ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

# ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΩΝ «DEEPFAKES» - ΤΕΧΝΟΛΟΓΙΚΗ ΚΑΙ ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

Διπλωματική Εργασία

της

Παναγιώτας Παναγοπούλου

Θεσσαλονίκη, 04/03/2023

**ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΩΝ «DEEPFAKES» - ΤΕΧΝΟΛΟΓΙΚΗ ΚΑΙ ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ**

Παναγιώτα Παναγοπούλου

Πτυχίο Νομικής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2017

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέποντες Καθηγητές:
Θεοχάρης Δαλακούρας
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04η Μαρτίου 2023.

| Καθ. Θεοχάρης Δαλακούρας | Καθ. Κωνσταντίνος Ψάννης | Καθ. Γεώργιος Δανιήλ |
|---|---|---|
| ..... | ..... | ..... |

Παναγιώτα Παναγοπούλου

**Περίληψη**

Η παρούσα διπλωματική πραγματεύεται το φαινόμενο των «deepfake», μια μάστιγα της εποχής μας, με την τρομακτική άνοδο της χρήσης αυτής της τεχνολογίας να δημιουργεί έντονες ανησυχίες για το μέλλον, καθώς και το νομικό πλαίσιο είναι νεφελώδες. Το «deepfake» πλέον μπορεί να χαρακτηριστεί ως μια ισχυρή απειλή μετατρέποντας τους ανθρώπους σε παραλήπτες εκφοβιστικών, εκβιαστικών και απειλητικών μηνυμάτων. Τα συνθετικά της λέξης «deepfake» αποτελούνται από τη λέξη «deep = βαθιά» που παραπέμπει στην τεχνολογία της «βαθιάς μάθησης» και της λέξης «fake» που σημαίνει ψεύτικο. Ο όρος «deepfake» αναφέρεται σε ένα ψεύτικο – παραποιημένο βίντεο, με πρωταγωνιστή κάποιον που λέει και κάνει κάτι, το οποίο στην πραγματικότητα δεν συνέβη ποτέ. Τα άτομα μπορεί να είναι αληθινά, όπως και το περιβάλλον, οι ενέργειες όμως όχι. Μπορούμε να φανταστούμε, λοιπόν, ότι η τεχνολογία αυτή εύκολα μπορεί να αποτελέσει εργαλείο από κάποιον κακόβουλο χρήστη που διαθέτει πρόσβαση στο Διαδίκτυο. Με την εξέλιξη της τεχνολογίας πλέον καθίσταται αδύνατο για κάποιον να ξεχωρίσει ποια είναι η αλήθεια και ποιο το ψέμα. Το Διαδίκτυο αποτελεί το βασικό περιβάλλον επικοινωνίας των ανθρώπων πλέον, ενώ θα μπορούσε κανείς να ισχυριστεί ότι αναπαριστά με επιτυχία τον «πραγματικό» κόσμο με αποτέλεσμα να αποτελεί πρόσφορο πεδίο παραβατικότητας και προσβολής δικαιωμάτων. Με την αλματώδη ανάπτυξη της τεχνολογίας τα τελευταία χρόνια οι περιπτώσεις ηλεκτρονικού εγκλήματος, τόσο σε Διεθνές όσο και σε εθνικό επίπεδο, γίνονται όλο και πολυπλοκότερες, με αποτέλεσμα και οι πολίτες μεμονωμένα αλλά και τα κράτη ως οντότητες να απειλούνται και καθίσταται έτσι επιτακτική η ανάγκη διευρυνόμενων γνώσεων για την παρακολούθηση και διαπίστωση της παράνομης συμπεριφοράς που λαμβάνει χώρα στο διαδίκτυο. Κάθε φορά που ένα νέο φαινόμενο, όπως αυτό των «deepfake» με αναμφισβήτητη κοινωνική και ηθική διάσταση λόγω της προσβολής εννόμων αγαθών εισβάλλει στην καθημερινότητά μας, τίθεται πάντα το ερώτημα: Επαρκεί το υφιστάμενο ποινικό οπλοστάσιο για να αντιμετωπιστεί το νέο αυτό φαινόμενο;

**Λέξεις Κλειδιά:** deepfakes, τεχνητή νοημοσύνη, μηχανική μάθηση, βαθιά μάθηση, τεχνητά νευρωνικά δίκτυα, γενετικά αντιπαραθετικά δίκτυα, αυτόματος κωδικοποιητής

**Abstract**

This thesis deals with the phenomenon of "deepfake", a scourge of our time, with the tremendous rise in the use of this technology creating strong concerns for the future, as the legal framework is nebulous. Deepfake can now be described as a powerful threat, turning people into recipients of intimidating, blackmailing and threatening messages. The synonyms of the word "deepfake" consist of the word "deep = deep" which refers to the technology of "deep learning" and the word "fake" which means fake. The term "deepfake" refers to a fake - doctored video, featuring someone saying and doing something that never actually happened. Individuals can be real, as can the environment, but actions are not. We can therefore imagine that this technology can easily be used as a tool by a malicious user with access to the Internet. With the evolution of technology, it is now impossible for anyone to distinguish between truth and lies. The Internet is now the main communication environment for people, and one could argue that it successfully represents the 'real' world, making it a fertile ground for crime and rights violations. With the rapid development of technology in recent years, cases of cybercrime, both at international and national level, are becoming increasingly complex, with the result that both individual citizens and states as entities are threatened, making it imperative to expand knowledge to monitor and detect illegal behaviour taking place online. Every time a new phenomenon, such as that of "deepfake" with an undeniable social and moral dimension due to the violation of legal rights, invades our everyday life, the question always arises: is the existing criminal arsenal sufficient to deal with this new phenomenon?

**Keywords:** Deepfakes, Artificial Intelligence, Machine Learning, Deep Learning, Artificial Neural Networks, Genetic Adversarial Networks, Autoencoder

**Περιεχόμενα**

**Κατάλογος Εικόνων**

**Συμβολισμοί**

**AI …… Artificial Intelligence**

**IOT …… Internet of Things**

**ML …… Machine Learning**

**DL …… Deep Learning**

**CI …… Computational Intelligence**

**NN …… Neural Network**

**CNN …… Convolutional Neural Network**

**DNN …… Deep Neural Network**

**GAN …… Generative Adversarial Network**

**ΓΚΠΔ …… Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων**

**ΤΝ …… Τεχνητή Νοημοσύνη**

**ΑΠΔ …… Αρχή Προστασίας Δεδομένων**

**ΑΠΔΠΧ …… Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**

**ΠΚ …… Ποινικός Κώδικας**

# Ι. ΕΙΣΑΓΩΓΗ

## Ι.1. ΠΡΟΒΛΗΜΑ – ΣΗΜΑΝΤΙΚΟΤΗΤΑ ΤΟΥ ΘΕΜΑΤΟΣ

Το φαινόμενο των fake news υπήρχε στην καθημερινότητά μας, αποτελώντας μεγάλο αγκάθι για το διαδίκτυο, όπλο παραπληροφόρησης και προπαγάνδας. Το τελευταίο όμως διάστημα εμφανίστηκε μία μετεξέλιξη των fake news τα λεγόμενα «deepfakes», τα οποία μπορούν να αφορούν μια εικόνα, ένα βίντεο ή ένα ηχητικό απόσπασμα. Πρόκειται για τεχνητά μέσα, εικόνες ή ηχητικά αποσπάσματα, κυρίως όμως βίντεο, τα οποία παράγονται μέσω ενός αλγορίθμου που λειτουργεί βάσει των τεχνολογιών της τεχνητής νοημοσύνης και των νευρωνικών δικτύων και, «μαθαίνοντας» τα χαρακτηριστικά ενός προσώπου, αντικαθίσταται το πρόσωπο ενός ανθρώπου με το πρόσωπο ενός άλλου.

Παρά το γεγονός ότι τα deepfakes χρησιμοποιούνται κυρίως για χιουμοριστικούς σκοπούς και για λόγους σάτιρας, τα deepfakes όταν βρεθούν στο δρόμο ενός κακόβουλου χρήστη δύνανται να αποτελέσουν ένα τρομακτικά επικίνδυνο εργαλείο. Με τη βοήθεια ενός άλλου ισχυρού όπλου, της Τεχνητής Νοημοσύνης και των τεχνολογιών που αυτή μας παρέχει, οι οποίες εξελίσσονται, βελτιώνονται και αναπτύσσονται ραγδαία, τα αποτελέσματα των deepfakes γίνονται ολοένα και πιο πειστικά και να καθίσταται εξαιρετικά δύσκολο να ξεχωρίζει το αληθινό από το ψεύτικο.

Τα κοινωνικά δίκτυα και τα μέσα μαζικής ενημέρωσης τα οποία φιλοξενούν εκατομμύρια χρήστες ανά τον κόσμο συμβάλλουν στη διάδοση των deepfakes, με αποτέλεσμα το φαινόμενο αυτό να έχει πάρει ανησυχητικές διαστάσεις εξαιτίας των αποτελεσμάτων που μπορεί να επιφέρει η τεχνολογία των deepfakes όταν χρησιμοποιείται με κακό σκοπό, τόσο στις δημοκρατικές συνθήκες μιας χώρας, όσο και στα μεμονωμένα άτομα όταν αυτά χρησιμοποιούνται με σκοπό να βλάψουν την προσωπικότητα του θύματος, τα προσωπικά του δεδομένα και άλλα θεμελιώδη δικαιώματα του ανθρώπου ή ακόμα και στα νομικά πρόσωπα όπως τα τελευταία εκπροσωπούνται, τα οποία μπορεί να πέσουν θύματα απάτης, πλαστογραφίας και άλλων εγκλημάτων.

Τα deepfakes όπως θα δούμε και παρακάτω στην παρούσα εργασία συγκεντρώνουν τα χαρακτηριστικά ενός κυβερνοεγκλήματος. Με την αλματώδη ανάπτυξη της τεχνολογίας τα τελευταία χρόνια οι περιπτώσεις ηλεκτρονικού εγκλήματος, τόσο σε Διεθνές όσο και σε εθνικό επίπεδο, γίνονται όλο και πολυπλοκότερες, με αποτέλεσμα και οι πολίτες μεμονωμένα αλλά και τα κράτη ως οντότητες να απειλούνται και καθίσταται έτσι επιτακτική η ανάγκη διευρυνόμενων γνώσεων για την παρακολούθηση και διαπίστωση της παράνομης συμπεριφοράς που λαμβάνει χώρα στο διαδίκτυο. Καθώς το φαινόμενο των deepfakes λαμβάνει πραγματικά τρομακτική

διάσταση γεννώνται διάφορα ηθικά και νομικά ζητήματα, τα οποία χρήζουν ανάλυσης και έρευνας.

## Ι.2. ΣΚΟΠΟΣ – ΜΕΘΟΔΟΛΟΓΙΑ

Η παρούσα εργασία έχει στόχο να αναδείξει τις βασικές πτυχές της τεχνολογίας deepfakes, ποια είναι η τεχνολογία αυτή, τί τεχνολογίες χρησιμοποιεί και πως λειτουργεί τελικά ο αλγόριθμος της τεχνολογίας αυτής. Επιπλέον, αφού η νομική επιστήμη πρέπει να συμβαδίζει με την τεχνολογική και να περιβάλλει τις νέες τεχνολογίες που δημιουργούνται, σκοπός της παρούσας εργασίας είναι η ενημέρωση του αναγνώστη για την τεχνολογία deepfakes, για την κακόβουλη χρήση του και την αναδεικνυόμενη απειλή για την κοινωνία, καθώς όπως θα αποδειχθεί στη συνέχεια τα deepfakes χαρακτηρίζονται περισσότερο ως αρνητική εξέλιξη παρά ως θετική για την κοινωνία σε παγκόσμιο επίπεδο, κατά τη γνώμη της γράφουσας. Εάν λοιπόν η τεχνολογία χρησιμοποιηθεί με κακό σκοπό υπάρχει μεγάλος κίνδυνος να τελεστούν διάφορα ποινικά αδικήματα. Το νέο φαινόμενο των «deepfakes» λαμβάνει μεγάλη κοινωνική και ηθική διάσταση απαξία και εξαιτίας της προσβολής εννόμων αγαθών προκύπτει το ζήτημα αν οι υπάρχουσες ποινικές διατάξεις και νόμοι θεωρούνται αρκετοί για την αντιμετώπιση του νέου αυτού φαινομένου ή κρίνεται απαραίτητη η θέσπιση νέων νόμων και διατάξεων. Επιπλέον, ανακύπτει ζήτημα με την αποτελεσματική και πραγματική προστασία των θυμάτων.

Για την επίτευξη των στόχων της παρούσας διπλωματικής εργασίας και την εκπόνησή της, αντλούνται βιβλιογραφικές αναφορές από ακαδημαϊκές μηχανές αναζήτησης και βάσεις δεδομένων που ενοποιούν μια πληθώρα ακαδημαϊκού περιεχομένου (π.χ., εργασίες συνεδρίων, άρθρα περιοδικών και κεφάλαια βιβλίων).

## Ι.3. ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ - ΥΠΟΘΕΣΕΙΣ – ΠΕΡΙΟΡΙΣΜΟΙ

Τα συνθετικά της λέξης «deepfake» αποτελούνται από τη λέξη «deep = βαθιά» που παραπέμπει στην τεχνολογία της «βαθιάς μάθησης» και της λέξης «fake» που σημαίνει ψεύτικο. Η βαθιά μάθηση ως μέθοδος Τεχνητής Νοημοσύνης με τη βοήθεια πολλαπλών επιπέδων αλγορίθμων μηχανικής εκμάθησης εξάγει νέα αποτελέσματα υψηλότερου επιπέδου από μη δομημένα δεδομένα - όπως το ανθρώπινο πρόσωπο. Ο όρος «deepfake» αναφέρεται σε ένα ψεύτικο – παραποιημένο βίντεο, με πρωταγωνιστή κάποιον που λέει και κάνει κάτι, το οποίο στην πραγματικότητα δεν συνέβη ποτέ. Τα άτομα μπορεί να είναι αληθινά, όπως και το περιβάλλον, οι ενέργειες όμως όχι.

Αν υποθέσουμε ότι το φαινόμενο αυτό αποτελεί πλέον κομμάτι της καθημερινότητάς μας, καταλαβαίνουμε αμέσως ότι επηρεάζει όλους τους τομείς μιας κοινωνίας και καθίσταται

απαραίτητη η αντιμετώπιση της κακόβουλης χρήσης του και η αποτελεσματική προστασία των θυμάτων της.

Αν και η παραποίηση και η χειραγώγηση της εικόνας υπήρχε εδώ και αρκετό διάστημα, το φαινόμενο των deepfakes έχει μικρή διάρκεια ζωής, αφού ο αλγόριθμος της τεχνολογίας αναπτύχθηκε, όπως θα δούμε και παρακάτω αναλυτικά, από τον Αμερικανό ερευνητή, Ian Goodfellow, μόλις το 2014. Ως όρος τα deepfakes εμφανίστηκαν στις 2 Νοεμβρίου 2017, στην πλατφόρμα Reddit, όταν ένας ανώνυμος χρήστης με το ψευδώνυμο «deepfakes» ξεκίνησε μια συζήτηση με το θέμα «Deepfakes». Χρησιμοποιώντας βαθιά μάθηση πόσταρε στο φόρουμ του ψεύτικα βίντεο με ερωτικό περιεχόμενο, όπου πρόσωπα διασημοτήτων του Hollywood, ανταλλάσσονταν με πρόσωπα ηθοποιών που πρωταγωνιστούν σε ταινίες ερωτικού περιεχομένου, τα οποία τα είχε δημιουργήσει ο ίδιος με εργαλεία ΤΝ.

Για την εκπόνηση της παρούσας εργασίας τέθηκαν περιορισμοί, καθώς όσον αφορά στο τεχνολογικό υπόβαθρο των deepfakes, οι πηγές – αναφορές περιορίστηκαν σε χρονολογία έως την τελευταία πενταετία (2018 – 2023). Πρόβλημα ανέκυψε στο νομικό υπόβαθρο της τεχνολογίας. Εξαιτίας του συντόμου ζωής της, ελάχιστες χώρες έχουν προβεί στην ποινικοποίηση της κακοπροαίρετης χρήσης της τεχνολογίας και μάλιστα το έχουν πράξει αυτό εντός του 2022, ενώ στην Ελλάδα το φαινόμενο φαίνεται ακόμα να βρίσκεται σε πρώιμο στάδιο, με αποτέλεσμα να μην υπάρχει σχετική νομολογία για να μπορέσουμε να διακρίνουμε πως αντιμετωπίζεται ένα deepfake video από την ελληνική έννομη τάξη.

### Ι.4. ΔΟΜΗ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η παρούσα διπλωματική εργασία διακρίνεται σε δύο μέρη, το πρώτο από τα οποία αφιερώνεται στην τεχνολογική προσέγγιση των deepfakes. Το πρώτο κεφάλαιο αποτελεί εισαγωγή στην τεχνολογία των deepfakes, παρουσιάζεται η ιστορία της τεχνολογίας, ο ορισμός αυτής, συνοπτικά οι τεχνολογίες που χρησιμοποιούνται, παραδείγματα υφιστάμενων πλατφορμών – εφαρμογών deepfakes και τέλος αναδεικνύονται τόσο τα θετικά όσο και τα αρνητικά χαρακτηριστικά της τεχνολογίας αυτής.

Στο δεύτερο, στο τρίτο, στο τέταρτο και στο πέμπτο κεφάλαιο γίνεται αναφορά στις εξής τεχνολογίες αντίστοιχα: στην τεχνητή νοημοσύνη, στη μηχανική μάθηση, στη βαθιά μάθηση και στην υπολογιστική νοημοσύνη, καθώς κρίνεται απαραίτητη η προσέγγιση των τεχνολογιών αυτών, προκειμένου να γίνουν κατανοητή η έννοια κάθε τεχνολογίας, αφού χάρην της τεχνητής νοημοσύνης αναδείχθηκε η τεχνολογία deepfakes.

Το έκτο κεφάλαιο του πρώτου μέρους της εργασίας είναι αφιερωμένο στα νευρωνικά δίκτυα και θα λέγαμε ότι είναι και το πιο σημαντικό κεφάλαιο καθώς χωρίς τα νευρωνικά δίκτυα δεν είναι

δυνατή η λειτουργία της τεχνολογίας deepfakes, και ειδικά των γενετικών αντιπαραθετικών δικτύων.

Αφού, λοιπόν, ο αναγνώστης έχει έρθει σε επαφή με τις έννοιες των βασικών τεχνολογιών που χρησιμοποιούνται για τη δημιουργία ενός deepfake, μπορεί πλέον στο έβδομο κεφάλαιο να κατανοήσει τον βασικό τρόπο υλοποίησης των deepfakes.

Στη συνέχεια στο δεύτερο μέρος της εργασίας γίνεται προσέγγιση του φαινομένου από νομικής πλευράς. Το πρώτο κεφάλαιο αποτελεί την εισαγωγή, στην οποία αναδεικνύεται ότι εάν τα deepfake χρησιμοποιηθούν κακόβουλα μπορούν να τελεστούν διάφορα ποινικά αδικήματα. Το δεύτερο κεφάλαιο αναφέρεται στα deepfakes ως κυβερνοέγκλημα, ενώ στη συνέχεια στο τρίτο κεφάλαιο γίνεται προσπάθεια προσέγγισης διαφόρων ποινικών αδικημάτων που θα μπορούσαν να τελεστούν στην περίπτωση κακόβουλης χρήσης και συγκεκριμένα αναφέρονται οι εξής περιπτώσεις και παραδείγματα αυτών: τα deepfakes α) ως μέσο παραπληροφόρησης, β) ως μέσο αλλοίωσης ενός προστατευόμενου έργου πνευματικής ιδιοκτησίας, γ) ως μέσο προσβολής πνευματικών δικαιωμάτων, δ) ως μέσο δυσφήμησης, δ) ως ρατσιστικό και ξενοφοβικό υλικό, ε) ως μέσο εκφοβισμού – εκβιασμού, στ) ως μέσο απάτης, ζ) ως μέσο πλαστογραφίας.

Στο προτελευταίο κεφάλαιο γίνεται μια προσέγγιση να αναδειχθεί ο κίνδυνος να χρησιμοποιηθούν τα deepfakes ως ψηφιακά πειστήρια στη δικαστηριακή πρακτική.

Το τελευταίο κεφάλαιο συνοψίζει τις ανησυχίες της τεχνολογίας αυτής ως υφιστάμενη απειλή και ολοκληρώνει με μια σειρά από προτάσεις για μελλοντική έρευνα.

## ΙΙ. Α' ΜΕΡΟΣ – ΤΕΧΝΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

## 1. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ DEEPFAKES

### 1.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η τεχνητή νοημοσύνη ήταν κάποτε αποκλειστικός τομέας της επιστημονικής φαντασίας. Τώρα είναι μια πρακτική πραγματικότητα. Πρόκειται να αλλάξει τη ζωή μας και τα μέσα ενημέρωσης είναι μόνο μία πτυχή από τις εκδηλώσεις της. Στις μέρες μας η τεχνολογία εξελίσσεται με τόσο ραγδαίο ρυθμό, ώστε το Ίντερνετ, οι έξυπνες συσκευές και τα μέσα κοινωνικής δικτύωσης έχουν μεταμορφώσει εντελώς το περιβάλλον πληροφορίας.[1] Τον τελευταίο καιρό, παρατηρούμε μια αυξανόμενη τάση οι συσκευές να συνδέονται με το διαδίκτυο. Οι συσκευές αυτές περιλαμβάνουν, μεταξύ άλλων, smartphones, IoT και δίκτυα cloud.[2]

[1] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 10,11, 33

[2] Brij B. Gupta, Krishna Yadav, Imran Razzak, Konstantinos Psannis, Arcangelo Castiglione, Xiaojun Chang,, A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment, Computer Communications, Volume 175, 2021, Pages 47-57,ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2021.04.023

Την περασμένη δεκαετία, το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) μπήκε σταδιακά στην καθημερινότητά μας, χάρη στην εξέλιξη των τεχνολογιών ασύρματης επικοινωνίας, όπως το WiFi, το 4G κ.λπ. Σύμφωνα με το IoT όλα τα καθημερινά "πράγματα" μπορούν να συνδέονται με το διαδίκτυο και να είναι μοναδικά αναγνωρίσιμα και πανταχού συνδεδεμένα μεταξύ τους, με αποτέλεσμα τη μεταξύ τους επικοινωνία με την ανταλλαγή πληροφοριών και δεδομένων. Με τη χρήση του IoT, τα πάντα γύρω μας, όπως υπολογιστές, κινητά τηλέφωνα, τηλεοράσεις, αυτοκίνητα κ.λπ., θα συλλέγουν όλες τις απαραίτητες πληροφορίες και στη συνέχεια θα τις στέλνουν στις σχετικές συσκευές χάρη στις ασύρματες τεχνολογίες, οι οποίες θα πραγματοποιήσουν αυτόματα τις κατάλληλες ενέργειες. Ο κύριος στόχος του IoT είναι η δημιουργία προηγμένης συνδεσιμότητας συστημάτων, συσκευών και υπηρεσιών. [3]

Σήμερα, το παγκόσμιο δίκτυο του Διαδικτύου των Πραγμάτων (IoT) αποτελείται από πολλές συσκευές που έχουν πρόσβαση στο Διαδίκτυο και ολοκληρώνουν συγκεκριμένες εργασίες για την ικανοποίηση των ανθρώπινων αναγκών. Χρησιμοποιώντας πολλαπλούς τρόπους πρόσβασης στο Διαδίκτυο, οι άνθρωποι απολαμβάνουν νέες δυνατότητες σε πολλούς τομείς της καθημερινής τους ζωής, και έτσι βελτιώνεται η ποιότητα ζωής τους. Επιπλέον, βελτιώνεται η εμπειρία τους με τη χρήση πολλών συσκευών που έχουν πρόσβαση στο Διαδίκτυο, όπως φορητούς υπολογιστές, tablet, smartphones, έξυπνες τηλεοράσεις, έξυπνα αυτοκίνητα, smartwatches κ.ο.κ. Επιπλέον, η ενσωμάτωση της τεχνητής νοημοσύνης (AI) σε αυτές τις έξυπνες συσκευές και πράγματα μπορεί να ενισχύσει ακόμη περισσότερο την ποιότητα ζωής, καθιστώντας το IoT μια παγκόσμια AI of Things (AIoT). Αλλάζει τον τρόπο μετακίνησης, εργασίας, μεταμορφώνοντας ακόμη και ολόκληρες πόλεις.[4]

Καθημερινά, παράγεται μεγάλος όγκος δεδομένων από πολλές συσκευές που βασίζονται στο IoT και μεταφέρονται μεταξύ τους, γεγονός που προκαλεί ανησυχία για τα δεδομένα. Κυρίως όσον αφορά στα ευαίσθητα προσωπικά δεδομένα σημαντική θέση κατέχει η διασφάλιση της ιδιωτικότητας των χρηστών. Επιπλέον, οι κακόβουλοι χρήστες, γνωστοί ως "black-hat hackers" ή "crackers", αναζητούν διάφορες μεθόδους και τρόπους για να εισβάλουν στις συσκευές των χρηστών, εκμεταλλευόμενοι τα τρωτά σημεία τους, προκειμένου να κλέψουν τα ευαίσθητα προσωπικά τους δεδομένα και να τα χρησιμοποιήσουν εις βάρος τους. [5]

[3] Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B. Gupta, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Future Generation Computer Systems, Volume 83, 2018, Pages 619-628, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.04.039

[4] Andreas P. Plageras, Kostas E. Psannis, Christos Stergiou, Haoxiang Wang, B.B. Gupta, Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings, Future Generation Computer Systems, Volume 82, 2018, Pages 349-357, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.09.082.

[5] V. Memos and K.E. Psannis, NFV-based Scheme for Effective Protection against Bot Attacks in AI-enabled IoT, IEEE Internet of Things Magazine, 2022.

Η έλευση της μαζικής υιοθέτησης των μέσων κοινωνικής δικτύωσης έχει προκαλέσει μια αλλαγή στον τρόπο που οι άνθρωποι επικοινωνούν, μοιράζονται γνώσεις, οι επιχειρήσεις λειτουργούν και ανταγωνίζονται και οι πολιτικοί αμφισβητούν και επηρεάζουν. Η εντυπωσιακή ανάπτυξη των μέσων αυτών μπορεί να θεωρηθεί ως η σπίθα που πυροδότησε την εποχή των μεγάλων δεδομένων. Κάνει διαθέσιμη μια άνευ προηγουμένου κλίμακα προσωπικών δεδομένων, δεδομένων σχετικά με γεγονότα και κοινωνικές σχέσεις, δημόσια συναισθήματα και συμπεριφορές που όταν εξορύσσονται και ερμηνεύονται έχουν τεράστια αξία. Τα μέσα κοινωνικής δικτύωσης είναι μια πλούσια πηγή κειμένου και πολυμεσικού περιεχομένου με άποψη που έχει αποκτήσει πρόσφατα τεράστια δημοτικότητα, ιδίως στον τομέα της παρακολούθησης πολιτικών εκστρατειών ή εκστρατειών μάρκετινγκ. Η διάδοση των έκτακτων ειδήσεων, ιδίως στο Twitter, θεωρείται ότι διαδίδεται πολύ ταχύτερα από ό,τι σε οποιοδήποτε συμβατικό μέσο ενημέρωσης.[6]

Το βίντεο και η εικόνα έχει πλέον εξελιχθεί στο κυριότερο και πιο δυναμικό μέσο επικοινωνίας. Τα μέσα κοινωνικής δικτύωσης παίζουν πλέον πολύ σημαντικό ρόλο ως μέσο διάδοσης ειδήσεων και έτσι οι διαδικτυακές εκστρατείες παραπληροφόρησης έχουν λάβει σημαντική διάσταση τα τελευταία χρόνια. Ενώ τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται για τη διάδοση ψευδών ειδήσεων, τα εργαλεία υπολογιστικής όρασης έχουν συμβάλλει σε αυτή την τάση διευκολύνοντας τη δημιουργία ψευδών εικόνων.[7]

Η μεγάλη εξέλιξη της τεχνολογίας έχει αυξήσει τον αριθμό των εγκλημάτων στον κυβερνοχώρο παγκοσμίως με γεωμετρική πρόοδο. Αυτά τα εγκλήματα συνήθως συμβαίνουν μέσω κυβερνοεπιθέσεων. Τα είδη των επιθέσεων αυτών μπορεί να είναι το γνωστό σε όλους hacking, η παραβίαση πνευματικών δικαιωμάτων (πειρατεία), η αδικαιολόγητη μαζική παρακολούθηση και η ευρέως διαδεδομένη στις μέρες μας παρενόχληση (με τη μορφή του εξαναγκασμού όπως το sextortion, της παιδικής πορνογραφίας, παιδικής διαπαιδαγώγησης), και γενικότερα έννοιες που άρχισαν να εμφανίζονται και να γίνονται μάστιγα της εποχής μας.[8],[9]

Ένας χειριστής εικόνων τα προηγούμενα χρόνια χρειαζόταν σημαντική εμπειρία με λογισμικό απόδοσης ή/και επεξεργασίας εικόνων. Οι σύγχρονες προσεγγίσεις με βάση τα δεδομένα έχουν καταστήσει πολύ πιο εύκολη τη δημιουργία τεχνητών εικόνων από το μηδέν. Έτσι, τα deepfake

[6] Androniki Sapountzi, Kostas E. Psannis, Social networking data analysis tools & challenges, Future Generation Computer Systems, Volume 86, 2018, Pages 893-913, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.10.019.
[7] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 10,11, 33
[8] V. Memos, and K. Psannis, "Artificial Intelligence ANTi-Attack System (AIANTAS) for IoT Cyberspace: An Upcoming Cloud-based Security Architecture for Police Authorities", 4th World Symposium on Communication Engineering (WSCE 2021) & 9th International Conference on Information, Communication and Networks (ICICN 2021), University of Macedonia (Greece), Shaanxi Normal University (Xi'an, China), November 2021
[9] V. Memos and K.E. Psannis, NFV-based Scheme for Effective Protection against Bot Attacks in AI-enabled IoT, IEEE Internet of Things Magazine, 2022.

βίντεο ή εικόνες μπορούν να προκαλέσουν πρωτοφανή ζημιά σε ένα πολιτικό περιβάλλον καθώς και στην προσωπική ζωή πολλών ανθρώπων.[10]

Τα μέσα της ΤΝ τείνουν να γίνουν η πιο σημαντική μορφή της ανθρώπινης επικοινωνίας – όχι μόνο είμαστε μάζα αποδεκτών – καταναλωτών οπτικοακουστικών μέσων, αλλά είμαστε επίσης και παραγωγοί αυτών. Μέσω των 5.6 δισεκατομμυρίων κινητών τηλεφώνων τους, οι άνθρωποι όχι μόνο βλέπουν και ακούν "online videos", αλλά δημιουργούν και κοινοποιούν ένα από αυτά.[11] Και βρισκόμαστε ακόμα στην αρχή της επανάστασης των συνθετικών μέσων, τα οποία αναφέρονται σε μέσα που παράγονται ή χειραγωγούνται με τη χρήση τεχνητής νοημοσύνης (AI).[12]

Τα συνθετικά μέσα που παράγονται με AI έχουν τρία αξιοσημείωτα χαρακτηριστικά. Πρώτον, είναι η ποιότητά τους. Η ΤΝ δημιουργεί και θα δημιουργήσει οπτικοακουστικά εφέ που είναι πολύ καλύτερα από οτιδήποτε άλλο στο παρελθόν. Δεύτερον, το Διαδίκτυο έχει καταστήσει την έρευνα στον τομέα της τεχνητής νοημοσύνης προσβάσιμη και πιο εύκολη σε όλους, αφού πλέον ο καθένας μπορεί να έχει πρόσβαση στα εργαλεία και στο λογισμικό που διαμοιράζονται ελεύθερα. Και τρίτον, καθώς η τεχνολογία βελτιώνεται, η παραγωγή αυτού του περιεχομένου θα γίνει φθηνότερη ή και δωρεάν.[13] Επιπλέον, λόγω των πολλών θετικών αποτελεσμάτων των εφαρμογών της τεχνητής νοημοσύνης, ο τομέας αναπτύσσεται χάρη και στην ακαδημαϊκή έρευνα που χρηματοδοτείται με τις ιδιωτικές επενδύσεις. Και όπως συμβαίνει με όλες τις εξελισσόμενες τεχνολογίες, αυτή η επανάσταση στις νέες τεχνολογίες θα χρησιμοποιηθεί τόσο για καλούς σκοπούς όσο και για κακόβουλους.[14]

Ήδη από τον 19ο αιώνα με την εφεύρεση της φωτογραφίας, οι άνθρωποι απέκτησαν για πρώτη φορά την ικανότητα να "αποτυπώνουν την πραγματικότητα" μέσω ενός μη ανθρώπινου μέσου. Γρήγορα αποδείχθηκε ότι αυτό το μέσο μπορούσε να χειραγωγηθεί από τον άνθρωπο. Για παράδειγμα, όταν δολοφονήθηκε ο Αβραάμ Λίνκολν τη δεκαετία του 1860, δεν υπήρχαν εικόνες του Προέδρου σε "ηρωικό στυλ" και για να αντιμετωπιστεί αυτό, ένας χαράκτης αποφάσισε σε μια φωτογραφία να τοποθετήσει το κεφάλι του Λίνκολν πάνω στο σώμα του πολιτικού John C Calhoun. Για έναν αιώνα, κανείς δεν το πρόσεξε. Μόλις πρόσφατα αποκαλύφθηκε ότι η φωτογραφία ήταν παραποιημένη.[15]

[10] Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054
[11] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 30
[12] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[13] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 49,50
[14] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 34
[15] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 26

Στην πορεία, τη δεκαετία του 1930, μεταξύ των όσων συνέβησαν στο όνομα του Ιωσήφ Στάλιν και της ιδεολογίας του, αναπτύχθηκε μια ολόκληρη βιομηχανία αφιερωμένη στην επεξεργασία φωτογραφιών. Πολλοί πολιτικοί εχθροί του Στάλιν δολοφονήθηκαν ή φυλακίστηκαν και ταυτόχρονα ως δια μαγείας αφαιρούνταν από τις φωτογραφίες. Παράδειγμα αποτελεί η εικόνα παρακάτω.[16]

Πηγή: Schick N. *Deepfakes : The Coming Infocalypse*. First U.S. ed. New York: Twelve; 2020, σελ. 28

Στα αριστερά, ο Στάλιν στέκεται με μια ομάδα αντιπροσώπων στη Συνδιάσκεψη του κόμματος τον Απρίλιο του 1925. Έξι από τους άνδρες πέθαναν αργότερα από αυτοκτονία, πυροβολισμό ή φυλάκιση, με αποτέλεσμα να "αποπροσωποποιηθούν", μέχρι που παρέμειναν μόνο ο Στάλιν και τρεις στενοί του φίλοι σε μια εκδοχή της ίδιας φωτογραφίας που αναπαράχθηκε το 1939.[17]

Ήδη από την εφεύρεση των υπολογιστών το 1950, οι επιστήμονες της πληροφορικής προσπαθούν να βρουν τρόπο να προσδώσουν στους υπολογιστές ανθρώπινα επίπεδα νοημοσύνης - ή τεχνητής νοημοσύνης (AI). Στο πλαίσιο αυτό, μια μερίδα επιστημόνων υπέθεσαν ότι ο καλύτερος τρόπος για να αναπτυχθεί η τεχνητή νοημοσύνη θα ήταν να δομηθούν οι μηχανές ώστε να μαθαίνουν μόνες τους, μιμούμενες τα νευρωνικά δίκτυα του ανθρώπινου εγκεφάλου για την επεξεργασία δεδομένων για τη λήψη αποφάσεων. Με αυτόν τον τρόπο, οι μηχανές θα μαθαίνουν μέσω της "εμπειρίας" όπως ακριβώς και οι άνθρωποι. Η θεωρία αυτή δεν είχε δοκιμαστεί σωστά μέχρι τη δεκαετία του 2000, όταν για πρώτη φορά υπήρχαν επαρκή δεδομένα και επεξεργαστική ισχύς για να δοκιμαστεί. Οι ερευνητές τεχνητής νοημοσύνης διαπίστωσαν τότε ότι αυτό λειτούργησε.[18]

Με τη δημιουργία τεχνητών νευρωνικών δικτύων, τα οποία έχουν ως πρότυπο τον ανθρώπινο εγκέφαλο, οι μηχανές θα μπορούσαν όντως να "μαθαίνουν", επεξεργαζόμενες τα δεδομένα που

[16] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 27
[17] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 27
[18] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 33

τους παρέχονται για να εκτελούν εργασίες και να λαμβάνουν αποφάσεις αυτόνομα. Αυτή η αποκαλούμενη διαδικασία "αυτόνομης μηχανικής μάθησης", η οποία στηρίζεται σε τεχνητά νευρωνικά δίκτυα, έγινε γνωστή ως "βαθιά μάθηση", όπου ένας υπολογιστής αναλύει σύνολα δεδομένων για να αναζητήσει μοτίβα με τη βοήθεια νευρωνικών δικτύων. [19]

Στη μηχανική μάθηση οι υπολογιστές βελτιώνονται αυτόματα μέσω της χρήσης δεδομένων. Η τεχνολογία της βαθιάς μάθησης, σε συνδυασμό με τη διαθεσιμότητα μεγάλων βάσεων δεδομένων με υλικό για την εκπαίδευση των γεννητικών μοντέλων, επέτρεψε την ταχεία βελτίωση της τεχνολογίας deepfake.[20]

Κατά την τελευταία δεκαετία, η ταχεία επιτάχυνση της βαθιάς μάθησης εκτοξεύει την ανάπτυξη της τεχνητής νοημοσύνης AI.[21] Τεχνικές της Τεχνητής Νοημοσύνης (ΤΝ), όπως ευρετικές μέθοδοι, εξόρυξη δεδομένων και νευρωνικά δίκτυα (NN), έχουν ήδη εφαρμοστεί σε πολλές εφαρμογές για την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο. Επιπλέον, οι τεχνικές μηχανικής μάθησης (ML) έχουν ήδη πολλές εφαρμογές, όπως η αναγνώριση προσώπου, το CAPTCHA, η ανακάλυψη ευπαθειών δικτύου, η ανίχνευση κακόβουλου λογισμικού, η ανακάλυψη επιθέσεων DDoS κ.λπ.[22]

