για την ανάπτυξη, το σχεδιασμό και την εφαρμογή της τεχνητής νοημοσύνης, με βάση τα πρότυπα του Συμβουλίου της Ευρώπης για τα ανθρώπινα δικαιώματα, τη δημοκρατία και το κράτος δικαίου*». Η συμμετοχή πολλών κρατών μελών θα συμβάλει στην εφαρμογή μιας παγκόσμιας συνθήκης για την τεχνητή νοημοσύνη τα επόμενα χρόνια, η οποία θα διαδραματίσει αποφασιστικό ρόλο.[98]

---

[97] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe, της Ευρωπαϊκής Επιτροπής, Βρυξέλλες, 25.4.2018 COM (2018) 237 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN ανευρεθείσα στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[98] Μελέτη του Cristo Velasco με τίτλο «*Cybercrime and Artificial Intelligence. An overview of the work of international organization on criminal justice and the international applicable instruments*», δημοσιευμένη στις 22/2/2022 στην ιστοσελίδα https://link.springer.com/article/10.1007/s12027-022-00702-z ανευρεθέν στις 28/2/2022 (τελευταία πρόσβαση: 28/2/2022)

«Λευκή βίβλος»

Τον Φεβρουάριο του 2020 η Ευρωπαϊκή Επιτροπή προχώρησε στην δημοσίευση της υπ' αριθμ. COM (2020) 65 «Λευκής βίβλου»[99] η οποία τόνισε την ανάγκη να υιοθετηθεί μια ενοποιημένη ευρωπαϊκή προσέγγιση για την ανάπτυξη της τεχνητής νοημοσύνης αλλά και την αντιμετώπιση των όποιων κινδύνων μπορεί να ελλοχεύουν από την χρήση της τεχνητής νοημοσύνης. Στόχος της Λευκής Βίβλου είναι η οικοδόμηση ενός πλαισίου αριστείας και εμπιστοσύνης όπου τα κράτη μέλη θα συνεργάζονται μεταξύ τους, θα προωθούνται οι καινοτόμες ιδέες και θα ενισχύονται οι επενδύσεις και η πρόοδος.

Μελέτη του CEPS(Centre for European Policy Studies) για την Κυβερνοασφάλεια και την Τεχνητή Νοημοσύνη[100]

Η τεχνολογία της τεχνητής νοημοσύνης πέρα από τα πολλά οφέλη και τις προκλήσεις που παρουσιάζει, μπορεί σε ορισμένους τομείς, όπως στον τομέα της κυβερνοασφάλειας και του κυβερνοεγκλήματος να οδηγήσει στην δημιουργία ορισμένων σημαντικών προβλημάτων στην κοινωνία, εάν δεν αντιμετωπιστούν σωστά τα ζητήματα ασφάλειας και ηθικής.
Το φθινόπωρο του 2019, το Κέντρο Μελετών Ευρωπαϊκής Πολιτικής (CEPS) δημιούργησε μια ομάδα εργασίας για την Τεχνητή Νοημοσύνη και την Κυβερνοασφάλεια, με σκοπό να εξετάσει τις ηθικές και τεχνικές προκλήσεις της, καθώς και τις προκλήσεις της αγοράς που προκύπτουν από την διασταύρωση της τεχνητής νοημοσύνης και της ασφάλειας στον κυβερνοχώρο. Η εν λόγω έκθεση συμβάλλει στις προσπάθειες της Ευρωπαϊκής Ένωσης για την δημιουργία ενός υγιούς πλαισίου πολιτικής για την τεχνητή νοημοσύνη και πιο συγκεκριμένα:

- Παρέχοντας μια τρέχουσα επισκόπηση της τεχνητής νοημοσύνης σχετικά με τις ευεργετικές εφαρμογές της στον τομέα της κυβερνοασφάλειας αλλά και τους κινδύνους που απορρέουν από την πιθανότητα

[99] Λευκή βίβλος| Τεχνητή νοημοσύνη-Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, της Ευρωπαϊκής Επιτροπής, Βρυξέλλες, 19.2.2020 COM (2020) 65 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf ανευρεθείσα στις 12/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[100] Μελέτη του CEPS(Centre for European Policy Studies) για την Κυβερνοασφάλεια και την Τεχνητή Νοημοσύνη δημοσιευμένη στην ιστοσελίδα https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf ανευρεθείσα στις 22/12/2021 (τελευταία πρόσβαση: 26/2/2022)

- Παρουσιάζοντας τις κύριες ηθικές επιπτώσεις και ζητήματα πολιτικής που σχετίζονται με την εφαρμογή της τεχνητής νοημοσύνης και της ασφάλειας στον κυβερνοχώρο
- Προτείνοντας συγκεκριμένες και ουσιαστικές συστάσεις πολιτικής προκειμένου να διασφαλιστεί πως η εφαρμογή της τεχνητής νοημοσύνης είναι ασφαλής και εναρμονισμένη με τους στόχους της ψηφιακής στρατηγικής της Ευρωπαϊκής Ένωσης.

Ηθικές αρχές σχετικά με την χρήση της Τεχνητής Νοημοσύνης στα δικαστικά συστήματα

Στα πλαίσια που η τεχνητή νοημοσύνη πλέον έχει ενεργό ρόλο και στην δικαιοσύνη, η Ευρωπαϊκή Επιτροπή για την αποτελεσματικότητα της δικαιοσύνης του Συμβουλίου της Ευρώπης[101] (CEPEJ)[102] προχώρησε στην έγκριση του πρώτου ευρωπαϊκού κειμένου, το οποίο αποτελείται από ένα σύνολο ηθικών αρχών -σχετικά με την χρήση της τεχνητής νοημοσύνης στα δικαστικά συστήματα-οι οποίες έχουν ως στόχο να βοηθήσουν τους νομοθέτες και τους «εργάτες» της δικαιοσύνης στην αντιμετώπιση της ταχείας ανάπτυξης της τεχνητής νοημοσύνης.[103]

Το κείμενο αυτό αποτελεί τον Ευρωπαϊκό Χάρτη Δεοντολογίας για την χρήση της Τεχνητής Νοημοσύνης στα δικαστικά συστήματα και στο περιβάλλον τους και διατύπωσε τις ακόλουθες πέντε βασικές ηθικές αρχές οι οποίες πρέπει να τηρούνται στην εφαρμογή της τεχνητής νοημοσύνης και της δικαιοσύνης:[104]

---

[101] Το Συμβούλιο της Ευρώπης είναι διεθνής οργανισμός, ο οποίος ασχολείται ιδιαίτερα με την προστασία των ανθρωπίνων δικαιωμάτων. Αποτελείται από 47 κράτη μέλη, στα οποία περιλαμβάνονται όλα τα μέλη της Ευρωπαϊκής Ένωσης. Όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης έχουν υπογράψει την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου, μια συμφωνία που έχει σκοπό την προστασία των ανθρωπίνων δικαιωμάτων, της δημοκρατίας και του κράτους δικαίου.

[102] European Commission for the Efficiency of Justice

[103] Άρθρο της Ε. Τζούλια/Justina με τίτλο «*Ευρωπαϊκός ηθικός χάρτης για τη χρήση της Τεχνητής Νοημοσύνης στο δικαιοδοτικό σύστημα*» δημοσιευμένο στις 15/9/2020 στην ιστοσελίδα http://www.justina.gr/πολιτική/διεθνή/ευρωπαϊκός-ηθικός-χάρτης-για-τη-χρήση/ ανευρεθέν στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[104] Ευρωπαϊκός Χάρτης Δεοντολογίας για την χρήση της Τεχνητής Νοημοσύνης στα δικαστικά συστήματα και στο περιβάλλον του δημοσιευμένος στις 4/12/2018 στην ιστοσελίδα https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

- **Αρχή του σεβασμού των θεμελιωδών δικαιωμάτων**| Με την διασφάλιση ότι οι εφαρμογές της τεχνητής νοημοσύνης είναι συμβατές με τα θεμελιώδη δικαιώματα.
- **Αρχή της μη διακριτικής μεταχείρισης**| Με την αποτροπή της ανάπτυξης οποιασδήποτε διάκρισης μεταξύ ατόμων ή ομάδων ατόμων.
- **Αρχή της ποιότητας και της ασφάλειας**| Σχετικά με την επεξεργασία των δικαστικών αποφάσεων να γίνεται χρήση έγκυρων και πιστοποιημένων πηγών που έχουν δημιουργηθεί σε ασφαλές τεχνολογικό περιβάλλον
- **Αρχή της διαφάνειας, της αμεροληψίας και της δίκαιης μεταχείρισης**| Με την ύπαρξη μεθόδων επεξεργασίας δεδομένων προσιτών, κατανοητών και διαθέσιμων στους εξωτερικούς ελέγχους
- **Αρχή του «ελέγχου από τον χρήστη»**| Με την εξασφάλιση πως οι χρήστες είναι ενημερωμένοι και δεν ακολουθείται μια τυποποιημένη διαδικασία.

Ο Κώδικας ορίζει πως η συμμόρφωση με τις παραπάνω αρχές αλλά και ο σεβασμός τους πρέπει να γίνεται κατά την επεξεργασία των δικαστικών αποφάσεων και δεδομένων μέσω στης τεχνητής νοημοσύνης καθώς, κάτι τέτοιο θα συνέβαλε και στην βελτίωση της προβλεψιμότητας της εφαρμογής του νόμου.

Πρόταση Κανονισμού για την «θέσπιση εναρμονισμένων κανόνων για την Τεχνητή Νοημοσύνη και τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης».[105]

Η συγκεκριμένη πρόταση είναι η πρώτη ειδική ρύθμιση για την Τεχνητή νοημοσύνη, πραγματοποιήθηκε μετά από πολλά χρόνια προπαρασκευαστικών εργασιών της Ευρωπαϊκής Ένωσης, αποτελεί μέρος των προσπαθειών που καταβάλει η Ευρωπαϊκή Ένωση με σκοπό να αναλάβει ηγετικό ρόλο σε διεθνές επίπεδο και έχει ως στόχο την διασφάλιση των θεμελιωδών δικαιωμάτων των πολιτών και των επιχειρήσεων. Στο άρθρο 3 της πρότασης του Κανονισμού ο όρος «σύστημα τεχνητής νοημοσύνης» ορίζεται ως «*λογισμικό που έχει αναπτυχθεί με μία ή περισσότερες από τις τεχνικές και προσεγγίσεις που*

[105] Πρόταση-Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης, Βρυξέλλες, 21.4.2021 COM (2021) 206 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF ανευρεθείσα στις 12/1/2022 (τελευταία πρόταση: 26/2/2022)

παρατίθενται στο παράρτημα Ι και μπορεί, για ένα δεδομένο σύνολο καθορισμένων από τον άνθρωπο στόχων, να παράγει αποτέλεσμα όπως περιεχόμενο, προβλέψεις, προτάσεις ή αποφάσεις που επηρεάζουν περιβάλλοντα με τα οποία αλληλεπιδρούν».

Νόμος περί Τεχνητής Νοημοσύνης

Στις 21 Απριλίου του 2021 η Ευρωπαϊκή Επιτροπή πρότεινε τον νόμο περί τεχνητής νοημοσύνης[106], με στόχο να κωδικοποιηθούν τα πρότυπα τα οποία ήθελε η τεχνητή νοημοσύνη, δηλαδή να είναι «*νομικά, ηθικά και τεχνικά ισχυρή, με σεβασμό των δημοκρατικών αξιών, των ανθρωπίνων δικαιωμάτων και του κράτους δικαίου*»[107] αλλά και να προωθηθεί μια ευρωπαϊκή προσέγγιση για την τεχνητή νοημοσύνη η οποία θα επικεντρώνεται στην αριστεία, στην αξιοπιστία και στην ασφαλή διασφάλιση των θεμελιωδών δικαιωμάτων. Η πρόταση αυτή περιέχει αυστηρούς κανόνες και υποχρεώσεις καθώς και σαφείς απαγορεύσεις πρακτικών τεχνητής νοημοσύνης οι οποίες ενδεχομένως θα αντιβαίνουν στις ηθικές αξίες της Ευρωπαϊκής Ένωσης και θα έθεταν σε κίνδυνο τα θεμελιώδη δικαιώματα των πολιτών.

3. ΕΓΚΛΗΜΑ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ[108]

Καθώς η τεχνητή νοημοσύνη ολοένα βελτιώνεται και εξελίσσεται, οι εγκληματίες του κυβερνοχώρου βρίσκουν πρόσφορο έδαφος και χρησιμοποιούν τόσο την τεχνητή νοημοσύνη όσο και την βαθιά μάθηση για να παραβιάσουν συστήματα ασφαλείας. Όπως είδαμε και παραπάνω, η τεχνητή νοημοσύνη μπορεί να ταξινομηθεί σε δύο κατηγορίες, με βάση και

[106] Proposal for a Regulation of the European Parliament and of the Council, Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, European Commission, Brussels, 21.4.2021 COM (2021) 206 final 2021/0106 (COD), ανευρεθέν στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (τελευταία πρόσβαση: 26/2/2022)

[107] *A European approach to artificial intelligence*, δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[108] Μελέτη του Doowon Jeong με τίτλο «*Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues*» δημοσιευμένη στις 7/10/2020 στην ιστοσελίδα https://ieeexplore.ieee.org/document/9216065 ανευρεθείσα στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

την ταξινόμηση των εγκλημάτων στον κυβερνοχώρο, αφενός να χρησιμοποιηθεί ως εργαλείο και αφετέρου ως στόχος[109].

Πιο συγκεκριμένα, η τεχνητή νοημοσύνη ορίζεται ως έγκλημα-εργαλείο, όταν υπάρχουν ήδη υφιστάμενα εγκλήματα τα οποία όμως πραγματοποιούνται στον κυβερνοχώρο (για παράδειγμα προηγμένο phishing, αυτοματοποιημένο hacking κλπ.) Από την άλλη πλευρά, η τεχνητή νοημοσύνη ως έγκλημα-στόχος αποτελεί έναν καινούργιο τομέα εγκληματικότητας.