Πρόσφατες εφευρέσεις στην ΤΝ δίνουν στις μηχανές τη δύναμη να παράγουν εξ ολοκλήρου συνθετικά μέσα. Αυτό έχει τεράστιες επιπτώσεις στο πως παράγουμε περιεχόμενο, επικοινωνούμε και αντιλαμβανόμαστε τον κόσμο. Αυτή η τεχνολογία είναι ακόμα σε πρώιμο στάδιο, αλλά σε μερικά χρόνια θα μπορούμε όλοι να δημιουργούμε βίντεο και εικόνες επιπέδου Hollywood, χωρίς κόστος, με τις ελάχιστες ικανότητες και προσπάθεια.[23] Παράδειγμα αποτελεί η τεχνολογία αναγνώρισης προσώπου, όπου τα συστήματα μηχανικής μάθησης εκπαιδεύονται χρησιμοποιώντας ένα τεράστιο σύνολο δεδομένων ανθρώπινων προσώπων, μέχρι να μάθουν αυτόνομα να τα αναγνωρίζουν με απόλυτη ακρίβεια.[24] Οι πρώτες βαθιές απομιμήσεις, οι ανταλλαγές προσώπων, βασίζονται σε μια κατηγορία συστημάτων βαθιάς μάθησης, γνωστών ως "αυτοκωδικοποιητές". [25]

Ωστόσο, μια πιο ευέλικτη κατηγορία συστημάτων βαθιάς μάθησης αναλαμβάνει τώρα τη δημιουργία συνθετικών μέσων και αυτό οφείλεται στον Αμερικανό ερευνητή Ian J. Goodfellow, και την εφεύρεση του, το έτος 2014, ενός συστήματος βαθιάς μάθησης, γνωστού ως GAN –

[19] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 33
[20] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[21] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 34
[22] V. Memos, and K. Psannis, "Artificial Intelligence ANTi-Attack System (AIANTAS) for IoT Cyberspace: An Upcoming Cloud-based Security Architecture for Police Authorities", 4th World Symposium on Communication Engineering (WSCE 2021) & 9th International Conference on Information, Communication and Networks (ICICN 2021), University of Macedonia (Greece), Shaanxi Normal University (Xi'an, China), November 2021
[23] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 8
[24] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 34
[25] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 43

Γεννητικά αντιπαραθετικά δίκτυα.[26] Οι πρώτες εξελίξεις στη βαθιά μάθηση σήμαιναν ότι οι μηχανές έχουν γίνει πολύ καλές στην κατηγοριοποίηση δεδομένων, αλλά δεν ήταν ακόμα πολύ καλές στη δημιουργία τους. Ο Goodfellow σκέφτηκε ότι αν έβαζες δύο δίκτυα βαθιάς μάθησης αντιμέτωπα το ένα με το άλλο σε ένα παιχνίδι, το ένα η γεννήτρια θα προσπαθούσε να δημιουργήσει νέες πληροφορίες και το άλλο ο ανιχνευτής θα προσπαθούσε να τις ανιχνεύσει. Μια μονομαχία σε μια συνεχή επαναληπτική διαδικασία, μέχρι η γεννήτρια να νικήσει τον ανιχνευτή. Ουσιαστικά, εφάρμοσε την ιδέα της "αντιθετικής προπόνησης" που χρησιμοποιείται συνήθως για την προπόνηση αθλητών για να δει αν μπορεί να λειτουργήσει στη βαθιά μάθηση.[27]

Έτσι, προγραμμάτισε δύο δίκτυα βαθιάς μάθησης μαζί σε ένα αντίπαλο παιχνίδι, για να δημιουργήσει ανθρώπινα πρόσωπα. Καθώς η γεννήτρια προσπαθούσε να νικήσει τον ανιχνευτή, γινόταν όλο και καλύτερη στο έργο της. Μέσα σε λίγες ώρες, το σύστημα που είχε δημιουργήσει - το πρώτο παραγωγικό αντιπαραθετικό δίκτυο (GAN) - παρήγαγε ανθρώπινα πρόσωπα που ήταν καλύτερα από οτιδήποτε άλλο είχε φτιάξει η ΤΝ πριν.[28]


Πηγή: https://twitter.com/goodfellow_ian/status/1084973596236144640

Η ασπρόμαυρη κοκκώδης φωτογραφία στα αριστερά είναι μία από αυτές που δημιούργησε ο Goodfellow εκείνο το βράδυ του 2014. Από την εφεύρεση των GANs εκείνο το βράδυ, η ποιότητα των αποτελεσμάτων τους έχει αναπτυχθεί ραγδαία. Το πρόσωπο στα δεξιά δημιουργήθηκε με τη χρήση ενός GAN μόλις τέσσερα χρόνια αργότερα, το 2018.[29]

Με τα αποτελέσματα αυτών των δοκιμών, τα μοντέλα βελτιώνονται συνεχώς μέχρι το παραγόμενο περιεχόμενο να είναι εξίσου πιθανό να προέρχεται από το παραγωγικό μοντέλο με τα δεδομένα εκπαίδευσης. Αυτή η ισχυρή μέθοδος αφενός απλοποιεί τη διαδικασία μάθησης, καθιστώντας την πιο προσιτή, και αφετέρου βελτιώνει το αποτέλεσμα, ενσωματώνοντας έναν μηχανισμό που έχει σχεδιαστεί για να ελαχιστοποιεί την πιθανότητα το προϊόν της να διακρίνεται από το αυθεντικό περιεχόμενο.[30]

[26] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 43
[27] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 44
[28] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 45
[29] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 45
[30] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

Όσο πιο εκτεταμένη είναι η βάση δεδομένων και όσο πιο πολύπλοκος γίνεται ο αλγόριθμος, τόσο περισσότερη υπολογιστική ισχύς είναι απαραίτητη. Η παραγωγή ποιοτικών δεδομένων απαιτεί μεγάλο όγκο και ποικιλία δεδομένων με αρκετά παραδείγματα παρόμοιων αλλά ελαφρώς διαφορετικών αναπαραστάσεων των ίδιων χαρακτηριστικών για να λειτουργήσει. Καθώς αυξάνεται ο αριθμός και ο όγκος των διαθέσιμων βάσεων δεδομένων, αυξάνεται η ποιότητα και η ποσότητα των δεδομένων εκπαίδευσης. Αυτό επέτρεψε στα μοντέλα που δημιουργούν τα deepfakes να γίνουν όλο και πιο εξελιγμένα.[31]

Χάρη στους GANs, η Al μπορεί ήδη να παράγει σχεδόν τέλειες συνθετικές εικόνες και βίντεο. Δεδομένης της επαναληπτικής και αντιφατικής διαδικασίας μάθησης που χρησιμοποιεί ένα GAN, θεωρητικά θα επιτρέψει σε όλα τα μέσα που παράγονται από τεχνητή νοημοσύνη να εξελιχθούν μέχρι το σημείο όπου κυριολεκτικά θα γίνουν τέλεια.[32] Όσο τα δίκτυα αυτά είναι τα πιο διαδεδομένα για την παραγωγή συνθετικών βίντεο, στο μέλλον οι ερευνητές θα βρουν πολύ περισσότερους και καλύτερους τρόπους δημιουργίας. Αυτή η ραγδαία εξέλιξη οφείλεται τόσο στον ανοιχτό κώδικα της ΤΝ όσο και στις μεγάλες ιδιωτικές επενδύσεις.[33]

Η χειραγώγηση μεταβάλλει το περιεχόμενο των αρχικών δεδομένων για να δημιουργήσει νέα κατασκευασμένα δεδομένα. Δυστυχώς, τα παραποιημένα δεδομένα έχουν αποκτήσει αυξανόμενο ενδιαφέρον όσον αφορά στη διάδοση παραπληροφόρησης μέσω της κοινής χρήσης δεδομένων στις έξυπνες κοινότητες. Η ανίχνευση πλαστών εικόνων παρουσιάζει μεγάλο ενδιαφέρον για τους ερευνητές επεξεργασίας εικόνας. Η πλαστογράφηση εικόνων εμπλέκεται σε διάφορους τομείς, όπως τα συστήματα ελέγχου πρόσβασης, η πλαστογράφηση ταυτότητας, η βιομετρική εγκληματολογία και η ασφάλεια στον κυβερνοχώρο.[34]

Το πρόσωπο είναι το πιο χαρακτηριστικό γνώρισμα του ανθρώπου. Με την τεράστια ανάπτυξη της τεχνολογίας σύνθεσης προσώπων, ο κίνδυνος ασφάλειας που ενέχει η χειραγώγηση των προσώπων γίνεται όλο και πιο σημαντική. Τα πρόσωπα των ατόμων μπορεί συχνά να ανταλλάσσονται με πρόσωπα άλλων και τα αποτελέσματα φαίνονται αυθεντικά λόγω των μυριάδων αλγορίθμων που βασίζονται στη βαθιά μάθηση .[35]

---

[31] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

[32] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 45

[33] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 4

[34] Ahmed Seddik, Yassine Maleh, Ghada M. El Banby, Ashraf A.M. Khalaf, Fathi E. Abd El-Samie, Brij B Gupta, Konstantinos Psannis, Ahmed A. Abd El-Latif, AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities, Technological Forecasting and Social Change, Volume 177, 2022, 121555, ISSN 0040-1625, [https://doi.org/10.1016/j.techfore.2022.121555]

[35] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341

Υπάρχουν διάφοροι τύποι πλαστογραφίας σε ψηφιακές εικόνες. Αυτοί οι τύποι μπορούν να χωριστούν σε α) συγχώνευση πολλών εικόνων σε μία, ή στη δημιουργία εικόνας που περιλαμβάνει αντικείμενα από περισσότερες εικόνες, β) μορφοποίηση που μπορεί να πραγματοποιηθεί με τη συγχώνευση σχημάτων από διαφορετικές εικόνες, γ) ρετουσάρισμα εικόνας που βασίζεται στην απόκρυψη ορισμένων χαρακτηριστικών με εφαρμογή μιας διαδικασίας φιλτραρίσματος στην εικόνα, δ) επαναδειγματοληψία, που σημαίνει αλλαγή μεγέθους ενός τέτοιου αντικειμένου στην εικόνα, καθώς και δ) το CMF το οποίο βασίζεται στην αντιγραφή μιας συγκεκριμένης περιοχής ή αντικειμένου από την εικόνα και την επικόλλησή του σε άλλο σημείο της ίδιας εικόνας. [36]

Με όλες αυτές τις εξελισσόμενες τεχνολογίες, η ΤΝ γίνεται αρκετά δυνατή, ώστε να κάνει τους ανθρώπους να κάνουν πράγματα που ποτέ δεν έκαναν πραγματικά και να λένε κουβέντες που ποτέ δεν εξέφρασαν αληθινά. Κάπως έτσι γεννήθηκε και το πρώτο deepfake. Ο καθένας μπορεί να στοχοποιηθεί και ο καθένας μπορεί να αρνηθεί τα πάντα. Η ΤΝ και τα deepfake ίσως να είναι η πιο πρόσφατη υπαρκτή απειλή.[37]

Στην ουσία, το Deepfake είναι ένας αναδυόμενος υποτομέας της τεχνητής νοημοσύνης στην οποία το πρόσωπο ενός ατόμου επικαλύπτεται πάνω από το πρόσωπο ενός άλλου ατόμου, και μέσω των πολλαπλών μεθόδων που βασίζονται στα γεννητικά αντιφατικά δίκτυα (GANs) μπορούν να παραχθούν εικόνες υψηλής ανάλυσης.[38]

Όλα ξεκίνησαν στο Reddit στις 2 Νοεμβρίου 2017. Ένας ανώνυμος χρήστης παρουσιάστηκε με το ψευδώνυμο «deepfakes» και ξεκίνησε μια συζήτηση με το θέμα «Deepfakes». Χρησιμοποιώντας βαθιά μάθηση πόσταρε στο φόρουμ του ψεύτικα βίντεο με ερωτικό περιεχόμενο, όπου πρόσωπα διασημοτήτων του Hollywood, ανταλλάσσονταν με πρόσωπα ηθοποιών που πρωταγωνιστούν σε ταινίες ερωτικού περιεχομένου, τα οποία τα είχε δημιουργήσει ο ίδιος με εργαλεία ΤΝ. Δημιούργησε τα βίντεο αυτά χρησιμοποιώντας ανοιχτό κώδικα που ο οποιοσδήποτε με στοιχειώδεις γνώσεις αλγορίθμων βαθιάς μάθησης μπορεί να χρησιμοποιήσει. Εάν, λοιπόν, ένας χρήστης του Reddit μπόρεσε να το κάνει αυτό, τι θα μπορούσε να σταματήσει τον οποιονδήποτε να το κάνει;[39]

[36] Ahmed Seddik, Yassine Maleh, Ghada M. El Banby, Ashraf A.M. Khalaf, Fathi E. Abd El-Samie, Brij B Gupta, Konstantinos Psannis, Ahmed A. Abd El-Latif, AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities, Technological Forecasting and Social Change, Volume 177, 2022, 121555, ISSN 0040-1625, [https://doi.org/10.1016/j.techfore.2022.121555]

[37] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 8

[38] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341

[39] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 35,36

Μετά από λίγες εβδομάδες, ο συγκεκριμένος χρήστης έκλεισε το φορουμ και εξαφανίστηκε. Ήταν όμως επαρκές το διάστημα, ώστε να προλάβει να διαδώσει τον κώδικα των deepfake.[40] Η ανακάλυψη προκάλεσε φρενίτιδα στα μέσα ενημέρωσης και στη συνέχεια άρχισε να εμφανίζεται μεγάλος αριθμός νέων βίντεο deepfake.[41] Άμεσα, πολλοί ξεκίνησαν να πειραματίζονται με τις δικές τους δημιουργίες. Πολλές διάσημες ηθοποιοί στοχοποιήθηκαν και βρέθηκαν θύματα της τεχνολογίας deepfake: η Taylor Swift, η Gal Gadot, η Meghan Markle είναι μερικές από αυτές ενώ μερικές στοχοποιημένες ηθοποιοί είχαν πρωτοεμφανιστεί ως παιδιά: η Μεσι Γουλιαμς που πρωταγωνίστησε στη σειρά Game of Thrones ως Arya Stark και η Emma Watson της ταινίας Harry Potter.[42] Στις Ηνωμένες Πολιτείες και στις ασιατικές κοινωνίες, κυρίως οι γυναίκες πέφτουν θύματα των βαθιά ψεύτικων τεχνολογιών. Η επιβλαβής χρήση των βαθιών απομιμήσεων μπορεί να επηρεάσει σημαντικά τον πολιτισμό μας και να αυξήσει την παραπλανητική πληροφόρηση, ιδίως στα μέσα κοινωνικής δικτύωσης.[43] Τα deepfakes έχουν χρησιμοποιηθεί για να στοχοποιήσουν γνωστούς πολιτικούς σε πλατφόρμες βίντεο ή chat rooms και να επηρεάσουν τον πολιτικό κόσμο ακόμα και να παραποιήσουν αποτελέσματα εκλογών.[44]

Σε ένα παράδειγμα από το 2018, ο σκηνοθέτης Jordan Peele και ο διευθύνων σύμβουλος του BuzzFeed Jordan Peretti δημιούργησαν ένα deepfake βίντεο για να προειδοποιήσουν το κοινό για την παραπληροφόρηση, ειδικά όσον αφορά την αντίληψη του για τους πολιτικούς ηγέτες. Ο Peele και ο Peretti χρησιμοποίησαν δωρεάν εργαλεία με τη βοήθεια ειδικών στο μοντάζ για να επικαλύψουν τη φωνή και το στόμα του Peele πάνω σε ένα προϋπάρχον βίντεο του Μπαράκ Ομπάμα. Στο βίντεο, ο Ομπάμα φέρεται να είπε: "Μπαίνουμε σε μια εποχή στην οποία οι εχθροί μας μπορούν να το κάνουν να φαίνεται ότι ο καθένας λέει οτιδήποτε, οποιαδήποτε στιγμή. Ακόμα κι αν δεν θα έλεγαν ποτέ αυτά τα πράγματα".[45] Το βίντεο δημιουργήθηκε χρησιμοποιώντας το λογισμικό του χρήστη του Reddit (FakeApp) και προκάλεσε ανησυχίες σχετικά με την κλοπή ταυτότητας, την πλαστοπροσωπία και τη διάδοση της παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης και έγινε ευρέως γνωστό το βίντεο με σχεδόν 7.5 εκατομμύρια θεατές. Στην ουσία ο Πρόεδρος Obama ποτέ δεν είπε όσα φαίνεται να λέει στο βίντεο. Το βίντεο δεν είναι παρά ένα

[40] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 38
[41] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
[42] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 38
[43] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341
[44] Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054
[45] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

βίντεο deepfake με στόχο να μας υποψιάσει και να μας προειδοποιήσει για το τι εμπιστευόμαστε στο διαδίκτυο.[46]

Μετά από αυτά τα γεγονότα, το θέμα των deepfakes κέρδισε έδαφος στην ακαδημαϊκή κοινότητα, και η τεχνολογία αναπτύχθηκε ραγδαία τα τελευταία χρόνια. Δυστυχώς, λόγω της ευρείας χρήσης των κινητών τηλεφώνων και της ανάπτυξης πολυάριθμων ιστότοπων κοινωνικής δικτύωσης, τα deepfake εξαπλώνονται ταχύτερα από ποτέ στον 21ο αιώνα, γεγονός που έχει μετατραπεί κατά κύριο λόγο σε παγκόσμιο κίνδυνο. Επιπλέον, η ανάπτυξη του 5G θα ενισχύσει τη συνδεσιμότητα και την επικοινωνία, την ιδιωτικότητα και την ασφάλεια τόσο των οργανισμών όσο και των ατόμων, ενώ ταυτόχρονα θα αξιοποιηθεί από τους εγκληματίες, καθώς το πρόσθετο εύρος ζώνης που προσφέρουν οι νέες τεχνολογίες επικοινωνίας επιτρέπει στους χρήστες να αξιοποιούν τη δύναμη του υπολογιστικού νέφους για να χειρίζονται ροές βίντεο σε πραγματικό χρόνο και οι τεχνολογίες Deepfake μπορούν να εφαρμοστούν σε ρυθμίσεις τηλεδιασκέψεων, σε υπηρεσίες ζωντανής ροής βίντεο και στην τηλεόραση.[47]

Μπορούμε, λοιπόν, να φανταστούμε τις νέες προκλήσεις που επισύρει ο νέος τύπος υποδομής ασύρματου δικτύου, η έκτη γενιά (6G), που παρέχει όλα τα πλεονεκτήματα των προηγούμενων εκδόσεών της και βελτιώνει επίσης ορισμένα προβλήματα που είχαν οι προκάτοχοί της. Όσον αφορά στα δεδομένα που χρησιμοποιούνται πρέπει να διασφαλιστεί η προστασία της ιδιωτικής ζωής που.[48] Αυτό δημιουργεί μια αυξανόμενη ανάγκη για περαιτέρω έρευνα σε τεχνολογίες ασφαλείας, προκειμένου να μπορούν να χειριστούν τον τεράστιο όγκο δεδομένων. Μια λύση στο πρόβλημα ασφάλειας της ιδιωτικότητας στην καθημερινότητα θα μπορούσε να δώσουν τα εργαλεία και οι υπηρεσίες ανάλυσης μεγάλων δεδομένων.[49],[50]

Στην εποχή μας οι εκστρατείες παραπληροφόρησης και το ψεύτικο περιεχόμενο ειδήσεων έχουν στόχο να παραπλανήσουν το κοινό σχετικά με γεγονότα, να επηρεάσουν τα αποτελέσματα στις εκλογές, να αυξήσουν τα ποσοστά απάτης κ.α. Πολλοί οργανισμοί έχουν πλέον αρχίσει να βλέπουν τα deepfakes ως κίνδυνο και για την κλοπή ταυτότητας, ειδικά τώρα που οι περισσότερες αλληλεπιδράσεις έχουν μεταφερθεί στο διαδίκτυο μετά την πανδημία COVID-19. Σε πρόσφατη

[46] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 9
[47] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[48] Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi, Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT, Sustainable Computing: Informatics and Systems, Volume 19, 2018, Pages 174-184, ISSN 2210-5379, https://doi.org/10.1016/j.suscom.2018.06.003.
[49] C. L. Stergiou, K. E. Psannis and B. B. Gupta, "IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5164-5171, 1 April1, 2021, doi: 10.1109/JIOT.2020.3033131.
[50] Stergiou, C., Psannis, K.E. Efficient and secure BIG data delivery in Cloud Computing. Multimed Tools Appl 76, 22803–22822 (2017). https://doi.org/10.1007/s11042-017-4590-4

έκθεση του το University College London (UCL) χαρακτηρίζει την τεχνολογία deepfake ως μια υφιστάμενη απειλή για την κοινωνία.[51]

## 1.2. ΟΡΙΣΜΟΣ ΤΩΝ DEEPFAKES - ΤΕΧΝΟΛΟΓΙΕΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ

Το Deepfake είναι μια τεχνολογία ανθρώπινης απεικόνισης που χρησιμοποιεί τεχνητή νοημοσύνη για να παράγει εναλλασσόμενες ανθρώπινες εικόνες ή να επεξεργάζεται το περιεχόμενο ενός βίντεο ή μιας εικόνας ώστε να δείχνει κάτι που δεν συνέβη ποτέ. Είναι ο τύπος ενός συνθετικού μέσου (μέσο που περιλαμβάνει εικόνες, ήχο και βίντεο), το οποίο είναι είτε παραποιημένο - επεξεργασμένο είτε έχει παραχθεί ολοκληρωτικά από την ΤΝ.[52] Με άλλα λόγια, το Deepfake χρησιμοποιεί τεχνητή νοημοσύνη με σκοπό τη δημιουργία πλαστών βίντεο, τα οποία δεν είναι ακριβώς ψεύτικα, αφού στην πραγματικότητα είναι πραγματικό περιεχόμενο που έχει μελετηθεί και αναδιαρθρωθεί για να εμφανίζει κάτι διαφορετικό από το πρωτότυπο.[53]

Η τεχνητή νοημοσύνη είναι η ραχοκοκαλιά αυτής της τεχνολογίας, η οποία χρησιμοποιεί εργαλεία βαθιάς μάθησης όπως τα νευρωνικά δίκτυα που είναι αλγόριθμοι που πραγματοποιούν τη διαδικασία κατασκευής.[54] Η τεχνολογία Deepfake χρησιμοποιεί Τεχνητή Νοημοσύνη σε ηχητικό και οπτικοακουστικό περιεχόμενο και μπορεί να παράγει περιεχόμενο που δείχνει πειστικά ανθρώπους να εκφράζουν και να ενεργούν πράγματα που δεν συνέβησαν ποτέ στην πραγματικότητα ή να δημιουργεί προσωπικότητες που δεν υπήρξαν ποτέ.[55]

Η εξέλιξη της τεχνολογίας έχει δημιουργήσει ευκαιρίες για οποιονδήποτε να δημιουργεί και να μοιράζεται deepfakes πολύ πιο εύκολα και αυτό μπορεί να οδηγήσει σε κοινωνικές ανησυχίες.[56] Ανάλογα με το σκοπό ή την πρόθεση οποιουδήποτε βρίσκεται πίσω από ένα περιεχόμενο που δημιουργήθηκε, η απίστευτα ισχυρή τεχνολογία του Deepfake μπορεί να χρησιμοποιηθεί για χρήσιμες εφαρμογές καθώς και να επιφέρει αρνητικές επιπτώσεις.[57] Η ποιότητα του περιεχομένου

[51] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[52] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 8
[53] Nobert Young "Deepfake Technology Complete Guide to Deepfakes Politics and Social Media", Printed in Great Britain by Amazon, σελ. 9, 10
[54] Nobert Young "Deepfake Technology Complete Guide to Deepfakes Politics and Social Media", Printed in Great Britain by Amazon, σελ. 14
[55] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[56] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.
[57] Nobert Young "Deepfake Technology Complete Guide to Deepfakes Politics and Social Media", Printed in Great Britain by Amazon, σελ. 14

που δημιουργείται από την τεχνολογία deepfake βελτιώνεται, καθιστώντας το δυσδιάκριτο από το πραγματικό περιεχόμενο.[58]

Ένα deepfake είναι περιεχόμενο, το οποίο είναι αυθεντικό στα μάτια ενός ανθρώπου. Η λέξη deepfake είναι ένας συνδυασμός των λέξεων "deep learning" και "fake" (ένα κράμα δύο ξεχωριστών λέξεων που σημαίνουν «Βαθιά μάθηση» και «Ψεύτικο») και αφορά κυρίως περιεχόμενο που παράγεται από ένα τεχνητό νευρωνικό δίκτυο για τη δημιουργία και την παραποίηση ανθρώπινων εικόνων.[59] Με τα deepfakes δημιουργείται πλαστό περιεχόμενο - συνήθως βίντεο, εικόνων, ήχου ή κειμένου - στο οποίο μεταφέρεται η φωνή, το βίντεο ή η εικόνα ενός ατόμου σε ένα άλλο, ώστε να αντικατοπτρίζεται το αρχικό πρόσωπο, το οποίο συνήθως συμβαίνει χωρίς τη συγκατάθεσή του.[60]

Σύμφωνα με έναν στενό ορισμό, τα deepfakes δημιουργούνται από τεχνικές που μπορούν να τοποθετήσουν το προσώπου ενός ατόμου που θεωρείται στόχος στο πρόσωπο που πρωταγωνιστεί σε ένα βίντεο με σκοπό τη δημιουργία ενός βίντεο με το άτομο-στόχο να κάνει ή να λέει πράγματα που κάνει το άτομο-πηγή. Αυτό αποτελεί μια κατηγορία deepfakes, δηλαδή την ανταλλαγή προσώπων. Σύμφωνα με έναν ευρύτερο ορισμό, τα deepfakes είναι περιεχόμενο που εμπίπτει σε δύο άλλες κατηγορίες, δηλαδή το lip-sync και το puppetmaster. Οι απομιμήσεις με συγχρονισμό χειλιών αναφέρονται σε βίντεο που τροποποιούνται ώστε οι κινήσεις του στόματος να συνάδουν με μια ηχογράφηση. Τα deepfakes του puppetmaster περιλαμβάνουν βίντεο με ένα άτομο-στόχο (μαριονέτα) που ακολουθεί τις εκφράσεις του προσώπου, τις κινήσεις των ματιών και του κεφαλιού ενός άλλου ατόμου (master) που κάθεται μπροστά σε μια κάμερα.[61]

Ενώ ορισμένα deepfakes μπορούν να δημιουργηθούν με παραδοσιακές προσεγγίσεις οπτικών εφέ ή γραφικών υπολογιστών, ο πιο πρόσφατος κοινός μηχανισμός για τη δημιουργία deepfakes είναι τα μοντέλα βαθιάς μάθησης, όπως οι αυτοκωδικοποιητές και τα γεννητικά αντιφατικά δίκτυα (GAN), τα οποία έχουν εφαρμοστεί ευρέως στον τομέα της υπολογιστικής όρασης. Τα μοντέλα αυτά χρησιμοποιούνται για την εξέταση των εκφράσεων και των κινήσεων του προσώπου ενός

[58] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.

[59] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[60] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

[61] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

ατόμου και τη σύνθεση εικόνων προσώπου ενός άλλου ατόμου που κάνει ανάλογες εκφράσεις και κινήσεις.[62]

Το Deepfake χρησιμοποιεί έναν αλγόριθμο που αναφέρεται ως "γενετικό ανταγωνιστικό δίκτυο", κατά το οποίο τοποθετείται μια διαφορετική φωτογραφία πάνω στη φωτογραφία πηγής, μια διαδικασία γνωστή στον ψηφιακό κόσμο των γραφικών ως "Superimposing". Σε άλλες περιπτώσεις, οι φωτογραφίες απλώς συνδυάζονται ή αναμειγνύονται. Στην πραγματικότητα, είναι ένας συνδυασμός δύο αλγορίθμων, του γεννήτορα/κωδικοποιητή («encoder») και του αποκωδικοποιητή («decoder»), οι οποίοι λειτουργούν παράλληλα και οι τεχνολογίες του συνδυάζονται για να παράγουν ένα deepfake. Ο κωδικοποιητής, από τα δεδομένα που εισάγονται στον αλγόριθμο, δημιουργεί ψεύτικα βίντεο κλπ και στη συνέχεια ο αποκωδικοποιητής προσδιορίζει την πρωτοτυπία. Ο κωδικοποιητής, όσο ακόμα ο χρήστης μπορεί να αναγνωρίσει το ψεύτικο, ενημερώνεται για το τι πρέπει να βελτιώσει, ώστε να είναι δύσκολο να αναγνωριστεί το βίντεο ως ψεύτικο. Στην ουσία, όσο πιο εύκολο είναι για κάποιον να διακρίνει τη διαφορά ανάμεσα στο ψεύτικο και το αληθινό, τόσο καλύτερος προσπαθεί να γίνει ο γεννήτορας/κωδικοποιητής στην προσπάθεια να παράγει ένα ψεύτικο και να το παρουσιάσει ως αληθινό.[63]

Οι μέθοδοι Deepfake απαιτούν συνήθως μεγάλο όγκο δεδομένων εικόνας και βίντεο για την εκπαίδευση μοντέλων που δημιουργούν φωτορεαλιστικές εικόνες και βίντεο. Τα δημόσια πρόσωπα, όπως οι διασημότητες και οι πολιτικοί, που έχουν μεγάλο αριθμό βίντεο και εικόνων διαθέσιμων στο διαδίκτυο, αποτελούν τους αρχικούς στόχους των deepfakes. Μέχρι σχετικά πρόσφατα, η χειραγώγηση των μιντια – φωτογραφίες, βίντεο και ήχος – ήταν αρμοδιότητα των ειδικών ή όσων κατέχουν τεράστιες ποσότητες πηγών, όπως μια κυβέρνηση ή ένα στουντιο του Hollywood. Η τεχνολογία όμως πλέον κάνει την ανθρώπινη χειραγώγηση πιο εύκολη και περισσότερο προσβάσιμη στον καθένα.[64]

Σε αντίθεση με άλλες τεχνολογίες όπως το Photoshop που χρειάζεται η καθοδήγηση ενός έμπειρου επαγγελματία, τα Deepfakes χρησιμοποιούν απλά αλγόριθμους μηχανικής μάθησης, χωρίς να χρειάζεται η ικανότητα ενός έμπειρου επαγγελματία. Ακόμη και ένας ερασιτέχνης μπορεί να κάνει το ψεύτικο να μοιάζει με αληθινό. Η τεχνολογία αυτή είναι δωρεάν και άμεσα διαθέσιμη μέσω Διαδικτύου και υπάρχουν όλα τα κατάλληλα εργαλεία. Με ένα καλό σύστημα υπολογιστή, το λογισμικό και τις πληροφορίες για τον τρόπο εκτέλεσης των εναλλαγών και ανταλλαγής

[62] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)
[63] Nobert Young “Deepfake Technology Complete Guide to Deepfakes Politics and Social Media”, Printed in Great Britain by Amazon, σελ. 9, 10, 11
[64] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 25

προσώπου, καθώς και την προσομοίωση ήχου, ο καθένας μπορεί να κατασκευάσει περιεχόμενο με ρεαλιστική εμφάνιση.[65]

Σήμερα η διαδικασία δημιουργίας αυτών των παραποιημένων εικόνων και βίντεο είναι πολύ πιο απλή, καθώς χρειάζεται μόνο μια φωτογραφία ταυτότητας ή ένα σύντομο βίντεο ενός ατόμου-στόχου. Απαιτείται όλο και λιγότερη προσπάθεια για την παραγωγή ενός εντυπωσιακά πειστικού υλικού. Οι πρόσφατες εξελίξεις μπορούν να δημιουργήσουν ένα deepfake ακόμα και με μια απλή ακίνητη εικόνα.[66] Οι υπάρχουσες εικόνες και βίντεο αρκούν για τη δημιουργία πειστικών, εξαιρετικά παραπλανητικών deepfakes, συνθετικών εικόνων και βίντεο, με το συνδυασμό ή την επικάλυψή τους σε εικόνες και βίντεο προέλευσης, τα οποία στη συνέχεια συμβάλλουν στη διάδοση ψευδών ειδήσεων, για κακόβουλες φάρσες, για παραβίαση προσωπικών δεδομένων, δυσφήμιση προσώπων ακόμα και με οικονομικό όφελος και για οικονομική απάτη, μεταξύ άλλων.[67]

### 1.3 ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΛΑΤΦΟΡΜΩΝ - ΕΦΑΡΜΟΓΩΝ

Δύο από τις πιο υποσχόμενες πλατφόρμες λογισμικού deepfake είναι η «DeepFaceLab» καθώς και η «Face Swap». Οι εφαρμογές αυτές παρέχουν δωρεάν λογισμικό σε όποιον θέλει να δημιουργήσει το συνθετικό του βίντεο. Αυτές οι πλατφόρμες έχουν κάνει διάσημους ανώνυμους YouTubers όπως οι "iFake", "Ctrl Shift Face" και "Shamook". Χρησιμοποιούν το ελεύθερο λογισμικό για κωμικούς σκοπούς, αντικαθιστώντας ηθοποιούς σε εμβληματικές ταινίες του Χόλιγουντ. Σε μια δημιουργία, ο χρήστης Ctrl Shift Face αντικαθιστά τον Macaulay Culkin στο Home Alone με τον Sylvester Stallone, μετονομάζοντάς το σε Home Stallone. Αυτά τα βίντεο είναι πολύ αστεία και έχουν συγκεντρώσει εκατομμύρια προβολές στο YouTube. Υπάρχουν δεκάδες πρώιμα deepfakes του πρωταγωνιστή του Χόλιγουντ Νίκολας Κέιτζ. Χάρη στην ενίοτε υπερβολικά δραματική υποκριτική του, ο Κέιτζ έχει γίνει ένα αγαπημένο διαδικτυακό μιμίδιο. Αυτό έχει οδηγήσει σε ένα κίνημα για την "αλλαγή προσώπου του Νίκολας Κέιτζ σε κάθε ταινία που γυρίστηκε ποτέ".[68]

Η κινεζική εφαρμογή Zao έχει γίνει viral τον τελευταίο καιρό, καθώς οι λιγότερο εξειδικευμένοι χρήστες μπορούν να ανταλλάξουν τα πρόσωπά τους με τα σώματα των αστέρων του κινηματογράφου και να μπουν σε γνωστές ταινίες και τηλεοπτικά κλιπ. Άλλες εφαρμογές είναι η εφαρμογή Face Swap Booth, η οποία χρησιμοποιείται για την ανταλλαγή προσώπων κυρίως με

[65] Nobert Young “Deepfake Technology Complete Guide to Deepfakes Politics and Social Media”, Printed in Great Britain by Amazon, σελ. 9, 10, 11
[66] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)
[67] Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054
[68] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 38, 39

εικόνες διασήμων, ενώ η εφαρμογή Mix Booth εχει διαφορετική λειτουργία από τις άλλες, καθώς αναμειγνύει δύο πρόσωπα σε ένα. [69]

Η εφαρμογή FakeApp, που αναπτύχθηκε από έναν χρήστη του Reddit χρησιμοποιώντας μια δομή ζεύξης αυτόματου κωδικοποιητή-αποκωδικοποιητή, ήταν η πρώτη προσπάθεια δημιουργίας βαθιάς απομίμησης. Ο αυτόματος κωδικοποιητής συλλέγει λανθάνοντα χαρακτηριστικά από εικόνες προσώπου και ο αποκωδικοποιητής ανακατασκευάζει τις εικόνες. Απαιτούνται δύο ζεύγη κωδικοποιητή-αποκωδικοποιητή για την εναλλαγή των προσώπων μεταξύ των εικόνων πηγής και στόχου- οι παράμετροι του κωδικοποιητή μοιράζονται μεταξύ των δύο ζευγών δικτύων και κάθε ζεύγος χρησιμοποιείται για την εκπαίδευση σε μια συλλογή εικόνων. Τα δίκτυα κωδικοποιητών αυτών των δύο ζευγών είναι πανομοιότυπα.[70]

Η εφαρμογή Cupace έχει τη δυνατότητα "PasteFace", η οποία εξάγει χειροκίνητα τις πλήρεις λεπτομέρειες του προσώπου από εικόνες. Με το Cupace, μπορεί κανείς εύκολα να αφαιρέσει το πρόσωπο από μια εικόνα, να επιλέξει μια άλλη εικόνα και να το τοποθετήσει σε αυτήν. Κάθε πρόσωπο που αφαιρείται αποθηκεύεται στην εφαρμογή και μπορεί να χρησιμοποιηθεί για επικόλληση σε διάφορες εφαρμογές που είναι διαθέσιμες στο Google play store.[71]

Οι χρήστες των social media σίγουρα διατηρούν προφίλ στα μέσα κοινωνικής δικτύωσης Snapchat, Tik Tok και Instagram. Από την πλατφόρμα snapchat ξεκίνησε η χρήση των λεγόμενων φίλτρων και στη συνέχεια η χρήση τους έγινε ευρέως διαδεδομένη, ώστε όλες οι υπόλοιπες εφαρμογές να προσθέσουν τις επιλογές των φίλτρων. Έτσι σήμερα οι περισσότεροι χρήστες των εφαρμογών αυτών έχουν στη διάθεσή τους αναρίθμητα φίλτρα, τα οποία παραποιούν την εικόνα τους ή των φίλων τους σε μια φωτογραφία ή βίντεο.[72]

Στις εφαρμογές αυτές υπάρχει και η δυνατότητα χρήση φίλτρων ανταλλαγής προσώπων, δηλαδή ο κάθε χρήστης μπορεί να ανταλλάξει το πρόσωπό του με αυτό κάποιου φίλου του ή διασήμου, ή και τρίτου. Για να γίνει η ανταλλαγή αυτή πρέπει να εξαχθούν πρόσωπα από φωτογραφίες. Μάλιστα αυτές τις φωτογραφίες ή βίντεο μπορεί κανείς να μοιραστεί με εκατοντάδες άλλους

[69] DeepFake Technology: Complete Guide to Deep Fakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 50,51
[70] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341
[71] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 47,48
[72] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 44

χρήστες των εφαρμογών αυτών, ειδικά στην περίπτωση που το προφίλ του χρήστη είναι δημόσιο και δεν υπάρχει περιορισμός χρηστών που έχουν πρόσβαση στο προφίλ. [73]

Ενώ το Snapchat κατέχει τον τίτλο της πιο δημοφιλούς εφαρμογής ανταλλαγής προσώπων, η εφαρμογή Face Swap Live, η οποία είναι διαθέσιμη μόνο στην Apple, προς το παρόν, κατέχει τον τίτλο της καλύτερης στο παιχνίδι ανταλλαγής προσώπων. Τα χαρακτηριστικά του επιτρέπουν στον χρήστη να ανταλλάσσει πρόσωπα με φίλους σε πραγματικό χρόνο. Αυτό μπορεί να γίνει κοιτώντας και οι δύο ταυτόχρονα στο πλαίσιο της κάμερας, ώστε η εφαρμογή να ανταλλάσσει τα πρόσωπα σε πραγματικό χρόνο.[74]

Αυτές οι πρώτες χρήσεις είναι αθώες και συχνά πραγματικά αστείες, αλλά η πιο διαδεδομένη χρήση της ανταλλαγής προσώπων μέχρι σήμερα είναι η δημιουργία μη συναινετικού βίντεο ερωτικού περιεχομένου.[75] Με την εμπορική ανάπτυξη εφαρμογών τεχνητής νοημοσύνης όπως οι ανωτέρω ή και ηχητικών εφαρμογών deepfake, όπως οι Resemble και Descript, καθώς και με τη χρήση συνθετικού κειμένου, είναι προφανές ότι αναδύονται επιθέσεις που περιλαμβάνουν αναπαραστάσεις και αντικατάσταση εικόνων από ανθρώπους. Αυτές οι μορφές παραποίησης δημιουργούν τεράστια απειλή για την ανθρωπότητα.[76]

Μια πρόσφατη κυκλοφορία ενός λογισμικού που ονομάζεται DeepNude δείχνει πιο ανησυχητικές απειλές, καθώς μπορεί να μεταφέρει τα στοιχεία εμφάνισης ενός ατόμου σε ένα βίντεο ερωτικού περιεχομένου χωρίς συναινέση. Αυτή η εφαρμογή απαγορεύτηκε λόγω της κακόβουλης λειτουργίας της. Ήταν ικανό να δημιουργεί ψεύτικες, γυμνές εικόνες των γυναικών των οποίων τις φωτογραφίες συνέλαβε. Δεν ήταν προσβάσιμο σε χρήστες Android, μόνο στα Windows και το Linux. Η εφαρμογή εφαρμόστηκε μόνο σε εικόνες γυναικών, ενώ δεν είναι πλέον διαθέσιμη.[77]

## 1.4. DEEPFAKE TECHNOLOGY - ΕΝΑ ΑΜΦΙΛΕΓΟΜΕΝΟ ΘΕΜΑ - ΟΦΕΛΟΣ Η ΑΠΕΙΛΗ ΓΙΑ ΤΗΝ ΚΟΙΝΩΝΙΑ

Τα deepfakes είναι βαθιά αμφιλεγόμενα - από τη μία πλευρά, υπονομεύουν την εμπιστοσύνη μας στο περιεχόμενο, και από την άλλη, ανοίγουν νέες δημιουργικές ευκαιρίες. Από μια απλή αναζήτηση στο Reddit σύμφωνα με μια έρευνα του 2022, προέκυψε ότι για τα έτη 2018 με 2021 βρέθηκαν 6.638 αναρτήσεις και 86.425 σχόλια που αναφέρονταν στις ανησυχίες σχετικά με την αξιοπιστία των deepfakes και τον περιορισμό τους από τις πλατφόρμες. Διαπιστώθηκε ότι οι

[73] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 44
[74] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 48,49
[75] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 39
[76] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.
[77] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 51,52

συζητήσεις στο Reddit ήταν υπέρ των deepfake και της δημιουργίας μιας κοινότητας που υποστηρίζει τη δημιουργία και την ανταλλαγή deepfake video και τη δημιουργία μιας αγοράς, ανεξάρτητα από τις συνέπειες.[78] Με την αρχική, αυστηρή έννοια, τα deepfakes διαδίδονται κυρίως με κακόβουλη πρόθεση, αν και τώρα χρησιμοποιούνται συχνά και για θετικές εφαρμογές. Οι ειδικοί εκτιμούν ότι έως το 2026 το 90 % του διαδικτυακού περιεχομένου μπορεί να είναι συνθετικά παραγόμενο.[79]

Η τεχνολογία deepfake έχει θετικές επιπτώσεις σε πολλούς τομείς, ενώ χάρη στην ανάπτυξη της τεχνητής νοημοσύνης έχουν δημιουργηθεί χρήσιμες και παραγωγικές εφαρμογές που πλέον είναι προσιτές σε όλους, όπως οι εφαρμογές στα οπτικά εφέ, τα ψηφιακά avatars, τα φίλτρα του Snapchat, η δημιουργία φωνών όσων έχουν χάσει τις δικές τους ή η ενημέρωση επεισοδίων ταινιών χωρίς νέα γυρίσματα.[80] Τα deepfakes και η καλοπροαίρετη χρήση τους θα τονώσει τους τομείς της διαφήμισης μόδας και της παραγωγής ταινιών, της φωτογραφίας, των βιντεοπαιχνιδιών, της εικονικής πραγματικότητας, των κινηματογραφικών παραγωγών και της ψυχαγωγίας.[81]

Ένα βασικό μέρος όπου έχουμε συνηθίσει να βλέπουμε επεξεργασμένο ήχο και βίντεο είναι οι ταινίες, τις οποίες αντιλαμβανόμαστε ως "ψεύτικες". Αν και τα πιο ισχυρά εργαλεία παρέμειναν στα χέρια των καλά εφοδιασμένων, όπως τα κινηματογραφικά στούντιο με προϋπολογισμούς πολλών εκατομμυρίων δολαρίων και ομάδες εμπειρογνωμόνων, πλέον υπάρχει πλήθος εμπορικών εφαρμογών και λογισμικού που χάρη στην AI έχουν κάνει την επεξεργασία βίντεο και τα ειδικά εφέ πιο προσιτά σε όλους και έχουν βελτιώσει τα εργαλεία που μέχρι πρότινος προορίζονταν για τα blockbusters του Χόλιγουντ.[82]

Χαρακτηριστικό παράδειγμα αποτελεί η ταινία The Irishman του 2019, όπου ο σκηνοθέτης Μάρτιν Σκορτσέζε χρησιμοποίησε μέρος του προϋπολογισμού των 140 εκατομμυρίων δολαρίων για να προσλάβει μια ομάδα ειδικών για να "κάνει πιο νέους" τους ηθοποιούς του χρησιμοποιώντας εφέ και υπολογιστικές μεθόδους. Τρεις μήνες μετά την κυκλοφορία της ταινίας, ένα κλιπ εμφανίστηκε στο YouTube με τίτλο "The Irishman De-Aging: Netflix Millions VS. Free Software!" Ένας ανώνυμος YouTuber με το όνομα "iFake" χρησιμοποίησε δωρεάν λογισμικό τεχνητής νοημοσύνης για να αντιμετωπίσει το πρόβλημα που ταλαιπώρησε τον Σκορτσέζε και το αποτέλεσμα μέσα σε πολύ λίγο χρόνο ήταν εξαιρετικό. Ο προϋπολογισμός του YouTuber ήταν μηδενικός και δούλευε

[78] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446

[79] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

[80] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

[81] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 12

[82] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 31

μόνος του. Ομολογουμένως, ο YouTuber δεν δούλευε από το μηδέν, αφού χρησιμοποίησε έτοιμο υλικό. Ωστόσο, το παράδειγμα αυτό αποτελεί μια πρώιμη ένδειξη της δύναμης των συνθετικών μέσων. Η παραγωγή του Σκορτσέζε ξεκίνησε το 2015, είχε εκατομμύρια δολάρια και μια ομάδα των καλύτερων ειδικών. Τον Δεκέμβριο του 2019, νικήθηκε από έναν μοναχικό YouTuber που χρησιμοποιούσε ελεύθερο λογισμικό. Τι συνέβη στην ανάπτυξη της τεχνητής νοημοσύνης για να γίνει αυτό εφικτό;[83]

Μπορούμε, επομένως, να φανταστούμε τι μπορούν τα deepfake να προσφέρουν στη βιομηχανία ταινιών. Νεκροί ηθοποιοί και μεγάλα ονόματα αυτών μπορούν να αναστηθούν και να παίξουν ξανά στη μεγάλη οθόνη, χωρίς να χρειάζεται οι σκηνές σε ταινίες να ξαναγυριστούν, κάτι που είναι ιδιαίτερα χρήσιμο για τη διατήρηση ταινιών που έχουν μείνει στην ιστορία (Westerlund, 2019). Τέτοιο παράδειγμα αποτελεί και το μουσείο Σαλβαντόρ Νταλί στη Φλόριντα που χρησιμοποίησε την ΤΝ για να επαναφέρει τον ζωγράφο στη ζωή σε ένα συνθετικό βίντεο που ο ζωγράφος καλωσόριζε τους επισκέπτες στο μουσείο.[84]

Λόγω της τεχνολογίας deepfake, οι άνθρωποι μπορούν να επιλέγουν τη μόδα τους πιο γρήγορα, γεγονός που ωφελεί τις βιομηχανίες μόδας και ηλεκτρονικού εμπορίου. Στον κόσμο της μόδας τα δίκτυα αυτά μπορούν να δημιουργήσουν εικονικά μοντέλα σε διάφορες πόζες με διάφορα ρούχα, ενώ μπορεί ο καθένας να δοκιμάζει εικονικά το ρούχο κατά τη διάρκεια αγορών. [85]

Επιπλέον, η τεχνολογία αυτή βοηθά τις επιχειρήσεις ψυχαγωγίας, καθώς τα συνθετικά βίντεο μπορούν να παίξουν δραματικό ρόλο και στα παιχνίδια, όπου για παράδειγμα στη FIFA οι παίκτες μπορούν να φαίνονται πραγματικά σαν αληθινοί,[86] ενώ πλήθος εφαρμογών δίνει τη δυνατότητα δημιουργίας ψυχαγωγικών μουσικών βίντεο ή memes, όπως τα βίντεο που κυκλοφόρησαν και έγιναν viral με τον ηθοποιό Nicolas Cage. [87]

Αλλά και στον τομέα της ιατρικής, η τεχνολογία Deepfake μπορεί δυνητικά να επιτρέψει στους ασθενείς με Αλτσχάιμερ να επικοινωνούν με μια νεότερη εκδοχή του εαυτού τους, γεγονός που μπορεί να τους βοηθήσει να διατηρήσουν τις αναμνήσεις τους.[88] Η τεχνολογία αυτή μπορεί επίσης

[83] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 32
[84] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 46
[85] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341
[86] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 47
[87] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
[88] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341

να χρησιμοποιηθεί για τη δημιουργία φωνών και προσωπικοτήτων βασισμένων στην τεχνητή νοημοσύνη για να βοηθήσουν τα τυφλά άτομα.[89]

Ωστόσο, παρά τις θετικές εφαρμογές των deepfakes, η τεχνολογία είναι διαβόητη για τις ανήθικες και κακόβουλες πτυχές της.[90] Παρά τα πλεονεκτήματα, η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί από τον οποιονδήποτε κακόβουλο χρήστη του Internet με πρόσβαση σε εργαλεία της Τεχνητής Νοημοσύνης ως όπλο. Δυστυχώς, ο αριθμός των κακόβουλων χρήσεων των deepfakes υπερτερεί σε μεγάλο βαθμό του αριθμού των θετικών χρήσεων. Η ανάπτυξη προηγμένων βαθιών νευρωνικών δικτύων και η τεράστια ποσότητα δεδομένων που διατίθεται συμβάλλουν στη δημιουργία πλαστών εικόνων και βίντεο που είναι σχεδόν δυσδιάκριτα για τους ανθρώπους, ακόμα και για τους πιο εξελιγμένους αλγόριθμους υπολογιστών.[91] Λόγω της προόδου και του εκδημοκρατισμού των εργαλείων ΤΝ, αναδύεται και η καθημερινή χρήση τέτοιων τεχνολογιών σε οικιακό επίπεδο, η οποία επηρεάζει όλο και περισσότερο την κοινωνία μας. Παρόλο που η βαθιά μάθηση που παράγει το deepfake είναι ευέλικτη και θα μπορούσε να είναι χρήσιμη για την επανάσταση σε διάφορους κλάδους, όπως αναφέρθηκαν ανωτέρω, τα αρνητικά περιστατικά εγείρουν συλλογικά ανησυχίες για τα κοινωνικά προβλήματα που προκύπτουν. [92]

Τα Deepfake είναι πολύ γνωστά στον ψηφιακό κόσμο επειδή η αξιοποίηση της καταστροφικής τους δύναμης χρησιμοποιείται για τη δημιουργία σκανδάλων, παραπληροφόρησης και διάδοσης κακόβουλων ειδήσεων. Η παραπληροφόρηση διαδίδεται με σκοπό την εξαπάτηση. Τα εργαλεία των εκστρατειών παραπληροφόρησης μπορεί να περιλαμβάνουν deepfakes, παραποιημένες φωτογραφίες, παραποιημένους ιστότοπους και άλλες πληροφορίες που έχουν αφαιρεθεί από τα συμφραζόμενα για να εξαπατήσουν το κοινό.[93] Τα deepfakes μπορούν να αποτελέσουν απειλή για να εξαπατηθούν φυσικά ή και νομικά πρόσωπα και να δυσφημιστεί η εικόνα δημοσίων προσώπων. Οι ερευνητές αναφέρουν ότι τα deepfakes θα έχουν επιπτώσεις στη νομοθεσία και στους κανονισμούς, στην πολιτική, στην παραγωγή των μέσων ενημέρωσης, στο κοινό τους και στις

[89] Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054

[90] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[91] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

[92] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.

[93] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

γενικότερες αλληλεπιδράσεις στα μέσα ενημέρωσης και στην κοινωνία, δημιουργώντας αρκετές ηθικές επιπτώσεις.[94]

Τα deepfakes μπορούν να βλάψουν τα θύματά τους εξαπατώντας ή εκφοβίζοντάς τους, προκαλώντας ζημιά στη φήμη τους και γενικότερα υπονομεύοντας τις κοινωνικές αξίες, δηλαδή την εμπιστοσύνη σε θεσμούς και άτομα. Η χρήση αυτής της τεχνολογίας μπορεί να αποβεί επιζήμια για τη δημοκρατία με τη διάδοση πολιτικής παραπληροφόρησης, να υπονομεύσει την εθνική και διεθνή ασφάλεια με την ανταλλαγή μη συναινετικού συνθετικού περιεχομένου και να περιπλέξει την επιβολή του νόμου. Συνολικά, σημαντικές έρευνες έχουν επισημάνει ότι τα deepfakes είναι πιθανό να επιτεθούν κυρίως στους τομείς της πολιτικής παραπληροφόρησης και της πορνογραφίας.[95]

Η ευκολία και η προσβασιμότητα των deepfakes έχουν ανοίξει μια νέα σφαίρα επιθέσεων κοινωνικής μηχανικής για τις οποίες τα σημερινά συστήματα κυβερνοασφάλειας μπορεί να μην είναι προετοιμασμένα. Δεδομένου ότι τα πάντα συμβαίνουν σε κανάλια πληροφοριών, όπως τα μέσα κοινωνικής δικτύωσης και τα μηνύματα ηλεκτρονικού ταχυδρομείου, δεν χρειάζεται να έχει κανείς ειδικές δεξιότητες hacking για να αναπτύξει επιθέσεις κυβερνοασφάλειας με βάση τα deepfakes. Οι επιτιθέμενοι μπορούν να δημιουργήσουν εξαιρετικά επιζήμια βίντεο και κλιπ ήχου και να αποσπάσουν χρήματα, δεδομένα ή και τα δύο. Το Deepfake ransomware είναι από τους πιο επίφοβους φορείς κυβερνοεπιθέσεων τον τελευταίο καιρό.[96]

Η ύπαρξη της τεχνολογίας deepfake χρησιμοποιείται ήδη για την αποσταθεροποίηση του κοινού δημόσιου λόγου και την υπονόμευση των πολιτικών αντιπάλων, της αλήθειας και της εμπιστοσύνης. Είναι απειλή για την παγκόσμια ασφάλεια τα deepfake βίντεο παγκόσμιων ηγετών με ψεύτικες ομιλίες για παραπλανητικούς σκοπούς.[97] Τα deepfakes μπορούν να προκαλέσουν πολιτικές ή θρησκευτικές εντάσεις μεταξύ χωρών, να ξεγελάσουν το κοινό και να επηρεάσουν τα αποτελέσματα σε προεκλογικές εκστρατείες ή να δημιουργήσουν χάος στις χρηματοπιστωτικές αγορές δημιουργώντας ψεύτικες ειδήσεις. Μπορούν να χρησιμοποιηθούν ακόμη και για τη δημιουργία ψεύτικων δορυφορικών εικόνων της Γης που περιέχουν αντικείμενα που δεν υπάρχουν στην πραγματικότητα για να μπερδέψουν τους στρατιωτικούς αναλυτές, π.χ. δημιουργώντας μια ψεύτικη γέφυρα σε ένα ποτάμι, παρόλο που δεν υπάρχει τέτοια γέφυρα στην πραγματικότητα.

[94] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 8,9, 10
[95] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446
[96] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.
[97] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 130

Αυτό μπορεί να παραπλανήσει ένα στράτευμα που έχει καθοδηγηθεί να διασχίσει τη γέφυρα σε μια μάχη.[98]

Για παράδειγμα, πριν από την εισβολή της Ρωσίας στην Ουκρανία το 2022, οι Ηνωμένες Πολιτείες αποκάλυψαν μια ρωσική συνωμοσία για τη χρήση deepfake βίντεο για να δικαιολογήσουν την εισβολή στην Ουκρανία. Αφού έγινε η εισβολή, αξιωματούχοι της ουκρανικής κυβέρνησης προειδοποίησαν ότι η Ρωσία ενδέχεται να διαδώσει ψεύτικα βίντεο που θα δείχνουν τον Ουκρανό πρόεδρο Βολοντίμιρ Ζελένσκι να παραδίδεται. Ο φόβος αυτός φαίνεται να έγινε πραγματικότητα αφού χάκερς ανάγκασαν έναν ουκρανικό ειδησεογραφικό ιστότοπο να προβάλει ένα βίντεο με τον πρόεδρο Ζελένσκι να λέει στους στρατιώτες του να παραδοθούν. Τη στιγμή που γράφονται αυτές οι γραμμές, πολλά είναι ακόμη ασαφή σχετικά με το βίντεο και δεν έχει επαληθευτεί ότι πρόκειται για πραγματικό deepfake ή άλλο ψεύτικο, αλλά δείχνει πώς η χρήση των (deep)fakes χρησιμοποιείται για σκοπούς παραπληροφόρησης.[99]

Ωστόσο, οι εκθέσεις για την ασφάλεια στον κυβερνοχώρο το 2019 προβλέπουν ότι το 96% των deepfakes αναφέρονταν στην πορνογραφία.[100] Η πρώτη και πιο κακόβουλη χρήση είναι το "deepfake porn", το οποίο είναι έμφυλο φαινόμενο, καθώς στρέφεται κατά κύριο λόγο εναντίον των γυναικών. Τα deepfakes είναι η τελευταία εξέλιξη του μη συναινετικού και ψεύτικου βίντεο ερωτικού περιεχομένου που στοχεύει ακόμα και απλές καθημερινές γυναίκες και όχι μόνο διάσημες. Το φαινόμενο του μη συναινετικού βίντεο ερωτικού περιεχομένου κατέστρεψε και καταστρέφει ακόμα ζωές. Όποια κι αν είναι η μορφή της, όπως το revenge porn ή το sex extortion, η έκθεση, ο εξευτελισμός και ο φόβος που συνοδεύουν την στοχοποίηση με αυτόν τον τρόπο καταστρέφουν τα θύματα, τα οποία δυσκολεύονται να συνδεθούν στο διαδίκτυο και να αισθάνονται ασφαλείς. Πρόκειται για εισβολή στην πιο προσωπική τους ζωή και στο δικαίωμα στην ασφάλεια.[101]

Τα δημόσια πρόσωπα, καλλιτέχνες, αθλητές και πολιτικοί, είναι τα χειρότερα θύματα των deepfakes, καθώς διαθέτουν σημαντικό αριθμό βίντεο και φωτογραφιών στο διαδίκτυο. Οι φωνές και τα πρόσωπα πολλών γνωστών προσώπων έχουν "μεταμοσχευθεί" στα σώματα μοντέλων της

[98] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)
[99] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
[100] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446
[101] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 155

βιομηχανίας ερωτικών ταινιών χωρίς φυσικά τη συγκατάθεσή τους και οι εικόνες αυτές είναι ευρέως διαθέσιμες στο Διαδίκτυο.[102]

Οποιοδήποτε μη συναινετικό πορνό, είτε είναι ψεύτικο είτε όχι, είτε είναι υψηλής τεχνολογίας είτε όχι, είναι τρομακτικό, ντροπιαστικό και εξευτελιστικό για τα θύματά του. Δεν είναι σαφές με τι τρόπο και κατά πόσο μπορούν πραγματικά τα θύματα να προστατευτούν.[103] Αν και οι πλατφόρμες κοινωνικής δικτύωσης απαγορεύουν αναρτήσεις που αφορούν σε deepfake βίντεο ή εικόνες λόγω παραβίασης των κανόνων της πλατφόρμας, οι κοινότητες του Reddit βοηθούν στην ανάκτησή τους σε οποιαδήποτε μορφή, καθώς χρησιμεύουν ως αρχείο για τα deepfakes.[104] Αυτό ισχύει ακόμη και για τα πιο πλούσια και με τα καλύτερα μέσα θύματα, όπως η Σκάρλετ Γιόχανσον. Σε συνέντευξή της το 2018, δήλωσε στην εφημερίδα Washington Post ότι δεν υπάρχει ουσιαστικά τίποτα που να μπορεί να κάνει η ίδια ή η ομάδα της γι' αυτό, επειδή είναι αδύνατο να αφαιρεθεί αυτό το είδος περιεχομένου. «Κάθε χώρα έχει τα δικά της νομικά δεδομένα σχετικά με το δικαίωμα στην εικόνα σας. Έτσι, ενώ έχετε τη δυνατότητα να καταργήσετε ιστοτόπους στις ΗΠΑ που χρησιμοποιούν το πρόσωπό σας, οι ίδιοι κανόνες μπορεί να μην ισχύουν στη Γερμανία»Φ", είπε και προειδοποίησε ότι σύντομα ο καθένας θα μπορούσε να γίνει στόχος.[105]

Το Cloud Computing - Υπολογιστικό Νέφος θα μπορούσε να αναφερθεί ως ένα εξαιρετικά επιτυχημένο παράδειγμα προσανατολισμένων υπηρεσιών πληροφορικής. Το Υπολογιστικό Νέφος έφερε μια νέα επανάσταση στον τρόπο με τον οποίο χρησιμοποιείται η υπολογιστική υποδομή, και επιπλέον θα μπορούσε να επεκταθεί στη Βάση Δεδομένων ως Υπηρεσία ή ως μέσο Αποθήκευσης. Επιπλέον, λόγω της μοναδικής χρήσης του περιβάλλοντος του νέφους, οι πάροχοι και οι πελάτες του υπολογιστικού νέφους επιθυμούν να μοιραστούν την ευθύνη για την ασφάλεια και την ιδιωτικότητα σε περιβάλλοντα υπολογιστικού νέφους- με τον περιορισμό, ωστόσο, ότι τα επίπεδα μοιράσματος θα διαφέρουν για διαφορετικά μοντέλα παράδοσης, τα οποία επιδρούν στην επεκτασιμότητα του νέφους.[106] Το απόρρητο των δεδομένων είναι σημαντικό και αποτελεί ένα από τα κύρια εμπόδια που περιορίζουν τους καταναλωτές από το να υιοθετήσουν το υπολογιστικό νέφος. Τα δεδομένα των χρηστών που είναι αποθηκευμένα στο νέφος μπορεί να περιλαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου, φορολογικές αναφορές, προσωπικές εικόνες, αναφορές μισθών και υγείας κ.λπ. και μπορεί να περιέχουν ευαίσθητες πληροφορίες. Ως εκ τούτου, οι

[102] Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341

[103] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 42

[104] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446

[105] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 43

[106] Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2022). InFeMo: Flexible Big Data Management Through a Federated Cloud System. In ACM Transactions on Internet Technology (Vol. 22, Issue 2, pp. 1–22). Association for Computing Machinery (ACM). https://doi.org/10.1145/3426972

καταναλωτές δεν μπορούν να αντέξουν οποιαδήποτε διαρροή απορρήτου, καθώς μπορεί να οδηγήσει σε οικονομικές απώλειες και νομικά ζητήματα. Η Ευρωπαϊκή Ένωση έχει ψηφίσει ορισμένους νόμους για τον χειρισμό των δεδομένων, σύμφωνα με τους οποίους οι διακομιστές αποθήκευσης δεδομένων πρέπει να βρίσκονται στις χώρες αυτές προκειμένου να παρέχεται επαρκής προστασία. Επιπλέον, σε ορισμένες περιπτώσεις πρέπει να είναι γνωστή η θέση αποθήκευσης των δεδομένων. Ωστόσο, αυτό δεν είναι πάντα εφικτό σε ένα περιβάλλον νέφους λόγω της απουσίας προτύπων.[107] Τι συμβαίνει λοιπόν όταν ένας κακόβουλος χρήστης χρησιμοποιεί το νέφος ως χώρο αποθήκευσης παράνομων βίντεο deepfake, στο οποίο κανείς άλλος εκτός από αυτόν δεν έχει πρόσβαση; Αυτό σημαίνει πρακτικά ότι ακόμα και αν γίνουν ενέργειες και αφαιρεθεί το deepfake από το διαδίκτυο ο χρήστης αυτός μπορεί να αναρτά ξανά και ξανά το κακόβουλο δεδομένο.

Τα Deepfakes μετατρέπουν τη μυθοπλασία σε πραγματικότητα. Ο ανθρώπινος εγκέφαλος συνδέει αυτό που τα μάτια βλέπουν ως απόδειξη για κάτι αληθινό. Το επακόλουθο αυτού είναι ότι υπάρχει μια γενική μείωση της εμπιστοσύνης για όλα τα βίντεο που προβάλλονται τώρα, επειδή το ευρύ κοινό δεν ξέρει πια τι να πιστέψει εάν τα βίντεο που παρακολουθεί είναι αληθινά ή τελικά ψεύτικα.[108]

Το επιχειρηματικό μοντέλο των σημερινών πλατφορμών βασίζεται στο περιεχόμενο και χρησιμοποιεί κίνητρα για να αυξάνονται οι προβολές και τα likes. Πλατφόρμες όπως το Facebook, το TikTok, το Twitter, το YouTube ή το Reddit λόγω των σημαντικών χρηματικών κινήτρων, προωθούν δραματικά ή σοκαριστικά βίντεο, όπου πιθανά deepfakes μπορεί να τραβήξουν την προσοχή του κοινού. Παρόλο που ορισμένες έρευνες δείχνουν ότι η αυξημένη διάδοση των deepfake βίντεο θα κάνει τελικά τους ανθρώπους να συνειδητοποιήσουν καλύτερα ότι δεν πρέπει πάντα να πιστεύουν αυτό που βλέπουν, είναι απαραίτητη η διεξαγωγή μεγάλης εμπειρικής έρευνας για την κατανόηση του αντίκτυπου και την εκτίμηση της πιθανής ζημίας, όπου απαιτούνται παρεμβάσεις πριν τα deepfake προκαλέσουν βλάβη.[109]

Τα deepfakes εκτείνονται πέρα από την απλή χειραγώγηση των μέσων ενημέρωσης. Επειδή μπορούν να δημιουργηθούν από το μηδέν με βάση εκπαιδευτικά δεδομένα, δίνουν στους εγκληματίες και τους απατεώνες τη δυνατότητα να κλέψουν και να χρησιμοποιήσουν

[107] Christos Stergiou and Kostas E. Psannis, Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey, International Journal of Network Management, doi: 10.1002/nem.1930 May 2016
[108] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 13, 14
[109] Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446

αποτελεσματικά τα βιομετρικά μας στοιχεία: μπορούν να πάρουν την εικόνα και τη φωνή μας για να κάνουν και να πουν πράγματα που δεν συνέβησαν ποτέ.[110]

Είμαστε όλοι πιθανοί στόχοι. Αν είστε παραγωγικός χρήστης των μέσων κοινωνικής δικτύωσης, το περιεχόμενό σας είναι διαθέσιμο για όλους. Ακόμα και αν δεν είστε χρήστης των μέσων κοινωνικής δικτύωσης, μπορεί να εμφανιστείτε σε περιεχόμενο που δημοσιεύεται από τα άτομα της οικογένειας ή τους φίλους. Μπορεί να έχετε κινηματογραφηθεί ή φωτογραφηθεί σε επαγγελματικό περιβάλλον. Το τηλέφωνό σας μπορεί να έχει παραβιαστεί και ιδιωτικές φωτογραφίες και βίντεο να έχουν κλαπεί για να δημιουργηθεί ένα deepfake. Δεν είναι υπερβολή να πούμε ότι αν έχετε ποτέ καταγραφεί σε οποιαδήποτε μορφή οπτικοακουστικής τεκμηρίωσης, είτε πρόκειται για φωτογραφία, είτε για βίντεο, είτε για ηχογράφηση, τότε θεωρητικά θα μπορούσατε να είστε θύμα μιας απάτης deepfake.[111]

Παρά την αυξανόμενη επικράτησή τους, μια βρετανική έρευνα του 2019 έδειξε ότι σχεδόν το 72% των ανθρώπων δεν γνώριζαν τα deepfakes και τον αντίκτυπό τους. Αυτό είναι ιδιαίτερα ανησυχητικό, καθώς οι άνθρωποι ενδέχεται να μην είναι σε θέση να αναγνωρίσουν τις βαθιές απομιμήσεις (βίντεο, φωτογραφίες, ηχητικά), καθώς δεν γνωρίζουν την ύπαρξη τέτοιων εικονικών πλαστογραφιών ή τον τρόπο λειτουργίας τους. Η έλλειψη κατανόησης των βασικών αρχών αυτής της τεχνολογίας δημιουργεί διάφορες προκλήσεις, ορισμένες από τις οποίες είναι σχετικές με την επιβολή του νόμου (όπως η παραπληροφόρηση και η απάτη με έγγραφα). Ακόμα πιο ανησυχητικά αποτελέσματα από πρόσφατα πειράματα έδειξαν ότι η αύξηση της ευαισθητοποίησης σχετικά με τα deepfakes μπορεί να μην βελτιώσει τις πιθανότητες των ανθρώπων να τα εντοπίσουν. Ως εκ τούτου, οι ερευνητές αναμένουν ότι οι εγκληματίες θα αυξήσουν τη χρήση των deepfakes τα επόμενα χρόνια. Αυτό δείχνει ότι είναι ζωτικής σημασίας να κατανοήσουμε την απειλή deepfake και να προετοιμαστούμε.[112]

# 2. ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

## 2.1 ΕΝΝΟΙΑ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ - ΟΡΙΣΜΟΙ

Η Τεχνητή Νοημοσύνη - ΤΝ (Artificial Intelligence – AI) είναι μια πτυχή της επιστήμης των υπολογιστών που εξελίσσεται συνεχώς. Έχει υιοθετήσει πολλές τεχνικές και ιδέες από άλλες επιστήμες όπως τα μαθηματικά, τη μηχανική, τη φιλοσοφία, τη τεχνολογία πληροφοριών, τη γλωσσολογία, τη ψυχολογία και φυσικά την επιστήμη των υπολογιστών. Η έρευνα στον τομέα αυτό αφορά τη μηχανική μάθηση, τη βέλτιστη επίλυση προβλημάτων, την απόδειξη θεωρημάτων, τους ευφυείς πράκτορες (agents), τη ρομποτική, τα έμπειρα συστήματα, τη μηχανική όραση κ.α..