Αρχικά, κακόβουλη χρήση της τεχνητής νοημοσύνης αποτελούν τα social bots, τα διαδικτυακά πρόσωπα, τα οποία δρουν και λειτουργούν ως άνθρωποι. Ενώ αρχικός τους στόχος ήταν να υποστηρίξει την συνεργασία μεταξύ των ανθρώπων, εν τέλει χρησιμοποιείται κακόβουλα.[110]

<u>Ο υπολογιστής ως εργαλείο του εγκλήματος:</u> Οι δράστες χρησιμοποιώντας τεχνικές της τεχνικής νοημοσύνης μπορούν να διαπράξουν ένα έγκλημα στον κυβερνοχώρο που ίσως χωρίς αυτές τις τεχνικές θα ήταν ανέφικτο να το πραγματοποιήσουν. Έχει παρατηρηθεί πως οι πιο κοινές μέθοδοι όπου χρησιμοποιείται η τεχνητή νοημοσύνη είναι το phising και συγκεκριμένα η απάτη μέσω email. Το πιο χαρακτηριστικό παράδειγμα είναι η στοχευμένη διαφήμιση, όπου δημιουργούνται συγκεκριμένα προφίλ με χρήση τεχνητής νοημοσύνης και στρέφονται προς τους χρήστες-πελάτες με βάση προηγούμενο ιστορικό και προφίλ πελατών. Αυτό το λογισμικό το ονόμασαν chatbot[111], μπορεί να πραγματοποιήσει ορισμένες συνομιλίες μέσω διαδικτύου και είναι σχεδιασμένο να προσομοιάζει με το πως θα συμπεριφερόταν ένας άνθρωπος ως συνομιλητής, αποστέλλοντας αυτοματοποιημένα μηνύματα. [112]

Επιπρόσθετα, ένα ακόμα σημαντικό παράδειγμα προηγμένου εγκλήματος είναι οι ψευδείς ειδήσεις (fake news), οι οποίες έχουν πολύ μεγάλη επίδραση κυρίως σε πολιτικά ζητήματα.

---

[109] Computer as tool crime, Computer as target crime

[110] Άρθρο των D.Assenmacher, L.Clever, L.Frischlich, T.Quandt, H.Trautmann, C.Grimme με τίτλο «*Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*» δημοσιευμένο στις 1/9/2020 στην ιστοσελίδα https://journals.sagepub.com/doi/10.1177/2056305120939264 ανευρεθέν στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[111] Άρθρο του Jake Frankenfield με τίτλο «*Chatbot*» δημοσιευμένο στις 27/6/2020 στην ιστοσελίδα https://www.investopedia.com/terms/c/chatbot.asp ανευρεθέν στις 19/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[112] Άρθρο της Amy Higgins με τίτλο «*What is a Chatbot? How Is it Changing Customer Experience?*» δημοσιευμένο στις 4/8/2021 στην ιστοσελίδα https://www.salesforce.com/blog/what-is-a-chatbot/ ανευρεθέν στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Δύο ερευνητές[113] μάλιστα παρουσίασαν ότι ένα ψεύτικο βίντεο που μιμείται κάποιους πολιτικούς μπορεί να βλάψει το κοινό και να το παραπλανήσει παρέχοντάς τους ψευδείς πληροφορίες και αναληθή στοιχεία.

Αξίζει να αναφερθεί ότι η Google σταμάτησε το 99% των εισερχόμενων ανεπιθύμητων μηνυμάτων, χρησιμοποιώντας τεχνολογίες μηχανικής μάθησης , όπως επίσης καθυστέρησε την αποστολή ορισμένων μηνυμάτων, έτσι ώστε να περάσουν πρώτα από κάποιους ελέγχους και έτσι να ανιχνεύονται οι κακόβουλες ενέργειες.[114]

Ο υπολογιστής ως έγκλημα-στόχος: Με την ευρεία χρήση των συστημάτων τεχνητής νοημοσύνης, ένας δράστης μπορεί να επιτεθεί στον στόχο του και έτσι η απειλή να εκτείνεται πέρα από τον κυβερνοχώρο. Το σύστημα της τεχνητής νοημοσύνης λειτουργεί εκπαιδευμένο με μοντέλα τα οποία το έχουν προγραμματίσει να δρα με συγκεκριμένο τρόπο και να φέρει εις πέρας συγκεκριμένα αποτελέσματα. Ως έγκλημα-στόχος διαπράττεται κυρίως με βάση τις απειλές των συστημάτων τεχνητής νοημοσύνης.

Γιατί οι εγκληματίες χρησιμοποιούν την τεχνητή νοημοσύνη για να πραγματοποιήσουν τα αδικήματά τους

Η χρήση της τεχνητής νοημοσύνης και ο αυτοματισμός επιτρέπει στους κυβερνοεγκληματίες να μπορούν να δημιουργούν κακόβουλο λογισμικό, και να διαπράττουν με ταχύτερους ρυθμούς τις επιθέσεις τους.

- **Αυτοματοποιημένο συμπέρασμα σχετικά με την εγκληματικότητα με την χρήση εικόνων προσώπων**

Το 2016 ορισμένοι ερευνητές στην Κίνα επινόησαν ένα σύστημα τεχνητής νοημοσύνης το οποίο «προβλέπει» τους εγκληματίες με βάση τα χαρακτηριστικά του προσώπου τους. Το εν λόγω σύστημα δημιουργήθηκε στο Shanghai Jiao Tong University και κατάφερε, σύμφωνα με

[113] Μελέτη των Hunt Allcott και Matthew Gentzkow με τίτλο «*Social Media and Fake News in the 2016 Election*» δημοσιευμένη το 2017 στην ιστοσελίδα https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211 ανευρεθείσα στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[114] Άρθρο του Ed Lauder με τίτλο «*Google's Machine Learning Tech Now Blocks 99.9% of Spam*» δημοσιευμένο στις 6/1/2017 στην ιστοσελίδα https://aibusiness.com/document.asp?doc_id=760333 ανευρεθέν στις 28/1/2022 (τελευταία πρόσβαση: 26/2/2022)

την έρευνα, μέσα από ένα υλικό 186 φωτογραφιών να εντοπίσει με ποσοστό επιτυχία περίπου στο 90% τους εγκληματίες, αξιολογώντας στοιχεία σχετικά με χαρακτηριστικά του προσώπου τους όπως το στόμα, τα μάτια, η μύτη και το μέτωπο.

4. Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΗΝ ΠΟΙΝΙΚΗ ΔΙΚΑΙΟΣΥΝΗ

Οι περισσότερους τομείς της ποινικής δικαιοσύνης και της εγκληματολογίας έχουν στραφεί στους μηχανισμούς της τεχνητής νοημοσύνης, καθώς έχουν βοηθήσει στο να περιοριστεί η εγκληματικότητα.[115]

Η προγνωστική φύση της τεχνητής νοημοσύνης, οι αλγοριθμικές εκτιμήσεις κινδύνου και η προγνωστική αστυνόμευση χρησιμοποιούνται για να προβλέψουν την πιθανότητα κάποιου να εμφανιστεί αυτοπροσώπως σε μια ημερομηνία δικασίμου ή να διαπράξει ένα έγκλημα. Μάλιστα κάποιες διαδικασίες, έχουν υιοθετήσει ορισμένα εργαλεία τεχνητής νοημοσύνης σχεδόν για κάθε στάδιο της διαδικασίας της ποινικής δικαιοσύνης. Έτσι, οι αλγόριθμοι ενημερώνουν σχετικά με την πορεία μιας δίκης, με την εγγύηση, την καταδίκη και την αναστολή μιας υπόθεσης. Αρκετοί δικαστές, στην περίπτωση των εκτιμήσεων κινδύνου πριν από την δίκη έχουν στραφεί σε προγνωστικές αναλύσεις όταν αποφασίζουν εάν θα προφυλακίσουν έναν ύποπτο για αδίκημα και που εκκρεμεί η δίκη του, ή θα τον αφήσουν ελεύθερο. [116]

Δεν υπάρχει αμφιβολία ότι οι προγνωστικές αναλύσεις που προσφέρει η τεχνητή νοημοσύνη έχουν την δυνατότητα να βελτιώσουν και να προχωρήσουν ένα βήμα μπροστά ένα ελαττωματικό σύστημα ποινικής δικαιοσύνης. Ωστόσο, δεν είναι λίγοι εκείνοι οι νομικοί, εμπειρογνώμονες και τεχνικοί οι οποίοι πιστεύουν πως αυτά τα εργαλεία όχι μόνο δεν θα βελτιώσουν την κατάσταση, αλλά θα την επιδεινώσουν. Μπορεί οι τεχνολογίες της τεχνητής νοημοσύνης να μην έχουν την μεγαλύτερη προγνωστική ακρίβεια σε σχέση με άλλα όργανα αξιολόγησης κινδύνου, όμως οι προκαταρκτικές εκτιμήσεις κινδύνου μπορούν να βελτιώσουν την κατάσταση λαμβάνοντας υπόψη πολλούς παράγοντες κινδύνου προτού

---

[115] Άρθρο του Christopher Rigano με τίτλο «*Using Artificial Intelligence to Address Criminal Justice Needs*» δημοσιευμένο στις 8/10/2018 στην ιστοσελίδα https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[116] Άρθρο του Carlow University με τίτλο «*Artificial Intelligence in Criminal Justice: How AI Impacts Pretrial Risk Assessment*» δημοσιευμένο στις 27/7/2021 στην ιστοσελίδα https://blog.carlow.edu/2021/07/27/artificial-intelligence-in-criminal-justice/ ανευρεθέν στις 3/1/2022 (τελευταία πρόσβαση: 26/2/2022)

προσδιορίσουν με ακρίβεια εάν ένας υπόδικος θα πρέπει να αποδεσμευτεί ή όχι. Επιπλέον, κάποιοι από τους παράγοντες κινδύνου μπορεί να ληφθούν υπόψη ύστερα από εξέταση της στιγμής του αδικήματος, προηγούμενων καταδικαστικών αποφάσεων, ακροάσεων στο δικαστήριο αλλά και ποινών σε φυλάκιση.

Ένας σημαντικός παράγοντας ελέγχου της ποινικής δικαιοσύνης μέσω των συστημάτων τεχνητής νοημοσύνης είναι και οι στατιστικές μέθοδοι για την εύρεση προτύπων και συνδέσεων. Τα πρότυπα αυτά θα εξετάζουν τις βαθύτερες αιτίες του εγκλήματος, θα αντικατοπτρίζουν τις κοινωνικές ανισότητες, ακόμα και να αφαιρεθούν μεταβλητές όπως το φύλο ή ο σεξουαλικός προσανατολισμός.

Η τεχνητή νοημοσύνη μπορεί να διαδραματίσει σημαντικό ρόλο και να βελτιώσει τη λήψη κρίσιμων αποφάσεων στην ποινική δικαιοσύνη, ιδιαίτερα στις εκτιμήσεις κινδύνου πριν από τη δίκη. Οι αλγόριθμοι, όταν χρησιμοποιούνται προσεκτικά, κάνουν τις αποφάσεις πιο και διαφανείς και ορθές.

Αξίζει να αναφερθεί, πως υπάρχουν κάποιες αλγοριθμικές τεχνικές, οι οποίες χρησιμεύουν στην κατάταξη των εγκληματιών σε κλίμακες επικινδυνότητας και αποτελούν εργαλεία αξιολόγησης κινδύνου από τους δικαστές σε διάφορα στάδια της ποινικής διαδικασίας, για την πιθανότητα υποτροπής των κρατουμένων (COMPAS). Το λογισμικό COMPAS[117] είναι ένα εργαλείο διαχείρισης υποθέσεων και υποστήριξης αποφάσεων, το οποίο χρησιμοποιείται από τις δικαστικές αρχές, προκειμένου να αξιολογήσει εάν ένας κρατούμενος έχει πιθανότητες να υποτροπιάσει.[118][119] Στο ίδιο πλαίσιο λειτουργεί και το σύστημα HART[120].

Επιπρόσθετα, μια άλλη εφαρμογή της τεχνητής νοημοσύνης η οποία βασίζεται στην προγνωστική ανάλυση (*predictive analytics*)[121] είναι η προγνωστική δικαιοσύνη (*predictive justice*), μια στατιστική ανάλυση μεγάλου όγκου δεδομένων από νομολογία, έτσι ώστε να

---

[117] Correctional Offender Management Profiling for Alternative Sanctions

[118] Άρθρο του Λεωνίδα Κανέλλου με τίτλο «*Η Τεχνητή Νοημοσύνη στην υπηρεσία μιας Έξυπνης Δικαιοσύνης*» δημοσιευμένο στις 8/5/2020 στην ιστοσελίδα https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis?lspt_destination=upgrade ανευρεθέν στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[119] Επιστημονική Μελέτη των Tim Brennan και William Dietrich με τίτλο «*Correctional Offender Management Profiles for Alternative Sanctions (COMPAS)*» δημοσιευμένη τον Νοέμβριο του 2017 στην ιστοσελίδα https://www.researchgate.net/publication/321528262_Correctional_Offender_Management_Profiles_for_Alternative_Sanctions_COMPAS ανευρεθείσα στις 6/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[120] Harm Assessment Risk Tool

[121] Η προγνωστική ανάλυση χρησιμοποιεί μεγάλους όγκους δεδομένων για να προβλέψει και να διαμορφώσει τα όποια πιθανά αποτελέσματα και αποτελεί μια αρκετά πολύπλοκη διαδικασία.

μπορούν να προβλεφθούν τα νομικά και δικαστηριακά αποτελέσματα.[122] Μακροπρόθεσμα μπορεί να βοηθήσει στην γενικότερη απονομή της δικαιοσύνης, σε ταχύτερα αποτελέσματα, σε πιο στοχευμένες έρευνες και σε ορθότερη δικανική κρίση.

Ρομποτικοί δικαστές

Όταν οι έξυπνες μηχανές υπάρχουν σε κάθε μορφή της ανθρώπινης δραστηριότητας, καθόλου απίθανο δεν είναι στο μέλλον να συναντήσουμε και τους ρομποτικούς δικαστές. [123]Θα μπορούσαν να προγραμματιστούν κατά τρόπον ώστε να έχουν υψηλή νομική κατάρτιση και να αποφασίζουν τηρώντας τους κανόνες της αμεροληψίας, της ουδετερότητας και της προσωπικής και λειτουργικής ανεξαρτησίας. Θα μπορούν να λειτουργούν σε γρήγορες ταχύτητες και με ευκολία, καθώς το λογισμικό από το οποίο θα αποτελούνται θα μπορεί να εξετάζει τις εκκρεμείς υποθέσεις λαμβάνοντας τα στοιχεία που απαιτούνται, μειώνοντας τον φόρτο εργασίας τόσο των δικαστικών λειτουργών όσο και των δικαστικών υπαλλήλων. Επιπλέον, ένας ρομποτικός δικαστής θα προβαίνει στην λήψη αποφάσεων χωρίς να είναι επιφορτισμένος με ορισμένες ανθρώπινες αδυναμίες όπως είναι η κούραση από τον όγκο των υποθέσεων η μεροληψία και η ελλιπής γνώση.