[110] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 141
[111] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 149
[112] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

Συχνά επιστήμονες και εκτός της πληροφορικής προσφεύγουν στην τεχνολογία αυτή με σκοπό να βρουν τρόπους αυτοματοποίησης της εργασίας τους. Τεράστια άλματα έχουν γίνει στον τομέα της πληροφορικής, του προγραμματισμού και της επικοινωνίας χάριν αυτής της καινοτομίας. [113, 114]

Οι μηχανές που μας έχει προσφέρει η σημερινή τεχνολογία έχουν μόνο την ικανότητα να αποθηκεύσουν και να προσπελάσουν τεράστιο όγκο πληροφοριών σε ελάχιστο χρόνο. Όμως ακόμα δεν είναι ικανές να λειτουργούν χωρίς ειδικές γνώσεις και να δίνουν λύση όχι μόνο σε αριθμητικά αλλά και σε καθημερινά και δύσκολα προβλήματα, προσαρμόζοντας τις ανάγκες του χρήστη και μαθαίνοντας από τα σφάλματά τους. Με τις θεωρίες, μεθόδους και τεχνολογίες της τεχνητής νοημοσύνης αναπτύσσονται έξυπνες μηχανές που σκέφτονται και δουλεύουν όπως οι άνθρωποι, ενσωματώνονται δηλαδή σε ένα σύστημα υπολογιστή τα κύρια χαρακτηριστικά της ανθρώπινης νοημοσύνης, ώστε με τη χρήση ευφυών και γρήγορων αλγορίθμων τα συστήματα να επιλύουν προβλήματα χωρίς την ανθρώπινη επέμβαση. Όπως οι άνθρωποι βρίσκουν λύσεις σε γρίφους και χρησιμοποιούν τη λογική για να εξάγουν συμπεράσματα από παρατηρήσεις, έτσι και η τεχνητή νοημοσύνη, χάρη σε ορισμένους αλγόριθμους που έχουν προγραμματιστεί για να μιμούνται αυτές τις ανθρώπινες γνωστικές λειτουργίες, μπορεί να κάνει το ίδιο πράγμα.[115, 116]

Η τεχνητή νοημοσύνη βασίζεται σε ένα σύνολο προγραμματισμένων εντολών που εκτελεί ένας υπολογιστής. Αυτοί οι αλγόριθμοι είναι προγραμματισμένοι να μαθαίνουν από τις πληροφορίες που έχουν συγκεντρωθεί. Η τεχνητή νοημοσύνη εξάγει συμπεράσματα και λαμβάνει αποφάσεις από μια συλλογή προηγούμενων περιστατικών και δεδομένων.[117]

Ένας ορισμός της ΤΝ θα μπορούσε να είναι ο εξής: *«ΤΝ είναι ο τομέας της Επιστήμης των Υπολογιστών που ασχολείται με τη σχεδίαση και την υλοποίηση προγραμμάτων τα οποία είναι ικανά να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες, εμφανίζοντας έτσι χαρακτηριστικά που αποδίδουμε συνήθως σε ανθρώπινη συμπεριφορά, όπως για παράδειγμα η επίλυση προβλημάτων, η αντίληψη μέσω της όρασης, η μάθηση, η εξαγωγή συμπερασμάτων, η κατανόηση φυσικής γλώσσας, κτλ.»*[118] Σύμφωνα με τους Barr και Feigenbaum *«ΤΝ είναι ο τομέας της επιστήμης των υπολογιστών, που ασχολείται με τη σχεδίαση ευφυών (νοημόνων) υπολογιστικών συστημάτων, δηλαδή συστημάτων που επιδεικνύουν χαρακτηριστικά που σχετίζονται με τη νοημοσύνη στην ανθρώπινη*

[113] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 1, 4, 7
[114] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 53
[115] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 4, 5
[116] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 53, 80
[117] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 53, 80
[118] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 4

*συμπεριφορά»*.[119] Για να προσδιορίσουμε ένα «νοήμον» υπολογιστικό σύστημα πρέπει πρώτα να ορίσουμε τη «νοημοσύνη».[120] Το ερμηνευτικό λεξικό του Cambridge αναφέρει στον όρο νοημοσύνη *«η ικανότητα για μάθηση, κατανόηση και κρίση ή αιτιολογημένη έκφραση γνώμης»*. [121]

Σύμφωνα με τους Russell & Norvig *«οι ορισμοί της ΤΝ ταξινομούνται σε τέσσερις μεγάλες κατηγορίες: συστήματα τα οποία σκέφτονται όπως οι άνθρωποι, συστήματα τα οποία σκέφτονται λογικά, συστήματα τα οποία συμπεριφέρονται όπως οι άνθρωποι και τέλος, συστήματα τα οποία αντιδρούν λογικά. Επιπλέον, υποστηρίζουν ότι ένας ευφυής πράκτορας (intelligent agent) είναι οτιδήποτε μπορεί να αντιλαμβάνεται το περιβάλλον του μέσω αισθητήρων και επενεργεί σε αυτό το περιβάλλον μέσω μηχανισμών δράσης.»* [122]

Η τεχνητή νοημοσύνη διαφέρει από την νοημοσύνη του ανθρώπου διότι στηρίζεται σε άλλους μηχανισμούς, οι οποίοι αντιμετωπίζοντας το ίδιο πρόβλημα διαφορετικά ο καθένας καταλήγουν σε διαφορετικές λύσεις. Ο πατέρας της ΤΝ Alan Turing (1912-1954), κατά το έτος 1950 εφηύρε μία δοκιμασία η οποία ονομάστηκε Turing test - δοκιμασία Turing και σχετίζεται με την αδυναμία να διακρίνει κανείς τον άνθρωπο από τη μηχανή και να χαρακτηρίσει μια μηχανή ως ευφυή. Μέσω ερωτήσεων που υποβάλλονται από τον άνθρωπο εξεταστή αν ο υπολογιστής δεν μπορεί να ξεχωρίσει αν οι απαντήσεις είναι ανθρώπινες ή μη τότε πετυχαίνει στη δοκιμασία και χαρακτηρίζεται ως ευφυής. Μέχρι σήμερα η δοκιμασία Turing χρησιμοποιείται ως μια καλή διαδικασία για να ξεχωρίσει η φυσική από την τεχνητή νοημοσύνη. [123]

Η ΤΝ μπορεί να διακριθεί σε κλασσική ή συμβολική τεχνητή νοημοσύνη (symbolic AI), όπου με τη χρήση συμβόλων που αναπαριστούν μια έννοια ή μια σχέση μεταξύ εννοιών η ΤΝ στοχεύει στην κατανόηση και στην προσομοίωση της ανθρώπινης νοημοσύνης μέσω αλγορίθμων (πχ. Λογική, κανόνες, πλαίσια κλπ.). Υπολογιστική Νοημοσύνη (computational intelligence) ή συνδετική (connectionist) ή μη συμβολική τεχνητή νοημοσύνη (non symbolic AI), όπου η νοημοσύνη αυτή μιμείται βιολογικές διεργασίες όπως το πως λειτουργεί ο ανθρώπινος εγκέφαλος. Τέλος μπορεί να διακριθεί σε ισχυρή, να χρησιμοποιείται δηλαδή σε γενικές εργασίες χωρίς να περιορίζεται, ή σε αδύναμη, να αναπτύσσεται και να προγραμματίζεται για μια συγκεκριμένη

[119] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 1
[120] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 1
[121] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 2
[122] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 31 - 35
[123] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 32 - 33

εργασία. Η ευφυΐα ή η ικανότητα μάθησης των αλγορίθμων περιορίζεται στα δεδομένα που τροφοδοτούνται σε αυτούς τους αλγορίθμους κατά την εκπαίδευση.[124]

## 2.2 ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

Η τεχνητή νοημοσύνη δεν εμφανίστηκε στον 21ο αιώνα, όπως πολλοί νομίζουν,[125] αλλά έχει συμπληρώσει ήδη μισό αιώνα ζωής και εξακολουθεί ακόμα να αποτελεί ένα σταθερό εξελισσόμενο και μοντέρνο πεδίο έρευνας.[126]

Η πρώτη προσέγγιση από τις πολλές, έγινε στην αρχαία Ελλάδα, από τον Αριστοτέλη (384-322π.Χ.), ο οποίος πρώτος έκανε προσπάθεια για την υπαγωγή της ανθρώπινης σκέψης σε «κωδικοποιημένη ορθή σκέψη, με σκοπό την εξαγωγή ορθών συμπερασμάτων». Αυτή είναι η αναντίρρητη διαδικασία συλλογισμού, όπου οι «συλλογισμοί», χρησιμοποιώντας υποδείγματα εκφράσεων, μπορούν από σωστές υποθέσεις να εξάγουν πάντα ορθά συμπεράσματα. Αυτοί οι κανόνες του Αριστοτέλη με τους οποίους περιγραφόταν η διαδικασία της σκέψης, ήταν η βάση της έρευνας της «λογικής». [127] Στα Ηθικά Νικομάχεια ο Αριστοτέλης επεξηγεί περισσότερο τη συλλογιστική του περιγράφοντας έναν αλγόριθμο, ο οποίος μετά από 2300 χρόνια χρησιμοποιήθηκε από τους Newell και Simon για τη δημιουργία του προγράμματος GPS. [128]

Η αναντίρρητη διαδικασία συλλογισμού εφαρμόστηκε και στην Τεχνητή Νοημοσύνη. Με τη χρήση αλγορίθμων σχεδιάστηκαν έξυπνα υπολογιστικά συστήματα, τα οποία διαθέτουν χαρακτηριστικά που προσομοιάζουν στην ανθρώπινη συμπεριφορά και έχουν σχέση με την ανθρώπινη νοημοσύνη. Με την εξέλιξη του διαδικτύου, την εδραίωση των υπολογιστικών συστημάτων, την ραγδαία εξάπλωση της πληροφορίας, την επεξεργασία δεδομένων μεγάλης κλίμακας (big data) και ακόμα και με την καθημερινή χρήση συσκευών στις οποίες περιλαμβάνονται, δημιουργήθηκε ένα καινούργιο περιβάλλον πληροφορικής, στο πλαίσιο του οποίου αναπτύχθηκε η Τεχνητή Νοημοσύνη και εξελίχθηκε η μηχανική μάθηση.[129]

Η πρώτη προσέγγιση της ΤΝ έγινε από τους Warren McCulloch και Water Pitts το έτος 1943, οι οποίοι πρότειναν ένα μοντέλο τεχνητών νευρώνων, όπου κάθε νευρώνας ενεργοποιούνταν από την επίδραση των γειτονικών νευρώνων τους. Αργότερα το έτος 1951 κατασκευάστηκε ο πρώτος

[124] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 5, 6
[125] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 51,52
[126] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 1, 7
[127] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 7
[128] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 37-38, 49
[129] https://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2021/milosi_2021.pdf

υπολογιστής νευρωνικού δικτύου από τους Marvin Minsky και Dean Edmonds, ο οποίος ονομάστηκε SNARC. [130]

Ως ακαδημαϊκό πεδίο ξεκίνησε το 1956 στο πανεπιστήμιο Dartmouth, όταν σε συνάντηση επιστημόνων (John McCarthy, ο Marvin Minsky, ο Claude Shannon και άλλων)[131] υιοθετήθηκε η ονομασία «Τεχνητή Νοημοσύνη» και συνδέθηκε με την αντιγραφή ανθρώπινων λειτουργιών όπως η χρήση γλώσσας με σκοπό τη δημιουργία μηχανών που λειτουργούν αυτόνομα μέσα σε πολύπλοκα, μεταβαλλόμενα περιβάλλοντα. Αργότερα, το έτος 1958 ο John McCarthy όρισε σε ένα υπόμνημα (MIT AI Lab Memo No. 1) τη γλώσσα υψηλού επιπέδου Lisp που έγινε η βασική γλώσσα προγραμματισμού.[132]

Η πρόοδος της ΤΝ έχει περάσει από πολλά στάδια, από περιόδους ανεπαρκής χρηματοδότησης, έντονης κριτικής και απαισιοδοξίας και δυσφήμησής της αλλά και περιόδους ανάκαμψης με επαρκή χρηματοδότηση και καινοτόμες προσεγγίσεις και υπερβολικής προβολής της. Εξαιτίας του βασικού της χαρακτηριστικού ότι δηλαδή ένα μηχάνημα μπορεί να μιμηθεί τον ανθρώπινο νου, δημιουργήθηκαν αντιθέσεις και γεννήθηκαν ηθικά διλήμματα στοχοποιώντας τη ως απειλή για την ανθρωπότητα.[133]

Σημαντική περίοδος για την ΤΝ ήταν η δεκαετία του 1960, όταν το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών παρείχε μεγάλη χρηματοδότηση για ερευνητικούς σκοπούς και ίδρυσε ερευνητικά κέντρα σε διάφορες τοποθεσίες για να επιταχυνθεί η μετάφραση ρωσικών επιστημονικών δημοσιευμάτων λόγω της εκτόξευσης του Sputnik το 1957.[134] Ωστόσο, η αισιοδοξία και ο ενθουσιασμός των ερευνητών σύντομα έδωσε τη θέση τους σε μια περίοδο έντονης κριτικής, καθώς οι υποθέσεις τους δεν πραγματοποιήθηκαν όπως είχαν προβλεφθεί, εξαιτίας κυρίως λόγω του ότι τα συστήματα περιείχαν ελάχιστη γνώση για το πρόβλημα που καλούνταν να λύσουν. Έτσι, η πρόοδος σταμάτησε και η βρετανική και η αμερικανική κυβέρνηση διέκοψαν τη χρηματοδότηση της έρευνας σε όλα τα πανεπιστήμια με την κατάσταση αυτή να συνεχίζεται μέχρι και τη δεκαετία του 1980, όπου έκανε την εμφάνισή της η Αναλυτική Τεχνητή Νοημοσύνη και το πρόγραμμα των Ιαπώνων κατασκευής υπολογιστών 5ης γενεάς, με γλώσσα

[130] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 31 - 35
[131] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 1
[132] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 31 – 35, 49
[133] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 51,52
[134] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 51-53

μηχανής την PROLOG, τα οποία ήταν ικανά να εξάγουν εκατομμύρια λογικά συμπεράσματα το δευτερόλεπτο.[135]

## 2.3 Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΗΜΕΡΑ

Σήμερα, διανύουμε τη μεταμοντέρνα περίοδο της ΤΝ, η οποία διαδραματίζει σημαντικό ρόλο στο νέο περιβάλλον πληροφορίας, βασικά χαρακτηριστικά του οποίου είναι η διεύρυνση του διαδικτύου και η είσοδος των υπολογιστικών συστημάτων σε κάθε συσκευή που χρησιμοποιούμε καθημερινά.[136] Τα τελευταία χρόνια εξελίχθηκαν σημαντικά η ρομποτική, η μηχανική μάθηση και η μηχανική όραση.[137]

Σήμερα συναντούμε έξυπνα συστήματα που βοηθούν το χρήστη σε συγκεκριμένα προγράμματα (όπως το Offlce Assistant) στην αναζήτηση πληροφοριών στο διαδίκτυο, στην αποστολή email, στην τήρηση ραντεβού, στη σύγκριση τιμών προϊόντων κ.ο.κ.. Σε ορισμένες περιπτώσεις μάλιστα έχουν τη δυνατότητα να μιλούν, ενώ γνωστά είναι επίσης τα συστήματα αναγνώρισης φωνής. Οι εταιρείες και οι ιδιώτες χρησιμοποιούν πλέον την τεχνητή νοημοσύνη ως υπηρεσία, δοκιμάζοντάς την σε πολλά επιχειρηματικά σχέδια και συμφέροντα και σε διαφορετικές πλατφόρμες πριν δεσμευτούν σε αυτές.[138]

Η τεχνητή νοημοσύνη έχει χρησιμοποιηθεί σε διάφορους τομείς. Στον τομέα της υγείας και της υγειονομικής περίθαλψης οι εταιρείες και οι υγειονομικές εγκαταστάσεις χρησιμοποιούν πλέον τη μηχανική μάθηση για καλύτερες και ακριβείς διαγνώσεις που δεν μπορούν να επιτευχθούν από τους ανθρώπους. Στόχος είναι η βελτίωση των αποτελεσμάτων των ασθενών με ταυτόχρονη μείωση του κόστους. Μία από τις καλύτερες τεχνολογίες υγείας στον κόσμο σήμερα είναι το IBM Watson, το οποίο απαντά σε ερωτήσεις και διαμορφώνει μια υπόθεση από δεδομένα ασθενών και άλλες διαθέσιμες πηγές. [139]

Η αξιοποίηση των αναδυόμενων τεχνολογιών, όπως η Τεχνητή Νοημοσύνη (AI), το Διαδίκτυο των Πραγμάτων (IoT), η Υπολογιστική Νέφους (CC), η Μηχανική Μάθηση (ML), η Εικονική Πραγματικότητα (VR), η Βαθιά Μάθηση (DL) μαζί με τα δίκτυα πέμπτης γενιάς (5G) θεωρείται

[135] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 53
[136] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 11
[137] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 55
[138] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ. 55
[139] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ 35

επιβεβλημένη στον κλάδο της Ιατρικής [140] και μπορούν να συμβάλουν στην ανίχνευση, διάγνωση και θεραπεία των σημαντικότερων ιατρικών πτυχών, οδηγώντας σε ένα έξυπνο σύστημα υγειονομικής περίθαλψης.[141]

Τα τελευταία χρόνια και ιδιαίτερα στις μέρες μας, έχει σημειωθεί έξαρση ιών που έχουν εξαπλωθεί σε όλο τον κόσμο, με υψηλό ποσοστό θνησιμότητας, όπως ο νέος κορονοϊός. Για την ανάπτυξη νέων θεραπειών κατά των ευρέως διαδεδομένων ιών, η χρήση της ΤΝ και της μηχανικής μάθησης μπορεί να διευκολύνει την αποτελεσματική εικονική εξέταση των εμβολίων με στόχο την εξάλειψη της εξάπλωσης του ιού. Σε διάφορες πτυχές της φαρμακευτικής εξερεύνησης έχουν ήδη χρησιμοποιηθεί με επιτυχία προσεγγίσεις μηχανικής μάθησης, όπως η πρόβλεψη αλληλεπιδράσεων φαρμάκων, η πρόβλεψη συνδυασμών φαρμάκων και η πρόβλεψη τοξικότητας φαρμάκων.[142] Όμως, η ασφάλεια των πληροφοριών στο σύστημα υγειονομικής περίθαλψης είναι πιο κρίσιμη από ποτέ, δεδομένης της διείσδυσης των συσκευών IoT. [143]

Στις επιχειρήσεις εργασίες που προηγουμένως εκτελούνταν από ανθρώπους εκτελούνται πλέον από μηχανές μέσω της αυτοματοποίησης ρομποτικών διαδικασιών. Οι αλγόριθμοι μηχανικής μάθησης βελτιώνουν την εξυπηρέτηση πελατών, ενώ οι ιστότοποι χρησιμοποιούν πλέον το chatbot για να παρέχουν άμεση εξυπηρέτηση στους πελάτες τους χωρίς ανθρώπινη παρέμβαση. Χάρη της ΤΝ παρουσιάζονται νέες επιχειρηματικές ευκαιρίες λόγω της δυνατότητας ανάλυσης μεγάλων και σύνθετων συνόλων δεδομένων. Τα συστήματα είναι ικανά να διεκπεραιώσουν σημαντικές επιχειρηματικές εργασίες ταχύτερα και ακριβέστερα, ενώ η λήψη αποφάσεων και η ροή των εργασιών (work flow) έχει αυτοματοποιηθεί. Για να χρησιμοποιηθεί η ΤΝ στις επιχειρήσεις θα πρέπει οι επιχειρηματικές διαδικασίες να κωδικοποιηθούν, να υφίσταται τεχνική υποδομή στην επιχείρηση που να μπορεί να αποστείλει με ασφάλεια δεδομένα στην εφαρμογή της ΤΝ, οι δραστηριότητες της επιχείρησης να χαρακτηρίζονται ως σύνθετες, να επαναλαμβάνονται και να έχουν βάση τη γνώση (knowledge based). Με αυτό τον τρόπο η ΤΝ μπορεί να διαδραματίσει κυρίαρχο ρόλο και να ενσωματωθεί μέσα στις πλατφόρμες και τις διαδικασίες που ήδη υπάρχουν

[140] Vasileios A. Memos, Georgios Minopoulos, Konstantinos Stergiou, and Kostas E. Psannis, "Internet-of-Things-Enabled Infrastructure Against Infectious Diseases", Vol. 4, No. 2, pp. 20-25, IEEE Internet of Things Magazine, June 2021, https://doi.org/10.1109/IOTM.0001.2100023

[141] Georgios M. Minopoulos, Vasileios A. Memos, Christos L. Stergiou, Konstantinos D. Stergiou, Andreas P. Plageras, Maria P. Koidou, and Konstantinos E. Psannis, "Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System," Applied Sciences, Vol. 12, No. 12, pp. 58-59, June 2022, https://doi.org/10.3390/app12125859

[142] K. D. Stergiou, G. M. Minopoulos, V. A. Memos, C. L. Stergiou, M. P. Koidou, and K. E. Psannis, "A Machine Learning-Based Model for Epidemic Forecasting and Faster Drug Discovery," Applied Sciences, vol. 12, no. 21, p. 10766, Oct. 2022, doi: 10.3390/app122110766.

[143] Vasileios A. Memos, Kostas E. Psannis, Sofoklis Kyriazakos, and Sotirios Goudos, "An Enhanced and Secure Cloud Infrastructure for e-Health Data Transmission", Wireless Personal Communications (WIRE), Vol. 117, pp. 109–127, Springer, 2021, https://doi.org/10.1007/s11277-019-06874-1

στην επιχείρηση. Τέλος, σημαντικό ρόλο διαδραματίζει η επαρκής τεχνογνωσία της επιχείρησης για να μπορούν να λειτουργούν οι εφαρμογές της ΤΝ και να βελτιώνονται συνεχώς.[144]

Η βιομηχανία 4.0 εμπλουτίζει την έννοια του έξυπνου εργοστασίου (ή της έξυπνης βιομηχανίας) με τη σύγκλιση των «κυβερνο-φυσικών συστημάτων» (CPS) με το «Διαδίκτυο των πραγμάτων» (IoT). Επιπλέον, με τη χρήση τεχνολογιών αιχμής, όπως τα ασύρματα δίκτυα αισθητήρων, η τεχνητή νοημοσύνη (AI), η ανάλυση μεγάλων δεδομένων, η υπολογιστική νέφους (CC), η ρομποτική, η νανοτεχνολογία, οι ασύρματες τεχνολογίες πέμπτης και έκτης γενιάς κ.λπ., μπορεί να βελτιώσει τη βιομηχανική νοημοσύνη, δημιουργώντας ένα πλήρως αυτοματοποιημένο βιομηχανικό περιβάλλον για την παραγωγική διαδικασία, το οποίο είναι επίσης γνωστό ως βιομηχανικό IoT (IIoT). Αυτή η αυτοματοποίηση οδηγεί σε έναν βελτιωμένο και γρήγορο κύκλο παραγωγής, εξοικονομώντας παράλληλα χρόνο και αυξάνοντας τα κέρδη της επιχείρησης. Άλλα οφέλη είναι η μεγαλύτερη καινοτομία, η καλύτερη επικοινωνιακή ικανότητα, η βελτιωμένη αποδοτικότητα, η μεγαλύτερη ευελιξία και ευκινησία και η βελτιωμένη εμπειρία των πελατών. Ωστόσο, αυτή η ταχεία βιομηχανική μετάβαση ενέχει κινδύνους όσον αφορά τα θέματα προστασίας της ιδιωτικότητας που προκύπτουν.[145], [146]

Στην εκπαίδευση με την Τεχνητή Νοημοσύνη, οι βαθμολογίες έχουν γίνει αυτόματες, δίνοντας έτσι στους εκπαιδευτικούς επιπλέον χρόνο για να επικεντρωθούν σε άλλες πτυχές. Με την ΤΝ, οι μαθητές μπορούν να διαβάζουν με το δικό τους ρυθμό. Οι καθηγητές της ΤΝ είναι επίσης διαθέσιμοι για να παρέχουν επιπλέον υποστήριξη στους μαθητές και να διασφαλίζουν ότι δεν ξεφεύγουν από την πορεία τους.[147]

Στα οικονομικά, εφαρμογές όπως το Turbo Tax ή το Mint χρησιμοποιούν την ΤΝ για να αποθηκεύουν τα προσωπικά δεδομένα των πελατών τους, τα οποία χρησιμοποιούν για την παροχή εξειδικευμένων οικονομικών συμβουλών. [148]

Στη δικαιοσύνη τις περισσότερες φορές είναι κουραστικό και επαχθές για τους δικηγόρους ή τους επαγγελματίες του δικαίου να περνούν από διάφορα έγγραφα πριν καταλήξουν σε ένα συμπέρασμα ή μια απόφαση. Είναι επομένως πολύ χρήσιμο να αυτοματοποιηθούν οι περισσότερες από αυτές τις διαδικασίες. Πολλές νεοσύστατες επιχειρήσεις σήμερα έχουν ενσωματώσει στους υπολογιστές

[144] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 16, 17
[145] V. Memos, K.E. Psannis, Z. Lv, A Secure Network Model against Bot Attacks in Edge-enabled Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 2022 [doi;10.1109/TII.2022.3162837]
[146] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ 35
[147] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ 84
[148] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ 33

τους βοηθούς ερωτήσεων και απαντήσεων, οι οποίοι μπορούν να προγραμματίζονται από την ταξινόμηση μιας βάσης δεδομένων.[149]

# 3. ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ

## 3.1 ΕΙΣΑΓΩΓΗ ΣΤΗ ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ

Η μηχανική μάθηση (machine learning) πρωτοεμφανίστηκε ως όρος το έτος 1980 και είναι ένας από τους πρώτους τομείς έρευνας της ΤΝ. Η μάθηση είναι το κυριότερο συστατικό για να χαρακτηριστεί μια «οντότητα» ως ευφυής και παίζει σημαντικό ρόλο σε ένα γνωστικό σύστημα (cognitive system). Ως γνωστικό σύστημα χαρακτηρίζεται ένα φυσικό ή τεχνητό σύστημα το οποίο επεξεργάζεται πληροφορίες και έχει την ικανότητα να αντιλαμβάνεται, να μαθαίνει, να συλλογίζεται, να λαμβάνει αποφάσεις, να επικοινωνεί και να δρα. Το χαρακτηριστικό της μάθησης συνδέεται με την ικανότητα συλλογής πληροφοριών από την επικοινωνία του συστήματος με το περιβάλλον που δρα και με την ικανότητα να αυξάνει την απόδοσή του μέσω της επανάληψης.[150]

Σύμφωνα με τους Russel και Norvig *«Για κάθε δυνατή ακολουθία αντιλήψεων, ένας ορθολογικός πράκτορας θα πρέπει να επιλέγει μια ενέργεια που αναμένεται να μεγιστοποιήσει το μέτρο της απόδοσής του, με δεδομένες τις μαρτυρίες που παρέχονται από την ακολουθία αντιλήψεων και την οποιαδήποτε ενσωματωμένη γνώση έχει ο πράκτορας.»* Με άλλα λόγια ένας ορθολογικός πράκτορας πρέπει να συλλέγει πληροφορίες και να μαθαίνει όσο το δυνατόν περισσότερα από όσα είναι σε θέση να αντιληφθεί. Καθώς ο πράκτορας αποκτά πείρα, η γνώση του μπορεί να αλλάζει και να αυξάνεται και η απόδοσή του να βελτιώνεται. [151]

## 3.2 ΟΡΙΣΜΟΣ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ

Για να καταλάβει το περιβάλλον του ο άνθρωπος το παρατηρεί και φτιάχνει ένα μοντέλο (model), μια απλοποιημένη εκδοχή του μέσω της διαδικασίας της επαγωγικής μεθόδου (inductive learning). Τα μοντέλα προσδιορίζουν τα δεδομένα και έχουν τη δυνατότητα να προβλέψουν μια τιμή μεταβλητής και πληροφόρησης γι' αυτά. Επίσης, οργανώνοντας και ομαδοποιώντας τις εμπειρίες και τις παραστάσεις του, ο άνθρωπος δημιουργεί νέες βάσεις, τα πρότυπα (patterns), τα οποία αναφέρονται σε κάποια δεδομένα και έχουν δυνατότητα να πληροφορούν (informative patterns) επειδή αναφέρονται στις σχέσεις μεταξύ των δεδομένων. Κατά αυτόν τον τρόπο, ένα υπολογιστικό σύστημα δημιουργεί από ένα σύνολο δεδομένων μοντέλα και πρότυπα και αυτή η διαδικασία

[149] DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019, σελ 34

[150] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 429, 431, 432

[151] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 68-70

ονομάζεται «μηχανική μάθηση». [152],[153] Έτσι, αναπτύσσονται υπολογιστικά προγράμματα που αναλύουν δεδομένα μέσω της αυτοματοποίησης και όχι με τις γνώσεις ενός χειριστή.[154]

### 3.3 ΕΙΔΗ ΜΗΧΑΝΙΚΗΣ ΜΑΘΗΣΗΣ

Ανάλογα με τη φύση του προβλήματος χρησιμοποιούνται διαφορετικές τεχνικές μηχανικής μάθησης. Στη «μάθηση με επίβλεψη» (supervised learning) ή «μάθηση με παραδείγματα» ή «επιβλεπόμενη μάθηση» (learning from examples), το σύστημα μαθαίνει από ένα σύνολο δεδομένων μια συνάρτηση, η οποία περιγράφει ένα μοντέλο, με τη βοήθεια κάποιου ως «επιβλέποντος», που δίνει μια τιμή εξόδου στην συνάρτηση, για τα δεδομένα που ελέγχονται. [155]

Στη «μάθηση χωρίς επίβλεψη» (unsupervised learning) ή «μάθηση από παρατήρηση» (learning from observation), το σύστημα μόνο του δημιουργεί πρότυπα για να εξεύρει συσχετίσεις σε ένα σύνολο δεδομένων. Στη μη επιβλεπόμενη μάθηση η μάθηση προτύπων εισόδου γίνεται χωρίς να παρέχονται συγκεκριμένες τιμές εξόδου. [156]

Στην ενισχυτική μάθηση (reinforcement learning), το σύστημα αντί να λάβει οδηγίες από τον επιβλέποντα ως προς το τι να κάνει, μαθαίνει από την ενίσχυση. Χωρίς κάποια ανατροφοδότηση το σύστημα δεν μπορεί να ξεχωρίσει το καλό και το κακό για εκείνο. Αυτό το είδος ανατροφοδότησης ονομάζεται ενίσχυση ή ανταμοιβή. Με αυτό τον τρόπο συντελείται η μάθηση μια βέλτιστης πολιτικής για το περιβάλλον που παρατηρεί το σύστημα. [157]

## 4. ΒΑΘΙΑ ΜΑΘΗΣΗ - DEEP LEARNING

Η βαθιά μάθηση (deep learning) είναι μέθοδος μηχανικής μάθησης και στοχεύει να εξάγει σύνθετα και συγκεκριμένα χαρακτηριστικά από δεδομένα, τα οποία χρησιμοποιούνται για να εκπαιδευτούν

---

[152] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 432, 433

[153] Machine Learning - Μηχανική μάθηση - τι είναι; _ CSC - Computer Science Center., Διαθέσιμο: https://www.csc.com.gr/machine-learning%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%BC%CE%AC%CE%B8%CE%B7%CF%83%CE%B7-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9/

[154] Machine Learning - Μηχανική μάθηση - τι είναι; _ CSC - Computer Science Center., Διαθέσιμο: https://www.csc.com.gr/machine-learning%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%BC%CE%AC%CE%B8%CE%B7%CF%83%CE%B7-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9/

[155] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 732

[156] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 732

[157] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 733, 852-853

με τη βοήθεια των νευρωνικών δικτύων (neural network architectures) τα μοντέλα βαθιάς μάθησης, τα οποία περιέχουν πολλαπλά στρώματα (layers). [158]

Η βαθιά μάθηση μελετά τα τεχνητά νευρωνικά δίκτυα και τους αλγορίθμους μηχανικής μάθησης. Αυτά τα βαθιά δίκτυα χρησιμοποιούν πολλά επίπεδα μη γραμμικών μονάδων επεξεργασίας για την εξάγουν και να αλλάξουν χαρακτηριστικά. Κάθε διαδοχικό επίπεδο κάνει χρήση της εξόδου του προηγούμενου επιπέδου ως είσοδο.[159]

Η βαθιά μάθηση αποτελεί μέρος μιας ευρύτερης οικογένειας μεθόδων μηχανικής μάθησης που βασίζονται στην (μη επιβλεπόμενη) εκμάθηση πολλαπλών επιπέδων χαρακτηριστικών ή αναπαραστάσεων δεδομένων. Τα πολλαπλά επίπεδα αναπαραστάσεων αντιστοιχούν σε διαφορετικά επίπεδα αφαίρεσης. [160], [161]

Σε μια απλή περίπτωση, μπορεί να υπάρχουν δύο σύνολα νευρώνων: ένα σύνολο που λαμβάνει ένα σήμα εισόδου και ένα που στέλνει ένα σήμα εξόδου. Όταν το επίπεδο εισόδου λαμβάνει μια είσοδο, μεταβιβάζει μια τροποποιημένη έκδοση της εισόδου στο επόμενο επίπεδο. Σε ένα βαθύ δίκτυο, υπάρχουν πολλά επίπεδα μεταξύ της εισόδου και της εξόδου, επιτρέποντας στον αλγόριθμο να χρησιμοποιεί πολλά επίπεδα επεξεργασίας, τα οποία αποτελούνται από πολλαπλούς γραμμικούς και μη γραμμικούς μετασχηματισμούς.

Η έρευνα σε αυτόν τον τομέα στοχεύει σε καλύτερες αναπαραστάσεις και προσπαθεί να δημιουργήσει μοντέλα που μαθαίνουν αυτές τις αναπαραστάσεις από μεγάλης κλίμακας χωρίς κατηγοριοποίηση δεδομένων. Κάποιες από τις αναπαραστάσεις είναι εμπνευσμένες από επιτεύγματα στην νευρολογία και είναι πρόχειρα βασισμένες σε αντιλήψεις από πληροφορίες διεργασίας και διόδους επικοινωνίας σε ένα νευρικό σύστημα, όπως ο νευρικός προγραμματισμός που προσπαθεί να προσδιορίσει μια σχέση μεταξύ των ποικίλων ερεθισμάτων και των σχετικών νευρικών αποκρίσεων στον εγκέφαλο.

Ποικίλες αρχιτεκτονικές βαθιάς μάθησης όπως τα βαθιά νευρωνικά δίκτυα, συνελικτικά βαθιά νευρωνικά δίκτυα, δίκτυα βαθιάς πεποίθησης και περιοδικά νευρωνικά δίκτυα έχουν εφαρμοστεί στη μηχανική όραση, αυτόματη αναγνώριση φωνής, αναγνώριση ήχου και βιοπληροφορικής. Τα

[158] Nielsen, Michael A. Neural networks and deep learning. Vol. 2018. San Francisco, CA: Determination press, 2015
[159] Ongsulee, Pariwat. "Artificial intelligence, machine learning and deep learning." 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE). IEEE, 2017
[160] Ongsulee, Pariwat. "Artificial intelligence, machine learning and deep learning." 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE). IEEE, 2017
[161] 10 Amazing Examples Of How Deep Learning AI Is Used In Practice. Διαθέσιμο: https://www.forbes.com/sites/bernardmarr/2018/08/20/10-amazing-examples-of-how-deep-learning-ai-isused-in-practice/?sh=12f48535f98a

δίκτυα βαθιάς μάθησης έχουν επιδείξει μια ικανότητα να αποδίδουν καλύτερα άλλους αλγόριθμους μηχανικής μάθησης σε εργασίες όπως αναγνώριση αντικειμένου στο πεδίο της μηχανικής όρασης.

Ενώ στη μηχανική μάθηση προγραμματιστές δημιουργούν τους αλγόριθμους, οι οποίοι παίζουν τον σημαντικό ρόλο στην ανάλυση των δεδομένων και τη μάθηση από αυτά, αντίθετα στη βαθιά γνώση δεν απαιτείται ένας προγραμματιστής για να δίνει εντολές σε σχέση με τα δεδομένα, καθώς αυτά αντλούνται από μεγάλη κλίμακα, η οποία αποτελεί την κύρια πηγή τους. Η εκμάθηση γίνεται με τη χρήση ενός νευρωνικού δικτύου, το οποίο λειτουργεί όπως ο ανθρώπινος εγκέφαλος και δύναται να αναλύει δεδομένα όπως και οι άνθρωποι. [162]

## 5. ΥΠΟΛΟΓΙΣΤΙΚΗ ΝΟΗΜΟΣΥΝΗ (COMPUTATIONAL INTELLIGENCE)

Η υπολογιστική νοημοσύνη (CI) αφορά τα Νευρωνικά δίκτυα (Neural Networks), τη Λογική της Ασάφειας (Fuzzy Systems) και τον Εξελικτικό Υπολογισμό (Evolutionary Computation). Ο κλάδος της υπολογιστικής νοημοσύνης συντίθεται επίσης και από τα Έμπειρα Συστήματα (Expert Systems) και τους Γενετικούς Αλγορίθμους (Genetic Algorithms). [163]

Ωστόσο, με την πάροδο του χρόνου η υπολογιστική νοημοσύνη έχει εξελιχθεί και αφορά και την περιβαλλοντική νοημοσύνη, τα τεχνητά ενδοκρινικά δίκτυα, τα δίκτυα τεχνητών ορμονών κ.α.. Οι μέθοδοι της υπολογιστικής νοημοσύνης αντιγράφουν τον τρόπο σκέψης του ανθρώπου.[164]

## 6. ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ

### 6.1. ΕΙΣΑΓΩΓΗ

Ο ανθρώπινος εγκέφαλος αποτελείται από κύτταρα που ονομάζονται νευρώνες, οι οποίοι έχουν ως βασική λειτουργία τη συλλογή, επεξεργασία και διάδοση ηλεκτρικών σημάτων. Η επεξεργασία των πληροφοριών από τον εγκέφαλο οφείλεται σε δίκτυα νευρώνων. Από αυτά τα δίκτυα και τη λειτουργία τους εμπνεύστηκε η ΤΝ η οποία έχει ως στόχο τη δημιουργία τεχνητών νευρωνικών δικτύων. [165] Η μέθοδος ανάπτυξης εφαρμογών τεχνητής νοημοσύνης με τη χρήση μοντέλων βαθιών νευρωνικών δικτύων ονομάζεται βαθιά μάθηση (deep learning).[166]

Τα νευρωνικά δίκτυα είναι βιολογικά, όταν πρόκειται για ένα τμήμα νευρικού ιστού και τεχνητά όταν πρόκειται για έναν αλγόριθμο προσομοίωσης της λειτουργίας του βιολογικού νευρωνικού δικτύου. Τα δίκτυα αυτά προέκυψαν και δημιουργήθηκαν κατά τις έρευνες στην τεχνητή νοημοσύνη,

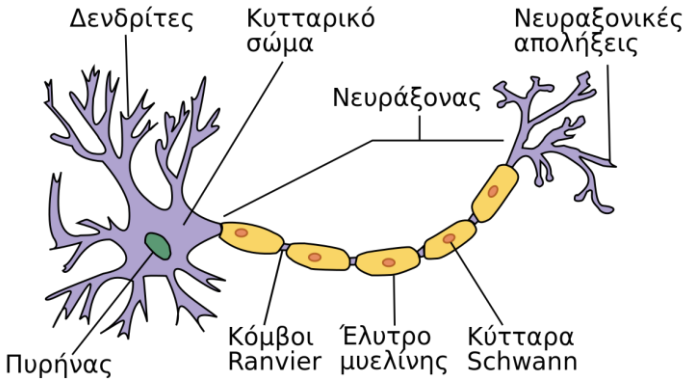
[162] Bhavsar, Hetal, and Amit Ganatra. "A comparative study of training algorithms for supervised machine learning." International Journal of Soft Computing and Engineering (IJSCE) 2.4 (2012): 2231-2307
[163] Engelbrecht, Andries P. Computational intelligence: an introduction. John Wiley & Sons, 2007
[164] Τι είναι η Υπολογιστική Νοημοσύνη; - IEEE Computational Intelligence Society. Διαθέσιμο: https://cis.ieee.org/about/what-is-ci
[165] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 824
[166] Aggarwal, Charu C. Neural networks and deep learning. Springer,, 2018

για να επιλύσουν ένα υπολογιστικό πρόβλημα, μιμούμενα τον τρόπο λειτουργίας των βιολογικών νευρωνικών δικτύων.[167] Τα νευρωνικά δίκτυα αφορούν νοήμον συστήματα τα οποία βασίζονται σε βιολογικά πρότυπα καθώς χρησιμοποιούν διαδικασίες του ανθρώπινου εγκεφάλου.[168]

Αρχικά εμπνευσμένα από τη νευροβιολογία, τα μοντέλα βαθιών νευρωνικών δικτύων έχουν γίνει ένα ισχυρό εργαλείο μηχανικής μάθησης και τεχνητής νοημοσύνης. Μπορούν να προσεγγίσουν συναρτήσεις και δυναμικές μαθαίνοντας από παραδείγματα. Οι επιστήμονες μοντελοποιούν την επεξεργασία πληροφοριών του εγκεφάλου με αλγόριθμους. Ανάμεσα σε αυτά τα μοντέλα προσομοίωσης του ανθρώπινου εγκεφάλου είναι και μια κατηγορία μοντέλων που έχει επικρατήσει να ονομάζεται τεχνητό νευρωνικό δίκτυο.[169]

## 6.2 ΒΙΟΛΟΓΙΚΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ

Ο άνθρωπος έχει την ικανότητα να σκέφτεται, να θυμάται και να λύνει προβλήματα χάριν του εγκεφάλου, δομική μονάδα του οποίου είναι ο νευρώνας (neuron), ο οποίος αποτελείται από επιμέρους συστήματα: το σώμα (body) που είναι ο πυρήνας του, τους δενδρίτες (dendrites), τα σημεία εισόδου του νευρώνα, οι οποίοι αποτελούν το μέσο λήψης σημάτων από γειτονικούς νευρώνες και τον άξονα (axon) που είναι το μέσο σύνδεσης του νευρώνα με άλλους και επομένως το σημείο εξόδου του νευρώνα.[170]

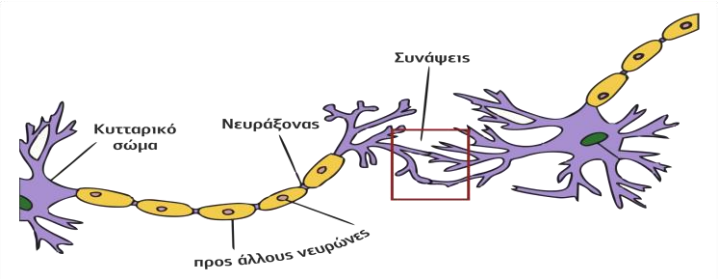



*Σχηματικό διάγραμμα ενός τυπικού νευρώνα*[171]

Σε κάθε δενδρίτη υπάρχει η σύναψη (synapse) σαν κενό, η οποία μέσω χημικών αντιδράσεων μεταβάλλει την αγωγιμότητα του νευρώνα, επιταχύνοντας ή επιβραδύνοντας τη ροή ηλεκτρικών φορτίων προς το σώμα του νευρώνα και σε αυτό οφείλεται η ικανότητα μάθησης και μνήμης που

[167] Kriegeskorte, Nikolaus, and Tal Golan. "Neural network models and deep learning." Current Biology 29.7 (2019): R231-R236.
[168] Anthony, Martin, and Peter L. Bartlett. Neural network learning: Theoretical foundations. Cambridge university press, 2009.
[169] Kriegeskorte, Nikolaus, and Tal Golan. "Neural network models and deep learning." Current Biology 29.7 (2019): R231-R236
[170] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 547, 548
[171] http://repfiles.kallipos.gr/html_books/93/04a-main.html

παρουσιάζει ο εγκέφαλος. Μέσω των δενδριτών τα ηλεκτρικά σήματα συνδυάζονται και το αποτέλεσμα του συνδυασμού αυτού διαδίδεται μέσω του άξονα προς άλλους νευρώνες.[172]




*Φυσικοί διασυνδεδεμένοι νευρώνες*[173]

Η πολυπλοκότητα του εγκεφάλου είναι γνωστή σε όλους και αποτελεί μεγάλη πρόκληση η χαρτογράφησή του και η προσομοίωσή του μέσω υπολογιστικών συστημάτων. Υπολογίζεται ότι στον ανθρώπινο εγκέφαλο υπάρχουν περίπου 100 δισεκατομμύρια νευρώνες κάθε ένας από τους οποίους συνδέεται μέσω του άξονα με περίπου 1000 άλλους δενδρίτες άλλων νευρώνων, και άρα προκύπτουν περίπου 100 τρισεκατομμύρια συνάψεις οι οποίες και επηρεάζουν τη λειτουργία του εγκεφάλου. Επομένως, κάθε προσπάθεια να αντιγραφεί η δομή και η λειτουργία του ανθρώπινου εγκεφάλου σε τέτοιου είδους βελτηνεκούς είναι αδιαμφισβήτητα δύσκολη έως πρακτικά αδύνατη, με αποτέλεσμα να κατασκευάζονται τεχνητοί νευρώνες με πολύ λιγότερες συνάψεις και με περιορισμένη λειτουργικότητα.[174]

### 6.3 Ο ΤΕΧΝΗΤΟΣ ΝΕΥΡΩΝΑΣ

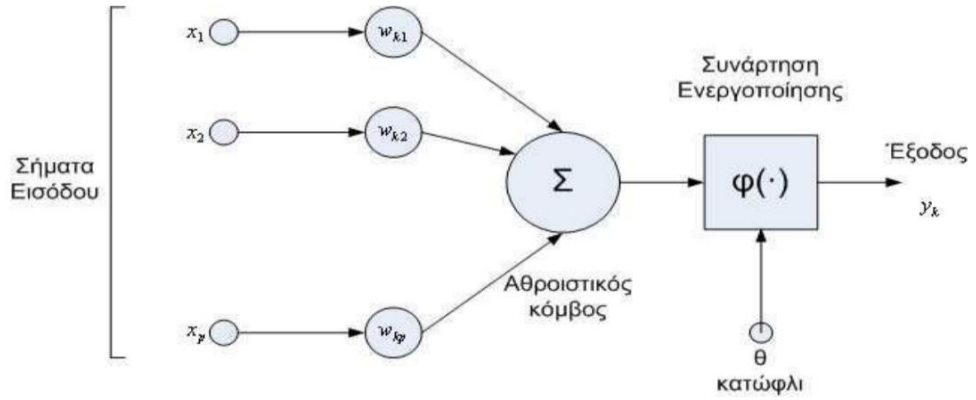
Ο τεχνητός νευρώνας (artificial neuron) είναι ένα σύστημα, τα μέρη του οποίου αντιστοιχίζονται με αυτά του βιολογικού νευρώνα. Ένας τεχνητός νευρώνας δέχεται κάποια σήματα εισόδου, όπως τα ηλεκτρικά φορτία του εγκεφάλου. Σε αντίθεση όμως με τα σήματα του ανθρώπινου εγκεφάλου, τα σήματα εισόδου του τεχνητού νευρώνα αντιστοιχούν σε συνεχείς μεταβλητές, καθεμία από τις οποίες καλείται τιμή βάρους (weight). Η τιμή βάρους μπορεί να έχει θετικό ή αρνητικό πρόσημο και αντιστοιχεί στη σύναψη του βιολογικού νευρώνα, η οποία μεταβάλλει την αγωγιμότητα του βιολογικού νευρώνα.[175]

Το σώμα του τεχνητού νευρώνα χωρίζεται σε δύο μέρη, τον αθροιστή (sum) και τη συνάρτηση ενεργοποίησης (activation function). Ο αθροιστής προσθέτει τα σήματα εισόδου που έχουν μεταβληθεί από τις τιμές βάρους και παράγει την ποσότητα S. Η συνάρτηση ενεργοποίησης είναι ένα φίλτρο διαμόρφωσης της τελικής τιμής του σήματος εξόδου y, σε συνάρτηση με την ποσότητα

[172] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 548
[173] http://repfiles.kallipos.gr/html_books/93/04a-main.html
[174] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 548
[175] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 553

S και την τιμή κατωφλίου της συνάρτησης ενεργοποίησης. Ένας τεχνητός νευρώνας μπορεί να έχει πολλές εξόδους, όμως όλες θα έχουν την ίδια τιμή.[176]

Πολλές φορές, εκτός από τα σήματα εισόδου και τις τιμές βάρους, ο τεχνητός νευρώνας μπορεί να έχει κάποιο βάρος w0, το οποίο ονομάζεται πόλωση (bias) ή παράγοντας προδιάθεσης του νευρώνα και το οποίο επιδρά συνεχώς σε μία τιμή εισόδου χ0=1. Η πόλωση είναι ένα εξωτερικό ερέθισμα του νευρώνα το οποίο προστίθεται μαζί με τα υπόλοιπα σήματα εισόδου.[177]




Η μορφή του τεχνητού νευρώνα (Amit,1989)

## 6.4 ΛΕΙΤΟΥΡΓΙΑ ΤΕΧΝΗΤΟΥ ΝΕΥΡΩΝΙΚΟΥ ΔΙΚΤΥΟΥ

Ο σύνδεσμος από τη μια μονάδα στην άλλη του νευρωνικού δικτύου εξυπηρετεί στη διάδοση ενεργοποίησης, ενώ ένα αριθμητικό βάρος στους συνδέσμους υπολογίζει την ισχύ και καθορίζει το πρόσημο της διασύνδεσης. Κάθε μονάδα πρώτα προσθέτει τις εισόδους της και μετά στο αποτέλεσμα εφαρμόζει μια συνάρτηση ενεργοποίησης για να παράγει την έξοδο. Η συνάρτηση ενεργοποίησης είναι σχεδιασμένη έτσι ώστε όταν η είσοδος είναι σωστή η μονάδα να είναι ενεργή και όταν είναι λανθασμένη να είναι ανενεργή. Δύο επιλογές για τη συνάρτηση ενεργοποίησης είναι η συνάρτηση κατωφλίου ή η σιγμοειδής συνάρτηση. Και οι δύο συναρτήσεις έχουν κατώφλι στο μηδέν. Το βάρος πόλωσης ορίζει το πραγματικό κατώφλι για τη μονάδα. Όταν το άθροισμα των εισόδων υπερβεί το βάρος πόλωσης ενεργοποιείται και η μονάδα. Οι μονάδες με συνάρτηση ενεργοποίησης κατωφλίου μοιάζουν σαν λογικές πύλες, που ενεργοποιούνται αν τους δοθούν τα σωστά βάρη εισόδου και πόλωσης. [178]

[176] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 553
[177] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 553
[178] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 825, 826

Τα τεχνητά νευρωνικά δίκτυα (artificial neural networks) αποτελούνται από τεχνητούς νευρώνες που είναι οργανωμένοι σε μία σειρά από στρώματα ή επίπεδα (layers). Τα επίπεδα αποτελούνται από μονάδες (units) ή κόμβους (nodes) που συνδέονται μεταξύ τους, ώστε να υπάρχουν διάφορες συνδέσεις μεταξύ των μονάδων των διαφόρων επιπέδων. Τα επίπεδα μπορούν να διαφοροποιηθούν ως εξής[179]:

Το πρώτο επίπεδο είναι η είσοδος των δεδομένων (input layer). Τα στοιχεία του δεν είναι νευρώνες, γιατί δεν έχουν βάρη εισόδου ούτε συνάρτηση ενεργοποίησης και δεν εκτελούν κάποιο υπολογισμό. Τα δεδομένα εισόδου λαμβάνονται από τον έξω κόσμο και ο αριθμός των νευρώνων του είναι ίσος με τις μεταβλητές των δεδομένων.[180]

Το επόμενο επίπεδο μπορεί να είναι ένα ή περισσότερα ενδιάμεσα ή κρυφά επίπεδα (hidden layers). Ένα κρυφό επίπεδο είναι η σύνδεση μεταξύ του προηγούμενου με το επόμενο. Ο σχεδιαστής του δικτύου μπορεί να ορίσει και τον αριθμός των κρυφών επιπέδων και ο σκοπός του είναι να μετατρέψει την είσοδο σε κάτι που η μονάδα εξόδου μπορεί να χρησιμοποιήσει με κάποιο τρόπο. Κάθε κρυμμένος νευρώνας συνδέεται πλήρως με κάθε νευρώνα, στο προηγούμενο στρώμα του και στο επόμενο στρώμα (εξόδου).[181]

Ο αριθμός των κρυφών στρωμάτων (hidden layers) σε ένα νευρωνικό δίκτυο παραπέμπει στον όρο deep.[182] Τα βαθιά δίκτυα (deep networks) δύνανται να περιέχουν έως και 150 κρυμμένα στρώματα (hidden layers), σε αντίθεση με τα απλά που περιέχουν δύο με τρία κρυμμένα στρώματα (hidden layers). Ο αυξημένος αριθμός στρωμάτων συνεπάγεται και τον αυξημένο αριθμό των τιμών βαρών του νευρωνικού δικτύου.[183]

Τέλος, το επίπεδο εξόδου (output layer) αποτελεί το τελευταίο επίπεδο του τεχνητού νευρωνικού δικτύου. Σε αυτά εμφανίζονται τα τελικά αποτελέσματα μετά το τέλος της εκμάθησης. Ο αριθμός των νευρώνων του είναι ίσος, με τις πιθανές μεταβλητές εξόδου των αποτελεσμάτων.[184]

Οι νευρώνες μπορεί να είναι πλήρως συνδεδεμένοι (fully connected) όταν υπάρχει σύνδεση μεταξύ όλων των νευρώνων, ενώ σε κάθε άλλη περίπτωση οι νευρώνες είναι μερικώς συνδεδεμένοι

[179] Wang, Sun-Chong. "Artificial neural network." Interdisciplinary computing in java programming. Springer, Boston, MA, 2003. 81-100
[180] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 564
[181]Wang, Sun-Chong. "Artificial neural network." Interdisciplinary computing in java programming. Springer, Boston, MA, 2003. 81-100
[182] Canziani, Alfredo, Adam Paszke, and Eugenio Culurciello. "An analysis of deep neural network models for practical applications." arXiv preprint arXiv:1605.07678 (2016)
[183] Aggarwal, Charu C. Neural networks and deep learning. Springer,, 2018
[184] Wang, Sun-Chong. "Artificial neural network." Interdisciplinary computing in java programming. Springer, Boston, MA, 2003. 81-100

(partially connected), όπως στην περίπτωση στην οποία υπάρχει σύνδεση μεταξύ των νευρώνων των συνεχών επιπέδων μόνο. [185]

## 6.5 ΒΑΣΙΚΕΣ ΜΕΘΟΔΟΙ ΕΚΠΑΙΔΕΥΣΗΣ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΤΝΔ

Οι κύριες λειτουργίες που επιτελούν τα ΤΝΔ είναι η μάθηση και η ανάκληση. Η Μάθηση (learning) ή αλλιώς εκπαίδευση (training) ονομάζεται η διαδικασία κατά την οποία δίνοντας μια συγκεκριμένη τιμή εισόδου έχει ως αποτέλεσμα μια συγκεκριμένη τιμή εξόδου και έτσι μεταβάλλονται οι τιμές των βαρών.[186] Ανάκληση (recall) είναι η διαδικασία υπολογισμού μια τιμής εξόδου για συγκεκριμένη τιμή εισόδου και τιμές βαρών.[187]

Η μέθοδος εκπαίδευσης γίνεται με τη χρήση παραδειγμάτων και ενός αλγορίθμου εκπαίδευσης και η διαδικασία αυτή γίνεται με σκοπό τη βελτίωση της απόδοσης ενός τεχνητού νευρωνικού δικτύου. Ο αλγόριθμος μάθησης εκτελεί επαναληπτικές λειτουργίες. Το σημείο που διαφέρουν είναι η τροποποίηση του δικτύου που εκπαιδεύεται με τις αλλαγές που υφίσταται στις παραμέτρους του λόγω της διέγερσης του δικτύου από το εξωτερικό περιβάλλον.[188]

Η πιο διαδεδομένη μάθηση στις εφαρμογές ΤΝΔ είναι η μάθηση με επίβλεψη (supervised learning), στην οποία εισάγονται στο νευρωνικό δίκτυο ζευγάρια τιμής εισόδου και τιμής επιθυμητής εξόδου. Το δίκτυο παράγει τελικά μια έξοδο διαφορετική από την επιθυμητή τιμή εξόδου και η διαφορά αυτή μεταξύ της παραχθείσας τιμής εξόδου με την επιθυμητή ονομάζεται σφάλμα (error), βάσει της οποίας και με τη βοήθεια ενός αλγορίθμου εκπαίδευσης γίνεται συνήθως η μεταβολή των βαρών. Η μάθηση με επίβλεψη χωρίζεται σε δομική, όπως η αναγνώριση και η κατηγοριοποίηση και σε προσωρινή, όπως είναι η πρόβλεψη και ο έλεγχος.[189]

Στη βαθμολογημένη μάθηση (graded learning) ή ενισχυτική μάθηση (reinforced training) χρησιμοποιείται μια αριθμητική κλίμακα για να χαρακτηριστεί μια έξοδος ως «θετική» ή «αρνητική» ώστε τα βάρη να αλλάζουν με βάση αυτό το πρόσημο.[190]

Τέλος, στη μάθηση χωρίς επίβλεψη (unsupervised learning) το νευρωνικό δίκτυο μπορεί να αυτο-οργανώνεται σύμφωνα με τις τιμές εισόδου μόνο καθώς δεν υπάρχουν αντίστοιχες τιμές εξόδου. Τα

---

[185] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 565

[186] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 551

[187] Zheng, Shuai, Abhinav Vishnu, and Chris Ding. "Accelerating deep learning with shrinkage and recall." 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2016.

[188] Zheng, Shuai, Abhinav Vishnu, and Chris Ding. "Accelerating deep learning with shrinkage and recall." 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2016

[189] Reed, Russell, and Robert J. MarksII. Neural smithing: supervised learning in feedforward artificial neural networks. Mit Press, 1999

[190] Vamvoudakis, Kyriakos G., Frank L. Lewis, and Draguna Vrabie. "Reinforcement Learning with Applications in Automation Decision and Feedback Control." Handbook on Computational Intelligence: Volume 1: Fuzzy Logic, Systems, Artificial Neural Networks, and Learning Systems. 2016. 401-439

σύνολα εισόδων αντιστοιχούν σε έννοιες και χαρακτηριστικά του πραγματικού κόσμου, τα οποία το νευρωνικό δίκτυο καλείται να μάθει να κατηγοριοποιεί, ώστε σε συγκεκριμένα σύνολα να αντιδρά ισχυρά ένας συγκεκριμένος νευρώνας.[191]

## 6.6 ΑΛΓΟΡΙΘΜΟΙ ΜΑΘΗΣΗΣ

Όσον αφορά στο πώς είναι συνδεδεμένες οι μονάδες των τεχνητών νευρωνικών δικτύων μεταξύ τους, υπάρχουν δύο βασικές κατηγορίες τεχνητού νευρωνικού δικτύου: τα μη κυκλικά δίκτυα ή δίκτυα με προς τα εμπρός τροφοδότηση του σήματος και τα κυκλικά ή αναδρομικά δίκτυα.[192] Όταν δεν υπάρχουν συνδέσεις μεταξύ νευρώνων ενός επιπέδου και νευρώνων προηγούμενου επιπέδου (όταν δηλαδή η ροή πληροφορίας είναι πρόσθιας κατεύθυνσης) τα ΤΝΔ χαρακτηρίζονται ως δίκτυα με πρόσθια τροφοδότηση (feedforward). Στην αντίθετη περίπτωση, χαρακτηρίζονται ως δίκτυα με οπίσθια τροφοδότηση (feed backward), καθώς και στην περίπτωση συνδέσεων μεταξύ νευρώνων ίδιου επιπέδου, τα ΤΝΔ χαρακτηρίζονται ως δίκτυα με ανατροφοδότηση (feedback ή recurrent).[193]

### 6.6.1 Νευρωνικά Δίκτυα Πρόσθιας Τροφοδότησης

Στα Τεχνητά Νευρωνικά Δίκτυα πρόσθιας τροφοδότησης (feedforward) η ροή της πληροφορίας μέσα στο δίκτυο είναι μονής κατεύθυνσης. Όπως σε όλα τα ΤΝΔ, έτσι και σε αυτά υπάρχει ένα επίπεδο εισόδου, ένα επίπεδο εξόδου και προαιρετικά, ένα ή περισσότερα ενδιάμεσα, κρυφά επίπεδα. Στα δίκτυα πρόσθετης τροφοδότησης χρησιμοποιούνται μέθοδοι μάθησης με επίβλεψη. Οι μονάδες του ενός επιπέδου τροφοδοτούν τις μονάδες του επόμενου επιπέδου, μέχρι η ροή να φτάσει το τελευταίο επίπεδο. Δηλαδή, δεν υπάρχει έξοδος μονάδας ενός επιπέδου που να αποτελεί είσοδο μονάδας του ίδιου ή προηγούμενων επιπέδου.[194]

### 6.6.2 Perceptron

Το Perceptron είναι ένα δίκτυο πρόσθιας τροφοδότησης χωρίς κρυφά επίπεδα. Στο δίκτυο αυτό όλες οι είσοδοι του είναι άμεσα συνδεδεμένες στις εξόδους. Το perceptron αναπτύχθηκε στη δεκαετία του 1950 από τον Rosenblatt, ενώ εξακολουθεί να υπάρχει μέχρι σήμερα. Η πιο απλή μορφή είναι το στοιχειώδες perceptron (elementary perceptron), το οποίο αποτελείται από έναν και μοναδικό τεχνητό νευρώνα, ο οποίος λειτουργεί με τη βηματική συνάρτηση ενεργοποίησης.[195] Συνήθως το δίκτυο αυτό χρησιμοποιείται στο να διακρίνει τα δεδομένα σε δύο ομάδες. Υπάρχει ένα επίπεδο

[191] Bornholdt, Stefan, and Torsten Röhl. "Self-organized critical neural networks." Physical Review E 67.6 (2003): 066118

[192] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 826

[193] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 826

[194] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 826

[195] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 558

εισόδου (input layer) και ένα επίπεδο εξόδου (output layer), στο τελευταίο να πραγματοποιούνται όλες τις επεξεργασίες.[196] Η διαδικασία εκπαίδευσης είναι επιβλεπόμενη και η μάθηση γίνεται με επίβλεψη από το σφάλμα (error driven). Λειτουργεί με τα σήματα εισόδου (input signals) και από το διάνυσμα των αντίστοιχων «επιθυμητών» αποτελεσμάτων (output signals) τους. Βάσει ενός δυαδικού διανύσματος εισόδου (που αποτελείται δηλαδή από 0 και 1) υπολογίζονται κατάλληλες τιμές βαρών $w_i$ έτσι ώστε να παραχθεί η επιθυμητή έξοδος t. Από το στοιχειώδες perceptron δύναται να αναπτυχθούν βελτιωμένα μοντέλα perceptron που περιλαμβάνουν πολλούς νευρώνες.[197]

### 6.6.3 Κανόνας Δέλτα

Ο κανόνας Δέλτα είναι μια περαιτέρω παραλλαγή του κανόνα του Perceptron και είναι ένας από τους πιο συχνά εφαρμοζόμενους διαθέσιμους τρόπους για την τροποποίηση των δυνάμεων των συνδέσεων εισόδου προκειμένου να μικρύνει η διαφορά μεταξύ της επιθυμητής τιμής εξόδου και της πραγματικής εξόδου του νευρώνα. Το σφάλμα διαδίδεται προς τα πίσω στα προηγούμενα στρώματα ένα στρώμα κάθε φορά. Η διαδικασία οπισθοδιάδοσης των σφαλμάτων του δικτύου συνεχίζεται μέχρι να φτάσει στο πρώτο επίπεδο.[198] Ο αλγόριθμος Δέλτα δεν μπορεί να εφαρμοστεί αυτούσιος σε δίκτυα με κρυφά επίπεδα.[199]

### 6.6.4 Ανάστροφη Μετάδοση Λάθους

Η ανάστροφη μετάδοση λάθους (back propagation) είναι η πιο διαδεδομένη μέθοδος εκπαίδευσης των τεχνητών νευρωνικών δικτύων που αποτελούνται από πολλά επίπεδα. Η μέθοδος αυτή στηρίζεται στον κανόνα Δέλτα που καθορίζει τις τιμές σφάλματος των βαρών του κάθε νευρώνα ακόμα και αυτών που ανήκουν σε κρυφά επίπεδα και δεν γνωρίζουμε την επιθυμητή τιμή εξόδου. Στη διαδικασία εκπαίδευσης αρχικά εισάγονται δεδομένα από κάποια συνάρτηση εκπαίδευσης, οπότε οι νευρώνες στο επίπεδο εισόδου παράγουν κάποιο αποτέλεσμα, το οποίο αποτελεί είσοδο για το επόμενο επίπεδο. Αυτή η διαδικασία είναι επαναλαμβανόμενη μέχρι το τελικό επίπεδο εξόδου και ονομάζεται πρόσθιο πέρασμα (forward pass). Προκειμένου να περιοριστεί το σφάλμα στην έξοδο οι τιμές βαρών που χρησιμοποιεί το δίκτυο για να κάνει υπολογισμούς πρέπει να αναπροσαρμόζονται και σε αυτό χρησιμεύει ο γενικευμένος κανόνας Δέλτα. Το στάδιο αναπροσαρμογής των βαρών

---

[196] Kanal, Laveen N. "Perceptron." Encyclopedia of Computer Science. 2003. 1383-1385.

[197] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 559

[198] M. k. Alsmadi, K. B. Omar, S. A. Noah and I. Almarashdah, "Performance Comparison of Multi-layer Perceptron (Back Propagation, Delta Rule and Perceptron) algorithms in Neural Networks," 2009 IEEE International Advance Computing Conference, 2009, pp. 296-299, doi: 10.1109/IADCC.2009.4809024.

[199] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 562,563

ονομάζεται «ανάστροφο πέρασμα» (backward pass) ή «ανάστροφη μετάδοση» (back propagation).[200], [201]

## 6.7 ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΝΕΥΡΩΝΙΚΩΝ ΔΙΚΤΥΩΝ

### 6.7.1 ΣΥΝΕΛΙΚΤΙΚΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ (CONVOLUTIONAL NEURAL NETWORKS CNN Η CONVNET)

Μια από τις πιο εντυπωσιακές μορφές αρχιτεκτονικής τεχνητών νευρωνικών δικτύων (Artificial Neural Network – ANN) είναι αυτή του Συνελικτικού Νευρωνικού Δικτύου (Convolutional Neural Networks - CNN - ConvNet), τα οποία αποτελούν μια από τις κύριες αρχιτεκτονικές των δικτύων βαθιάς μάθησης (Deep Learning Networks) και είναι από τα πιο γνωστά μοντέλα νευρωνικών δικτύων.[202] Τα CNN χρησιμοποιούνται κυρίως για την επίλυση δύσκολων καθηκόντων αναγνώρισης προτύπων με βάση την εικόνα.[203]

Τα συνελικτικά νευρωνικά δίκτυα (CNN) αποτελούνται από νευρώνες που βελτιώνονται μόνα τους μέσω της μάθησης. Η βασική διαφορά από τα πολυεπίπεδα νευρωνικά δίκτυα τύπου Perceptron, είναι ότι χρησιμοποιούνται κυρίως στον τομέα του εντοπισμού και της αναγνώρισης προτύπων σε εικόνες, οι οποίες είναι και τα δεδομένα εισόδου, σε προβλήματα ανάλυσης και επεξεργασίας εικόνων ή βίντεο, εντοπισμού αντικειμένων σε εικόνες και αποτελούνται από πολλά επίπεδα.[204] Στα δίκτυα αυτά χρησιμοποιείται η μάθηση με επίβλεψη, καθώς εισάγονται εικόνες ως τιμές εισόδου και εξάγονται χαρακτηριστικά απευθείας χωρίς προρύθμιση κατά την ταξινόμηση εικόνων.[205] Τα δίκτυα αυτά δεν χρειάζονται ανθρώπινη επίβλεψη και κατά τη λειτουργία τους ενώνουν μικρά τμήματα πληροφορίας και δημιουργούν από αυτά πληροφορία υψηλότερου επιπέδου.

Υπάρχουν διάφοροι τρόποι που χρησιμοποιούνται για την ταξινόμηση αντικειμένων. Στην εκπαίδευση από την αρχή συγκεντρώνεται από την αρχή ένας μεγάλος όγκος δεδομένων και σχεδιάζεται το μοντέλο και η αρχιτεκτονική του που πρόκειται να μάθει τα χαρακτηριστικά των δεδομένων εισόδου. Αυτή η τεχνική χρησιμοποιείται σε εφαρμογές με μεγάλο αριθμό χαρακτηριστικών εξόδου. Ωστόσο δεν χρησιμοποιείται τόσο συχνά καθώς απαιτεί εξ αρχής μεγάλο όγκο δεδομένων και κρίνεται χρονοβόρα καθώς για να μάθει το μοντέλο τα χαρακτηριστικά εισόδου

[200] M. k. Alsmadi, K. B. Omar, S. A. Noah and I. Almarashdah, "Performance Comparison of Multi-layer Perceptron (Back Propagation, Delta Rule and Perceptron) algorithms in Neural Networks," 2009 IEEE International Advance Computing Conference, 2009, pp. 296-299, doi: 10.1109/IADCC.2009.4809024.
[201] Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ' Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας, σελ. 568, 569, 570
[202] Nielsen, Michael A. Neural networks and deep learning. Vol. 2018. San Francisco, CA: Determination press, 2015
[203] O'Shea, Keiron, and Ryan Nash. "An introduction to convolutional neural networks." arXiv preprint arXiv:1511.08458 (2015).
[204] O'Shea, Keiron, and Ryan Nash. "An introduction to convolutional neural networks." arXiv preprint arXiv:1511.08458 (2015).
[205] Kalchbrenner, Nal, Edward Grefenstette, and Phil Blunsom. "A convolutional neural network for modelling sentences." arXiv preprint arXiv:1404.2188 (2014)

και να εκπαιδευτεί απαιτούνται από ημέρες έως και εβδομάδες ανάλογα με το μέγεθος των δεδομένων.[206]

Η μεταφορά μάθησης (transfer learning), η οποία χρησιμοποιείται από τις περισσότερες εφαρμογές βαθιάς μάθηση, όπως το AlexNet και το GoogleNet, τελειοποιεί το προρυθμισμένο μοντέλο, τροφοδοτώντας το με νέα δεδομένα, ώστε μετά από αλλαγές το δίκτυο να μπορεί να κάνει καινούργια εργασία.[207] Κατά την ταξινόμηση, το δίκτυο μπορεί να κατηγοριοποιήσει συγκεκριμένα αντικείμενα. Το πλεονέκτημα της μεταφοράς μάθησης είναι ότι απαιτεί πολύ λιγότερα δεδομένα και πολύ λιγότερο χρόνο καθώς η διαδικασία διαρκεί λεπτά ή ώρες. Έχει αποδειχθεί ότι η ταυτόχρονη εκμάθηση από πολλαπλά υποκείμενα βελτιώνει σημαντικά την απόδοση των CNN, ενώ παράλληλα μειώνει το μέγεθος του απαιτούμενου συνόλου δεδομένων εκπαίδευσης που συνήθως παρατηρείται στους αλγορίθμους βαθιάς μάθησης. [208]

Μια πιο συγκεκριμένη λειτουργία είναι η εξαγωγή χαρακτηριστικών (feature extractor). Όλα τα επίπεδα του δικτύου μαθαίνουν συγκεκριμένα χαρακτηριστικά από εικόνες, τα οποία αποθηκεύονται με αποτέλεσμα να έχει μειωθεί ο χρόνος εκπαίδευσης των μοντέλων και έτσι η ταξινόμηση δεδομένων μπορεί να διαρκέσει ώρες μόνο.[209]

Κάθε νευρώνας εξακολουθεί να δέχεται μια είσοδο και να εκτελεί μια λειτουργία. Στοιχεία εισόδου αποτελούν ακατέργαστα διανύσματα εικόνων και το επίπεδο εισόδου θα περιέχει τις τιμές των «pixel» της εικόνας. Μέσω μιας ενιαίας συνάρτησης βαθμολογίας, που ονομάζεται βάρος, καταλήγει το δίκτυο στην βαθμολογίας κλάσης, ως έξοδο. Η έξοδος του δικτύου είναι κάποιες αριθμητικές τιμές που ισοδυναμούν με το ενδεχόμενο μια εικόνα (ως στοιχείο εισόδου) να ανήκει σε κάποια κατηγορία ή αλλιώς κλάση. Μια άλλη λειτουργία είναι η επίλυση προβλημάτων ανίχνευσης αντικειμένων. Η έξοδος του δικτύου είναι και πάλι κάποιες αριθμητικές τιμές που υποδεικνύουν το ακριβές σημείο στην εικόνα που μπορεί να βρίσκεται κάποιο αντικείμενο. Μια τρίτη λειτουργία είναι ο συνδυασμός των δύο ανωτέρω προβλημάτων, δηλαδή, η έξοδος του δικτύου μας δείχνει και το σημείο του αντικειμένου και την κατηγορία στην οποία ανήκει η εικόνα.[210]

---

[206] Chaudhari, Poonam, and Himanshu Agarwal. "Progressive review towards deep learning techniques." Proceedings of the International Conference on Data Engineering and Communication Technology. Springer, Singapore, 2017

[207] Chaudhari, Poonam, and Himanshu Agarwal. "Progressive review towards deep learning techniques." Proceedings of the International Conference on Data Engineering and Communication Technology. Springer, Singapore, 2017

[208] U. Côté-Allard et al., "Deep Learning for Electromyographic Hand Gesture Signal Classification Using Transfer Learning," in IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 27, no. 4, pp. 760-771, April 2019, doi: 10.1109/TNSRE.2019.2896269.

[209] Maghrebi, Houssem, Thibault Portigliatti, and Emmanuel Prouff. "Breaking cryptographic implementations using deep learning techniques." International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, Cham, 2016

[210] Kalchbrenner, Nal, Edward Grefenstette, and Phil Blunsom. "A convolutional neural network for modelling sentences." arXiv preprint arXiv:1404.2188 (2014)

Λόγω των εκατοντάδων κρυφών επιπέδων τους μαθαίνουν να εντοπίζουν διαφορετικά χαρακτηριστικά σε μια εικόνα. Όσο πιο πολλά επίπεδα υπάρχουν στο δίκτυο, τόσο πιο πολύπλοκα χαρακτηριστικά ανιχνεύονται σε μια εικόνα.[211] Τα CNN αποτελούνται από τρεις τύπους επιπέδων, τα συνελικτικά στρώματα (convolutional layers), τα στρώματα συγκέντρωσης (pooling layers) και τα πλήρως συνδεδεμένα στρώματα (fully-connected layers).[212]

### 6.7.2 ΑΥΤΟΜΑΤΟΣ ΚΩΔΙΚΟΠΟΙΗΤΗΣ

Οι αυτόματοι κωδικοποιητές είναι απλά κυκλώματα μάθησης που στοχεύουν στη μετατροπή των εισόδων σε εξόδους με τη μικρότερη δυνατή παραμόρφωση. Αν και η έννοια τους είναι απλή, παίζουν σημαντικό ρόλο στη μηχανική μάθηση. Οι αυτόματοι κωδικοποιητές εισήχθησαν για πρώτη φορά τη δεκαετία του 1980 από τον Hinton για να αντιμετωπίσουν το πρόβλημα της «οπισθοδιάδοσης χωρίς δάσκαλο», χρησιμοποιώντας τα δεδομένα εισόδου ως δάσκαλο. Σε ένα νευρωνικό δίκτυο κάθε στρώμα περιλαμβάνει έναν κωδικοποιητή και έναν αποκωδικοποιητή. Ο κωδικοποιητής εξάγει αποτελέσματα υψηλότερου επιπέδου σε σχέση με αυτά των εισόδων, ενώ ο αποκωδικοποιητής ανακτά τα δεδομένα εισόδου από τις προβολές χαμηλής διάστασης ελαχιστοποιώντας την ανακατασκευή. [213]

Ένας αυτόματος κωδικοποιητής είναι ένα μοντέλο μηχανικής μάθησης που μπορεί να χρησιμοποιηθεί για την εκμάθηση αποτελεσματικών αναπαραστάσεων (κωδικοποίηση) από ένα σύνολο δεδομένων και στη συνέχεια, για την ανάκτηση των δεδομένων από αυτές τις κωδικοποιημένες αναπαραστάσεις. Εσωτερικά, ένα κρυφό στρώμα περιγράφει μια κωδικοποίηση διάστασης -h που χρησιμοποιείται για την αναπαράσταση της εισόδου. Μαζί με τη συνάρτηση κωδικοποιητή, μαθαίνεται και ένας αποκωδικοποιητής που παράγει μια ανακατασκευή των δεδομένων εισόδου από το κρυφό στρώμα.[214] Οι βαθιοί αυτόματοι κωδικοποιητές έχουν χρησιμοποιηθεί σε πολλές διαφορετικές εφαρμογές, όπως συμπίεση, αποθορυβοποίηση, μείωση διαστάσεων και εξαγωγή χαρακτηριστικών.[215]

Πιο συγκεκριμένα, είναι ένα τεχνητό νευρωνικό δίκτυο χωρίς επίβλεψη, το οποίο έχει σχεδιαστεί για να ελαχιστοποιεί τα μεγέθη των δεδομένων μαθαίνοντας πώς να αγνοεί το θόρυβο και τις ανωμαλίες στα δεδομένα. Πρώτα συμπιέζει και κωδικοποιεί αποτελεσματικά τα δεδομένα και τα

[211] Kalchbrenner, Nal, Edward Grefenstette, and Phil Blunsom. "A convolutional neural network for modelling sentences." arXiv preprint arXiv:1404.2188 (2014)
[212] O'Shea, Keiron, and Ryan Nash. "An introduction to convolutional neural networks." arXiv preprint arXiv:1511.08458 (2015).
[213] Baldi, Pierre. "Autoencoders, unsupervised learning, and deep architectures." Proceedings of ICML workshop on unsupervised and transfer learning. 2012.
[214] Lerch S, Polsterer KL. Convolutional autoencoders for spatially-informed ensemble post-processing. 2022. Accessed May 22, 2022.
[215] Kong Q, Chiang A, Aguiar AC, Fernández-Godino MG, Myers SC, Lucas DD. Deep Convolutional Autoencoders as Generic Feature Extractors in Seismological Applications. 2021. Accessed May 22, 2022

ανακατασκευάζει από τη μειωμένη κωδικοποιημένη αναπαράσταση για να παράγει μια έξοδο που μοιάζει όσο περισσότερο μπορεί στην αρχική είσοδο. [216]

Οι αυτόματοι κωδικοποιητές αποτελούνται από 4 κύρια μέρη: τον κωδικοποιητή, όπου μαθαίνει πώς να μειώνει τα μεγέθη εισόδου και να συμπιέζει τα δεδομένα εισόδου σε μια κωδικοποιημένη αναπαράσταση, το εμπόδιο (Bottleneck) (πρόκειται για τις χαμηλότερες δυνατές διαστάσεις των δεδομένων εισόδου), τον αποκωδικοποιητή, όπου το μοντέλο μαθαίνει πώς να ανακατασκευάζει τα δεδομένα από την κωδικοποιημένη αναπαράσταση ώστε να είναι όσο το δυνατόν πιο κοντά στην αρχική είσοδο και την απώλεια ανακατασκευής, η οποία είναι η μέθοδος που μετράει πόσο καλά αποδίδει ο αποκωδικοποιητής και πόσο κοντά είναι η έξοδος στην αρχική είσοδο.[217]

Οι αυτόματοι κωδικοποιητές είναι μια κατηγορία τεχνητών νευρωνικών δικτύων που έχουν κερδίσει μεγάλη προσοχή στο πρόσφατο παρελθόν, κυρίως στην ανακατασκευή εικόνων. Τα συνελικτικά νευρωνικά δίκτυα έχουν παρουσιάσει σημαντική βελτίωση σε εργασίες αναγνώρισης και ταξινόμησης αντικειμένων. Μια βελτίωση του αυτόματου κωδικοποιητή είναι ο αυτόματος κωδικοποιητής με συνελικτική διασύνδεση, όπου τα πλήρως συνδεδεμένα στρώματα τροποποιούνται σε συνελικτικά στρώματα. Ο κωδικοποιητής αποτελείται από συνελικτικά στρώματα και ο αποκωδικοποιητής αποτελείται από μετατοπισμένα συνελικτικά στρώματα.[218] Στην πραγματικότητα, διατηρούν τα μεγέθη των εικόνων που εισάγονται και εξάγονται δεδομένα μέσω ενός επιπέδου τη Συνέλιξη (Convolution).[219]

### 6.7.3 ΓΕΝΕΤΙΚΑ ΑΝΤΙΠΑΡΑΘΕΤΙΚΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ (GENERATIVE ADVERSARIAL NEURAL NETWORK - GAN)

Η ιδέα πίσω από τα γενετικά αντιπαραθετικά δίκτυα δημοσιεύτηκε για πρώτη φορά από τον Olli Niemitalo, ωστόσο δεν εφαρμόστηκαν ποτέ και μια παρόμοια ιδέα παρουσιάστηκε από τους Li, Gauci και Gross το 2013. Οι υλοποιήσεις των δικτύων αυτών περιγράφηκαν για πρώτη φορά με επιτυχία το 2014 από τον Ian Goodfellow. Μέχρι το 2017 η χρήση των GANs περιορίζεται μόνο στη βελτίωση εικόνων για τη δημιουργία εικόνων υψηλής ποιότητας. Το 2017 τα GANs χρησιμοποιήθηκαν για πρώτη φορά για τη δημιουργία νέων εικόνων προσώπου και η ιδέα άρχισε να γίνεται περισσότερο γνωστή.[220]