Ήδη στην Αμερική γίνεται συζήτηση σχετικά με την υιοθέτηση του συγκεκριμένου μέτρου και όπως είναι λογικό εκφράζονται ορισμένες επιφυλάξεις όπως η εξής, της δικαστού Wendy Chang του Ανώτατου Δικαστηρίου του Los Angeles: «*Αν ένα αυτοματοποιημένο σύστημα βγάζει την απόφασή του με βάση τις πληροφορίες που λαμβάνει, πώς θα το εκπαιδεύσουμε ώστε να λάβει υπόψη και άλλους παράγοντες; Για μένα κάποια πράγματα είναι πολύ υποκειμενικά, έχουν να κάνουν με τη στιγμή*».[124]

Στην Κίνα πολλές υποθέσεις λαμβάνουν χώρα στα «ψηφιακά δικαστήρια», όπου οι διάδικοι δεν απαιτείται να εμφανιστούν αυτοπροσώπως στο δικαστήριο. Μάλιστα, το πρώτο ψηφιακό δικαστήριο ιδρύθηκε στην πόλη Hangzhou της Κίνας, στις 18 Αυγούστου του 2017 με στόχο

---

[122] Άρθρο του Bhishm Khanna, με τίτλο «*Predictive Justice: Using AI for Justice*», δημοσιευμένο στις 21/5/2021 στο Centre for Public Policy Research ανευρεθέν στην ιστοσελίδα https://www.cppr.in/wp-content/uploads/2021/05/PREDICTIVE-JUSTICE-USING-AI-FOR-JUSTICE-2.pdf στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[123] Άρθρο της Priya Dialani με τίτλο «*AI in Future courtrooms.Will they replace Judges?*» δημοσιευμένο στις 4/3/2021 στην ιστοσελίδα https://www.analyticsinsight.net/ai-will-have-robot-judges-soon-what-about-human-judges/ ανευρεθέν στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[124] Άρθρο της Absenta Mia με τίτλο «*AI στα δικαστήρια: Μήπως οι δικαστές του μέλλοντος θα είναι ρομπότ;*» δημοσιευμένο στις 22/1/2020 στην ιστοσελίδα https://www.secnews.gr/209014/ai-dikastiria-apofaseis/ ανευρεθέν στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

την μείωση του φόρτου εργασίας δικαστικών και υπαλλήλων και την γρηγορότερη και αποτελεσματικότερη απονομή της δικαιοσύνης. Επιπλέον, λόγω της ψηφιακής φύσης του, εκδικάζει υποθέσεις σχετικά με το Διαδίκτυο, τις ηλεκτρονικές αγορές και παραβιάσεις πνευματικών δικαιωμάτων.[125] Την ίδια χρονιά η Εσθονία ανακοίνωσε την εφαρμογή του «δικαστή-ρομπότ» για υποθέσεις μικροδιαφορών κάτω των 7.000 ευρώ, ούτως ώστε να επέλθει άμεση απονομή της δικαιοσύνης.[126]

Ωστόσο μια τέτοια συνθήκη, αφενός δεν μπορεί να υποκαταστήσει τους φυσικούς δικαστές, αλλά προτείνεται ως μια συμπληρωματική διαδικασία, αφετέρου ενέχει κινδύνους, οι οποίοι σχετίζονται με την «ταυτότητα» των μηχανών, ειδικότερα, με το να προσβληθεί η μηχανή από κάποιο ιό, να γίνει προσβολή στο λογισμικό (hacking), αλλά και να μην είναι δυνατή η ορθή συγγραφή της απόφασης ως προς το νομικό σκέλος του διατακτικού αλλά και η κατανόηση του νοήματός της από τους ενδιαφερόμενους και τους διαδίκους. [127]

Τεχνητή νοημοσύνη και επιβολή του νόμου[128]

Όπως είδαμε και παραπάνω, η χρήση της τεχνητής νοημοσύνης μπορεί να συμβάλει στην βελτίωση των αποτελεσμάτων της επιβολής του νόμου μειώνοντας κατά πολύ το ανθρώπινο λάθος και τις πολύωρες διαδικασίες. Υπάρχουν ορισμένες μέθοδοι, οι οποίες έχουν αποδείξει πως χρησιμοποιούνται προς τον σκοπό της επιβολής του νόμου και επιφέρουν θετικά αποτελέσματα ως επί το πλείστον. Συγκεκριμένα:

- Ανάλυση βίντεο και εικόνες: Αυτή η μέθοδος, όπου χρησιμοποιούνται αλγόριθμοι οι οποίοι ανιχνεύουν μέσω έξυπνων καμερών την ανθρώπινη παρουσία αλλά και

[125] Άρθρο του Xinhua με τίτλο «*China first internet court handles over 10,000 cases*» δημοσιευμένο στις 18/8/2018 στην ιστοσελίδα https://www.chinadaily.com.cn/a/201808/18/WS5b77c8f4a310add14f386801.html ανευρεθέν στις 18/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[126] Άρθρο του Victor Tangermann με τίτλο «*Estonia is building a "Robot Judge" to help clear legal backlog*» δημοσιευμένο στις 25/3/2017 στην ιστοσελίδα https://futurism.com/the-byte/estonia-robot-judge ανευρεθέν στις 18/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[127] Μελέτη του Χρήστου Τσουραμάνη από το 7ο Συνέδριο Security Project με τίτλο «*Η αντιμετώπιση του εγκλήματος με τη Συνδρομή της Τεχνητής Νοημοσύνης*» δημοσιευμένη στις 1/3/2019 στην ιστοσελίδα https://www.securityproject.gr/presentations/2019/day1-tsouramanis.pdf ανευρεθείσα στις 11/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[128] Άρθρο των Asma Idder και Stephane Coulaux με τίτλο «*Artificial intelligence in criminal justice: invasion or revolution?*» δημοσιευμένο στις 13/12/2021 στην ιστοσελίδα https://www.ibanet.org/dec-21-ai-criminal-justice ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

τα οχήματα, έχει στόχο στην κατανόηση των εικόνων που παρατηρεί αλλά και την ανάλυσή τους, προς σκοπό της ανίχνευσης εγκληματικών δράσεων.[129]

- Αναγνώριση: Μέσω αυτής της μεθόδου, αξιολογούνται οι κινήσεις του σώματος, τα ρούχα, οι εκφράσεις του προσώπου και έτσι ανιχνεύονται οι μη φυσιολογικές και αναμενόμενες συμπεριφορές οι οποίες υποκρύπτουν παραβατική συμπεριφορά. Το ίδιο συμβαίνει και με τα οχήματα, όπου οι μηχανές τεχνητής νοημοσύνης είναι προγραμματισμένα να αποκρυπτογραφούν ακόμα και τις πινακίδες κυκλοφορίας. Στον Καναδά, ήδη η μέθοδος της αναγνώρισης προσώπων εφαρμόζεται.[130]
- Κλειστό κύκλωμα τηλεόρασης: Πολλά τροχαία ατυχήματα έχουν εντοπιστεί χάρη στο κλειστό κύκλωμα τηλεόρασης, καθώς και εγκλήματα που λαμβάνουν χώρα στο διαδίκτυο όπως το ξέπλυμα βρώμικου χρήματος, η σεξουαλική κακοποίηση ή η εμπορία ανθρώπων.

Clearview AI: Πρόκειται για την μεγαλύτερη ιδιωτική εταιρεία δικτύων προσώπου παγκοσμίως, η οποία έχει ως βασική μέθοδο την αναγνώριση προσώπου μέσω αλγορίθμων που αναγνωρίζουν πρόσωπα από πολλαπλές βάσεις δεδομένων, οι οποίες βρίσκονται στο διαδίκτυο.[131]

NLP(Natural Language Processing): Η λεγόμενη επεξεργασία της φυσικής γλώσσας αποτελεί κλάδο της τεχνητής νοημοσύνης και της πληροφορικής, όπου οι μηχανές κατανοούν την ανθρώπινη γλώσσα, την μεταφράζουν, αναλύουν τις προτάσεις και στην συνέχεια με την χρήση αλγορίθμων μπορούν και οδηγούνται σε συμπεράσματα.[132]

---

[129] Άρθρο του Nik Gagvani, με τίτλο «*Introduction to video analytics*» δημοσιευμένο στις 22/8/2008 στην ιστοσελίδα https://www.eetimes.com/introduction-to-video-analytics/# ανευρεθέν στις 13/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[130] Police use of Facial Recognition Technology in Canada and the way forward, 10/6/2021 δημοσιευμένο στην ιστοσελίδα https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[131] Επίσημη ιστοσελίδα της Clearview.ai https://www.clearview.ai

[132] Άρθρο με τίτλο «*The role of natural language processing in AI*» δημοσιευμένο στις 12/10/2021 στην ιστοσελίδα του University of York https://online.york.ac.uk/the-role-of-natural-language-processing-in-ai/ ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Από τα πιο χαρακτηριστικά παραδείγματα NLP είναι το *Siri*  [133]όπου βρίσκεται ως λειτουργικό σύστημα στα iOS και macOS.[134], όπου με μια φωνητική εντολή, ο υπολογιστής απαντάει σε ερωτήματα, αφού πρώτα έχει «ακροαστεί» την φωνή του χρήστη, επομένως μπορεί να την αναγνωρίζει κάθε φορά που θέτει το ερώτημα και να προσαρμόζεται στις προτιμήσεις του.

Στα ίδια πλαίσια λειτουργεί και το ρομπότ *Alexa*  [135]ένας τεχνολογικός βοηθός που αναπτύχθηκε από την εταιρεία Amazon.[136] Πρόκειται για μια φωνητική υπηρεσία, βασισμένη σε τεχνολογίες cloud όπου μπορεί να ανταποκριθεί στις απαιτήσεις των χρηστών, να δώσει πρόγνωση για τον καιρό, να αναπαράγει μουσική, να ενημερώσει για τις ειδήσεις και την τρέχουσα επικαιρότητα κ.ά.

Επίσης, το *Google Assistant*  [137]της Google λειτουργεί στα ίδια πλαίσια, μπορεί να προχωρήσει στην ανταλλαγή ερωτημάτων[138] και στην συνομιλία με τους χρήστες. Σύμφωνα με μια πρόσφατη μελέτη του 2021, ο βοηθός google είναι ο πιο ακριβής φωνητικός βοηθός, ο πιο εξελιγμένος, καθώς υποστηρίζει και πληθώρα έξυπνων συσκευών, συμπεριλαμβανομένων των αυτοκινήτων και των έξυπνων οικιακών συσκευών, ενώ η Siri και η Alexa ακόμα χρειάζονται ορισμένες βελτιώσεις, δεδομένου ότι είναι και πιο σύγχρονες.[139]

---

[133] Σύμβολο του Siri ανευρεθέν στις 27/1/2022 στην ιστοσελίδα https://techblog.gr/software/i-siri-etoimazetai-na-milisei-ellinika-apokleistiko/ (τελευταία πρόσβαση: 26/2/2022)

[134] Άρθρο του Ilya Dudkin με τίτλο «*How does SIRI work: Technology and Algorithm*» δημοσιευμένο στις 12/11/2018 στην ιστοσελίδα https://skywell.software/blog/how-does-siri-work-technology-and-algorithm/ ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[135] Εικόνα συσκευής Alexa ανευρεθείσα στις 27/1/2022 στην ιστοσελίδα https://www.istockphoto.com/photos/alexa (τελευταία πρόσβαση: 26/2/2022)

[136] Άρθρο του Jenn Henry Horowitz με τίτλο «*Is Alexa an AI*» δημοσιευμένο στις 10/12/2020 στην ιστοσελίδα https://itchronicles.com/artificial-intelligence/is-alexa-an-ai/ ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[137] Λογότυπο της Google Assistant ανευρεθέν στις 27/1/2022 στην ιστοσελίδα https://el.m.wikipedia.org/wiki/Αρχείο:Google_Assistant_logo.svg (τελευταία πρόσβαση: 26/2/2022)

[138] Το Google Assistant δεν υποστηρίζεται ακόμα στα Ελληνικά.

[139] Άρθρο της Jill McKeon με τίτλο «*Google's Artificial Intelligence Voice Assistant Bests Siri, Alexa*» δημοσιευμένο στις 24/5/2021 στην ιστοσελίδα https://healthitanalytics.com/news/googles-artificial-intelligence-voice-assistant-bests-siri-alexa ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Τεχνητή Νοημοσύνη και Προληπτική Αστυνόμευση

Η μαζική παρακολούθηση είναι ένα από τα ζητήματα τα οποία έχουν απασχολήσει πολύ την ευρωπαϊκή και διεθνή κοινότητα. Πρόσφατα μάλιστα, το Ευρωπαϊκό Κοινοβούλιο δεν συμφώνησε στην μαζική παρακολούθηση των πολιτών και ζήτησε την απαγόρευση των μεθόδων ιδιωτικών δεδομένων αναγνώρισης προσώπων όπως είναι το Clearview[140] , καθώς και της προληπτικής αστυνόμευσης η οποία βασίζεται σε συμπεριφορικά γεγονότα, βασίζοντας αυτήν την τοποθέτηση στο γεγονός ότι κατά την χρήση αυτών των τεχνολογιών δεν διασφαλίζονται τα θεμελιώδη δικαιώματα των πολιτών και δεν αποδεικνύεται η διαφάνεια των αλγορίθμων.[141] Ο επικεφαλής του Ευρωπαϊκού Κοινοβουλίου Peter Vitanov[142] δήλωσε πως: «*Τα θεμελιώδη δικαιώματα είναι άνευ όρων. Για πρώτη φορά, ζητάμε μορατόριουμ για την ανάπτυξη συστημάτων αναγνώρισης προσώπου για σκοπούς επιβολής του νόμου, καθώς η τεχνολογία έχει αποδειχθεί αναποτελεσματική και συχνά οδηγεί σε μεροληπτικά αποτελέσματα. Είμαστε ξεκάθαρα αντίθετοι στην προληπτική αστυνόμευση που βασίζεται στην χρήση AI καθώς και σε οποιαδήποτε επεξεργασία βιομετρικών δεδομένων που οδηγεί σε μαγική παρακολούθηση. Αυτή είναι μια τεράστια νίκη για όλους τους Ευρωπαίους πολίτες*».[143]Τα συστήματα τεχνητής νοημοσύνης θα πρέπει να βρίσκονται υπό ανθρώπινη εποπτεία και οι αλγόριθμοι θα πρέπει να είναι «ανοιχτοί».