---

[216] Alessandri, Luca, et al. "Sparsely-Connected Autoencoder (SCA) for single cell RNAseq data mining." bioRxiv (2020).
[217] Auto-Encoder: What Is It? And What Is It Used For? (Part 1) | by Will Badr | Towards Data Science https://towardsdatascience.com/auto-encoder-what-is-it-and-what-is-it-used-for-part-1-3e5c6f017726
[218] Nag S. Lookahead optimizer improves the performance of Convolutional Autoencoders for reconstruction of natural images. 2020. Accessed May 22, 2022.
[219] Manakov, Ilja, Markus Rohm, and Volker Tresp. "Walking the Tightrope: investigation of the Convolutional Autoencoder Bottleneck." arXiv preprint arXiv:1911.07460 (2019)
[220] Singh, Simranjeet, Rajneesh Sharma, and Alan F. Smeaton. "Using GANs to Synthesise Minimum Training Data for Deepfake Generation." arXiv preprint arXiv:2011.05421 (2020)

Τα γενετικά αντιπαραθετικά δίκτυα είναι ένα σύστημα που αποτελείται από δύο νευρωνικά δίκτυα (το δίκτυο δημιουργίας και το δίκτυο διακρίσεων) που ανταγωνίζονται μεταξύ τους όπως σε ένα παιχνίδι. Συγκεκριμένα, τα δίκτυα αυτά αποτελούνται από δύο βαθιά νευρωνικά δίκτυα, το γεννήτορα (generator) ή δίκτυο δημιουργίας που δημιουργεί νέα αληθοφανή δεδομένα, τα οποία γίνονται αρνητικά παραδείγματα εκπαίδευσης για τον διευκρινιστή (discriminator) ή δίκτυο διακρίσεων, ο οποίος διαφοροποιεί τα ψεύτικα δεδομένα που παράγει η γεννήτρια από τα πραγματικά. [221]

Στα γενετικά αντιπαραθετικά δίκτυα, το ένα νευρωνικό δίκτυο ο γεννήτορας τροφοδοτείται με τυχαίες εικόνες στην είσοδο και παράγει μία νέα εικόνα. Στη συνέχεια, η δημιουργηθείσα εικόνα καθώς και οι αληθινές εικόνες που εισήχθησαν τροφοδοτούν το δεύτερο νευρωνικό δίκτυο, τον διευκρινιστή, ο οποίος στην πορεία προβλέπει αν η παραγόμενη εικόνα είναι αληθινή ή ψεύτικη. Επομένως, υπάρχει μια διπλή ανατροφοδότηση, καθώς ο γεννήτορας ανατροφοδοτείται με τον διευκρινιστή, ώστε να βελτιώνει τις εικόνες που παράγει και να μπορεί να τον ξεγελάσει και ο διευκρινιστής ανατροφοδοτείται με αληθινές εικόνες για να βελτιώνεται και να μην μπορεί να ξεγελαστεί από τον γεννήτορα. Θα μπορούσε κανείς να πει ότι πρόκειται για έναν αγώνα, όπου κάθε παίκτης είναι είτε ένας διαχωριστής που προσπαθεί να διακρίνει μεταξύ πραγματικών και ψεύτικων δεδομένων είτε μια γεννήτρια που προσπαθεί να ξεγελάσει τους διαχωριστές ώστε να δεχτούν ψεύτικα δεδομένα ως πραγματικά.[222]

## 7. ΒΑΣΙΚΟΣ ΤΡΟΠΟΣ ΥΛΟΠΟΙΗΣΗΣ ΤΩΝ DEEPFAKES

### 7.1 ΛΕΙΤΟΥΡΓΙΑ ΔΙΚΤΥΟΥ DEEPFAKE

Τα deepfakes είναι μια τεχνολογία η οποία χρησιμοποιεί γενετικά αντιπαραθετικά δίκτυα (generative adversarial networks - GAN), τα οποία ανήκουν στην οικογένεια των βαθιών συνελικτικών δικτύων και βασίζονται σε αυτόματους κωδικοποιητές (autoencoder). Τα DeepFakes (συνδυασμός των όρων "deep learning" και "fakes") επιτρέπουν στους επιτιθέμενους ή ακόμη και σε μη τεχνικούς χρήστες μηχανικής μάθησης να τροποποιήσουν μια εικόνα ή ένα βίντεο αντικαθιστώντας το περιεχόμενο και δημιουργώντας μια νέα εικόνα ή βίντεο που δεν μπορεί να διαφοροποιηθεί από ανθρώπους ή υπολογιστές.[223]

---

[221] Overview of GAN Structure | Generative Adversarial Networks | Google Developers https://developers.google.com/machine-learning/gan/gan_structure

[222] Borji, Ali. "Pros and cons of gan evaluation measures." Computer Vision and Image Understanding 179 (2019): 41-65

[223] Asad Malik, Minoru Kuribayashi, Sani M. Abdullahi, Ahmad Neyaz Khan. DeepFake Detection for Human Face Images and Videos: A Survey. IEEE Access. 2022;10:18757-18775. doi:10.1109/ACCESS.2022.3151186

Τα Deepfakes είναι μια μορφή χειραγώγησης βίντεο όπου δύο εκπαιδευμένα δίκτυα αντιπαρατίθενται μεταξύ τους για να δημιουργήσουν μια έξοδο επαρκούς ποιότητας, ώστε να είναι σχεδόν μη αποκρυπτογραφημένη. Λειτουργούν εισάγοντας ένα σύνολο εικόνων ενός υποκειμένου από τις οποίες δημιουργούν ένα μοντέλο του προσώπου και στη συνέχεια τοποθετούν αυτό το μοντέλο προσώπου στο πρόσωπο-στόχο σε ένα αρχικό βίντεο. [224]

Το deepfake είναι ένα πρόγραμμα γενετικού αντιπαραθετικού δικτύου (Generative Adversarial Networks (GAN)) δυνάμει του οποίου είναι δυνατό οι εκφράσεις ενός προσώπου σε μια εικόνα ή σε ένα βίντεο να κωδικοποιηθούν και να μεταφερθούν, με αποτέλεσμα τη δημιουργία ενός νέου προσώπου – μοντέλου σε ένα νέο βίντεο ή σε μια νέα εικόνα. Οι τομείς των ψηφιακών εικόνων προσώπου και του χειρισμού βίντεο παρουσιάζουν κορυφαίο ενδιαφέρον επειδή χρησιμοποιούν τη δύναμη των συνελικτικών νευρωνικών δικτύων, τα οποία είναι σε θέση να παράγουν πολύ ρεαλιστικά αποτελέσματα.[225]

Αυτός ο αλγόριθμος είναι το εργαλείο της τεχνητής νοημοσύνης που χρησιμοποιείται για τη δημιουργία των Deepfakes. Τροφοδοτώντας το σύστημα των γενετικών ανατιπαραθετικών δικτύων με ένα συγκεκριμένο σύνολο δεδομένων εκπαίδευσης, μπορεί να δημιουργηθούν νέα δεδομένα που να αποτελούνται από τα ίδια στατιστικά στοιχεία με τα δεδομένα προέλευσης. Παραδείγματος χάρη, μια εικόνα που εισάγεται ως δεδομένο εκπαίδευσης στα δίκτυα αυτά μπορεί να οδηγήσει τους αλγορίθμους αυτούς να δημιουργήσουν μια νέα εικόνα που με μια πρώτη ματιά θα φαίνεται γνήσια σε όποιον την παρατηρήσει.[226]

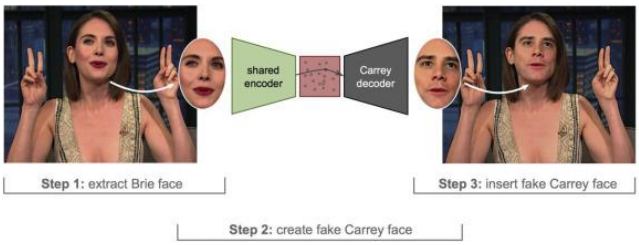
Η αντίστροφη διάδοση κάνει αυτούς τους δύο αλγορίθμους, δηλαδή τη γεννήτρια και τον διευκρινιστή στο γενετικό αντιπαραθετικό δίκτυο του deepfake, να γίνονται καλύτεροι μετά από κάθε «μάχη» μεταξύ τους. Η γεννήτρια γίνεται καλύτερη στο να δημιουργεί κατασκευασμένα δεδομένα που θα μπορούσαν να περάσουν για αληθινά, ενώ ο διαχωριστής γίνεται καλύτερος στο να ανιχνεύει αυτά τα Deepfakes.[227]

Και στην περίπτωση των deepfakes κεντρικό ρόλο παίζει ένας συνελικτικός αυτόματος κωδικοποιητής (Autoencoder). Ο αυτόματος κωδικοποιητής τροφοδοτείται με διαφορετικές εικόνες του προσώπου κάποιου ατόμου. Κάθε φωτογραφία απεικονίζει το ίδιο πρόσωπο αλλά διαφέρουν οι εκφράσεις του, ο φωτισμός, η θέση και η ανάλυση. Ο κωδικοποιητής κωδικοποιεί τα δεδομένα από τις φωτογραφίες με βάση κάποιες παραμέτρους. Στην ουσία τα δεδομένα

[224] Singh, Simranjeet, Rajneesh Sharma, and Alan F. Smeaton. "Using GANs to Synthesise Minimum Training Data for Deepfake Generation." arXiv preprint arXiv:2011.05421 (2020)
[225] Kim, Hyeongwoo, et al. "Deep video portraits." ACM Transactions on Graphics (TOG) 37.4 (2018): 1-14
[226] Borji, Ali. "Pros and cons of gan evaluation measures." Computer Vision and Image Understanding 179 (2019): 41-65
[227] Nobert Young “Deepfake Technology Complete Guide to Deepfakes Politics and Social Media”, Printed in Great Britain by Amazon, σελ. 116

διοχετεύονται στον κωδικοποιητή και κάθε επίπεδο είναι μικρότερο από το προηγούμενο. Κάθε επόμενο επίπεδο περιλαμβάνει δηλαδή λιγότερους νευρώνες σε σχέση με το προηγούμενο. Μετά των κωδικοποιητή σειρά έχει ο αποκωδικοποιητής, ο οποίος αντίθετα από τον κωδικοποιητή ξεκινάει με τα λιγότερα στρώματα (ίδιο αριθμό νευρώνων με το τέλος του κωδικοποιητή) και στη συνέχεια αυτά αυξάνονται σταδιακά χρησιμοποιώντας τα χαρακτηριστικά που κωδικοποίησε ο κωδικοποιητής. Αποτέλεσμα είναι η δημιουργία ενός νέου προσώπου παρόμοιου με του αρχικού.[228]

Το συγκεκριμένο νευρωνικό δίκτυο έχει ως στόχο να δημιουργήσει ένα νέο πρόσωπο, το οποίο να είναι όσο το δυνατό ίδιο με το αρχικό. Πρόκειται δηλαδή για ένα σύστημα συμπίεσης και αποσυμπίεσης δεδομένων, η με άλλα λόγια για ένα νευρωνικό δίκτυο του οποίου ο κωδικοποιητής, αποτελείται από επίπεδα, τα οποία καθρεφτίζονται στα επίπεδα του αποκωδικοποιητή και μέσω μιας συγκεκριμένης εκπαίδευσης τα δεδομένα εικόνας που εισάγονται κωδικοποιούνται, συμπιέζονται και στη συνέχεια αποσυμπιέζονται. Τα κωδικοποιημένα χαρακτηριστικά μιας εικόνας εισόδου από τον κωδικοποιητή, τροφοδοτούν τον αποκωδικοποιητή, ο οποίος στη συνέχεια τα χρησιμοποιεί ώστε να δημιουργήσει μια νέα εικόνα προσώπου όσο το δυνατόν πιο αληθινή και πανομοιότυπη με την αρχική εικόνα εισόδου.[229]




J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600

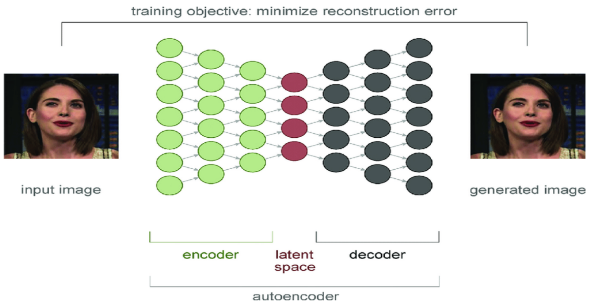
Ένας αυτόματος κωδικοποιητής εκπαιδεύεται να αναγνωρίζει τα βασικά χαρακτηριστικά ενός προσώπου και στη συνέχεια να αναδημιουργεί εικόνες εισόδου ως έξοδο. Η διαδικασία της αναγνώρισης αρχικά ενός συγκριτικά μικρού αριθμού χαρακτηριστικών προσώπου στην είσοδο και στη συνέχεια της δημιουργίας πραγματικών προσώπων ως έξοδο πραγματοποιείται σε τρία επιμέρους τμήματα: στον κωδικοποιητή, στον λανθάνοντα χώρο και στον αποκωδικοποιητή. [230]

Όπως ένας καλλιτέχνης που σχεδιάζει μια εικόνα, έτσι και ο κωδικοποιητής περνάει από μια παρόμοια διαδικασία συμπίεσης. Λαμβάνει δεκάδες χιλιάδες εικονοστοιχεία και τα συμπιέζει σε συνήθως 300 μετρήσεις που σχετίζονται με συγκεκριμένα χαρακτηριστικά του προσώπου.

[228] Mescheder, Lars, Sebastian Nowozin, and Andreas Geiger. "Adversarial variational bayes: Unifying variational autoencoders and generative adversarial networks." arXiv preprint arXiv:1701.04722 (2017)
[229] Li, Kai, et al. "A data-driven approach for facial expression synthesis in video." 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2012
[230] J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600

Κωδικοποιεί αν τα μάτια είναι ανοιχτά ή κλειστά, τη στάση του κεφαλιού, τη συναισθηματική έκφραση, τις εκφράσεις των ματιών, το φως του περιβάλλοντος ή το χρώμα του δέρματος - όλα τα χαρακτηριστικά στα οποία μπορεί να δώσει προσοχή ένας καλλιτέχνης. Η δουλειά ενός επιτυχημένου κωδικοποιητή είναι να μεταφέρει μια εικόνα εισόδου σε αυτές τις 300 μετρήσεις. Για να το θέσουμε διαφορετικά, ο κωδικοποιητής επιτρέπει τη ροή πληροφοριών από μια πολύ λεπτομερή εικόνα εισόδου σε αυτό που είναι γνωστό ως συμπιεσμένη πληροφοριακή συμφόρηση - bottleneck.[231]

Οι λανθάνουσες περιοχές – latent spaces συγκρίνονται συχνά με τα σημεία συμφόρησης πληροφοριών. Για τον αυτόματο κωδικοποιητή, αυτή η συμφόρηση είναι απαραίτητη ώστε το δίκτυο να μπορεί να μάθει πιο γενικά χαρακτηριστικά του προσώπου αντί να απομνημονεύει όλα τα παραδείγματα εισόδου συγκεκριμένων ανθρώπων. Η συμπίεση που επιτυγχάνεται με την κωδικοποίηση μιας εικόνας εισόδου στον λανθάνων χώρο είναι αξιοσημείωτη. Αν ο λανθάνων χώρος αποτελούνταν από 300 μετρήσεις, θα απαιτούσε μόνο το 0,1% της μνήμης που απαιτείται για την αποθήκευση της αρχικής εικόνας εισόδου. Όπως αναφέρθηκε προηγουμένως, ο λανθάνων χώρος αναπαριστά διάφορες πτυχές του προσώπου στο οποίο εκπαιδεύεται. Ένας αυτόματος κωδικοποιητής που εκπαιδεύεται σε εικόνες που δείχνουν το πρόσωπο της Alison Brie, για παράδειγμα, θα μάθει να αντιστοιχίζει μια δεδομένη εικόνα εισόδου της σε έναν λανθάνων χώρο που αντιπροσωπεύει ειδικά την ίδια.[232]




J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600

Ο αποκωδικοποιητής είναι το μονοπάτι από το σημείο συμφόρησης της πληροφορίας μέχρι την έξοδο και αναδημιουργεί μια εικόνα από τον λανθάνοντα χώρο. Ενώ η δουλειά του κωδικοποιητή είναι να συμπιέσει μια εικόνα εισόδου σε ένα σύνολο μόνο 300 μετρήσεων (δηλαδή ένα συγκεκριμένο σημείο στο λανθάνοντα χώρο), ο σκοπός του αποκωδικοποιητή είναι να αποσυμπιέσει αυτές τις πληροφορίες προκειμένου να ανακατασκευάσει μια εικόνα όσο το δυνατόν πιο αληθινή. Στο παράδειγμά μας, η δουλειά του είναι να ανακατασκευάσει την εικόνα εισόδου

[231] J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600
[232] J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600

της Alison Brie από την αναπαράστασή της στον λανθάνοντα χώρο. Η απόδοση ολόκληρου του δικτύου αυτόματου κωδικοποιητή μετριέται από το πόσο μοιάζουν μεταξύ τους οι εικόνες εισόδου και εξόδου.[233]

Ένα deepfake είναι μια εικόνα ή ένα βίντεο που δημιουργείται με τη χειραγώγηση μιας αρχικής εικόνας ή ενός αρχικού βίντεο χρησιμοποιώντας προηγμένες τεχνικές μηχανικής μάθησης. Αυτό περιλαμβάνει την αντικατάσταση του προσώπου ενός ατόμου από μια εικόνα ή ένα βίντεο προέλευσης με το πρόσωπο ενός δεύτερου ατόμου στην εικόνα ή στο βίντεο προορισμού. Ένα μοντέλο του προσώπου του δεύτερου ατόμου, αυτού που τοποθετείται στην εικόνα ή στο βίντεο προορισμού, δημιουργείται με βάση μια τυπικά μεγάλη συλλογή εικόνων προσώπου. Τις πρώτες ημέρες των deepfake βίντεο, οι διασημότητες χρησιμοποιούνταν στα βίντεο προορισμού επειδή είναι εύκολο να βρεις χιλιάδες εικόνες διασημοτήτων από το διαδίκτυο και οι περισσότερες από αυτές τις εικόνες έχουν το θέμα στραμμένο προς την κάμερα. Ο ηθοποιός του Χόλιγουντ Νίκολας Κέιτζ έγινε ακόμη πιο διάσημος, εξαιτίας ενός μοντέλου που βασίστηκε σε φωτογραφίες του προσώπου του και έγινε ένα από τα πρώτα δημόσια διαθέσιμα για τη δημιουργία deepfakes, όταν το ενδιαφέρον ήταν η ποιότητα των παραγόμενων βίντεο και λιγότερο το ποιοι ήταν οι εικονιζόμενοι.[234]

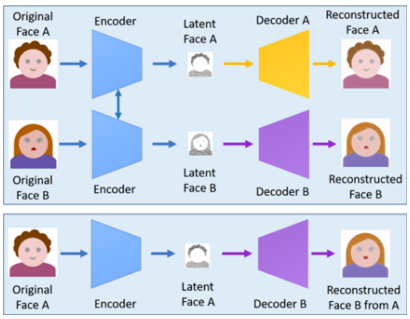
Το πρόβλημα προκύπτει στα μη διάσημα πρόσωπα, καθώς ο αλγόριθμος του deepfake για να λειτουργήσει και να εκπαιδευτεί απαιτεί να τροφοδοτηθεί με πολλά δεδομένα εικόνας ενός προσώπου. Ένα μη διάσημο πρόσωπο συνήθως έχει προσβάσιμο στο κοινό περιορισμένο αριθμό εικόνων του προσώπου του. Μια λύση είναι τα δεδομένα εκπαίδευσης, δηλαδή οι εικόνες του προσώπου, να μπορούν να ληφθούν από μικρά βίντεο κλιπ που έχουν καταγραφεί ειδικά για το σκοπό αυτό. Επιπλέον, απαιτείται να λαμβάνονται υπόψη ως παράμετροι διαφορετικές εκφράσεις του προσώπου του υποκειμένου.[235]

Σε αυτή τη μέθοδο, ο αυτόματος κωδικοποιητής εξάγει λανθάνοντα χαρακτηριστικά των εικόνων προσώπου και ο αποκωδικοποιητής χρησιμοποιείται για την ανακατασκευή των εικόνων προσώπου. Για την ανταλλαγή προσώπων μεταξύ εικόνων πηγής και εικόνων στόχου, χρειάζονται δύο ζεύγη κωδικοποιητών-αποκωδικοποιητών, όπου κάθε ζεύγος χρησιμοποιείται για εκπαίδευση σε ένα σύνολο εικόνων και οι παράμετροι του κωδικοποιητή μοιράζονται μεταξύ των δύο ζευγών δικτύων. Με άλλα λόγια, δύο ζεύγη έχουν το ίδιο δίκτυο κωδικοποιητή. Αυτή η στρατηγική επιτρέπει στον κοινό κωδικοποιητή να βρίσκει και να μαθαίνει την ομοιότητα μεταξύ δύο συνόλων

[233] J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600
[234] Singh, Simranjeet, Rajneesh Sharma, and Alan F. Smeaton. "Using GANs to Synthesise Minimum Training Data for Deepfake Generation." arXiv preprint arXiv:2011.05421 (2020)
[235] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

εικόνων προσώπου, οι οποίες είναι σχετικά απλές, επειδή τα πρόσωπα έχουν συνήθως παρόμοια χαρακτηριστικά, όπως τα μάτια, η μύτη, η θέση του στόματος.[236]

Πιο συγκεκριμένα, όπως φαίνεται στην εικόνα παρακάτω, ένα μοντέλο δημιουργίας deepfake χρησιμοποιεί δύο ζεύγη κωδικοποιητών-αποκωδικοποιητών. Δύο νευρωνικά δίκτυα χρησιμοποιούν τον ίδιο κωδικοποιητή αλλά διαφορετικούς αποκωδικοποιητές για τη διαδικασία εκπαίδευσης. Μια εικόνα του προσώπου Α κωδικοποιείται με τον κοινό κωδικοποιητή και αποκωδικοποιείται με τον αποκωδικοποιητή Β για να δημιουργηθεί μια βαθιά απομίμηση.




Πηγή: Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

Η ανακατασκευασμένη εικόνα στο κάτω μέρος της εικόνας από πάνω είναι το πρόσωπο Β με το σχήμα του στόματος του προσώπου Α. Το πρόσωπο Β έχει αρχικά το στόμα μιας ανάποδης καρδιάς, ενώ το ανακατασκευασμένο πρόσωπο Β έχει το στόμα μιας συμβατικής καρδιάς.

Προσθέτοντας στην αρχιτεκτονική αυτή την αντιφατική απώλεια και την αντιληπτική απώλεια επιτεύχθηκε μια βελτιωμένη έκδοση του deepfakes που βασίζεται στο γενετικό αντιφατικό δίκτυο, δηλαδή το faceswap-GAN. Η αντιληπτική απώλεια κάνει τις κινήσεις των ματιών να είναι πιο ρεαλιστικές και πιο ακριβείς με τα πρόσωπα εισόδου και εξομαλύνει τη διαδικασία κωδικοποίησης των χαρακτηριστικών, οδηγώντας σε υψηλότερης ποιότητας βίντεο εξόδου. Αυτό το μοντέλο διευκολύνει τη δημιουργία εξόδων με αναλύσεις 64x64, 128x128 και 256x256. Επιπλέον, χρησιμοποιείται από πολλά νευρωνικά δίκτυα deepfake (όπως η εφαρμογή FaceNet) για να γίνει πιο σταθερή η ανίχνευση προσώπων και πιο αξιόπιστη η ευθυγράμμιση τους.[237]

Όπως ήδη αναφέραμε και παραπάνω, ένα συμβατικό μοντέλο GAN περιλαμβάνει δύο νευρωνικά δίκτυα: μια γεννήτρια και έναν διαχωριστή. Το ίδιο συμβαίνει και στο μοντέλο ενός δικτύου deepfake, καθώς τα δεδομένα εισόδου που εισάγονται είναι ένα σύνολο εικόνων ενός προσώπου. Στόχος της γεννήτριας είναι να παράγει εικόνες παρόμοιες με τις πραγματικές εικόνες με κάποια σήματα θορύβου με κατανομή. Στόχος του διαχωριστή είναι να ταξινομήσει σωστά και τις εικόνες

[236] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

[237] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

που παράγονται από την γεννήτρια και τις πραγματικές εικόνες. Ο διαχωριστής εκπαιδεύεται για να βελτιώσει την ικανότητα ταξινόμησής του, δηλαδή για να τη μεγιστοποιήσει, το οποίο αντιπροσωπεύει την πιθανότητα ότι η εικόνα που παράγει η γεννήτρια είναι μια πραγματική εικόνα και όχι μια ψεύτικη εικόνα που δημιουργήθηκε από την γεννήτρια. Από την άλλη πλευρά, η γεννήτρια εκπαιδεύεται για να ελαχιστοποιήσει την πιθανότητα οι έξοδοί της - εικόνες να ταξινομηθούν από τον διαχωριστή ως συνθετικές εικόνες, δηλαδή έχει στόχο να ελαχιστοποιήσει την ικανότητα ταξινόμησης του διαχωριστή. Μετά από επαρκή εκπαίδευση, και τα δύο δίκτυα βελτιώνουν τις ικανότητές τους, δηλαδή, η γεννήτρια είναι σε θέση να παράγει εικόνες που είναι πραγματικά παρόμοιες με τις πραγματικές εικόνες, ενώ ο διαχωριστής είναι ιδιαίτερα ικανός να διακρίνει τις πλαστές εικόνες από τις πραγματικές.[238]

## 7.2 ΤΡΟΠΟΙ ΚΑΤΑΣΚΕΥΗΣ ΕΝΟΣ DEEPFAKE

### 7.2.1 ΑΝΑΠΑΡΑΣΤΑΣΗ

Μια αναπαράσταση deepfake είναι όταν μια εικόνα ενός προσώπου χρησιμοποιείται για να καθοδηγήσει την έκφραση, το στόμα, το βλέμμα, τη στάση ή το σώμα μιας εικόνας ενός άλλου προσώπου, του προσώπου στόχου.

#### 7.2.1.1 ΑΝΑΠΑΡΑΣΤΑΣΗ ΕΚΦΡΑΣΗΣ

Η αναπαράσταση της έκφρασης είναι όπου η έκφραση του προσώπου – πηγή οδηγεί την έκφραση του προσώπου - στόχου. Είναι η πιο κοινή μορφή αναπαράστασης, καθώς οι τεχνολογίες αυτές συχνά οδηγούν το στόμα και τη στάση του στόχου, παρέχοντας ένα ευρύ φάσμα ευελιξίας. Καλοήθεις χρήσεις υπάρχουν στη βιομηχανία ταινιών και βιντεοπαιχνιδιών, όπου οι ερμηνείες των ηθοποιών βελτιώνονται, και στα εκπαιδευτικά μέσα ενημέρωσης όπου αναπαριστώνται ιστορικά πρόσωπα. [239]

Η αναπαράσταση έκφρασης μπορεί να προκύψει από αντιστοίχιση δεδομένων από ένα αντικείμενο εικόνας σε ένα άλλο (one to one identity), όπου κατά κύριο λόγο χρησιμοποιείται το νευρωνικό δίκτυο CycleGan. Ωστόσο, στη συγκεκριμένη αναπαράσταση μεταξύ των δύο αντικειμένων (πρόσωπο πηγής και πρόσωπο στόχος) πρέπει να υπάρχουν παρόμοια χαρακτηριστικά έκφρασης (π.χ. πόζες). [240]

---

[238] Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)

[239]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[240]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

Στην αναπαράσταση έκφρασης από πολλές εικόνες σε μια (πολλά διαφορετικά πρόσωπα συνθέτουν μια εικόνα – many to one identity), πλέον τα deepfakes προχώρησαν ένα βήμα παραπέρα, επιτυγχάνοντας πλήρη προσωπογραφική αναπαράσταση (βλέμμα, ανοιγοκλείσιμο των ματιών, πόζα, στόμα κ.λπ.) με ένα μόνο 1 λεπτού εκπαιδευτικό βίντεο. Τρισδιάστατα μοντέλα προσώπου της πηγής εξάγονται από εικόνες 2D με τη χρήση μονόφθαλμης ανακατασκευής. Στη συνέχεια, για κάθε πλαίσιο η στάση και η έκφραση του προσώπου της πηγής μεταφέρεται στο τρισδιάστατο μοντέλο του στόχου. [241]

Τέλος, από πολλές εικόνες μπορεί να προκύψουν επίσης πολλές εικόνες (many identities to many). Σε αυτού του είδους την αναπαράσταση οι εικόνες πηγής πρέπει να κατηγοριοποιούνται με βάση τα χαρακτηριστικά τους (έκφρασης, πόζας κλπ) για να μπορέσουν να χρησιμοποιηθούν. [242]

Προς το τέλος του 2019 και στις αρχές του 2020, οι ερευνητές άρχισαν να εξετάζουν την περαιτέρω ελαχιστοποίηση του όγκου των δεδομένων εκπαίδευσης μέσω της μάθησης με ένα ή με λίγα βήματα. Για να πετύχει αυτό, εκτελείται μάθηση μετα-μεταφοράς, όπου το δίκτυο εκπαιδεύεται πρώτα σε πολλές διαφορετικές ταυτότητες και στη συνέχεια προσαρμόζεται στην ταυτότητα του στόχου.[243]

#### 7.2.1.2 ΑΝΑΠΑΡΑΣΤΑΣΗ ΣΤΟΜΑΤΟΣ (DUBBING)

Η ομιλία είναι η κύρια δίοδος επικοινωνίας μεταξύ των ανθρώπων και η αναγνώριση της από τις μηχανές και η κατανόησή της είναι χρήσιμη και σημαντική για τη δημιουργία ενός βίντεο deepfake.[244] Η αναπαράσταση στόματος, γνωστή και ως «μεταγλώττιση» (dubbing), είναι η περίπτωση όπου το στόμα του προσώπου στόχου οδηγείται από το στόμα του προσώπου πηγής, ή από μια ηχητική είσοδο που περιέχει ομιλία. Σε αντίθεση με την αναπαράσταση έκφρασης, η αναπαράσταση στόματος (ή αλλιώς μεταγλώττιση βίντεο ή εικόνας) αφορά την οδήγηση του στόματος ενός στόχου με ένα τμήμα ήχου. [245]

Στην αναπαράσταση του στόματος από πολλά αντικείμενα σε ένα, με μια χρονική καθυστέρηση σε τμήματα ήχου όπως αυτά εξάγονται μετά από φιλτράρισμα από μια μη γραμμική κλίμακα Mel

[241]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[242]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[243]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[244] Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004, σελ. 644

[245]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

(μέσω των συντελεστών Mel-Frequency Cepstral, οι οποίοι προσομοιάζουν περισσότερο τον τρόπο με τον οποίο αντιλαμβάνεται τον ήχο το ανθρώπινο αυτί), δημιουργείται μια σειρά από χαρακτηριστικά στόματος (σχήματα). Στη συνέχεια, δημιουργείται με βάση αυτά τα χαρακτηριστικά του στόματος (μύτη και στόμα) και σχηματίζονται τα δόντια με τη μεταφορά λεπτομερειών υψηλής συχνότητας και τέλος χρησιμοποιώντας ένα δυναμικό πρόγραμμα χρονομετρείται το βίντεο προορισμού για να ταιριάζει με τον ήχο προέλευσης και τελικά αυτά τα δύο δεδομένα αναμειγνύονται και συγχρονίζονται. [246]

Στην αναπαράσταση στόματος μπορεί να εισάγονται και κείμενα αντί για ηχητικά τμήματα. Τα κείμενα αυτά μετατρέπονται σε ήχο μέσω αλγορίθμων και στη συνέχεια αντιστοιχίζεται το κείμενο – ήχος με το στόμα του προσώπου στόχου στο βίντεο. Το τελευταίο διάστημα έχουν γίνει αρκετές προσπάθειες και πλέον για τη σύνθεση ενός πλαστού βίντεο στοχεύονται ταυτόχρονα και το στόμα και η ομιλία ενός προσώπου. Αυτό σημαίνει πρακτικά πως εκτός από τα χαρακτηριστικά προσώπου εξάγονται και χαρακτηριστικά της φωνής του προσώπου στόχου και δημιουργείται ένα τρισδιάστατο παραμετρικό μοντέλο κεφαλής. Ο συγχρονισμός των χειλιών μπορεί να βελτιωθεί όταν το δίκτυο εστιάζει σε συγκεκριμένους συσχετισμούς μεταξύ του οπτικοακουστικού σήματος και του περιεχομένου ομιλίας. [247]

Ο ήχος προς βίντεο (A2V) και το κείμενο σε βίντεο (T2V) είναι διαδικασίες συγχρονισμού χειλιών για τη δημιουργία deepfake. Η έκφραση του προσώπου σε ένα βίντεο συντίθεται με ήχο ή κείμενο. Ένα παράδειγμα ψεύτικου βίντεο περιγράφει μια μέθοδο για τη σύνθεση ταινιών υψηλής ποιότητας ενός ατόμου (όπως η γνωστή υπόθεση Μπαράκ Ομπάμα) το οποίο μιλάει με έναν ακριβή τρόπο συγχρονισμού χειλιών. Πρόκειται για μια διαδικασία κατά την οποία από ένα βίντεο μιας μεμονωμένης ομιλίας λαμβάνονται οι απαραίτητες πληροφορίες και το απαραίτητο περιεχόμενο που πρέπει να ειπωθεί και στη συνέχεια οι πληροφορίες αυτές αναμειγνύονται με πλαστές ηχητικές εγγραφές και δημιουργείται ένα άλλο βίντεο όπου τα χείλη του ατόμου συγχρονίζονται με τα νέα λόγια. [248]

#### 7.2.1.3 ΑΝΑΠΑΡΑΣΤΑΣΗ ΒΛΕΜΜΑΤΟΣ

Η αναπαράσταση του βλέμματος είναι η περίπτωση όπου η κατεύθυνση των ματιών του προσώπου στόχου και η θέση των βλεφάρων καθοδηγούνται από αυτά του προσώπου πηγής. Για να αντιμετωπιστεί αυτό το ζήτημα προτάθηκε ένα δίκτυο ανακατεύθυνσης βλέμματος. Στο δίκτυο

[246]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[247]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[248] A. Malik, M. Kuribayashi, S. M. Abdullahi and A. N. Khan, "DeepFake Detection for Human Face Images and Videos: A Survey," in IEEE Access, vol. 10, pp. 18757-18775, 2022, doi: 10.1109/ACCESS.2022.3151186.

αυτό, το περικομμένο μάτι, η στάση κεφαλής και η γωνία πηγής του στόχου κωδικοποιούνται ξεχωριστά και στη συνέχεια περνούν μέσα από ένα άλλο δίκτυο για τη δημιουργία οπτικού πεδίου ροής. [249]

#### 7.2.1.4 ΑΝΑΠΑΡΑΣΤΑΣΗ ΣΤΑΣΗΣ

Η αναπαράσταση της στάσης είναι όπου η θέση της κεφαλής του προσώπου στόχου καθορίζεται από το πρόσωπο πηγής. Για την καλύτερη αναπαράσταση της στάσης προτείνεται η χρήση δύο αντιπαραθετικών νευρωνικών δικτύων, το οποίο το ένα αντιμετωπίζει το πρόσωπο και παράγει ένα χάρτη του προσώπου με τα χαρακτηριστικά που ενδιαφέρουν και το δεύτερο περιστρέφει το πρόσωπο δεδομένης της γωνίας στόχου. Το αποτέλεσμα είναι ότι κάθε μοντέλο εκτελεί μια λιγότερο περίπλοκη λειτουργία και ως εκ τούτου τα μοντέλα μπορούν να παράγουν μια εικόνα υψηλότερης ποιότητας. Η αναπαράσταση σώματος, ή αλλιώς μεταφορά στάσης και σύνθεση ανθρώπινης στάσης, είναι παρόμοια με τις αναπαραστάσεις προσώπου που αναφέρονται παραπάνω, με τη διαφορά ότι πρόκειται για τη στάση του σώματος του προσώπου στόχου που οδηγείται. [250]

Στην αναπαράσταση σώματος ενός μόνο αντικειμένου εκτός από το πρόσωπο χρησιμοποιείται και μέρος του σώματος (χέρια και μπράτσα). Ένα αντιπαραθετικό δίκτυο μετατρέπει τα όρια του προσώπου πηγής σε αυτά του στόχου και στη συνέχεια τα αντιγράφει πάνω σε μια πόζα του σκελετού της πηγής. [251]

Στην αναπαράσταση σώματος από πολλά αντικείμενα δύναται οι στόχοι να χορεύουν και αυτό επιτυγχάνεται μέσα από ένα αντιπαραθετικό νευρωνικό δίκτυο με μια προσαρμοσμένη λειτουργία απώλειας. Η γεννήτρια λαμβάνει μια εικόνα του συλληφθέντος σκελετού πόζας και ο διαχωριστής λαμβάνει την τρέχουσα και τελευταία εικόνα που εξαρτάται από τις πόζες τους. [252]

### 7.2.2 ΑΝΤΙΚΑΤΑΣΤΑΣΗ

Μια αντικατάσταση deepfake είναι όταν το περιεχόμενο του προσώπου στόχου αντικαθίσταται με αυτό του προσώπου πηγής, διατηρώντας την ταυτότητα του προσώπου πηγής. Το περιεχόμενο του προσώπου στόχου αντικαθίσταται με αυτό του προσώπου πηγής. Ένας συνηθισμένος τύπος

[249]The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
[250] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
[251] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
[252] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

μεταφοράς είναι η μεταφορά προσώπου, που χρησιμοποιείται στη βιομηχανία της μόδας για την απεικόνιση ενός ατόμου με διαφορετικά ρούχα.[253]

Ανταλλαγή είναι η περίπτωση αντικατάστασης όπου το περιεχόμενο που μεταφέρεται στο πρόσωπο στόχος από το πρόσωπο πηγής καθοδηγείται από το πρόσωπο στόχος. Ο πιο δημοφιλής τύπος αντικατάστασης ανταλλαγής είναι η «ανταλλαγή προσώπου», η οποία χρησιμοποιείται συχνά για τη δημιουργία μιμιδίων ή σατιρικού περιεχομένου με την ανταλλαγή της ταυτότητας ενός ηθοποιού με την ταυτότητα ενός διάσημου ατόμου. Μια άλλη καλοήθης χρήση της ανταλλαγής προσώπων περιλαμβάνει την ανωνυμοποίηση της ταυτότητας κάποιου σε δημόσιο περιεχόμενο στη θέση της θόλωσης ή της εικονοστοιχειοποίησης.[254]

Ωστόσο, για μεγαλύτερο έλεγχο, χρησιμοποιείται ένα δίκτυο κωδικοποιητή – αποκωδικοποιητή, το οποίο αποσυνδέει την ταυτότητα από τα χαρακτηριστικά (πόζα, μαλλιά, φόντο και φωτισμό) κατά τη διαδικασία εκπαίδευσης. Οι κωδικοποιήσεις ταυτότητας είναι το τελευταίο επίπεδο συγκέντρωσης ενός ταξινομητή προσώπου και ο κωδικοποιητής χαρακτηριστικών εκπαιδεύεται χρησιμοποιώντας μια σταθμισμένη απώλεια και μια απώλεια απόκλισης για να μετριάσει τη διαρροή ταυτότητας. Μέσω παρεμβολής των κωδικοποιήσεων δύναται να προσαρμοστούν τα χαρακτηριστικά, η έκφραση και η στάση του προσώπου. Αντί να ανταλλάσσονται ταυτότητες, δύναται να μεταβληθούν – τροποποιηθούν τα χαρακτηριστικά της ταυτότητας του προσώπου στόχου και αυτό επιτυγχάνεται μέσω ενός δικτύου κωδικοποιητή – αποκωδικοποιητή, το οποίο προβλέπει τις τρισδιάστατες παραμέτρους της κεφαλής, οι οποίες είτε τροποποιήθηκαν είτε αντικαταστάθηκαν με αυτές της πηγής. Τέλος, ένα GAN χρησιμοποιείται για να σχηματίσει το πρόσωπο του στόχου με βάση τις τροποποποιημένες παραμέτρους του μοντέλου κεφαλής.[255]

### 7.2.3. ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΣΥΝΘΕΣΗ

Μια πλαστογράφηση deepfake είναι η προσθήκη, η τροποποίηση ή η αφαίρεση των χαρακτηριστικών του προσώπου στόχου. Ορισμένα παραδείγματα περιλαμβάνουν την αλλαγή των ρούχων, των μαλλιών στο πρόσωπο, της ηλικίας, του βάρους, της ομορφιάς και της εθνικότητας του στόχου. [256]

---

[253] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[254] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[255] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[256] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

Η σύνθεση είναι το σημείο όπου δημιουργείται ένα deepfake χωρίς στόχο ως βάση. Οι τεχνικές σύνθεσης ανθρώπινων προσώπων και σωμάτων μπορούν να δημιουργήσουν υλικό χωρίς δικαιώματα ή να δημιουργήσουν χαρακτήρες για ταινίες και παιχνίδια. Ωστόσο, παρόμοια με την επεξεργασία deepfakes, μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία ψεύτικων προσωπικοτήτων στο διαδίκτυο. Παρόλο που η επεξεργασία και η σύνθεση εικόνων από τον άνθρωπο είναι ενεργά ερευνητικά θέματα, η αναπαράσταση και η αντικατάσταση βαθιών απομιμήσεων αποτελούν τη μεγαλύτερη ανησυχία, επειδή δίνουν σε έναν επιτιθέμενο τον έλεγχο της ταυτότητας κάποιου. [257]

Μια προσέγγιση για τη σύγκριση δύο μη ευθυγραμμισμένων εικόνων είναι να τις περάσουμε από ένα άλλο δίκτυο (ένα αντιληπτικό μοντέλο) και να μετρήσουμε τη διαφορά μεταξύ των ενεργοποιήσεων των επιπέδων (χάρτες χαρακτηριστικών). Αυτή η απώλεια ονομάζεται αντιληπτική απώλεια. Κατά τη δημιουργία ενός deepfake, η αντιληπτική απώλεια συχνά υπολογίζεται χρησιμοποιώντας ένα δίκτυο αναγνώρισης προσώπου. Επομένως, μετρώντας την απόσταση μεταξύ των χαρτών χαρακτηριστικών δύο διαφορετικών εικόνων, ουσιαστικά μετράμε τη σημασιολογική τους διαφορά (π.χ. πόσο παρόμοιες είναι οι μύτες μεταξύ τους και άλλες λεπτότερες λεπτομέρειες).[258]

Για τη δημιουργία ενός deepfake, τα δίκτυα αναπαράστασης και ανταλλαγής προσώπων ακολουθούν κάποια παραλλαγή αυτής της διαδικασίας: περνούν την εικόνα μέσω ενός αγωγού που (1) ανιχνεύει και περικόπτει το πρόσωπο, (2) εξάγει ενδιάμεσες αναπαραστάσεις, (3) παράγει ένα νέο πρόσωπο με βάση κάποιο οδηγό σήμα (π.χ. ένα άλλο πρόσωπο) και στη συνέχεια (4) αναμειγνύει το παραγόμενο πρόσωπο πίσω στο πλαίσιο-στόχο.[259]

## ΙΙΙ. Β' ΜΕΡΟΣ – ΝΟΜΙΚΗ ΠΡΟΣΕΓΓΙΣΗ

### Α. ΕΙΣΑΓΩΓΗ

Η εξάπλωση του διαδικτύου και των τεχνολογιών πληροφορικής και επικοινωνιών είναι η μάστιγα της εποχής και το μόνο σίγουρο είναι ότι από τη στιγμή που γεννιέται μια τεχνολογία θα συνεχίσει να υπάρχει και θα εξελίσσεται για να γίνει καλύτερη. Έτσι, λοιπόν και η τεχνολογία των deepfakes ήδη από την εμφάνισή της έχει κάνει άλματα προόδου. Η εξέλιξη της τεχνητής νοημοσύνης είναι ραγδαία και θα φέρει ακόμα πιο σημαντικές εξελίξεις στην τεχνολογία των deepfakes, αφού, όπως

[257] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[258] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

[259] The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete

ήδη αναφέραμε, η εικόνα και το βίντεο παίζουν πλέον το σημαντικότερο ρόλο στην καθημερινή ζωή των ανθρώπων όλου του πλανήτη.

Εφόσον τα deepfakes έχουν γίνει «viral» και καθημερινό φαινόμενο παγκοσμίως, η χρήση τους γεννά νομικά, ηθικά και κοινωνικά διλήμματα και ερωτήματα. Και όπως σε όλα τα ζητήματα της καθημερινότητας η νομική επιστήμη βάζει το δικό της ένδυμα, έτσι και στην περίπτωση αυτή ενδιαφέρουσα αποτελεί η προσέγγιση του φαινομένου από νομική σκοπιά, αφού κοινός τόπος είναι ότι η νομική επιστήμη πρέπει να συμβαδίζει όσο το δυνατόν περισσότερο με την τεχνολογική ανάπτυξη.

Η ελευθερία της έκφρασης, η προσιτή χρήση του διαδικτύου, των μέσων κοινωνικής δικτύωσης, η εύκολη πρόσβαση σε εργαλεία και μέσα που προσφέρει η τεχνολογία της τεχνητής νοημοσύνης, καθιστούν το φαινόμενο ραγδαία αναπτυσσόμενο χωρίς κάποιον περιορισμό ή εμπόδιο. Ανακύπτει, λοιπόν, εύλογα το ερώτημα η τεχνολογία των deepfakes επιφέρει τελικά περισσότερα θετικά αποτελέσματα στους διαφόρους τομείς της ζωής των ανθρώπων ή οι αρνητικές επιπτώσεις υπερτερούν;

Ο κάθε χρήστης του διαδικτύου βέβαια μπορεί να μην έχει κακό σκοπό και να μην θέλει να βλάψει - με οποιονδήποτε τρόπο - κάποιον άλλον, ωστόσο άξιο απορίας είναι ότι ακόμη και στην περίπτωση της θεμιτής χρήσης τους, μήπως προκύπτουν αρνητικές συνέπειες και πρέπει τελικά να τεθούν όρια και να προβλεφθούν εξαιρέσεις όσον αφορά στη χρήση των deepfakes;

Τα deepfakes γεννήθηκαν επίσημα μόλις το 2014. Ποιος μπορούσε όμως να φανταστεί την εξέλιξη αυτής της τεχνολογίας και τη χρήση της ως όπλο οποιουδήποτε κακόβουλου χρήστη του διαδικτύου; Από τη στιγμή που ο αλγόριθμος deepfake αποτέλεσε εργαλείο ανοιχτού κώδικα, ο οποιοσδήποτε με απλή πρόσβαση σε υπολογιστή συνδεδεμένο στο διαδίκτυο, και χωρίς να έχει στοιχειώδεις γνώσεις τεχνητής νοημοσύνης και των άμεσα συνδεδεμένων με αυτήν τεχνολογιών - όπως αναφέρθηκαν ανωτέρω - μπορεί να κάνει χρήση του αλγορίθμου αυτού, προκειμένου να παράγει υλικό είτε για λόγους αναψυχής, είτε για λόγους έρευνας, είτε για λόγους βελτίωσης κάποιου έργου, είτε όμως με σκοπό τη βλάβη άλλου ατόμου προκειμένου να έχει αυτός ο χρήστης κάποιο όφελος. Το λογισμικό για τη δημιουργία ψεύτικων εικόνων, βίντεο και ήχου είναι ήδη ελεύθερα διαθέσιμο στο διαδίκτυο και αρκετά εύκολο στη χρήση. Καθώς η τεχνολογία εξελίσσεται ραγδαία, θα γίνεται όλο και πιο δύσκολο τόσο για τους ανθρώπους όσο και για τους υπολογιστές να διακρίνουν ένα ψεύτικο βίντεο από ένα πραγματικό.

Συνεπώς, εγείρονται διάφορα νομικά ερωτήματα σε σχέση με την τεχνολογία deepfake, καθώς μπορεί να χρησιμοποιηθεί ως μέσο για την τέλεση διαφόρων ποινικών αδικημάτων. Η έκρηξη της κυκλοφορίας των deepfake video ίσως πρέπει να οδηγήσει στη θέσπιση ειδικής νομοθεσίας

σχετικά με το φαινόμενο αυτό, ή να ερμηνευτεί ως ευκαιρία αναδιαμόρφωσης νομικών διατάξεων που δεν εμφανίζονται συμβατές με τις προκλήσεις της σύγχρονης ψηφιακής κοινωνίας.[260]

Μέχρι στιγμής, οι περισσότερες από τις προσπάθειες αντιμετώπισης του φαινομένου έχουν επικεντρωθεί στο πώς να αποτρέψουμε, να μετριάσουμε και να τιμωρήσουμε την κατάχρηση της τεχνολογίας deepfake για επιβλαβείς σκοπούς. Όταν τα deepfakes προκαλούν βλάβη - είτε σε ένα μεμονωμένο άτομο είτε σε μεγάλη κλίμακα π.χ. στην εθνική ασφάλεια - πώς πρέπει να αντιδράσει ο νόμος; Ποιους υφιστάμενους αστικούς και ποινικούς νόμους θα μπορούσαν να επικαλεστούν για να αποκαταστήσουν αυτές τις βλάβες, ποια ένδικα μέσα είναι διαθέσιμα στους ζημιωθέντες και ποιες νέες ρυθμίσεις μπορεί να απαιτηθούν; Εάν είναι όντως κατάλληλοι οι νέοι νόμοι, ποιοί άλλοι τρόποι θα μπορούσαν να περιορίσουν το πεδίο εφαρμογής τους.

Η χρήση της τεχνολογίας ως εργαλείο παραπλάνησης εμπίπτει στο αδίκημα της παραπληροφόρησης, ως μορφή αλλοίωσης ενός προστατευόμενου οπτικοακουστικού έργου, εγείρει ζητήματα πνευματικής ιδιοκτησίας. Το πλέον προφανές αδίκημα που μπορεί να φανταστεί κάποιος ότι μπορεί να τελεστεί είναι αυτό της παραβίασης ζητημάτων προστασίας προσωπικών δεδομένων. Από την άλλη, εύκολα ένα deepfake video μπορεί να λειτουργήσει δυσφημιστικά για κάποιο άτομο, μπορεί όμως επιπλέον να αποτελέσει ρατσιστικό ή εκφοβιστικό υλικό ή μέσο εκβίασης. Τέλος, από την ονομασία και μόνο του φαινομένου και ιδίως του δεύτερου συνθετικού της λέξης, «fake» που σημαίνει ψευδές, αντιλαμβάνεται κανείς πως εφαρμογή μπορεί να βρουν οι διατάξεις σχετικές με την απάτη και την πλαστογραφία.

Μπορούμε με ασφάλεια να υποθέσουμε ότι η εύκολη διαθεσιμότητα των εργαλείων deepfake και οι αντικοινωνικές χρήσεις τους θα συνεχιστούν ανεξάρτητα από το πώς ο νόμος μπορεί να προσπαθήσει να περιορίσει, να ρυθμίσει και να τους τιμωρήσει. Αν τα deepfakes είναι εδώ για να μείνουν, τότε ο νόμος πρέπει να είναι έτοιμος να ανταποκριθεί στις επιπτώσεις τους στο νομικό μας σύστημα.

Καθίσταται, λοιπόν, αναμφισβήτητο ότι τα deepfakes έχουν μια ψηφιακή διάσταση και επομένως στην περίπτωση που αυτά επιφέρουν αρνητικές επιπτώσεις - κυρίως κατά την κακόβουλη χρήση τους - η συγκεκριμένη πράξη μπορεί να χαρακτηριστεί ως κυβερνοέγκλημα, το οποίο παράγει άμεσα απρόβλεπτες απειλές για την κοινωνική ευταξία, όταν χρησιμοποιείται σε βάρος φυσικών και νομικών προσώπων, όσο και κατά κρατικών οντοτήτων και πολιτικών, όπως αποδεικνύουν οι κυβερνοεπιθέσεις κατά την εκλογική διαδικασία. Εφόσον τα δεδομένα που μπορούν να χρησιμοποιηθούν είναι παγκόσμια, τα deepfakes ως κυβερνοέγκλημα αποτελούν κίνδυνο για την ασφάλεια της πληροφορίας, αλλά και για έννομα αγαθά και ελευθερίες των πολιτών σε παγκόσμιο

[260] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

επίπεδο.[261] Καθίσταται, λοιπόν, αναγκαίο πριν αναλυθούν τα επιμέρους εγκλήματα, τα οποία δύνανται να τελεστούν κατά τη χρήση των deepfakes, να αναφερθούν η έννοια, οι διακρίσεις και τα χαρακτηριστικά του κυβερνοεγκλήματος, αφού ως τέτοιο δύναται να χαρακτηριστεί πρωτίστως η κακόβουλη χρήση ενός deepfake.

## Β. ΤΑ DEEPFAKES ΩΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Η παγκοσμιότητα του φαινομένου deepfake αναδεικνύει την αναγκαιότητα δικαστικής και αστυνομικής συνεργασίας τόσο σε εσωτερικό όσο και σε διεθνές επίπεδο, με σκοπό την αποτελεσματική πρόληψη και αντιμετώπιση του κυβερνοεγκλήματος, λόγω του διασυνοριακού χαρακτήρα του, θέση η οποία αποτυπώθηκε στη με αριθμό 4 Αιτιολογική σκέψη της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφορικής, η οποία όμως βρίσκει έρεισμα και στην περίπτωση των deepfakes, κατά τη γνώμη της γράφουσας.

Στο πλαίσιο της προώθησης διεθνούς νομοθεσίας για την καταστολή της εγκληματικότητας στον Κυβερνοχώρο καταρτίστηκε στη Βουδαπέστη στις 23.11.2001 η υπ' αρ. 185 Σύμβαση του Συμβουλίου της Ευρώπης, η οποία έχει ήδη επικυρωθεί από πολλά κράτη, με σκοπό την προστασία της κοινωνίας από το κυβερνοέγκλημα.[262] Η επικύρωση της Σύμβασης της Βουδαπέστης και η ενσωμάτωση της 2013/40/ΕΕ Οδηγίας στην ελληνική έννομη τάξη επιτεύχθηκε με τον Ν 4411/2016 (ΦΕΚ Α΄ 142/3.8.2016), στον οποίο περιλαμβάνονται διατάξεις ουσιαστικού ποινικού δικαίου, ποινικού δικονομικού δικαίου και τέλος, διατάξεις διεθνούς δικαστικής συνεργασίας. Η θέσπιση κατάλληλης νομοθεσίας με ορισμένες και σαφείς ρυθμίσεις καθίσταται επιτακτική για την προστασία εννόμων αγαθών που βλάπτονται από τη διάπραξη εγκλημάτων είτε α) μόνο στο περιβάλλον του κυβερνοχώρου είτε β) τόσο σε πραγματικό όσο και σε ηλεκτρονικό περιβάλλον (δικτύου) είτε γ) μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών χωρίς σύνδεση στο διαδίκτυο.[263]

Το γεγονός ότι το deepfake μπορεί να αποτελέσει κυβερνοέγκλημα ενισχύεται από το ότι μπορεί να στραφεί κατά αυτών των εννόμων αγαθών, τα οποία αναφέρονται ευθέως σε θεμελιώδη δικαιώματα του Συντάγματος αλλά και διεθνούς προστασίας, όπως η προσωπικότητα, η υγεία, η

[261] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η έκδοση 2023, σελ. 1

[262] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 2

[263] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 2

ιδιοκτησία, η περιουσία, η επικοινωνία, ο ιδιωτικός βίος, τα απόρρητα, τα προσωπικά δεδομένα, τα πνευματικά δικαιώματα κ.α.

Οι όροι e-crime, computer-crime, cybercrime και internet related crime χρησιμοποιούνται διεθνώς για να αποδώσουν την έννοια του ηλεκτρονικού εγκλήματος. Στην ελληνική γλώσσα χρησιμοποιείται ο γενικότερος όρος ηλεκτρονικό έγκλημα και οι ειδικότεροι διαδικτυακό έγκλημα και κυβερνοέγκλημα ή έγκλημα του κυβερνοχώρου.

Το ηλεκτρονικό έγκλημα μπορεί να χαρακτηριστεί α) ως έγκλημα που διαπράττεται με τη χρήση ηλεκτρονικών υπολογιστών (computer crimes) β) ως ένα ήδη υπάρχον έγκλημα με τη διαφορά ότι διαπράττεται με υπολογιστή και γ) ως μια εγκληματική συμπεριφορά που εκδηλώνεται με την με οποιοδήποτε τρόπο συμμετοχή ενός ηλεκτρονικού υπολογιστή ή μέσω διαδικτύου (cyber crimes).[264]

Επιπρόσθετα, το κυβερνοέγκλημα μπορεί να διακριθεί ως: α) γνήσιο πληροφορικό έγκλημα, όταν διαπράττεται μέσω ηλεκτρονικού υπολογιστή και μέσω συστημάτων πληροφοριών (λ.χ. απάτη, πλαστογραφία), β) έγκλημα με ψηφιακό περιεχόμενο, όταν διακινείται παράνομο περιεχόμενο μέσω συστημάτων πληροφοριών (λ.χ. παιδική πορνογραφία), γ) έγκλημα κατά πληροφοριακών συστημάτων, όταν προσβάλλεται η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των πληροφοριακών συστημάτων και των ψηφιακών δεδομένων.[265] Συνεπώς, βασικό στοιχείο της διάπραξης κυβερνοεγκλημάτων είναι ο ηλεκτρονικός υπολογιστής με σύνδεση σε σύστημα πληροφοριών, ο οποίος είναι ή ο στόχος της επίθεσης, ή το βασικό μέσο / εργαλείο της επίθεσης, ή το βοηθητικό μέσο / εργαλείο για την επίθεση.[266]

Το κυβερνοέγκλημα διακρίνεται για τα ιδιαίτερα χαρακτηριστικά του. Το μέσο τέλεσης των εγκλημάτων του κυβερνοχώρου, ήτοι ο ηλεκτρονικός υπολογιστής ή τα έξυπνα κινητά τηλέφωνα που έχουν πλέον καταστεί κοινά και διαδεδομένα παγκοσμίως, έχουν καταστήσει εύκολη την τέλεση τέτοιων εγκλημάτων. Η εγκληματική δράση συμβαίνει στον οικείο χώρο του δράστη, χωρίς

[264] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 4

[265] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ.7

[266] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη

να χρειάζεται μετακίνηση. Σημαντικό ρόλο διαδραματίζει η ανωνυμία του δράστη και η ταχύτητα τέλεσής του εγκλήματος.[267]

Ιδιαίτερο ενδιαφέρον αποτελεί το γεγονός ότι το ηλεκτρονικό έγκλημα είναι έγκλημα που τελείται από απόσταση, αφού αλλού ενεργεί ο δράστης και αλλού επέρχεται το αξιόποινο αποτέλεσμα. Εφόσον, τα δεδομένα διακινούνται παντού μέσω του διαδικτύου, το διαδικτυακό έγκλημα αποκτά διασυνοριακό χαρακτήρα, αφού περισσότερα κράτη δύνανται να αποτελέσουν τόπο τέλεσης. Επιπλέον, μπορεί να υπάρχει διαφοροποίηση στην αντιμετώπιση μιας πράξης ως αξιόποινης από χώρα σε χώρα, καθώς αλλού μπορεί η πράξη να τιμωρείται και αλλού να μένει ατιμώρητη.[268] Σύμφωνα με το άρθρο 16 ΠΚ τόπος τέλεσης ενός εγκλήματος είναι και ο τόπος που ο δράστης προέβη στην εγκληματική πράξη όσο και ο τόπος που επήλθε το αποτέλεσμα.[269]

Όλα τα ανωτέρω χαρακτηριστικά μπορούν κάλλιστα να προσδιορίσουν και μια εγκληματική συμπεριφορά σχετιζόμενη με διακίνηση υλικού που προέρχεται από την τεχνολογία deepfake και ως εκ τούτου, και ειδικά εξαιτίας του διασυνοριακού χαρακτήρα λόγω της παγκοσμιότητας του φαινομένου, η κακόβουλη χρήση των deepfake μπορεί να αναφερθεί ως κυβερνοέγκλημα, το οποίο στην ελληνική έννομη τάξη μπορεί να τιμωρηθεί με την εφαρμογή σωρείας ποινικών διατάξεων τόσο του νέου Ποινικού Κώδικα όσο και ειδικών νομοθετημάτων.

## Γ. Η ΚΑΚΟΒΟΥΛΗ ΧΡΗΣΗ ΤΩΝ DEEPFAKES ΚΑΙ Η ΣΤΟΙΧΕΙΟΘΕΤΗΣΗ ΕΓΚΛΗΜΑΤΩΝ

### Γ.1 ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ

Αναφερθήκαμε ήδη στη μεγάλη σημασία που διαδραματίζουν τα μέσα κοινωνικής δικτύωσης στις μέρες μας. Η εξάρτηση πλέον είναι μεγάλη, ενώ χωρίς αυτά και την ευκολία που μας παρέχει το διαδίκτυο και η πρόσβαση σε αυτό ανά πάσα στιγμή δεν θα μπορούσαμε πλέον να φανταστούμε τη ζωή μας. Δεν είναι υπερβολή να πούμε πως τα κοινωνικά δίκτυα έχουν αντικαταστήσει τόσο τη δημοσιογραφική έρευνα, όσο και τους παραδοσιακούς τρόπους ενημέρωσης του κοινού. Πλέον ο οποιοσδήποτε δεν χρειάζεται να μεταβεί σε κάποιο περίπτερο για να αγοράσει εφημερίδα. Μπορεί απλά να ανοίξει το λαπτοπ, η πιο απλά την οθόνη του smartphone του και να δει και να διαβάσει

[267] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (N 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ.7

[268] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (N 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σελ.7 και Ο τόπος τέλεσης του διαδικτυακού εγκλήματος, Δημήτριος Κιούπης, Αναπλ. Καθηγητής ΕΚΠΑ, Δικηγόρος, σελ. 41 σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023

[269] https://www.lawspot.gr/nomika-nea/psifiaki-edafikotita-topos-telesis-egklimatos-meso-diadiktyoy

ειδήσεις και να ενημερωθεί κάθε στιγμή τι συμβαίνει σε κάθε άκρη του πλανήτη μας και έξω από αυτόν.

Λόγω της γρήγορης και άκοπης πρόσβασης και της ραγδαίας αύξησης των χρηστών του διαδικτύου, η διάδοση και η διασπορά ειδήσεων καθίσταται άμεση και εύκολη. Μέσω των διάσημων πλατφορμών των μέσων κοινωνικής δικτύωσης, όπως είναι το Tik Tok, το Twitter, το Instagram και το Facebook εύκολα μια είδηση μπορεί να γίνει «viral», να διαδοθεί δηλαδή σε όλους τους χρήστες με ραγδαίο ρυθμό και να υιοθετηθεί το γεγονός, η άποψη, η στάση από την πλειοψηφία.

Κάπως έτσι η παραπληροφόρηση και η διασπορά ψευδών ειδήσεων (fake news) έχει λάβει ήδη διαστάσεις επιδημίας. Και αυτό κυρίως αν αναλογιστούμε ότι πλέον μια είδηση δεν γίνεται γνωστή από κάποιον επαγγελματία δημοσιογράφο σε κάποιο τηλεοπτικό / ραδιοφωνικό σταθμό ή εφημερίδα / περιοδικό αλλά ο καθένας που διαθέτει λογαριασμό σε κάποιο μέσο κοινωνικής δικτύωσης μπορεί να γίνει ένας μικρός δημοσιογράφος που θα διασπείρει μια αληθινή αλλά και μια ψεύτικη είδηση. Όπως πολλοί δημοσιογράφοι ανά καιρούς διέδιδαν ψευδείς ειδήσεις με κακόβουλο σκοπό έτσι και ο κάθε χρήστης σήμερα με καλοπροαίρετη διάθεση μπορεί να διασπείρει μια ψευδή είδηση με σκοπό να παραπλανήσει το κοινό του.

Στην εποχή μας η δύναμη της εικόνας είναι αδιαμφισβήτητη. Θα μπορούσε να πει κανείς πως πλέον από την εικόνα περνάμε στην εποχή του βίντεο. Η πλατφόρμα κοινωνικής δικτύωσης Tik Tok έχει συμβάλλει αρκετά σε αυτή τη μετάβαση. Πλέον οι περισσότεροι χρήστες ενδιαφέρονται να κοινοποιήσουν κάποιο βίντεο («reel») παρά μια απλή φωτογραφία. Αυτή η μετάβαση από την εικόνα στο βίντεο δίνει το πάτημα στην τεχνολογία του deepfake να αναπτυχθεί και να διαδοθεί περισσότερο με σκοπό να χρησιμοποιηθεί ως μέσο παραπληροφόρησης και διασποράς ψευδών ειδήσεων, οι οποίες μπορούν να έχουν αντίκτυπο παγκοσμίως. Η τεχνολογία deepfake επιτρέπει σε οποιονδήποτε να διανείμει βίντεο τα οποία «δανείζονται» το πρόσωπο πολιτικών, επιστημόνων ή διασήμων ατόμων, εκμεταλλευόμενη τον βαθμό αξιοπιστίας του ονόματος αυτών των προσώπων, με στόχο την προώθηση οποιουδήποτε μηνύματος.[270]

Η χρήση αυτής της τεχνολογίας για έναν τέτοιο σκοπό αποτελεί πλήγμα για την δημοκρατία καθώς επηρεάζει την κρίση των πολιτών με αθέμιτο τρόπο και με ενδεχόμενες καταστροφικές συνέπειες για την κοινωνία σε επίπεδο ασφάλειας, υγείας ή για την καταπολέμηση του μισαλλόδοξου λόγου.

[270] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

Συνεπώς η συμπεριφορά αυτή ορθά ενεργοποιεί τις πρόνοιες του Ποινικού Κώδικα. Συγκεκριμένα, τιμωρείται κλασσικά μέσω του άρθρου 191 του ΠΚ η διασπορά ψευδών ειδήσεων. [271]

Η παραπληροφόρηση γνωστή ως «fake news» ή «hoax» και η διασπορά ψευδών ειδήσεων έχουν λάβει νέες διαστάσεις στην ψηφιακή εποχή και απασχολούν τα νομικά συστήματα σε εθνικό και διεθνές επίπεδο.[272] Fake news είναι οι ψευδείς ειδήσεις, οι οποίες διαδίδονται από ειδησεογραφικές ιστοσελίδες, ψεύτικους λογαριασμούς προσώπων σε μέσα κοινωνικής δικτύωσης, καθώς και από τα λεγόμενα «troll».[273] Πλέον, τα μέσα κοινωνικής δικτύωσης όπως π.χ. το "Facebook" έχουν λάβει μέτρα για να μετριάσουν τη διασπορά ψευδών ειδήσεων[274]. Ακόμα και με ένα "tweet" ο πρώην Πρόεδρος των ΗΠΑ Ντόναλντ Τραμπ αναφέρθηκε στις δημοσκοπήσεις του Fox News ως "fake news", αφού έδιναν προβάδισμα στις προεδρικές εκλογές του 2020 σε αντίπαλό του.[275]

Τον Οκτώβριο του έτους 2018 εκπρόσωποι διαφόρων διαδικτυακών πλατφορμών και άτομα της διαφημιστικής βιομηχανίας (Facebook, Google, Twitter, Youtube κ.λπ.) συμφώνησαν σε μια κοινή αντιμετώπιση της εξάπλωσης της διαδικτυακής παραπληροφόρησης με τη διασπορά ψευδών ειδήσεων.[276]

Ο κίνδυνος πλέον που προκύπτει από τη διασπορά ψευδών ειδήσεων είναι μεγάλος και πολλές χώρες όπως η Γερμανία[277] ή η Γαλλία[278] ψήφισαν ήδη από το 2018 νόμους για την καταπολέμηση

---

[271] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[272] Γ. Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022, σ. 97 = sakkoulas-online

[273] Ποινική ευθύνη ενδιάμεσων παρόχων, ιδίως φορέων μέσων κοινωνικής δικτύωσης, για fake news και προσβολές της τιμής στο διαδίκτυο (υπό το νέο Ποινικό Κώδικα), Ιωάννης Μοροζίνης, Δικηγόρος, ΔΝ, Εντεταλμένος Διδάσκων Νομικής Σχολής ΔΠΘ, σελ. 107 σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 95

[274]Dave Lee, Matter of fact-checkers: Is Facebook winning the fake news war?, BBC News, 02 Απριλίου 2019, (https://www.bbc.com/news/technology-47779782)

[275] βλ. Harry Cockburn, Trump calls Fox 'fake news' for citing unfavorable 2020 election polls, The Independent, 19 Ιουνίου 2019,https://www.independent.co.uk/news/world/americas/uspolitics/trump-fox-news-poll-fake-news-joe-biden-2020-election-us-a8963786.html

[276] http://www.aereurope.org/wpcontent/uploads/2018/10/CodeofPracticeonDisinformation.pdf

[277] Τον Ιούνιο του έτους 2017 το Ομοσπονδιακό Κοινοβούλιο της Γερμανίας (Bundestag) υπερψήφισε το λεγόμενο Netzwerkdurchsetzungsgesetz (στα Αγγλικά: The Network Enforcement Act, στα Γερμανικά: Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, γνωστό επίσης ως the Facebook Act), όπου επιχειρείται η αντιμετώπιση της διασποράς ψευδών ειδήσεων στα μέσα κοινωνικής δικτύωσης [(βλ. ανάλυση του Netzwerkdurchsetzungsgesetz στο πόνημα του Δ. Καραγκούνη, Η επιβολή περιορισμών στα μέσα κοινωνικής δικτύωσης μετά τον νέο Γερμανικό Νόμο περί Βελτίωσης της Νομοθεσίας στα Κοινωνικά Δίκτυα (Netzwerkdurchsetzungsgesetz) Επίθεση στην
ελευθερία έκφρασης ή αναγκαίο μέσο καταπολέμησης της διαδικτυακής εγκληματικότητας;, εις: Θ. Δαλακούρα, Ηλεκτρονικό έγκλημα, σελ. 223 επ.].

[278] Στις 22 Δεκεμβρίου 2018 ο Πρόεδρος της Δημοκρατίας της Γαλλίας εξέδωσε τον νόμο αριθ. 2018- 1202 και τον οργανικό νόμο αριθ. 2018-1201 για την καταπολέμηση της χειραγώγησης των πληροφοριών (για το κείμενο του νόμου στην πρωτότυπη μορφή του βλ. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id&fbclid=IwAR1bXQ7K6gnVGUJN4SkTsfMFTX8BCyG-P123bLVmfWz8KXRShGEGmMttluw Τον Μάιο του 2020 ψηφίστηκε νέος νόμος με τον οποίο οι διαδικτυακές πλατφόρμες υποχρεούντο να «κατεβάζουν» εντός είκοσι τεσσάρων ωρών παράνομο περιεχόμενο, συμπεριλαμβανομένου περιεχομένου ρητορικής

της παραπληροφόρησης. Στην Ελλάδα η διάδοση και διασπορά ψευδών ειδήσεων και της παραπληροφόρησης αντιμετωπίζεται από πληθώρα διατάξεων που δύνανται να συρρέουν μεταξύ του και συγκεκριμένα το άρθρο 162 και 191 του Ποινικού Κώδικα, το άρθρο 182 του ν. 1815/1988, το άρθρο 112 παρ. 2 του ΠΔ 26/2012 και τα άρθρα 31 και 37 του ν. 4443/2016.

### Γ.1.1. ΤΟ ΑΔΙΚΗΜΑ ΤΟΥ ΑΡΘΡΟΥ 191 ΠΚ

Κυρίως όμως το εν λόγω έγκλημα ρυθμίζεται από τη διάταξη του άρθρου 191 ΠΚ, η οποία σύμφωνα με το νέο Ποινικό Κώδικα, όπως είχε αντικατασταθεί το άρθρο 191 ΠΚ με το άρθρο 36 Ν.4855/2021, ΦΕΚ Α` 215/12.11.2021, το οποίο τροποποιήθηκε πολύ πρόσφατα με το άρθρο 41 Ν.5005/2022, ΦΕΚ Α 236/21.12.2022, έχει ως εξής: *"Όποιος δημόσια ή μέσω του διαδικτύου διαδίδει ή διασπείρει με οποιονδήποτε τρόπο ψευδείς ειδήσεις με αποτέλεσμα να προκαλέσει φόβο σε αόριστο αριθμό ανθρώπων ή σε ορισμένο κύκλο ή κατηγορία προσώπων που αναγκάζονται έτσι να προβούν σε μη προγραμματισμένες πράξεις ή σε ματαίωσή τους, με κίνδυνο να προκληθεί ζημία στην οικονομία, στην αμυντική ικανότητα της χώρας ή στη δημόσια υγεία τιμωρείται με φυλάκιση έως τρία (3) έτη ή με χρηματική ποινή. Με την ίδια ποινή τιμωρείται και ο πραγματικός ιδιοκτήτης ή εκδότης του μέσου με το οποίο τελέστηκαν οι πράξεις του παρόντος.»* [279]

Το αδίκημα του άρθρου 191 ΠΚ είναι έγκλημα συγκεκριμένης διακινδύνευσης, καθώς για την πλήρωση της αντικειμενικής υπόστασης απαιτείται η πρόκληση φόβου ως αποτελέσματος σε αόριστο αριθμό ανθρώπων ή σε ορισμένο κύκλο ή κατηγορία προσώπων που αναγκάζονται έτσι να προβούν σε μη προγραμματισμένες πράξεις ή σε ματαίωσή τους, με κίνδυνο να προκληθεί ζημία στα πεδία της εθνικής οικονομίας, της αμυντικής ικανότητας της χώρας και της δημόσιας υγείας.[280]

Η ισχύουσα διάταξη αναφέρεται στην παραβίαση της ελευθερίας της ενημέρωσης και πληροφόρησης του λαού, αφού προσδιορίστηκαν μόνο εκείνες οι πράξεις που θέτουν σε κίνδυνο τη δημόσια τάξη και θεμελιώδεις τομείς της, όπως η οικονομία, η αμυντική ικανότητα της χώρας και η δημόσια υγεία. Πλέον δεν ποινικοποιείται η διασπορά απλών «φημών», όπως στο άρθρο 191 προϊσχύσαντος ΠΚ, αλλά μόνον ψευδών ειδήσεων.[281] Έπειτα, απαιτείται η επέλευση αποτελεσμάτων με αιτιώδη συνάφεια, δηλαδή ο φόβος των ανθρώπων λόγω των ψευδών ειδήσεων και ο εξαναγκασμός τους να προχωρήσουν σε ενέργειες που δεν έχουν προγραμματίσει ή να ματαιώσουν άλλες. Περαιτέρω, εξαιτίας αυτής της συμπεριφοράς των πολιτών απαιτείται όχι μόνο

μίσους, υπό την απειλή υψηλότατων προτίμων και φυλάκισης (βλ. url: https://techcrunch.com/2020/05/14/france-passes-law-forcing-onlineplatforms-to-delete-hate-speech-content-within-24-hours/?guccounter=2), διατάξεις που όμως κρίθηκαν αντισυνταγματικές μόλις τον επόμενο μήνα από το Συνταγματικό Δικαστήριο της χώρας (για την απόφαση, στη γαλλική γλώσσα βλ. https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm).