Στην Σουηδία το 2016, με μια απόφαση-σταθμό, το Ανώτατο Δικαστήριο της Σουηδίας απαγορεύει τις πτήσεις drones με ενσωματωμένη κάμερα, με το αιτιολογικό ότι θεωρούνται μηχανές παρακολούθησης και θα έπρεπε να έχουν ειδική άδεια για να κυκλοφορούν.[144] Το

---

[140] Άρθρο με τίτλο «*Use of artificial intelligence by the police: MEPS oppose mass surveillance*», δημοσιευμένο στις 6/10/2021 στην επίσημη ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance ανευρεθέν στις 26/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[141] Άρθρο με τίτλο «*Τεχνητή νοημοσύνη και αστυνόμευση: Κατά της μαζικής παρακολούθησης το Ευρωπαϊκό Κοινοβούλιο*» δημοσιευμένο στις 8/10/2021 στην ιστοσελίδα του Lawspot https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-kai-astynomeysi-kata-tis-mazikis-parakoloythisis-eyropaiko-koinovoylio?lspt_destination=upgrade ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[142] Προφίλ του Peter Vitanov στην επίσημη ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου

[143] Άρθρο με τίτλο «*Use of artificial intelligence by the police: MEPs oppose mass surveillance | EU Parliament Press*» δημοσιευμένο στις 6/10/2021 στην ιστοσελίδα https://www.pubaffairsbruxelles.eu/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance-eu-parliament-press/ ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[144] Άρθρο με τίτλο «*Sweden bans camera on drones*» δημοσιευμένο στις 25/10/2016 στην ιστοσελίδα https://www.bbc.com/news/technology-37761872 ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

γεγονός όμως ότι στην Σουηδία είναι επιτρεπτή η λήψη φωτογραφιών και βίντεο σε δημόσιους χώρους, η εν λόγω απόφαση κρίθηκε ιδιαιτέρως περίεργη. Μάλιστα, το Δικαστήριο μέσα στην απόφασή του αναφέρει ότι *«η κάμερα (drone) μπορεί να χρησιμοποιηθεί για προσωπική παρακολούθηση, παρόλο που δεν είναι αυτός ο σκοπός της. Συνεπώς, η κάμερα πρέπει να θεωρείται ως κάμερα παρακολούθησης»*.[145]

Στην Γαλλία, το Συμβούλιο της Επικρατείας, σε μια σημαντική απόφαση με διεθνή χαρακτήρα, απαγορεύει την χρήση των drones από την αστυνομία στο πλαίσιο των διαδηλώσεων στο Παρίσι, καθώς υποστήριξε πως υπάρχει *«σοβαρή αμφιβολία για την νομιμότητα»* των drones και πως η καταγραφή των δεδομένων παραβιάζει την ελευθερία των διαδηλωτών.[146] Στην απόφαση αναφέρεται πώς το Δικαστήριο διέταξε την κυβέρνηση *«να σταματήσει, χωρίς καθυστέρηση την διενέργεια μέτρων επιτήρησης με χρήση drones για την παρακολούθηση της συμμόρφωσης, στο Παρίσι, με τους κανόνες υγειονομικής ασφάλειας που ισχύουν κατά την διάρκεια της ευκολίας του περιορισμού»*.[147]

Απαγόρευση της Μαζικής Βιομετρικής Παρακολούθησης: Το δίκτυο οργανώσεων της European Digital Rights (EDRi)[148] δημοσίευσε στις 13/5/2020 μελέτη με τίτλο *«Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States»*.[149] Η συγκεκριμένη μελέτη απαιτεί από τους θεσμούς της ευρωπαϊκής ένωσης αλλά και από τα κράτη μέλη να σταματήσουν κάθε πρακτική που εφαρμόζεται αλλά και

---

[145] *«that the [drone] camera can be used for personal monitoring, although it is not the purpose. The camera is therefore to be regarded as a surveillance camera»* απόσπασμα της απόφασης στα αγγλικά, από το άρθρο του Tom Mendelshon *«Sweden's highest court bans drones with cameras»* δημοσιευμένο στις 25/10/2016 στην ιστοσελίδα https://arstechnica.com/tech-policy/2016/10/camera-spy-drones-banned-sweden-highest-court/ ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[146] Άρθρο με τίτλο *«Η Γαλλία απαγορεύει τη χρήση drones από την αστυνομία στο πλαίσιο διαδηλώσεων στο Παρίσι»* δημοσιευμένο στις 23/12/2020 στην ιστοσελίδα https://www.lawspot.gr/nomika-nea/i-gallia-apagoreyei-ti-hrisi-drones-apo-tin-astynomia-sto-plaisio-diadiloseon-sto-parisi?lspt_destination=upgrade ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[147] Άρθρο των Freshfields Bruckhaus Deringer LLP με τίτλο *«French court rules on use of drones by Paris police»* δημοσιευμένο στις 11/6/2020 στην ιστοσελίδα https://www.lexology.com/library/detail.aspx?g=e81fdeeb-b669-456a-a600-b220129e57e7 ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[148] Πρόκειται για μια διεθνή ομάδα εμπειρογνωμόνων, υποστηρικτών και ακαδημαϊκών με έδρα τις Βρυξέλλες, η οποία έχει ως στόχο την υπεράσπιση και την προώθηση των ψηφιακών δικαιωμάτων.

[149] Ολόκληρο το κείμενο της μελέτης δημοσιευμένο στις 13/5/2020 στην ιστοσελίδα https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf ανευρεθέν στις 27/1/2022 (τελευταία πρόσβαση: 26/2/2022)

μελλοντικές προοπτικές σχετικά με την μαζική παρακολούθηση μέσω της χρήσης βιομετρικών δεδομένων.

5. BLOCKCHAIN ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Η τεχνολογία blockchain στις μέρες μας έχει κατακτήσει επάξια μια θέση στις νέες τεχνολογίες οι οποίες έχουν συμβάλει στον ψηφιακό μετασχηματισμό. Πρόκειται για την λεγόμενη τεχνολογία της «αλυσίδας των μπλοκ», ένα είδος βάσης δεδομένων , που έχει ως στόχο να βελτιώσει την ποιότητα των συναλλαγών και μπορεί να χρησιμοποιηθεί για τους σκοπούς της απόδειξης, και αυτό κυρίως, επειδή τα δεδομένα στα «μπλοκ» δεν μπορούν να τροποποιηθούν μετά την καταχώρησή τους, έτσι φαίνεται ποιες πράξεις τελέστηκαν και αυτό δεν μπορεί να αλλοιωθεί.

Το 2018, το Δικαστήριο του Διαδικτύου Hangzhou στην Κίνα[150], σε μια υπόθεση πνευματικής ιδιοκτησίας, έκρινε πως τα δεδομένα που συλλέχτηκαν, μέσω της τεχνολογίας blockchain, θα πρέπει να έχουν ψηφιακές υπογραφές, σφραγίδες που πιστοποιούν την γνησιότητα και να μπορούν να επαληθευθούν. Έτσι, η τεχνολογία blockchain θα πρέπει να θεωρείται ως νόμιμη και παραδεκτή απόδειξη, σε περιπτώσεις που χρησιμοποιείται για την επαλήθευση της γνησιότητας της ψηφιακής απόδειξης.[151]

Μαζί με την τεχνητή νοημοσύνη αποτελούν δύο τεχνολογίες καινοτόμες οι οποίες έχουν την ικανότητα να βελτιώσουν τις δημιουργήσουν νέα μοντέλα και να αναδιαμορφώσουν ολόκληρους κλάδους. Δεδομένου ότι κάθε τεχνολογία επιτελεί το δικό της έργο μπορούν να συνυπάρχουν σε μια εφαρμογή χωρίς απαραίτητα να αλληλεπιδρούν μεταξύ τους. Συγκεκριμένα, η τεχνητή νοημοσύνη μπορεί να ανιχνεύει μοτίβα και να βελτιώνει τις διαδικασίες ενώ το Blockchain παρέχει ένα κοινόχρηστο περιβάλλον λειτουργίας αυξάνοντας την ασφάλεια και το απόρρητο των διαδικασιών.

---

[150] Βλ. υποσημείωση 102

[151] Μελέτη του Frederick Mostert, King's College London με τίτλο «*The Application and Challenges of Blockchain in Intellectual Property Driven Businesses in China*» δημοσιευμένη στις 8/6/2020 στην ιστοσελίδα https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600115 ανευρεθείσα στις 22/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Στις 19 Οκτωβρίου 2017, η Σύνοδος του Ευρωπαϊκού Συμβουλίου για την ψηφιακή Ευρώπη διατυπώνει στα συμπεράσματά της[152], την ανάγκη αυξημένης ενασχόλησης με τις νέες τεχνολογίες, όπως είναι η Τεχνητή Νοημοσύνη και οι τεχνολογίες αλυσίδων μπλοκ (blockchain) με σεβασμό σε ζητήματα προστασίας δεδομένων, ψηφιακών δικαιωμάτων και προτύπων δεοντολογίας.

Ο συνδυασμός της τεχνητής νοημοσύνης με την τεχνολογία blockchain παραμένει ακόμα αρκετά ανεξερεύνητος, καθώς οι δύο αυτές τεχνολογίες έχουν την δυνατότητα να αξιοποιήσουν τα δεδομένα που λαμβάνουν με έναν πρωτοποριακό τρόπο. Βασικό συστατικό για την ανάπτυξη των αλγορίθμων της τεχνητής νοημοσύνης είναι τα δεδομένα και το blockchain μπορεί να τα προστατέψει αλλά και να ελέγξει για την προέλευση αλλά και την χρησιμότητά τους.

6. ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Οι κυβερνοεπιθέσεις με τεχνητή νοημοσύνη είναι συμβατικές κυβερνοεπιθέσεις οι οποίες χρησιμοποιούν αυξημένες τεχνολογίες τεχνητής νοημοσύνης και μηχανικής μάθησης.[153] Οι αλγόριθμοι της τεχνητής νοημοσύνης έχουν την δυνατότητα μέσω των δεδομένων να εντοπίζουν τις ασυνήθιστες δραστηριότητες και να μπορούν να προχωρήσουν στην διαπίστωση εάν υπάρχει παραβίαση στο υπολογιστικό σύστημα.[154]

Εκτός από τους αναφερθέντες αλγορίθμους, υπάρχει και η μέθοδος της λεγόμενης «*εποπτευόμενης μάθησης*»,[155] όπου στόχος είναι η πρόληψη των κυβερνοεπιθέσεων. Με αυτή την μέθοδο, ανιχνεύονται οι απειλές και τα κακόβουλα λογισμικά με βάση τα ήδη υπάρχοντα δεδομένα.

---

[152] Διαβιβαστικό σημείωμα του Ευρωπαϊκού Συμβουλίου, Βρυξέλλες, 19 Οκτωβρίου 2017 (OR.en) EUCO 14/17 δημοσιευμένο στην ιστοσελίδα https://www.consilium.europa.eu/media/21603/19-euco-final-conclusions-el.pdf ανευρεθέν στις 17/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[153] Άρθρο της Kyle Wiggers με τίτλο «*Dear enterprise IT: Cybercriminals use AI too*» δημοσιευμένο στις 17/6/2021 στην ιστοσελίδα https://venturebeat.com/2021/06/17/dear-enterprise-it-cybercriminals-use-ai-too/ ανευρεθέν στις 5/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[154] Άρθρο του Vinod Vasudevan με τίτλο «*How AI Is Transforming Cyber Defense*» δημοσιευμένο στις 24/7/2018 ανευρεθέν στην ιστοσελίδα https://www.forbes.com/sites/forbestechcouncil/2018/07/24/how-ai-is-transforming-cyber-defense/ στις 19/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[155] Άρθρο του Francis Knott με τίτλο «*The Surprising Role of AI in Cybercrime*» δημοσιευμένο στην ιστοσελίδα https://www.attilasec.com/blog/ai-in-cybercrime ανευρεθέν στις 19/1/2022 (τελευταία πρόσβαση: 26/2/2022)

7. ΟΙ ΑΠΕΙΛΕΣ ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΕΜΦΑΝΙΣΕΙ ΜΙΑ ΕΠΙΧΕΙΡΗΣΗ[156]

Ενώ οι περισσότερες επιχειρήσεις προσπαθούν να διατηρήσουν ασφαλή τα δεδομένα τους από τα συστήματα τεχνητής νοημοσύνης τα οποία λόγω της αυξημένης χρήσης τους και των σύγχρονων λειτουργιών τους έχουν μεγάλη δύναμη, πολλοί οργανισμοί ακόμα δεν έχουν καθοδήγηση σχετικά με τον τρόπο ασφαλούς εφαρμογής τεχνολογιών τεχνητής νοημοσύνης στα συστήματά τους και έτσι υπάρχουν απειλές οι οποίες ελλοχεύουν και θέτουν σε κίνδυνο τις επιχειρήσεις.

Αυτοματοποιημένες επιθέσεις μεγάλης κλίμακας

Οι μηχανές και οι εφαρμογές της τεχνητής νοημοσύνης έχουν την ικανότητα να μιμούνται τα πρότυπα της ανθρώπινης σκέψης και τους τρόπους λειτουργίας της, με αποτέλεσμα αυτά τα συστήματα να μπορούν να εκπαιδεύονται να εκτελούν συντονισμένες κυβερνοεπιθέσεις χωρίς να τους το έχει υπαγορεύσει κάποιος ένας εγκληματίας στον κυβερνοχώρο. Η ταχύτητα που παρέχει η τεχνητή νοημοσύνη, ωθεί τους εγκληματίες του κυβερνοχώρου να προχωρούν στον συντονισμό μιας μεγάλης επίθεσης στο σύστημα δεδομένων ενός οργανισμού, με γρήγορα αποτελέσματα και χωρίς την απαραίτητη παρέμβαση του ανθρώπου.

Hacking τεχνολογιών επιτήρησης

Επειδή τα συστήματα ασφαλείας βίντεο που βασίζονται σε τεχνητή νοημοσύνη δημιουργούν δεδομένα βασισμένα σε πλάνα ασφαλείας, οι εγκληματίες του κυβερνοχώρου που παραβιάζουν αυτά τα συστήματα μπορούν να αποκτήσουν πρόσβαση στα εξαιρετικά ευαίσθητα δεδομένα στα οποία η τεχνητή νοημοσύνη είχε εξακριβώσει σχετικά με το υλικό.

Αλγοριθμικός χειρισμός

[156] Άρθρο με τίτλο «*Artificial Intelligence and Cyber Crime: Facing New Threats*» δημοσιευμένο στις 17/7/2020 στην ιστοσελίδα https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/ ανευρεθέν στις 4/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Χρησιμοποιώντας έναν αλγόριθμο τεχνητής νοημοσύνης, οι χάκερς μπορούν να τον προσαρμόσουν και να εισβάλλουν σε ένα σύστημα δεδομένων τεχνητής νοημοσύνης και να προκαλέσουν βλάβη ή να καταστρέψουν ολόκληρο το σύστημα πληροφοριών. Αυτές οι επιθέσεις επηρεάζουν άμεσα την διαδικασία μηχανικής εκμάθησης του συστήματος τεχνητής νοημοσύνης, καθώς αποτελούν την βάση με την οποία τα συστήματα επεξεργάζονται τις πληροφορίες τις οποίες συναντούν.

Παράκαμψη της φυσικής αναγνώρισης

Με αφορμή μια χαρακτηριστική επίθεση που έγινε στον κυβερνοχώρο το 2019, γίνεται αντιληπτό πως τα συστήματα τεχνητής νοημοσύνης είναι πλέον τόσο ικανά να αναπαράγουν με πειστικό τρόπο τα φυσικά χαρακτηριστικά των ανθρώπων που μπορούν να δημιουργήσουν μεγάλη ζημιά στις επιχειρήσεις και να πείσουν τον συνομιλητή τους πως μιλούν με φυσικό πρόσωπο. Στην υπόθεση που αναφέρθηκε, ένας χάκερ χρησιμοποίησε συστήματα τεχνητής νοημοσύνης για να μιμηθεί την φωνή ενός στελέχους ευρωπαϊκής εταιρείας και κατάφερε να μεταφέρει πάνω από 240.000 δολάρια από τα κεφάλια της εταιρείας απευθείας στον λογαριασμό του χάκερ[157].

8. ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΕΥΘΥΝΗ[158]

Το ζήτημα της ευθύνης στην τεχνητή νοημοσύνη αποτελεί ένα ακανθώδες νομικό και ηθικό ζήτημα, καθώς εγείρονται ερωτήματα κατά πόσο μπορεί μια μηχανή να ευθύνεται και τι μερίδιο ευθύνης πρέπει να της αποδοθεί. Έχουν διατυπωθεί τρία πιθανά μοντέλα ευθύνης.[159] Το πρώτο μοντέλο, το PVM[160], θεωρεί την μηχανή της τεχνητής νοημοσύνης ως μια

[157] Άρθρο του Drew Harwell με τίτλο «*An-artificial intelligence first: Voice-mimicking software reportedly used in a major theft*» δημοσιευμένο στις 4/9/2019 στην ιστοσελίδα https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/ ανευρεθέν στις 4/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[158] Επιστημονική μελέτη του Peter Yeoh με τίτλο «*Artificial intelligence: accelerator or panacea for financial crime?*» δημοσιευμένο τον Φεβρουάριο του 2019 στην ιστοσελίδα https://www.emerald.com/insight/publication/issn/1359-0790 ανευρεθείσα στις 10/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[159] Επιστημονική μελέτη του Gabriel Hallevy με τίτλο «*The Criminal Liability of Artificial Intelligence Entities-from Science Fiction to Legal Social Control*» δημοσιευμένο τον Μάρτιο του 2016 στην ιστοσελίδα https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1037&context=akronintellectualproperty ανευρεθείσα στις 10/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[160] The Perpetration-via-Another Liability Model

απαλλαγμένη από την ευθύνη οντότητα, αλλά ένα ενδιάμεσο όργανο μέσω του οποίου ο δράστης διαπράττει το έγκλημά του. Ο δράστης-προγραμματιστής σχεδίασε ένα λογισμικό, το οποίο είναι ικανό να πραγματοποιήσει όλες τις κακόβουλες ενέργειες τις οποίες επιθυμεί ο δράστης. Επομένως, το πρώτο μοντέλο θέτει ως ποινικά υπεύθυνο τον προγραμματιστή και τον χρήστη και όχι την μηχανή. Το δεύτερο μοντέλο, το NPCLM[161], ασχολήθηκε με την εμπλοκή προγραμματιστών σε καθημερινές δραστηριότητες της τεχνητής νοημοσύνης, χωρίς όμως να υπάρχει η πρόθεση για διάπραξη κάποιου αδικήματος. Το μοντέλο βασίζεται στην ικανότητα που έχουν οι προγραμματιστές να προβλέψουν την πιθανή διάπραξη εγκλημάτων μέσω τεχνολογιών και μηχανών τεχνητής νοημοσύνης. Προσομοιάζει θα λέγαμε με την ποινική ευθύνη σε περιπτώσεις αμέλειας του ελληνικού Ποινικού Κώδικα, καθώς εδώ ο δράστης-προγραμματιστής δεν απαιτείται να γνωρίζει ότι μέσα από τις δραστηριότητές του θα διαπράξει κάποιο αδίκημα, αλλά να το προβλέψει ως φυσική πιθανή συνέπεια των πράξεών του. Σε αυτή την περίπτωση διατυπώνονται δύο απόψεις σχετικά με την ευθύνη. [162]Η πρώτη βασίζεται στο ότι η οντότητα της τεχνητής νοημοσύνης δεν ευθύνεται καθώς δεν είχε το προσωπικό στοιχείο της θέλησης για διάπραξη αδικήματος, ενώ η δεύτερη την θεωρεί υπεύθυνη καθώς προγραμματίστηκε με τρόπο ώστε να μπορεί να πραγματοποιήσει μια συγκεκριμένη εγκληματική ενέργεια άμεσα. Το τρίτο μοντέλο, το DLM[163], το οποίο αναφέρεται στην άμεση ευθύνη, αντιμετωπίζει τις μηχανές της τεχνητής νοημοσύνης ως ανθρώπους και τις πράξεις τους ως ανθρώπινες παραβιάσεις και ως εκ τούτου ορίζει πως η ποινική ευθύνη μιας μηχανής δεν πρέπει να διαφέρει από την αντίστοιχη ποινική ευθύνη ενός ανθρώπου.

Αυτά τα τρία μοντέλα τα οποία αναπτύχθηκαν παραπάνω, σίγουρα δεν αποτελούν οδηγό σχετικά με την ευθύνη, θα μπορούσαν όμως να αποτελούν μια αξιολόγηση σχετικά με το πως θα πρέπει να αντιμετωπίζεται μια οντότητα τεχνητής νοημοσύνης και σε ποια πλαίσια θα πρέπει να υπάρχει τιμώρηση σχετικά με τους κανόνες του ποινικού δικαίου.

---

[161] The Natural-Probable-Consequence Liability Model

[162] Επιστημονική μελέτη του Evan Goldstick με τίτλο «*Accidental Vitiation: The Natural and Probable Consequence of Rosemond v. United States on the Natural and Probable Consequence Doctrine*» δημοσιευμένο το 2016 στην ιστοσελίδα https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5268&context=flr ανευρεθείσα στις 10/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[163] The Direct Liability Model

9. ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΑΠΟ ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Καθώς ολοένα και περισσότερες επιχειρήσεις ενσωματώνουν τεχνολογίες τεχνητής νοημοσύνης, υπάρχουν περισσότερα διαθέσιμα μέτρα ασφάλειας στον κυβερνοχώρο τα οποία μπορούν να χρησιμοποιηθούν με στόχο την προστασία των ευαίσθητων δεδομένων και των συστημάτων τεχνητής νοημοσύνης από επιθέσεις στον κυβερνοχώρο.

Προώθηση στρατηγικών για την ανθεκτικότητα στον κυβερνοχώρο

Ως ανθεκτικότητα στον κυβερνοχώρο ορίζεται η ικανότητα ενός συστήματος δεδομένων να συνεχίζει τις κανονικές του λειτουργίες μετά την επίθεση που δέχθηκε. Μάλιστα, λαμβάνεται υπόψη και η ικανότητα του συστήματος να επαναφέρει κλεμμένα δεδομένα ή μηχανικές και τεχνικές λειτουργίες μετά την εμφάνιση δεδομένων ή βλάβης του συστήματος. Η τεχνική αυτή της ανθεκτικότητας είναι ζωτική για την ασφάλεια στον κυβερνοχώρο καθώς συνδέεται άμεσα με την δυνατότητα ανάκτησης και επαναφοράς σε περίπτωση επίθεσης του συστήματος. Ένα αναπόσπαστο κομμάτι για την ανάπτυξη της ανθεκτικότητας στον κυβερνοχώρο είναι τα αντίγραφα ασφαλείας δεδομένων που βασίζονται σε τεχνητή νοημοσύνη και τα πρωτόκολλα ανάκτησης συστήματος. Χρησιμοποιούνται νέες τεχνολογίες οι οποίες αξιοποιούν την τεχνητή νοημοσύνη και την μηχανική μάθηση για να αυτοματοποιήσουν την συνεχιζόμενη εργασία δημιουργίας αντιγράφων ασφαλείας κρίσιμων δεδομένων και στοιχείων λογισμικού. Αυτά τα εργαλεία είναι απαραίτητη προϋπόθεση για την διατήρηση μιας αποτελεσματικής διαδικασίας δημιουργίας αντιγράφων ασφαλείας που μπορεί να αντιδράσει γρήγορα στις μεταβαλλόμενες απαιτήσεις. Επιπλέον, η εξοικονόμηση ενέργειας αυτών των εφεδρικών αντιγράφων ασφαλείας μπορεί να είναι αποτελεσματική. Τα συστήματα ανάκτησης και δημιουργίας αντιγράφων ασφαλείας τεχνητής νοημοσύνης μπορούν να περιλαμβάνουν αλγόριθμους που έχουν σχεδιαστεί για να βοηθούν τις ομάδες αντιμετώπισης περιστατικών επίθεσης στον κυβερνοχώρο αλλά και να θωρακίζουν ένα ασφαλές πλαίσιο προστασίας μέσα από το οποίο θα προστατεύονται τα δεδομένα και δεν θα κινδυνεύει ο ολική απώλεια και καταστροφή τους. Καθώς οι οργανισμοί συνεχίζουν να μεγαλώνουν και να επεκτείνουν τους ορίζοντες των ψηφιακών λειτουργιών τους, η ανάγκη για έξυπνα και αυτοματοποιημένα συστήματα δημιουργίας αντιγράφων ασφαλείας θα αυξηθεί. Με τις ρυθμιστικές αρχές να απαιτούν τον χειρισμό των δεδομένων με διαφορετικό τρόπο,

ανάλογα με τα ζητήματα απορρήτου και ασφάλειας, οι μεγάλοι οργανισμοί θα πρέπει να αυτοματοποιήσουν τη διαχείριση των αποθηκών δεδομένων τους. Είτε κατά τη διάρκεια λειτουργιών ρουτίνας δημιουργίας αντιγράφων ασφαλείας είτε στη μέση της ανάκαμψης από μια καταστροφή, ο χειρισμός δεδομένων θα απαιτεί προσεκτική διαχείριση για να διασφαλιστεί η συμμόρφωση και η επιχειρηματική συνέχεια. Τα αυτοματοποιημένα συστήματα θα είναι ένας τρόπος για να γίνει αυτό με μια εύλογη ανθρώπινη επίβλεψη.[164]

Εφαρμογή λύσεων επιθετικής και αμυντικής ασφάλειας

Ο καλύτερος τρόπος για να προστατευθεί μια επιχείρηση από τις απειλές και τις επιθέσεις στον κυβερνοχώρο είναι η χρήση της προληπτικής και αντιδραστικής ασφάλειας στον κυβερνοχώρο με την χρήση της τεχνητής νοημοσύνης. Η αμυντική τεχνητή νοημοσύνη μπορεί να διακόψει τις επιθέσεις που είναι εν ενεργεία χωρίς να επηρεάσει την κανονική λειτουργία ενός συστήματος. Οι αλγόριθμοι αυτοεκμάθησης κατανοούν τα συνήθη πρότυπα χρηστών, συστημάτων και συσκευών σε έναν οργανισμό, εντοπίζουν την ασυνήθιστη δραστηριότητα και προσπαθούν να χτίσουν ένα πέπλο ασπίδας και προστασίας. Τα συστήματα τεχνητής νοημοσύνης μπορούν να εκπαιδευτούν ώστε να εντοπίζουν ακόμα και τις πιο μικρές συμπεριφορές, οι οποίες υποδηλώνουν επίθεση και εμπεριέχουν κακόβουλο λογισμικό, πριν υπεισέλθει στο σύστημα και στην συνέχεια του προκαλέσει βλάβη.[165]

Πρόσληψη ειδικών τεχνητής νοημοσύνης και εγκλήματος στον κυβερνοχώρο

Για κάθε οργανισμό που θέλει να ενσωματώσει την τεχνητή νοημοσύνη στα συστήματά του, θα πρέπει να προχωρήσει στην πρόσληψη τυπικού προσωπικού πληροφορικής αλλά και εσωτερικών και εξωτερικών ειδικών σε θέματα ασφάλειας και συντήρησης τεχνητής νοημοσύνης. Η υψηλή κατάρτιση αυτών των επαγγελματιών θα βοηθήσει στο να

[164] Άρθρο της Ashley Wilson με τίτλο «*4 Ways AI Can Make Data Backup More Efficient*» δημοσιευμένο στις 7/11/2019 στην ιστοσελίδα https://www.kolabtree.com/blog/4-ways-ai-can-make-data-backup-more-efficient/ ανευρεθέν στις 4/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[165] Άρθρο της Aimee Laurence με τίτλο «*The Impact of Artificial Intelligence on Cyber Security*» δημοσιευμένο στις 22/8/2019 στην ιστοσελίδα https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/ ανευρεθέν στις 4/1/2022 (τελευταία πρόσβαση: 26/2/2022)

εφαρμοστούν τα πρωτόκολλα ασφαλείας στα συστήματα αλλά και να διασφαλιστεί η αποτελεσματικότητα των αλγορίθμων ενός συστήματος τεχνητής νοημοσύνης.

Η τεχνητή νοημοσύνη με την ισχυρή της παρουσία στον τεχνολογικό και νομικό κόσμο, μπορεί όχι μόνο να βοηθήσει τους επιτιθέμενους/χάκερς να εξελίσσονται και να επιτίθενται κακόβουλα σε ξένα υπολογιστικά συστήματα, αλλά μπορεί να σταθεί και ως αρωγός προς τους προγραμματιστές ασφαλείας οι οποίοι θα κάνουν χρήση των αλγορίθμων μηχανικής μάθησης και θα μπορούν να εντοπίζουν σημάδια κυβερνοεπιθέσεων και να τις προλαμβάνουν.

Όσο περνάει ο χρόνος, οι αλγόριθμοι εξελίσσονται και έτσι πολλές φορές οι χρήστες δεν μπορούν να αντιληφθούν ότι έχουν προσβληθεί. Όμως, εάν πρόκειται για έναν έμπειρο χρήστη, ο οποίος έχει και κάποιες τεχνικές γνώσεις, μπορεί να εντοπίσει την προέλευση του ηλεκτρονικού μηνύματος.

Η τεχνητή νοημοσύνη ήδη χρησιμοποιεί συστήματα, τα οποία είναι ενσωματωμένα σε πλατφόρμες με αλγορίθμους μηχανικής μάθησης. Ένα τέτοιο σύστημα θα μπορούσε να χρησιμοποιηθεί και σε περιπτώσεις phising. Συγκεκριμένα, μια πλατφόρμα έχει την δυνατότητα να ελέγχει και να παρακολουθεί τις κινήσεις ενός χρήστη, τα email του, τις αναζητήσεις του στο διαδίκτυο, έτσι ώστε να διαμορφωθεί ένα προφίλ το οποίο θα είναι εξατομικευμένο και θα μπορεί να το στοχεύσει ο δράστης. Έτσι, ο τελευταίος θα μπορεί να προσποιηθεί πως είναι ο νόμιμος χρήστης και να αποστείλει μηνύματα και να πραγματοποιήσει συναλλαγές, χωρίς ο παραλήπτης να αντιληφθεί πως δεν μιλάει με τον πραγματικό χρήστη.

Η λύση στο παραπάνω πρόβλημα είναι ένα ισχυρό σύστημα το οποίο θα είναι σε θέση να αναγνωρίζει πότε μια συμπεριφορά προέρχεται από κανονικό χρήστη και πότε είναι αυτοματοποιημένη. Ο αλγόριθμος θα μπορεί να ανιχνεύει τους κινδύνους αυτόματα και να προλαμβάνει την όποια βλάβη θα δημιουργούταν χωρίς να απαιτείται η ανθρώπινη επίβλεψη. Αυτή η βάση δεδομένων μόλις πληροφορηθεί για την παραβίαση του συστήματος, θα μπορεί να επικοινωνήσει με τους χρήστες και να τους ενημερώνει σχετικά με πιθανή παράνομη πρόσβαση στο σύστημά τους, αναφέροντάς τους λεπτομέρειες σχετικά με την απειλή.[166]

[166] Άρθρο του Roman Zhidkov με τίτλο «*The Future Impact of AI on Cyber Crime*» δημοσιευμένο στις 14/2/2020 στην ιστοσελίδα https://becominghuman.ai/the-future-impact-of-ai-on-cyber-crime-f9659cf354a6 ανευρεθέν στις 20/1/2022 (τελευταία πρόσβαση: 26/2/2022)

Το 2019, η Amazon βρέθηκε στην θέση να της παραβιαστούν τα δεδομένα της δημιουργώντας μεγάλη κρίση στην εταιρεία. Ωστόσο, το τμήμα ασφαλείας της εταιρείας δεν ενημέρωσε τους χρήστες για την προσβολή, ώστε να προβούν σε αλλαγή κωδικών χρήστης και δημιουργία προφίλ ασφαλείας, τα οποία θα τους προστάτευαν από την διαρροή προσωπικών τους στοιχείων στο σκοτεινό διαδίκτυο.[167]

10. ΕΦΑΡΜΟΓΗ ΤΕΧΝΙΚΩΝ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΩΝ

Οι τεχνικές της τεχνητής νοημοσύνης και οι δυνατότητές της είναι τόσες πολλές πλέον που έχουν πολυάριθμες εφαρμογές στην αντιμετώπιση των κυβερνοεγκλημάτων. Μια από αυτές είναι και τα *νευρωνικά δίκτυα*. Τα νευρωνικά δίκτυα αποτελούν μια μορφή της μηχανικής μάθησης, βασίζονται στην λειτουργικότητα του ανθρώπινου εγκεφάλου και στην νευρο-γνωστική επεξεργασία του και έχουν την ικανότητα να προβλέψουν τα εγκλήματα, τα οποία πρόκειται να τελεστούν.[168] Με την συλλογή ενός τεράστιου όγκου δεδομένων τα συστήματα ΝΝ μπορούν και εντοπίζουν αυτόματα τις εγκληματικές δραστηριότητες στον διαδικτυακό χώρο, την ενδεχόμενη υποτροπή τους αλλά και πραγματοποιούν έρευνες οι οποίες βοηθούν τις αρχές στην αμεσότερη διαλεύκανση των επιθέσεων που σχετίζονται με τον κυβερνοχώρο.[169] Τα δεδομένα που χρησιμοποιούνται μέσω των νευρωνικών δικτύων είναι η ώρα, η ημέρα και ο τόπος του εγκλήματος καθώς επίσης και ο ταχυδρομικός κώδικας που εντοπίζεται το έγκλημα, το οποίο όμως λειτουργεί ως ανεξάρτητη μεταβλητή για την πρόβλεψη της συγκεκριμένης τοποθεσίας.[170]

---

[167] Άρθρο της Lisa Eadicicco με τίτλο «*Elisabeth Warren is urging the FTC to investigate Amazon over concerns that it played a role in the massive Capital One data breach that affected 100 million people*» δημοσιευμένο στις 24/10/2019 στην ιστοσελίδα https://www.businessinsider.com/senators-urge-ftc-investigate-amazon-over-capital-one-data-breach-2019-10 ανευρεθέν στις 20/1/2022 (τελευταία πρόσβαση: 26/2/2022)

[168] Mena J., «*Machine Learning Forensics for Law Enforcement, Security, and Intelligence*» , 2011,Boca Raton, FL: CRC Press, διαθέσιμο σε https://books.google.gr/books?hl=el&lr=&id=dO7RBQAAQBAJ&oi=fnd&pg=PP1&ots=RSyjiMD2Bk&sig=N_HJtqJrsi9jVEgn_WP4MOoXVYY&redir_esc=y#v=onepage&q&f=false ανευρεθέν στις 11/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[169] Μελέτη των A.P.Patil, D.J.Nawal, D.Jain, με τίτλο «*Crime Prediction Application Using Artificial Intelligence*» δημοσιευμένη στις 24/9/2019 στην ιστοσελίδα https://link.springer.com/chapter/10.1007/978-3-030-30577-2_20 ανευρεθείσα στις 11/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[170] Άρθρο του Steven Walczak με τίτλο «*Predicting Crime and Other Uses of Neural Networks in Police Decision Making*» δημοσιευμένο στις 7/10/2021 στην ιστοσελίδα

Στα ίδια πλαίσια κινείται και το σύστημα ανίχνευσης και πρόληψης παραβιάσεων IDS[171] το οποίο είναι μια συσκευή λογισμικού που παρακολουθεί τις δραστηριότητες του δικτύου και προειδοποιεί τον χρήση για τις ενδεχόμενες κακόβουλες επιθέσεις που μπορεί να δεχτεί. Επιπλέον, το IDS είναι σε θέση να ανιχνεύει τις κακόβουλες επιθέσεις και εάν κάποιος επιχειρεί να διαρρήξει το τείχος προστασίας του χρήστη και να έχει πρόσβαση στον υπολογιστή του. Προσομοιάζει με τον ανιχνευτή καπνού, καθώς ειδοποιεί με «συναγερμό» όταν αντιληφθεί περίεργη δραστηριότητα στο δίκτυο, για να προλάβει ο χρήστης να αντιληφθεί τι συμβαίνει και να προβεί στις απαραίτητες ενέργειες για να προστατευτεί.[172]
Ενδεικτικά επίσης αναφέρονται ως εργαλεία για την αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο το *Τεχνητό Νευρωνικό Δίκτυο (Artificial Neural Network)*, ένας επεξεργαστής ο οποίος μπορεί να ανιχνεύει ενδεχόμενες «κρυφές» επιθέσεις στα δίκτυα, οι *Ευφυείς Πράκτορες (Intelligent Agents)*, οι οποίοι δημιουργούνται μέσω του υπολογιστή και έχουν την δυνατότητα να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα και άρα αυτή η συνεργασία μπορεί να αποφέρει άμεσα αποτελέσματα για την πρόληψη των κυβερνοεγκλημάτων, τα *Τεχνητά Ανοσοποιητικά Συστήματα (Artificial Immune Systems_AIS)* τα οποία αποτελούν κατηγορία των υπολογιστικά ευφυών συστημάτων και μιμούνται τις ανθρώπινες δραστηριότητες, αποτελώντας πολύ σημαντική πρακτική για την ασφάλεια στον κυβερνοχώρο και τέλος έχουμε τον *Γενετικό Αλγόριθμο (Genetic Algorithm)*, μια πρακτική η οποία εμφανίζει υψηλό βαθμό αυτοματοποίησης για την ανίχνευση των κακόβουλων συμπεριφορών επίθεσης.[173]

---

https://www.frontiersin.org/articles/10.3389/fpsyg.2021.587943/full ανευρεθέν στις 15/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[171] Intrusion Detection and Prevention System

[172] Μελέτη των S.R.Alkhaldi/Dr.S.M.Alzahrani με τίτλο «*Intrusion detection systems based on Artificial Intelligence techniques*» δημοσιευμένο στις 5/1/2021 στην ιστοσελίδα https://www.ajrsp.com/en/Archive/issue-21/Intrusion%20detection%20systems%20based%20on%20Artificial%20Intelligence.pdf ανευρεθέν στις 15/2/2022 (τελευταία πρόσβαση: 26/2/2022)

[173] Μελέτη των J.S.Mohan/Nilina T. με τίτλο «*Prospects of Artificial Intelligence in Tackling Cyber Crimes*» δημοσιευμένο στις 6/6/2015 στην ιστοσελίδα του International Journal of Science and Research (IJSR) https://www.ijsr.net/archive/v4i6/SUB155595.pdf ανευρεθείσα στις 15/2/2022 (τελευταία πρόσβαση: 26/2/2022)

ΑΝΤΙ ΕΠΙΛΟΓΟΥ

Εξετάζοντας όλα τα παραπάνω, διαπιστώνει κανείς πως η σύνδεση του κυβερνοεγκλήματος με την τεχνητή νοημοσύνη αποτελεί πραγματικά ένα ακανθώδες ζήτημα το οποίο απαιτεί πολλή και ενδελεχή έρευνα.

Η τεχνητή νοημοσύνη, χωρίς αμφιβολία έχει προσφέρει τεράστια οφέλη στην ανθρωπότητα τα τελευταία χρόνια, και γίνεται σταδιακά μέρος των καθημερινών ψηφιακών υπηρεσιών που χρησιμοποιούμε. Όπως είδαμε και παραπάνω, πολλά κράτη και οργανισμοί επενδύουν και προχωρούν στην ανάπτυξη εφαρμογών τεχνητής νοημοσύνης οι οποίες θα βοηθήσουν στην αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο, καθώς επίσης και η ύπαρξη ευρείας νομοθεσίας γύρω από αυτά τα ζητήματα, αναμένεται να απασχολήσουν πολύ περισσότερο στο μέλλον την ανθρωπότητα. Η αρωγή των διεθνών και ευρωπαϊκών οργανισμών θα διαδραματίσει και στο μέλλον πολύ σημαντικό ρόλο για τους υπεύθυνους χάραξης πολιτικής αλλά και στις αρχές επιβολής του νόμου, καθώς θα υπάρχει σωστή καθοδήγηση για την εφαρμογή των ανάλογων εθνικών και κοινοτικών πολιτικών για την τεχνητή νοημοσύνη και το κυβερνοέγκλημα. Ήδη τα επιτεύγματα της τεχνητής νοημοσύνης είναι πολλά και σπουδαία, η πρακτική τους εφαρμογή ωστόσο ακόμα έχει πολύ δρόμο μπροστά της, παρόλο το γεγονός ότι διανύουμε μια εποχή ψηφιοποίησης και τεχνολογικού μετασχηματισμού. Στο μέλλον θα ζήσουμε ακόμα πιο σπουδαίες εξελίξεις οι οποίες θα σχετίζονται με την τεχνητή νοημοσύνη και ο ψηφιακός κόσμος θα με εκπλήξει ευχάριστα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α. ΕΛΛΗΝΟΓΛΩΣΣΗ

Γιαννόπουλος Γ. *«Εισαγωγή στην Νομική Πληροφορική»*, εκδόσεις Νομική Βιβλιοθήκη, 2018 σελ. 154-155

Β. ΝΟΜΟΘΕΣΙΑ

Νομοθετικό κείμενο του Ν.3625/2007, δημοσιευμένο στην ιστοσελίδα https://www.e-nomothesia.gr/kat-anilikoi/n-3625-2007.html

Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο (ελληνικά) διαθέσιμο στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0?lspt_destination=upgrade

The Convention on Cybercrime, Margaret Killerby, Head of Department of Crime of Problems DGI, Council of Europe, Strasbourg δημοσιευμένο στην ιστοσελίδα https://www.itu.int/osg/spu/cybersecurity/2006/presentations/killerby-15-may-2006.pdf

Πρόσθετο Πρωτόκολλο της Σύμβασης για το έγκλημα στον κυβερνοχώρο, δημοσιευμένο στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/prostheto-protokollo-tis-symvasis-gia-egklima-ston?lspt_destination=upgrade

Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32013L0040

Recommendation No. R (89) 9, on computer-related crime, Council of Europe, Committee of Ministers, δημοσιευμένο στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804f1094

Recommendation No. R (95) 13, Concerning Problems of Criminal Procedural Law connected with Information Technology, Council of Europe Committee of Ministers δημοσιευμένο στις 11/9/1995 στην ιστοσελίδα https://rm.coe.int/16804f6e76

Recommendation No. R (2001) 8, on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services), Council of Europe, Committee of Ministers δημοσιευμένο στις 5/9/2001 στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804d5105

Recommendation CM/Rec (2011) 8, on the protection and promotion of the universality, integrity and openness of the Internet, Council of Europe Committee of Ministers δημοσιευμένο στην ιστοσελίδα https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f8

Απόφαση-πλαίσιο 2001/413/ΔΕΥ- Καταπολέμηση της απάτης και της πλαστογραφίας που αφορού τα μέσα πληρωμής πλην των μετρητών δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/LSU/?uri=CELEX:3
F0413

Απόφαση-πλαίσιο 2004/68/ΔΕΥ του Συμβουλίου της 22ας Δεκεμβρίου 2003 για την καταπολέμηση της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM%3Al33138

Απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου της 24ης Φεβρουαρίου 2005 για τις επιθέσεις κατά των συστημάτων πληροφοριών δημοσιευμένη στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX:32005F0222

European Cybercrime Centre-EC3, Combating crime in a digital age δημοσιευμένο και αναθεωρημένο το 2021 στην επίσημη ιστοσελίδα της Europol
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Νόμος 4411/2016:Κύρωση της Σύμβασης για το έγκλημα στον Κυβερνοχώρο δημοσιευμένος στην ιστοσελίδα https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

Ν.4002/2011 (ΦΕΚ Α'180/22-08-2011) ΜΕΡΟΣ Δ- ΡΥΘΜΙΣΗ ΤΗΣ ΑΓΟΡΑΣ ΠΑΙΓΝΙΩΝ ΚΑΙ ΑΛΛΕΣ ΔΙΑΤΑΞΕΙΣ δημοσιευμένος στην ιστοσελίδα
https://www.taxheaven.gr/law/4002/2011

Ν.4267/2014- ΦΕΚ 137/Α/12-6-2014 Καταπολέμησης της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας και άλλες διατάξεις, δημοσιευμένος στην ιστοσελίδα https://www.e-nomothesia.gr/kat-anilikoi/n-4267-2014.html

Ν.4481/2017- ΦΕΚ Α'100/20.07.2017 Συλλογική διαχείριση δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων, χορήγηση πολυεδαφικών αδειών για επιγραμμικές χρήσεις μουσικών έργων και άλλα θέματα αρμοδιότητας Υπουργείου Πολιτισμού και Αθλητισμού δημοσιευμένος στην ιστοσελίδα
https://www.kodiko.gr/nomothesia/document/272968/nomos-4481-2017

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe, της Ευρωπαϊκής Επιτροπής, Βρυξέλλες, 25.4.2018 COM (2018) 237 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

Cristos Velasco (22/2/2022) «*Cybercrime and Artificial Intelligence. An overview of the work of international organization on criminal justice and the international applicable instruments*», διαθέισμο στην ιστοσελίδα https://link.springer.com/article/10.1007/s12027-022-00702-z

Λευκή βίβλος| Τεχνητή νοημοσύνη-Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης, της Ευρωπαϊκής Επιτροπής, Βρυξέλλες, 19.2.2020 COM (2020) 65 final

δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf

Πρόταση-Κανονισμός του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και για την τροποποίηση ορισμένων νομοθετικών πράξεων της Ένωσης, Βρυξέλλες, 21.4.2021 COM (2021) 206 final, διαθέσιμο στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF

Proposal for a Regulation of the European Parliament and of the Council, Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, European Commission, Brussels, 21.4.2021 COM (2021) 206 final 2021/0106 (COD), διαθέσιμο στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)) δημοσιευμένο στην επίσημη ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EL.html

Ευρωπαϊκός Χάρτης Δεοντολογίας για την χρήση της Τεχνητής Νοημοσύνης στα δικαστικά συστήματα και στο περιβάλλον του, διαθέσιμο στην ιστοσελίδα https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

Γ. ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ

Ορισμός του κυβερνοεγκλήματος από την Britannica δημοσιευμένος στην ιστοσελίδα https://www.britannica.com/topic/cybercrime

Dr. Marco Gercke (2012) «*Understanding Cybercrime: Phenomena, Challenges and Legal Response*», διαθέσιμο στην ιστοσελίδα https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Θεώνη Γ.Σπαθή (2016) «*Νέες τεχνολογίες και έγκλημα*» διαθέσιμο στην ιστοσελίδα http://www.indeepanalysis.gr/nomika-themata/nees-technologies-kai-egklhma

«*Τι είναι το ηλεκτρονικό έγκλημα*» δημοσιευμένο στην ιστοσελίδα https://sites.google.com/site/elektronikoenklema2012/ti-einai-elektroniko-enklema

James Andrew Lewis (2018) «*Economic Impact of Cybercrime*» διαθέσιμο στην ιστοσελίδα https://www.csis.org/analysis/economic-impact-cybercrime

XiaoLing Wang (2020) «*Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime*» διαθέσιμο στην ιστοσελίδα https://iopscience.iop.org/article/10.1088/1742-6596/1533/3/032014/pdf?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

Ορισμός του κυβερνοεγκλήματος δημοσιευμένος στην ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

Helga George (2021) «*Phising Emails are Homeland Security's Most Feared Cyber Threat*» https://www.homelandsecurityedu.org/2017/01/phishing-emails-are-homeland-securitys-most-feared-cyber-threat/

Jennifer van der Kleut ,«*What is vishing? Tips for spotting and avoiding voice scams*» δημοσιευμένο στην ιστοσελίδα https://us.norton.com/internetsecurity-online-scams-vishing.html

David Nield (2021) «*How to Guard Against Smishing Attacks on Your Phone*» διαθέσιμο στην ιστοσελίδα https://www.wired.com/story/smishing-sms-phishing-attack-phone/

«*What is Keystroke Logging and Keyloggers?*» δημοσιευμένο στην ιστοσελίδα https://www.kaspersky.com/resource-center/definitions/keylogger

Κέντρο ΠΛΗ.ΝΕ.Τ.Ν. ΦΛΩΡΙΝΑΣ «*Οι Hackers και οι Crackers*» δημοσιευμένη στην ιστοσελίδα http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html

«Hacking definition: What is hacking» δημοσιευμένο στην ιστοσελίδα https://www.malwarebytes.com/hacker

«*Difference between Hackers and Crackers*» δημοσιευμένο στην ιστοσελίδα https://www.geeksforgeeks.org/difference-between-hackers-and-crackers/

«*What is Spam: The Essential Guide to Detecting and Preventing Spam*» δημοσιευμένο στην ιστοσελίδα https://www.avast.com/c-spam

«*What is a computer virus?*» δημοσιευμένο στην ιστοσελίδα https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

«*What is a Trojan horse and what damage can it do?*» δημοσιευμένο στην ιστοσελίδα https://www.kaspersky.com/resource-center/threats/trojans

«*Τι είναι το Spyware? Οδηγός άμυνας*» δημοσιευμένο στην ιστοσελίδα https://el.safetydetectives.com/blog/τι-είναι-το-spyware-οδηγός-άμυνας/

«*Τι είναι το κακόβουλο λογισμικό Logic Bomb και πώς μπορείτε να το αποτρέψετε;*» δημοσιευμένο στην ιστοσελίδα https://el.denizatm.com/pages/46845-what-is-logic-bomb-malware-and-how-can-you-prevent-it

«*What is Sniffer?*» δημοσιευμένο στην ιστοσελίδα https://www.netscout.com/what-is/sniffer

Xue Ping-Chen (2011) «*SQL injection attack and guard technical research*» διαθέσιμο στην ιστοσελίδα https://www.sciencedirect.com/science/article/pii/S1877705811022764?via%3Dihub

Ορισμός του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης, , διαθέσιμο στην ιστοσελίδα
https://el.wikipedia.org/wiki/Οργανισμός_Οικονομικής_Συνεργασίας_και_Ανάπτυξης

Stein Schjolberg (2008) «*The History of Global Harmonization on Cybercrime Legislation- The Road to Geneva*» διαθέσιμο στην ιστοσελίδα
https://cybercrimelaw.net/documents/cybercrime_history.pdf

«Cyber Crime Legislation» (2018) Tala Tafazzoli, διαθέσιμο στην ιστοσελίδα
https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf

M.Chawki «*A Critical Look at the Regulation of Cybercrime*» δημοσιευμένη στην ιστοσελίδα
https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiU8rT6t_X1AhUoRvEDHdotCXMQFnoECBMQAQ&url=https%3A%2F%2Fwww.ie-ei.eu%2FIE-EI%2FRessources%2Ffile%2Fbiblio%2FCriticalLookattheRegulationofCybercrime.doc&usg=AOvVaw2j24pxOk_-l2IE9cZbelYn

Xingan Li, (2007) «*International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene*» διαθέσιμο στην ιστοσελίδα
https://www.webology.org/2007/v4n3/a45.html#13

(2010) «Κινητοποιήσεις Ευρωπαϊκής Ένωσης σχετικά με το Ηλεκτρονικό Έγκλημα» διαθέσιμο στην ιστοσελίδα https://electroniccrime.wordpress.com

Αξιολόγηση απειλών για το οργανωμένο έγκλημα στο Διαδίκτυο (IOCTA)- Στρατηγικές, πολιτικές και τακτικές ενημερώσεις για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, διαθέσιμο στην ιστοσελίδα https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment

Artificial Intelligence and Robotics for Law, διαθέσιμη στην ιστοσελίδα http://www.unicri.it/artificial-intelligence-and-robotics-law-enforcement

Global Meeting 23-27 Nov, διαθέσιμο στην ιστοσελίδα http://www.unicri.it/News/AI-UNICRI-INTERPOL-Lawenforcement c

Europol, «*New report finds that criminals leverage AI for malicious use-and it's not just deep fakes*» δημοσιευμένο στην ιστοσελίδα https://www.europol.europa.eu/media-press/newsroom/news/new-report-finds-criminals-leverage-ai-for-malicious-use-—-and-it's-not-just-deep-fakes

Lawspot (2017) «*Το ευρωπαϊκό πλαίσιο για τις επιθέσεις κατά των συστημάτων πληροφοριών*», διαθέσιμο στην ιστοσελίδα https://www.lawspot.gr/nomikes-plirofories/voithitika-kemena/eyropaiko-plaisio-gia-tis-epitheseis-kata-ton-systimaton?lspt_destination=upgrade

Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) ανευρεθέν στην επίσημη ιστοσελίδα της Ευρωπαϊκής Ένωσης https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_el

Joint Cybercrime Action Taskforce (J-CAT), Fighting cybercrime around the world, δημοσιευμένο στις 14/12/2021 στην επίσημη ιστοσελίδα της Europol https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce

ΚΟΙΝΗ ΑΝΑΚΟΙΝΩΣΗ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ, Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο, Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο, Βρυξέλλες, 7.2.2014 JOIN (2013) 1 final δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαικής Επιτροπής https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001

Adminlaw (2020) «*Νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια*» διαθέσιμο στην ιστοσελίδα https://lawnet.gr/law-news/nea-stratigiki-tis-ee-gia-tin-kyvernoasfaleia/

Ιγγλεζάκη (2015) «*Επιθέσεις κατά συστημάτων πληροφοριών*» διαθέσιμο στην ιστοσελίδα http://www.cybercc.gr/m/filer_public/2015/10/09/igglezakhs_epitheseis_kata_systimatwn_pliroforiwn.pdf

Craven S./Brown S./Gilchrist E. «*Sexual grooming of children: Review of literature and theoretical considerations*» διαθέσιμο στην ιστοσελίδα https://psycnet.apa.org/record/2006-23335-007

Ελληνικό Κέντρο για το Κυβερνοέγκλημα, δημοσιευμένο στην ιστοσελίδα του Κέντρου Μελετών Ασφαλείας http://www.kemea.gr/el/epikairotita/153-elliniko-kentro-gia-to-kyvernoegklima

(2010) «*Δικαιοδοσία στο Διαδίκτυο*» διαθέσιμο στην ιστοσελίδα https://electroniccrime.wordpress.com/2010/09/17/δικαιοδοσία-στο-διαδίκτυο/

Prashant Mali (2008) «*TEXT BOOK OF CYBERCRIME AND PENALTIES {AS PER ITA A 2008 AND IPC}(DRAFT VERSION)*» διαθέσιμο στην ιστοσελίδα https://ia600709.us.archive.org/21/items/ATextBookOfCyberCrimeAndPenalties/ATextBookOfCyberCrimesAndPenaltiesByAdv.PrashantMali.pdf

Gabriel Olano (2021) «Artificial intelligence a valuable tool in combating cybercrime» διαθέσιμο στην ιστοσελίδα https://www.insurancebusinessmag.com/us/risk-management/cyber/artificial-intelligence-a-valuable-tool-in-combating-cybercrime-246315.aspx

«*Αρχές που Εποπτεύον την Προστασία του Διαδικτύου στην Ελλάδα*» δημοσιευμένη στην ιστοσελίδα https://sites.google.com/site/elektronikoenklema2012/arches-pou-epopteuoun-ten-prostasia-tou-diadiktyou-sten-ellada

Επίσημη ιστοσελίδα της Αρχής Προστασίας Προσωπικών Δεδομένων https://www.dpa.gr/el

Επίσημη ιστοσελίδα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών http://www.adae.gr

Επίσημη ιστοσελίδα της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων https://www.eett.gr/opencms/opencms/EETT/EETT

Επίσημη ιστοσελίδα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος https://cyberalert.gr/

Επίσημη ιστοσελίδα του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου https://saferinternet4kids.gr

Επίσημη ιστοσελίδα της helpline http://www.help-line.gr

Laura Steele/Queen's Management School «*From Aristotle to Artificial Intelligence Can Ancient Theories be Applied to Modern Ethical Challenges* διαθέσιμο στην ιστοσελίδα https://www.qub.ac.uk/schools/QueensManagementSchool/Ethics/FileUpload/Filetoupload,895822,en.pdf

Graham Oppy/David Dowe (2021) «*The Turing Test*» διαθέσιμο στην ιστοσελίδα https://plato.stanford.edu/entries/turing-test/

Επιστημονικό άρθρο με τίτλο «Τεστ Τούρινγκ» δημοσιευμένο στην ιστοσελίδα https://atozofai.withgoogle.com/intl/el/turing-test/

Ευρωπαϊκό Κοινοβούλιο, «*Τι είναι η τεχνητή νοημοσύνη και πως χρησιμοποιείται*» διαθέσιμο στην ιστοσελίδα https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

Ανακοίνωση της Ευρωπαϊκής Επιτροπής-Τεχνητή νοημοσύνη για την Ευρώπη, Βρυξέλλες, 25.4.2018 COM (2018) 237 final, διαθέσιμο στην ιστοσελίδα https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:52018DC0237&from=MT

John McCarthy (1927-2011): Artificial Intelligence (complete) - Thinking Allowed -Jeffrey Mishlove. Απόσπασμα ανευρεθέν στην ιστοσελίδα **https://www.youtube.com/watch?v=Ozipf13jRr4**

Bernard Marr (2018) «*What is Deep Learning AI? A Simple Guide With 8 Practical Examples*» διαθέσιμο στην ιστοσελίδα https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/?sh=77f0dce08d4b

SecNews (2019) «*Σύνδεση μεταξύ data science, machine learning and artificial intelligence*» διαθέσιμο στην ιστοσελίδα https://www.secnews.gr/205498/syndesi-metaksi-data-science-machine-learning-artificial-intelligence/

Σταύρου Κιτσάκη (2018) «*Τεχνητή νοημοσύνη και συμβατική διαδικασία, Εισαγωγή στα βασικά προβλήματα*», δημοσιευμένη στις «Εφαρμογές ΑΣΤΙΚΟΥ ΔΙΚΑΙΟΥ & ΠΟΛΙΤΙΚΗΣ ΔΙΚΟΝΟΜΙΑΣ» Τεύχος 6/ Έτος 2018 διαθέσιμο στην ιστοσελίδα

https://www.researchgate.net/publication/326711736_Technete_noemosyne_kai_symbatike_dia dikasia_Artificial_Intelligence_and_contract_law_An_introduction στις 17/1/2022 (τελευταία πρόσβαση:)

CEPS(Centre for European Policy Studies) για την Κυβερνοασφάλεια και την Τεχνητή Νοημοσύνη διαθέσιμο στην ιστοσελίδα https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

Ε. Τζούλια/Justina (2020) «*Ευρωπαϊκός ηθικός χάρτης για τη χρήση της Τεχνητής Νοημοσύνης στο δικαιοδοτικό σύστημα*» διαθέσιμο στην ιστοσελίδα http://www.justina.gr/πολιτική/διεθνή/ευρωπαϊκός-ηθικός-χάρτης-για-τη-χρήση/

A European approach to artificial intelligence, δημοσιευμένη στην επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Doowon Jeong (2020) «*Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues*» διαθέσιμο στην ιστοσελίδα https://ieeexplore.ieee.org/document/9216065

D.Assenmacher, L.Clever, L.Frischlich, T.Quandt, H.Trautmann, C.Grimme (2020) «*Demystifying Social Bots: On the Intelligence of Automated Social Media Actors*» διαθέσιμο στην ιστοσελίδα https://journals.sagepub.com/doi/10.1177/2056305120939264

Jake Frankenfield (2020) «*Chatbot*» διαθέσιμο στην ιστοσελίδα https://www.investopedia.com/terms/c/chatbot.asp

Amy Higgins (2021)«*What is a Chatbot? How Is it Changing Customer Experience?*» διαθέσιμο στην ιστοσελίδα https://www.salesforce.com/blog/what-is-a-chatbot/

Hunt Allcott /Matthew Gentzkow (2017) «*Social Media and Fake News in the 2016 Election*» διαθέσιμο στην ιστοσελίδα https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211

Ed Lauder (2017) «*Google's Machine Learning Tech Now Blocks 99.9% of Spam*» δ διαθέσιμο στην ιστοσελίδα https://aibusiness.com/document.asp?doc_id=760333

Christopher Rigano (2018) «*Using Artificial Intelligence to Address Criminal Justice Needs*» διαθέσιμο στην ιστοσελίδα https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

Carlow University (2021) «*Artificial Intelligence in Criminal Justice: How AI Impacts Pretrial Risk Assessment*» διαθέσιμο στην ιστοσελίδα https://blog.carlow.edu/2021/07/27/artificial-intelligence-in-criminal-justice/

Λεωνίδα Κανέλλου (2020) «*Η Τεχνητή Νοημοσύνη στην υπηρεσία μιας Έξυπνης Δικαιοσύνης*» διαθέσιμο στην ιστοσελίδα https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis?lspt_destination=upgrade

Tim Brennan και William Dietrich (2017) «*Correctional Offender Management Profiles for Alternative Sanctions (COMPAS)*» διαθέσιμο στην ιστοσελίδα

https://www.researchgate.net/publication/321528262_Correctional_Offender_Management_Profiles_for_Alternative_Sanctions_COMPAS

Bhishm Khanna, (2021) «*Predictive Justice: Using AI for Justice*», διαθέσιμο στην ιστοσελίδα του Centre for Public Policy Research https://www.cppr.in/wp-content/uploads/2021/05/PREDICTIVE-JUSTICE-USING-AI-FOR-JUSTICE-2.pdf

Priya Dialani (2021) «*AI in Future courtrooms.Will they replace Judges?*» διαθέσιμο στην ιστοσελίδα https://www.analyticsinsight.net/ai-will-have-robot-judges-soon-what-about-human-judges/

Absenta Mia (2020) «*AI στα δικαστήρια: Μήπως οι δικαστές του μέλλοντος θα είναι ρομπότ;*» διαθέσιμο στην ιστοσελίδα https://www.secnews.gr/209014/ai-dikastiria-apofaseis/

Xinhua (2018) «*China first internet court handles over 10,000 cases*» διαθέσιμο στην ιστοσελίδα https://www.chinadaily.com.cn/a/201808/18/WS5b77c8f4a310add14f386801.html

Victor Tangermann (2017) «*Estonia is building a "Robot Judge" to help clear legal backlog*» διαθέσιμο στην ιστοσελίδα https://futurism.com/the-byte/estonia-robot-judge

Χρήστου Τσουραμάνη από το 7ο Συνέδριο Security Project το 2019 με τίτλο «*Η αντιμετώπιση του εγκλήματος με τη Συνδρομή της Τεχνητής Νοημοσύνης*» διαθέσιμο στην ιστοσελίδα https://www.securityproject.gr/presentations/2019/day1-tsouramanis.pdf

Asma Idder και Stephane Coulaux (2021) «*Artificial intelligence in criminal justice: invasion or revolution?*» διαθέσιμο στην ιστοσελίδα https://www.ibanet.org/dec-21-ai-criminal-justice

Nik Gagvani, (2008) «*Introduction to video analytics*» διαθέσιμο στην ιστοσελίδα https://www.eetimes.com/introduction-to-video-analytics/#

(2021) Police use of Facial Recognition Technology in Canada and the way forward, διαθέσιμο στην ιστοσελίδα https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

Επίσημη ιστοσελίδα της Clearview.ai https://www.clearview.ai

University of York (2021)«*The role of natural language processing in AI*» διαθέσιμο στην ιστοσελίδα https://online.york.ac.uk/the-role-of-natural-language-processing-in-ai/

Σύμβολο του Siri διαθέσιμο στην ιστοσελίδα https://techblog.gr/software/i-siri-etoimazetai-na-milisei-ellinika-apokleistiko/

Ilya Dudkin (2018) «*How does SIRI work: Technology and Algorithm*» διαθέσιμο στην ιστοσελίδα https://skywell.software/blog/how-does-siri-work-technology-and-algorithm/

Εικόνα συσκευής Alexa διαθέσιμο στην ιστοσελίδα https://www.istockphoto.com/photos/alexa

Jenn Henry Horowitz (2020) «*Is Alexa an AI*» διαθέσιμο στην ιστοσελίδα https://itchronicles.com/artificial-intelligence/is-alexa-an-ai/

Λογότυπο της Google Assistant διαθέσιμο στην ιστοσελίδα https://el.m.wikipedia.org/wiki/Αρχείο:Google_Assistant_logo.svg

Jill McKeon (2021)«*Google's Artificial Intelligence Voice Assistant Bests Siri, Alexa*» διαθέσιμο στην ιστοσελίδα https://healthitanalytics.com/news/googles-artificial-intelligence-voice-assistant-bests-siri-alexa

(2021)«*Use of artificial intelligence by the police: MEPS oppose mass surveillance*», διαθέσιμο στην επίσημη ιστοσελίδα του Ευρωπαϊκού Κοινοβουλίου https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

Lawspot (2021) «*Τεχνητή νοημοσύνη και αστυνόμευση: Κατά της μαζικής παρακολούθησης το Ευρωπαϊκό Κοινοβούλιο*» διαθέσιμο στην ιστοσελίδα https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-kai-astynomeysi-kata-tis-mazikis-parakoloythisis-eyropaiko-koinovoylio?lspt_destination=upgrade

(2021) «*Use of artificial intelligence by the police: MEPs oppose mass surveillance | EU Parliament Press*» διαθέσιμο στην ιστοσελίδα https://www.pubaffairsbruxelles.eu/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance-eu-parliament-press/

(2016) «*Sweden bans camera on drones*» διαθέσιμο στην ιστοσελίδα https://www.bbc.com/news/technology-37761872

Tom Mendelshon (2016)«*Sweden's highest court bans drones with cameras*» διαθέσιμο στην ιστοσελίδα https://arstechnica.com/tech-policy/2016/10/camera-spy-drones-banned-sweden-highest-court/

Lawspot, (2020)«*Η Γαλλία απαγορεύει τη χρήση drones από την αστυνομία στο πλαίσιο διαδηλώσεων στο Παρίσι*» διαθέσιμο στην ιστοσελίδα https://www.lawspot.gr/nomika-nea/i-gallia-apagoreyei-ti-hrisi-drones-apo-tin-astynomia-sto-plaisio-diadiloseon-sto-parisi?lspt_destination=upgrade

Freshfields Bruckhaus Deringer LLP(2020) «*French court rules on use of drones by Paris police*» διαθέσιμο στην ιστοσελίδα https://www.lexology.com/library/detail.aspx?g=e81fdeeb-b669-456a-a600-b220129e57e7

Ολόκληρο το κείμενο της μελέτης δημοσιευμένο στις 13/5/2020 στην ιστοσελίδα https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

Frederick Mostert, King's College London (2020) «*The Application and Challenges of Blockchain in Intellectual Property Driven Businesses in China*» διαθέσιμο στην ιστοσελίδα https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600115

Διαβιβαστικό σημείωμα του Ευρωπαϊκού Συμβουλίου, Βρυξέλλες, 19 Οκτωβρίου 2017 (OR.en) EUCO 14/17 δημοσιευμένο στην ιστοσελίδα https://www.consilium.europa.eu/media/21603/19-euco-final-conclusions-el.pdf

Kyle Wiggers (2021)«*Dear enterprise IT: Cybercriminals use AI too*» διαθέσιμο στην ιστοσελίδα https://venturebeat.com/2021/06/17/dear-enterprise-it-cybercriminals-use-ai-too/

Vinod Vasudevan (2018) «*How AI Is Transforming Cyber Defense*» διαθέσιμο στην ιστοσελίδα https://www.forbes.com/sites/forbestechcouncil/2018/07/24/how-ai-is-transforming-cyber-defense/

Francis Knott «*The Surprising Role of AI in Cybercrime* διαθέσιμο στην ιστοσελίδα https://www.attilasec.com/blog/ai-in-cybercrime

SDi (2020) «*Artificial Intelligence and Cyber Crime: Facing New Threats*» διαθέσιμο στην ιστοσελίδα https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/

Drew Harwell (2019) «*An-artificial intelligence first: Voice-mimicking software reportedly used in a major theft*» διαθέσιμο στην ιστοσελίδα https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/

Peter Yeoh (2019) με τίτλο «*Artificial intelligence: accelerator or panacea for financial crime?*» διαθέσιμο στην ιστοσελίδα https://www.emerald.com/insight/publication/issn/1359-0790

Gabriel Hallevy (2016) «*The Criminal Liability of Artificial Intelligence Entities-from Science Fiction to Legal Social Control*» διαθέσιμο στην ιστοσελίδα https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=1037&context=akronintellectualproperty

Evan Goldstick (2016) «*Accidental Vitiation: The Natural and Probable Consequence of Rosemond v. United States on the Natural and Probable Consequence Doctrine*» διαθέσιμο στην ιστοσελίδα https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5268&context=flr

Ashley Wilson (2019) «*4 Ways AI Can Make Data Backup More Efficient*» διαθέσιμο στην ιστοσελίδα https://www.kolabtree.com/blog/4-ways-ai-can-make-data-backup-more-efficient/

Aimee Laurence(2019) «*The Impact of Artificial Intelligence on Cyber Security*» διαθέσιμο στην ιστοσελίδα https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/

Roman Zhidkov (2020)«*The Future Impact of AI on Cyber Crime*» διαθέσιμο στην ιστοσελίδα https://becominghuman.ai/the-future-impact-of-ai-on-cyber-crime-f9659cf354a6

Lisa Eadicicco (2019)«*Elisabeth Warren is urging the FTC to investigate Amazon over concerns that it played a role in the massive Capital One data breach that affected 100 million people*» διαθέσιμο στην ιστοσελίδα https://www.businessinsider.com/senators-urge-ftc-investigate-amazon-over-capital-one-data-breach-2019-10

Mena J., (2016)«*Machine Learning Forensics for Law Enforcement, Security, and Intelligence*» , 2011,Boca Raton, FL: CRC Press, διαθέσιμο σε https://books.google.gr/books?hl=el&lr=&id=dO7RBQAAQBAJ&oi=fnd&pg=PP1&ots=RSyjiMD2Bk&sig=N_HJtqJrsi9jVEgn_WP4MOoXVYY&redir_esc=y#v=onepage&q&f=false

A.P.Patil, D.J.Nawal, D.Jain, (2019)«*Crime Prediction Application Using Artificial Intelligence*» διαθέσιμο στην ιστοσελίδα https://link.springer.com/chapter/10.1007/978-3-030-30577-2_20

S.Walczak (20210«*Predicting Crime and Other Uses of Neural Networks in Police Decision Making*» διαθέσιμο στην ιστοσελίδα https://www.frontiersin.org/articles/10.3389/fpsyg.2021.587943/full

S.R.Alkhaldi/Dr.S.M.Alzahrani (2021)«*Intrusion detection systems based on Artificial Intelligence techniques*» διαθέσιμο στην ιστοσελίδα https://www.ajrsp.com/en/Archive/issue-21/Intrusion%20detection%20systems%20based%20on%20Artificial%20Intelligence.pdf

J.S.Mohan/Nilina T.(2013)«*Prospects of Artificial Intelligence in Tackling Cyber Crimes*» διαθέσιμο στην ιστοσελίδα του International Journal of Science and Research (IJSR) https://www.ijsr.net/archive/v4i6/SUB155595.pdf