[279] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/

[280] https://www.lawspot.gr/nomika-nea/fake-news-tropopoieitai-i-diataxi-toy-poinikoy-kodika-gia-ti-diaspora-pseydon-eidiseon

[281] ΑναφΕισΠλημΑθ 116/2021, NOMOS

να προκλήθηκε πραγματική ζημία στην οικονομία, στην αμυντική ικανότητα της χώρας ή στη δημόσια υγεία, αλλά και κίνδυνος πρόκλησης αυτής της ζημίας με αποτέλεσμα την κοινωνική αναταραχή.[282]

Προστατευόμενο έννομο αγαθό είναι η δημόσια τάξη τόσο στην κοινωνική όσο και στην πολιτειακή της μορφή.[283] Ειδικότερα, εκτός από την κοινωνική ευταξία, την ειρηνική και ήρεμη συνύπαρξη των πολιτών στην κοινωνία, προσβάλλεται και η απρόσκοπτη επιβολή της κρατικής βούλησης στους τομείς της οικονομίας, της αμυντικής ικανότητας της χώρας ή της δημόσιας υγείας.[284]

Δράστης μπορεί να είναι οποιοσδήποτε, ενώ αντικείμενο του εγκλήματος είναι αόριστος αριθμός προσώπων που ειρηνικά συνυπάρχουν σε ορισμένο κοινωνικό χώρο σε κατάσταση ευταξίας αλλά και ορισμένος κύκλος προσώπων. Εγκληματική συμπεριφορά συνιστά η δημόσια ή μέσω του διαδικτύου διάδοση ή διασπορά με οποιονδήποτε τρόπο ψευδών ειδήσεων, με αποτέλεσμα να προκληθεί φόβος σε αόριστο αριθμό ανθρώπων ή σε ορισμένο κύκλο ή κατηγορία προσώπων. Ως συνέπεια του φόβου τους, οι αποδέκτες των ψευδών ειδήσεων αναγκάζονται να προβούν σε μη προγραμματισμένες πράξεις ή σε ματαίωση προγραμματισμένων πράξεων. Εξαιτίας αυτών των ενεργειών τους, δημιουργείται κίνδυνος να προκληθεί ζημία στην οικονομία, στην αμυντική ικανότητα της χώρας ή στη δημόσια υγεία.[285]

Είδηση είναι η ανακοίνωση γεγονότος του παρόντος ή του πρόσφατου παρελθόντος και όχι του μέλλοντος ή του απώτερου παρελθόντος.[286] Δεν αρκούν απλά σχόλια ή εσφαλμένες εκτιμήσεις ή κρίσεις (βλ. Γνωμ. ΕισΑΠ 3/64 ΠΧ ΙΔ 119). Ψευδής είναι η είδηση που δεν ανταποκρίνεται αντικειμενικά -και όχι κατά την εντύπωση του δράστη- στην αλήθεια, επειδή αναφέρεται σε ανύπαρκτο γεγονός. [287]

---

[282] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη

[283] ΑΠ Ολ 212017 ΠοινΧρ 2018, 22, ΑΠ 1519/2004 2004, 1552, ΑΠ 1126/1994 ΝΟΒ 1995, 93, ΑΠ 1463/1981 1982, 312, 45/2015 ΠοινΔικ 2015, 521

[284] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη

[285] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη

[286] ΑΠ 781/1976 ποινχρ 1977, 221, ΠλημΡοδοπ 80/1974 ποινχρ 1974, 709, ΓνωμΕισΑΠ 3/1964 ποινχρ 1964, 119

[287] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 532

Το έγκλημα τελείται και με διασπορά της ψευδούς είδησης και με διάδοσή της, αρκεί να γίνεται δημόσια αντιληπτή από αόριστο αριθμό ανθρώπων, γιατί μόνον τότε προσβάλλεται η δημόσια τάξη. Η διασπορά μπορεί να τελεστεί επανειλημμένα ή και μόνο μια φορά, με οποιονδήποτε τρόπο και μέσο, προφορικά, εγγράφως, με συμβολικές παραστάσεις, μέσω του τύπου ή μέσω του διαδικτύου και των μέσων κοινωνικής δικτύωσης, εφόσον λαμβάνει γνώση αόριστος αριθμός ανθρώπων και όχι μόνο φίλοι του δράστη στα μέσα κοινωνικής δικτύωσης (facebook, instagram κ.λπ.), διότι τότε λείπει ο «δημόσιος» χαρακτήρας της διάδοσης ή διασποράς. Αυτές δε οι αντιδράσεις αόριστου αριθμού πολιτών ή ενός κύκλου ή κατηγορίας ανθρώπων αποτελούν τη βλάβη που υφίσταται το έννομο αγαθό της δημόσιας τάξης, με την προϋπόθεση ότι εξαιτίας των αντιδράσεων αυτών κινδύνευσε να ζημιωθεί η οικονομία κ.λπ. (λ.χ. μαζική ανάληψη τραπεζικών καταθέσεων και κίνδυνος κατάρρευσης του τραπεζικού συστήματος). Όσον αφορά στην υποκειμενική υπόσταση του εγκλήματος απαιτείται δόλος, τουλάχιστον ενδεχόμενος, που να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης. Ο εκ δόλου δράστης τιμωρείται με φυλάκιση έως 3 έτη ή χρηματική ποινή.[288]

### Γ.1.2. ΠΑΡΑΔΕΙΓΜΑΤΑ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ ΜΕ ΤΗ ΧΡΗΣΗ ΤΩΝ DEEPFAKES

Ένα από τα πρώτα deepfake video είναι αυτό του προέδρου Μπαράκ Ομπάμα, το οποίο φυσικά δημιουργήθηκε με σκοπό να δείξει πόσο εύκολο είναι να βάλεις κάποιον να λέει πράγματα που δεν έχει πει ποτέ. Σε αυτό το βίντεο, ο Πρόεδρος Ομπάμα μιλούσε με τη δική του φωνή και "μιμούνταν" τα λόγια του δημιουργού του βίντεο, μερικά από τα οποία ήταν απίθανο να ειπωθούν από τον πραγματικό Ομπάμα. Οι βαθιές ψευδείς ειδήσεις μπορούν να έχουν τεράστιες αρνητικές συνέπειες για τις δημοκρατίες: τα fake news στοχεύουν στη βλάβη της φήμης ορισμένων ατόμων, παρουσιάζουν ψεύτικα γεγονότα ως αληθινά ή επηρεάζουν δημοκρατικές διαδικασίες όπως εκλογικές εκστρατείες.

Πρόσφατα είδαμε ότι τα deepfake μπορούν να έχουν τρομακτικά αποτελέσματα και να αποτελέσουν απειλή για την εθνική ασφάλεια ή να βλάψουν τις διεθνείς σχέσεις. Τρομακτικό παράδειγμα αποτελεί τα video που δημιουργήθηκαν με πρωταγωνιστή τον πρόεδρο της Ουκρανίας Volodymyr Zelensky κατά τη ρωσική εισβολή στη χώρα. Αυτό το τρομακτικό παράδειγμα μεταδόθηκε από έναν χακαρισμένο ουκρανικό τηλεοπτικό σταθμό μόλις ένα μήνα μετά τη ρωσική εισβολή στη χώρα. Δείχνει τον Zelensky να διατάζει τα στρατεύματα της χώρας να παραδοθούν στη Ρωσία. Αν και η ποιότητα είναι κακή και δεν φαίνεται πολύ πειστική, είναι ένα παράδειγμα του γιατί οι άνθρωποι ανησυχούν τόσο πολύ ότι τα deepfakes θα μπορούσαν να χρησιμοποιηθούν για τη διάδοση ψευδών ειδήσεων.

[288] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 533

Χαρακτηριστικό παράδειγμα αποτελούν και τα ψευδή βίντεο που έχουν δημιουργηθεί στο πλαίσιο της εκλογικής εκστρατείας του Ντόναλντ Τραμπ. Στις τελευταίες εκλογές στις ΗΠΑ, διαδόθηκαν διάφορα deepfake, είτε με τη μορφή video, είτε με τη μορφή εικόνων ή memes, με πρωταγωνιστή τον σημερινό πρόεδρο των ΗΠΑ, Τζό Μπάιντεν. Τα πλάνα του Μπάιντεν που τον δείχνουν να μιλάει με τη γλώσσα του έξω διαδόθηκαν κατά τη διάρκεια των εκλογών στις ΗΠΑ το 2020 (Frum, 2020). Τα βίντεο ήταν μονταρισμένα και παραποιημένα σε μια προσπάθεια να διακωμωδήσουν τον Μπάιντεν, ωστόσο παρά το γεγονός ότι πολλοί από τους υποστηρικτές του Τραμπ είδαν και κοινοποίησαν το βίντεο ακόμη και κατά τη διάρκεια των κρίσιμων ημερών πριν από τις αμερικανικές εκλογές του 2020, τα βίντεο ήταν μετρίως αποτελεσματικά στην υποτίμηση της εικόνας του Μπάιντεν (Burns, 2020).[289]

Πολλές χώρες όπως οι ΗΠΑ έχουν ψηφίσει ειδικές διατάξεις για να αντιμετωπίσουν τη διάδοση deepfake που βάζουν σε κίνδυνο τις δημοκρατικές διαδικασίες. Από την άλλη όμως, ίσως η παραχώρηση υπερβολικών δικαιωμάτων "λογοκρισίας" σε διοικητικές υπηρεσίες μπορεί να λειτουργήσει ως αντισυνταγματικός περιορισμός της ελευθερίας του λόγου. Μπορεί να υποστηριχθεί η άποψη ότι οι ψεύτικες ειδήσεις (συμπεριλαμβανομένων των deepfakes) που μοιράζονται στα μέσα κοινωνικής δικτύωσης τείνουν να έχουν ισχυρότερη επίδραση από τις συνηθισμένες πολιτικές εκστρατείες.[290]

Άλλο χαρακτηριστικό παράδειγμα από το σύντομο παρελθόν, αποτελούν οι ψευδείς ειδήσεις σχετικά με τα εμβόλια Covid, οδηγώντας σε μείωση των ατόμων που θέλουν να εμβολιαστούν. Επιπλέον, έχουμε δει ότι μπορεί ένας πολιτικός ηγέτης να διανείμει ένα βίντεο, κάνοντας να φαίνεται ότι υπάρχουν χιλιάδες υποστηρικτές στις συγκεντρώσεις του, ενώ στην πραγματικότητα παρευρίσκονται ελάχιστα άτομα.[291]

## Γ.2. ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΑΛΛΟΙΩΣΗΣ ΕΝΟΣ ΠΡΟΣΤΑΤΕΥΟΜΕΝΟΥ ΕΡΓΟΥ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ

Ζητήματα τίθενται σχετικά με την χρήση της Deepfake τεχνολογίας και από την σκοπιά της πνευματικής ιδιοκτησίας. Πρώτον, ανακύπτει το ερώτημα κατά πόσο επιτρέπεται η αναμετάδοση και αλλοίωση του βίντεο. Επιπλέον, πρόβλημα προκύπτει και κατά τη χρήση βιβλιοθήκης φωτογραφιών ενός ατόμου, τις οποίες ο δημιουργός του deepfake μπορεί να τροφοδοτήσει στο λογισμικό, ενώ ζήτημα ανακύπτει σχετικά με την παραβίαση του ατόμου επί της ίδιας εικόνας του.

[289] Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054

[290] DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society

[291] DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society

## Γ.2.1. Η ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ ΥΠΟ ΤΟ ΦΩΣ ΤΩΝ ΔΙΑΤΑΞΕΩΝ ΤΟΥ Ν. 2121/1993

Πριν όμως αναφερθούμε επί της ουσίας στα ζητήματα αυτά, κρίνεται σκόπιμο να αναφερθούν βασικές έννοιες, ορισμοί και διατάξεις περί προστασίας έργων πνευματικής ιδιοκτησίας. Η πνευματική ιδιοκτησία συγκαταλέγεται στα δικαιώματα που προστατεύει η Διακήρυξη των Δικαιωμάτων του Ανθρώπου του ΟΗΕ (άρ. 27 παρ. 2) και ο Χάρτης Θεμελιωδών Δικαιωμάτων στο άρ. 17 παρ. 2.

Η πνευματική ιδιοκτησία συνιστά κατ' αρχάς ιδιοκτησία, δηλαδή κάθε περιουσιακό δικαίωμα ή αγαθό του προσώπου. Από την άλλη πλευρά η πνευματική ιδιοκτησία αποτελεί συμμετοχή στην οικονομική ζωή. Ως μέσο χρηματοδότησης του δημιουργού, ώστε αυτός να συνεχίσει να προσφέρει στην κοινή απόλαυση, το δικαίωμα πνευματικής ιδιοκτησίας θα μπορούσε να εύρει κατά το περιουσιακό του σκέλος συνταγματικό έρεισμα στην διάταξη του άρθρου 5 παρ. 1 του Συντάγματος και στη ΣΛΕΕ 28 επ. 56 επ. Ακόμη η πνευματική ιδιοκτησία αποτελεί εκδήλωση της προσωπικότητας του δημιουργού.[292]

Βασική έννοια της πνευματικής ιδιοκτησίας είναι αυτή του έργου. Ως έργο νοείται το ανθρώπινο δημιούργημα, χωρίς πάντως να αποκλείεται η χρήση τεχνικών μέσων. Ως πνευματικό νοείται το έργο αξιολογούμενο αυτό καθ' αυτό, ανεξάρτητα από την περαιτέρω χρησιμότητά του.[293] Κατ' άρθρο 2 παρ. 1 Ν. 2121/1993 το έργο θα πρέπει να είναι πρωτότυπο, να μπορεί δηλαδή να χαρακτηρίζει τον συγκεκριμένο πνευματικό δημιουργό, να φέρει την προσωπική του σφραγίδα. Το άρθρο 6 ν 2121/1993 ορίζει ότι ο δημιουργός του έργου είναι ο αρχικός δικαιούχος του περιουσιακού και του ηθικού δικαιώματος επ' αυτού.[294]

Περιουσιακό δικαίωμα εννοείται η οικονομική εκμετάλλευση του έργου, δηλαδή το οικονομικό όφελος που μπορεί να προσπορίσει στον δημιουργό του. Το έργο θα πρέπει να απευθύνεται στο κοινό, που σύμφωνα με τη νομολογία του ΔΕΕ και των εθνικών δικαστηρίων κοινό είναι αόριστος αριθμός δυνητικών αποδεκτών, κατά δε το άρθρο 3 παρ. 2 ν. 2121/1993 κύκλος προσώπων ευρύτερος από την οικογένεια ή το άμεσο κοινωνικό περιβάλλον.

Το σύνολο των εξουσιών του έργου που ανήκουν στον δημιουργό, απαριθμούνται ενδεικτικά στο άρθρο 3 ν. 2121/1993, σύμφωνα με το οποίο *«Το περιουσιακό δικαίωμα δίνει στους δημιουργούς ιδίως την εξουσία (δικαίωμα) να επιτρέπουν ή να απαγορεύουν: α) Την εγγραφή και την άμεση ή έμμεση, προσωρινή ή μόνιμη αναπαραγωγή των έργων τους με οποιοδήποτε μέσο και μορφή, εν όλω*

[292] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018
[293] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018
[294] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/

*ή εν μέρει β) Τη μετάφραση των έργων τους γ) Τη διασκευή, την προσαρμογή ή άλλες μετατροπές των έργων τους. δ) Όσον αφορά το πρωτότυπο ή τα αντίτυπα (αντίγραφα) των έργων τους, τη διανομή τους στο κοινό με οποιαδήποτε μορφή μέσω πώλησης ή με άλλους τρόπους. ... ε) Την εκμίσθωση, όσον αφορά το πρωτότυπο ή τα αντίτυπα των έργων τους. ... στ) Τη δημόσια εκτέλεση των έργων τους ζ) Τη μετάδοση ή αναμετάδοση των έργων τους στο κοινό με τη ραδιοφωνία και την τηλεόραση, με ηλεκτρομαγνητικά κύματα ή με καλώδια ή με άλλους υλικούς αγωγούς ή με οποιονδήποτε άλλο τρόπο, παραλλήλως προς την επιφάνεια της γης ή μέσω δορυφόρων η) Την παρουσίαση στο κοινό των έργων τους, ενσυρμάτως ή ασυρμάτως ή με οποιονδήποτε άλλο τρόπο, καθώς και να καθιστούν προσιτά τα έργα τους στο κοινό κατά τρόπο ώστε οποιοσδήποτε να έχει πρόσβαση στα έργα αυτά, όπου και όταν επιλέγει ο ίδιος. ... θ) Την εισαγωγή αντιτύπων των έργων τους που παρήχθησαν στο εξωτερικό χωρίς τη συναίνεση του δημιουργού...»*[295]

Σύμφωνα με το αρ. 1 ν. 2121/1993 ο δημιουργός έχει εκτός από τα περιουσιακά δικαιώματα εξουσίες και το ηθικό δικαίωμα πάνω στο έργο του, δηλαδή την προστασία του προσωπικού δεσμού του δημιουργού προς το έργο του. Στο άρθρο 4 ν. 2121/1993 καθορίζονται η επιμέρους ηθικές αξίες και συγκεκριμένα: *«Το ηθικό δικαίωμα δίνει στο δημιουργό ιδίως τις εξουσίες: α) της απόφασης για το χρόνο, τον τόπο και τον τρόπο κατά τους οποίους το έργο θα γίνει προσιτό στο κοινό (δημοσίευση), β) της αναγνώρισης της πατρότητάς του πάνω στο έργο και ειδικότερα την εξουσία να απαιτεί, στο μέτρο του δυνατού, τη μνεία του ονόματός του στα αντίτυπα του έργου του και σε κάθε δημόσια χρήση του έργου του ή, αντίθετα, να κρατάει την ανωνυμία του ή να χρησιμοποιεί ψευδώνυμο, γ) της απαγόρευσης κάθε παραμόρφωσης, περικοπής ή άλλης τροποποίησης του έργου του, καθώς και κάθε προσβολής του δημιουργού οφειλομένης στις συνθήκες παρουσίασης του έργου στο κοινό, δ) της προσπέλασης στο έργο του, έστω και αν το περιουσιακό δικαίωμα στο έργο ή η κυριότητα στον υλικό φορέα του έργου ανήκει σε άλλον, οπότε η προσπέλαση πρέπει να πραγματοποιείται κατά τρόπο που προκαλεί τη μικρότερη δυνατή ενόχληση στο δικαιούχο, ε) προκειμένου περί έργων λόγου ή επιστήμης, της υπαναχώρησης από συμβάσεις μεταβίβασης του περιουσιακού δικαιώματος ή εκμετάλλευσής του ή άδειας εκμετάλλευσής του εφόσον αυτό είναι αναγκαίο για την προστασία της προσωπικότητάς του εξαιτίας μεταβολής στις πεποιθήσεις του ή στις περιστάσεις και με καταβολή αποζημίωσης στον αντισυμβαλλόμενο για τη θετική του ζημία.»*[296]

Κανένα δικαίωμα δεν είναι απεριόριστο, ούτε η πνευματική ιδιοκτησία. Στο νόμο 2121/1993 οι περιορισμοί του δικαιώματος της πνευματικής ιδιοκτησίας περιγράφονται στα άρθρα 18-28Γ. Ο κανόνας των τριών βαθμίδων (3 step test) απευθύνεται στον εθνικό νομοθέτη και του επιβάλλει να θέσει περιορισμούς στο δικαίωμα πνευματικής ιδιοκτησίας. Ο οποιοσδήποτε εθνικός νομοθετικός περιορισμός του δικαιώματος πνευματικής ιδιοκτησίας επιβάλλεται να πληροί σωρευτικά τους

[295] https://opi.gr/vivliothiki/2121-1993#a3
[296] https://opi.gr/vivliothiki/2121-1993#a4

ακόλουθους τρεις όρους, κατά τρόπο που να μην είναι αποδεκτός από την έννομη τάξη, αν δεν ανταποκρίνεται έστω και σε έναν από αυτούς: α) να είναι ειδικώς καθορισμένοι ευθύς εξαρχής, β) να μην παραβλάπτουν την κανονική εκμετάλλευση του έργου και γ) να είναι αντικειμενικώς δικαιολογημένοι.[297]

Τα δικαιώματα κάθε ιδιοκτησίας δεν δύνανται να ασκούνται σε βάρος του γενικού συμφέροντος. Στο νόμο 2121/1993 προβλέπονται περιορισμοί προς χάριν του γενικού συμφέροντος και συγκεκριμένα, εξαιρέσεις α) υπέρ της ελευθερίας της έκφρασης, ήτοι το επιτρεπτό της παράθεσης αποσπασμάτων προς υποστήριξη ή κριτική της γνώμης άλλου, όπως αυτές ορίζονται στο άρθρο 19 ν. 2121/1993, β) υπέρ της διαδόσεως της γνώσης, της συμμετοχής στην κοινωνία της πληροφορίας του δικαιώματος να γίνεται κανείς αποδέκτης της έκφρασης, του λόγου και της τέχνης του δημιουργού, γ) υπέρ της ενημερώσεως του κοινού για επίκαιρα καλλιτεχνικά γεγονότα κ.α. όπως ορίζονται στο άρθρο 25 ν. 2121/1993 δ) υπέρ του παθητικού δικαιώματος του κοινού στην Τέχνη, ήτοι της περιστασιακής δημόσιας εκτέλεσης έργων για επίσημες ή εκπαιδευτικές τελετές ή εκδηλώσεις και της περιστασιακής δημόσιας εκθέσεως εικόνων εικαστικών και φωτογραφικών έργων όπως ορίζονται στο άρθρο 26 ν. 2121/1993.

Περιορισμοί τίθενται και για χάρη των συμφερόντων ιδιωτών. Επί αναπαραγωγής για ιδιωτική χρήση ο χρήστης δεν εκμεταλλεύεται οικονομικώς το έργο, ακόμη και όταν το αποθηκεύει. Η ιδιωτικότητα σημαίνει έλλειψη κοινού και απεύθυνσης σ' αυτό. Συνεπώς, θα πρέπει να περιορίζεται σε περιορισμένο αριθμό προσώπων με φιλικό ή οικογενειακό δεσμό.[298] Σύμφωνα με το άρθρο 28 ν. 2121/1993 *«1. Επιτρέπεται, χωρίς την άδεια του δημιουργού και χωρίς αμοιβή, η παρουσίαση στο κοινό έργων των εικαστικών τεχνών μέσα σε μουσεία, που έχουν την κυριότητα του υλικού φορέα όπου έχει ενσωματωθεί το έργο, ή στο πλαίσιο εκθέσεων, που οργανώνονται σε μουσεία. 2. Επιτρέπεται, χωρίς την άδεια του δημιουργού και χωρίς αμοιβή, η παρουσίαση στο κοινό και η αναπαραγωγή σε καταλόγους έργου των εικαστικών τεχνών στο μέτρο που αυτό είναι αναγκαίο για την διευκόλυνση της πώλησης του έργου. 3. Στις περιπτώσεις των δύο προηγούμενων παραγράφων, η αναπαραγωγή επιτρέπεται μόνο εφόσον δεν παρεμποδίζει την κανονική εκμετάλλευση του έργου και δεν βλάπτει τα νόμιμα συμφέροντα του δημιουργού.»* [299]

Πέραν των περιουσιακών υπάρχουν και τα συγγενικά δικαιώματα, τα οποία απαριθμούνται περιοριστικά στα άρθρα 46 - 51Α του ν. 2121/1993 και αντικείμενα αυτών αποτελούν όσα μοιάζουν με τη δημιουργία του πνευματικού έργου ή ακριβέστερα "τα μέσα μεταφοράς" του

[297] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018
[298] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018
[299] https://opi.gr/vivliothiki/2121-1993#a28

πνευματικού έργου στο κοινό. Στην ουσία αντικείμενο συγγενικού δικαιώματος αποτελεί μια συγκεκριμένη μορφή προσφοράς του έργου στο κοινό, πχ. απαγγελία, ερμηνεία κλπ.[300]

Προσβολή των πνευματικών δικαιωμάτων συντρέχει όταν τρίτος θίγει την άσκηση της εξουσίας του δικαιούχου, ήτοι προβαίνει σε συμπεριφορά στην οποία μόνον ο δικαιούχος νομιμοποιείται. Προσβολή του δικαιώματος συντρέχει όχι μόνο όταν κάποιος εκμεταλλεύεται το έργο, αλλά και όταν κάποιος απλώς ματαιώνει η διακωλύει την εκμετάλλευση αυτή.[301] Οι κυρώσεις διακρίνονται σε αστικές, οι οποίες αναφέρονται στο άρθρο 65 ν. 2121/1993. Όσον αφορά στις διοικητικές κυρώσεις αυτές προβλέπονται στο άρθρο 65Α ν. 2121/1993.

Τέλος, οι ποινικές κυρώσεις προβλέπονται στο άρθρο 66 του ν. 2121/1993, σύμφωνα με το οποίο «*1. Τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή 2.900 -15.000 ευρώ όποιος χωρίς δικαίωμα και κατά παράβαση των διατάξεων του παρόντος νόμου ή διατάξεων των κυρωμένων με νόμο πολυμερών διεθνών συμβάσεων για την προστασία της πνευματικής ιδιοκτησίας εγγράφει έργα ή αντίτυπα, αναπαράγει αυτά άμεσα ή έμμεσα, προσωρινά ή μόνιμα, με οποιαδήποτε μορφή, εν όλω ή εν μέρει, μεταφράζει, διασκευάζει, προσαρμόζει ή μετατρέπει αυτά, προβαίνει σε διανομή αυτών στο κοινό με πώληση ή με άλλους τρόπους ή κατέχει με σκοπό διανομής, εκμισθώνει, εκτελεί δημόσια, μεταδίδει ραδιοτηλεοπτικά κατά οποιονδήποτε τρόπο, παρουσιάζει στο κοινό έργα ή αντίτυπα με οποιονδήποτε τρόπο, εισάγει αντίτυπα του έργου που παρήχθησαν παράνομα στο εξωτερικό χωρίς τη συναίνεση του δημιουργού και γενικά εκμεταλλεύεται έργα, αντίγραφα ή αντίτυπα που είναι αντικείμενο πνευματικής ιδιοκτησίας ή προσβάλλει το ηθικό δικαίωμα του πνευματικού δημιουργού να αποφασίζει για τη δημοσίευση του έργου στο κοινό, καθώς και να παρουσιάζει αυτό αναλλοίωτο χωρίς προσθήκες ή περικοπές (άρθρο 8 παρ.1 Οδηγίας 2001/29). 2. Με την ίδια ποινή τιμωρείται όποιος κατά παράβαση των διατάξεων του παρόντος νόμου ή διατάξεων των κυρωμένων με νόμο διεθνών συμβάσεων για την προστασία συγγενικών δικαιωμάτων προβαίνει στις ακόλουθες πράξεις: Α) Χωρίς την άδεια των ερμηνευτών ή εκτελεστών καλλιτεχνών: α) εγγράφει σε υλικό φορέα την ερμηνεία ή εκτέλεση, β) αναπαράγει άμεσα ή έμμεσα, προσωρινά ή μόνιμα με οποιοδήποτε μέσο και μορφή, εν όλω ή εν μέρει, την εγγραφή της ερμηνείας ή εκτέλεσής τους σε υλικό φορέα, γ) προβαίνει σε διανομή στο κοινό του υλικού φορέα με την εγγραφή της ερμηνείας ή εκτέλεσης ή κατέχει με σκοπό διανομής, δ) εκμισθώνει τον υλικό φορέα με την εγγραφή της ερμηνείας ή εκτέλεσης, ε) μεταδίδει ραδιοτηλεοπτικά με οποιονδήποτε τρόπο τη ζωντανή ερμηνεία ή εκτέλεση, εκτός αν η μετάδοση αυτή αποτελεί αναμετάδοση νόμιμης μετάδοσης, στ) παρουσιάζει στο κοινό τη ζωντανή ερμηνεία ή εκτέλεση που γίνεται με οποιονδήποτε τρόπο, εκτός από ραδιοτηλεοπτική μετάδοση, ζ) διαθέτει στο κοινό, ενσυρμάτως ή ασυρμάτως, κατά τρόπο ώστε οποιοσδήποτε να έχει*

[300] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018

[301] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018

*πρόσβαση, όπου και όταν επιλέγει ο ίδιος, στην εγγραφή σε υλικό φορέα της ερμηνείας ή της εκτέλεσής τους Β) Χωρίς την άδεια των παραγωγών φωνογραφημάτων (παραγωγών υλικών φορέων ήχου) : α) αναπαράγει άμεσα ή έμμεσα, προσωρινά ή μόνιμα με οποιοδήποτε μέσο και μορφή, εν όλω ή εν μέρει, τα φωνογραφήματά τους, β) προβαίνει σε διανομή στο κοινό των ως άνω υλικών φορέων ή κατέχει με σκοπό διανομής, γ) εκμισθώνει τους ως άνω υλικούς φορείς, δ) διαθέτει στο κοινό, ενσυρμάτως ή ασυρμάτως, κατά τρόπο ώστε οποιοσδήποτε να έχει πρόσβαση, όπου και όταν ο ίδιος επιλέγει, στα φωνογραφήματά τους, ε) εισάγει τους ως άνω υλικούς φορείς που παρήχθησαν στο εξωτερικό χωρίς τη συναίνεσή του Γ) Χωρίς την άδεια των παραγωγών οπτικοακουστικών έργων (παραγωγών υλικών φορέων εικόνας ή ήχου και εικόνας) : α) αναπαράγει άμεσα ή έμμεσα, προσωρινά ή μόνιμα με οποιοδήποτε μέσο και μορφή, εν όλω ή εν μέρει, το πρωτότυπο και τα αντίτυπα των ταινιών τους, β) προβαίνει σε διανομή στο κοινό των ως άνω υλικών φορέων συμπεριλαμβανομένων και των αντιγράφων τους ή κατέχει με σκοπό διανομής, γ) εκμισθώνει τους ως άνω υλικούς φορείς, δ) διαθέτει στο κοινό, ενσυρμάτως ή ασυρμάτως, κατά τρόπο ώστε οποιοσδήποτε να έχει πρόσβαση στο πρωτότυπο και τα αντίτυπα των ταινιών τους, όπου και όταν ο ίδιος επιλέγει, ε) εισάγει τους ως άνω υλικούς φορείς που παρήχθησαν στο εξωτερικό χωρίς τη συναίνεσή του, στ) μεταδίδει ραδιοτηλεοπτικά τους ως άνω υλικούς φορείς με οποιονδήποτε τρόπο συμπεριλαμβανομένης και της δορυφορικής μετάδοσης ή καλωδιακής αναμετάδοσης, καθώς και της παρουσίασης στο κοινό Δ) Χωρίς την άδεια των ραδιοτηλεοπτικών οργανισμών: α) αναμεταδίδει τις εκπομπές τους με οποιονδήποτε τρόπο, β) παρουσιάζει στο κοινό τις εκπομπές τους σε χώρους όπου η είσοδος επιτρέπεται με εισιτήριο, γ) εγγράφει τις εκπομπές τους σε υλικούς φορείς ήχου ή εικόνας ή ήχου και εικόνας, είτε οι εκπομπές αυτές μεταδίδονται ενσυρμάτως είτε ασυρμάτως, συμπεριλαμβανομένης της καλωδιακής ή δορυφορικής μετάδοσης, δ) προβαίνει σε άμεση ή έμμεση, προσωρινή ή μόνιμη αναπαραγωγή με οποιοδήποτε μέσο και μορφή, εν όλω ή εν μέρει, της υλικής ενσωμάτωσης των εκπομπών τους, ε) προβαίνει σε διανομή στο κοινό των υλικών φορέων με την εγγραφή των εκπομπών τους, στ) εκμισθώνει τον υλικό φορέα με την εγγραφή των εκπομπών τους, ζ) διαθέτει στο κοινό, ενσυρμάτως ή ασυρμάτως, κατά τρόπο ώστε οποιοσδήποτε να έχει πρόσβαση, όπου και όταν ο ίδιος επιλέγει, στην υλική ενσωμάτωση των εκπομπών τους (άρθρο 8 παρ. 1 Οδηγίας 2001/29).»*[302] Στην τρίτη δε παράγραφο του άρθρου προβλέπονται και επιβαρυντικές περιστάσεις, ενώ στο ίδιο άρθρο υπάρχει πρόβλεψη για την προστασία των βάσεων δεδομένων ως πνευματικό έργο.

Με το άρθρο 81 του Ν 3057/2002 συμπληρώθηκε και τροποποιήθηκε ο Ν 2121/1993, με σκοπό να εισαχθούν οι ειδικότερες ρυθμίσεις της Οδηγίας 2001/29 ΕΕ για την ψηφιακή μορφή και κυκλοφορία των έργων λόγου και τέχνης. Έτσι, εισήχθησαν τα άρθρα 66Α και 66Β στο Ν 2121/1993. Αντίστοιχα, κατ' εφαρμογή των διατάξεων της Ευρωπαϊκής Οδηγίας 91/250 ΕΟΚ, με

[302] https://opi.gr/vivliothiki/2121-1993#a66

την οποία αναγνωρίστηκαν πνευματικά δικαιώματα σε Η/Υ, εξειδικεύτηκε η προστασία των πνευματικών δικαιωμάτων στο ελληνικό δίκαιο μέσω τροποποίησης του Ν. 2121/1993.[303]

## Γ.2.2. ΖΗΤΗΜΑΤΑ ΠΑΡΑΒΙΑΣΗΣ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΜΕ ΤΗ ΧΡΗΣΗ ΤΩΝ DEEPFAKES

### Γ.2.2.1. Δημοσίευση του αλλοιωμένου βίντεο

Στόχος του δημιουργού ενός αλλοιωμένου βίντεο, είναι να διανείμει αυτό εγκαίρως στο κοινό, γεγονός το οποίο συμβαίνει μέσω της δυνατότητας επικοινωνίας των κοινωνικών δικτύων.[304] Παράδειγμα αποτελεί το βίντεο στην πλατφόρμα Youtube με μια σκηνή από την ταινία "Shining,, όπου αντικαθίσταται το πρόσωπο του πρωταγωνιστή Jack Nicholson με αυτό του ηθοποιού Jim Carrey.[305]

Βασική προϋπόθεση για την παραβίαση δικαιώματος πνευματικής ιδιοκτησίας είναι η απουσία της συγκατάθεση του δικαιούχου. Ορισμένα δικαιώματα που παραβιάζονται είναι το περιουσιακό δικαίωμα αναπαραγωγής (το οποίο εφαρμόζεται ακόμη και όταν αλλοιώνεται η μορφή του προστατευόμενου έργου), το περιουσιακό δικαίωμα παρουσίασης στο κοινό, το δικαίωμα διασκευής και το ηθικό δικαίωμα του δημιουργού.[306]

Ωστόσο, υπάρχουν εξαιρέσεις και δεν υπάρχει πάντα προσβολή των δικαιωμάτων πνευματικής ιδιοκτησίας με τη χρήση της τεχνολογίας deepfake, οι οποίες προβλέπονται κυρίως στο άρθρο 5 της Οδηγίας 2001/29, το οποίο επιτρέπει την χρήση ενός προστατευόμενου έργου «για γελοιογραφία, παρωδία ή μίμηση». Δυστυχώς, ο Έλληνας νομοθέτης δεν θεώρησε απαραίτητο να ενσωματώσει την ανωτέρω διάταξη στην ελληνική νομοθεσία. Ενδεχομένως επειδή η σάτιρα προστατεύεται από το συνταγματικό δικαίωμα της ελευθερίας της έκφρασης. Μια τέτοια προσέγγιση όμως πρέπει πλέον να απορριφθεί έπειτα από τρεις πρόσφατες αποφάσεις του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), οι οποίες εκδόθηκαν την ίδια μέρα και επεσήμαναν

[303] Ουσιαστικές και δικονομικές διατάξεις της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο (Ν 4411/2016), Θεοχάρης Δαλακούρας, Καθηγητής Νομικής Σχολής ΔΠΘ, Δικηγόρος σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023

[304] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[305] https://youtu.be/HG_NZpkttXE

[306] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

με σαφήνεια ότι η άμεση επίκληση στα ανθρώπινα δικαιώματα ως μορφή περιορισμού των δικαιωμάτων των δικαιούχων δεν επιτρέπεται.[307]

Χαρακτηριστικό παράδειγμα δημοσίευσης αλλοιωμένου βίντεο αποτελεί αυτό που παραθέσαμε στο πρώτο κεφάλαιο της παρούσας εργασίας, σχετικά με την ταινία The Irishman του 2019, και το κλιπ που εμφανίστηκε, μετά την πρεμιέρα της ταινίας, στο YouTube με τίτλο "The Irishman De-Aging: Netflix Millions VS. Free Software!", το οποίο δημιούργησε και κοινοποίησε ένας ανώνυμος YouTuber με το όνομα "iFake".

Ακόμα και στην περίπτωση ενός βίντεο με πορνογραφικό περιεχόμενο, σε δικαιοδοσίες όπου η πορνογραφία προστατεύεται από πνευματικά δικαιώματα, οι δημιουργοί της ταινίας μπορούν να εγείρουν αξιώσεις σχετικά με την τροποποίηση του βίντεο.[308]

### Γ.2.2.2. Η χρήση της βιβλιοθήκης φωτογραφιών

Όπως αναφέρθηκε αναλυτικά στο πρώτο μέρος της εργασίας, για να γίνει η ανταλλαγή προσώπου, πρέπει να εισαχθούν ως δεδομένα εικόνες του προσώπου πηγής και του προσώπου στόχου, ώστε ο αλγόριθμος να μάθει το πρόσωπο το οποίο θα επικολλήσει στο βίντεο. Ωστόσο, είναι συμβατή η χρήση αυτών των φωτογραφιών με την πνευματική ιδιοκτησία; Στο αμερικανικό δίκαιο η δραστηριότητα αυτή θεωρείται δίκαιη. Στο ενωσιακό δίκαιο, όμως, η δραστηριότητα πρέπει να εμπίπτει σε συγκεκριμένη εξαίρεση ή περιορισμό, και προκύπτει το ζήτημα του κατά πόσο καλύπτεται η δραστηριότητα από την εξαίρεση της αναπαραγωγής για ιδιωτική χρήση.

Πρόσφατα, μέσω της Οδηγίας 2019/790, προστέθηκε μια νέας εξαίρεση σχετικά με την εξόρυξη δεδομένων (data mining), η οποία είναι υποχρεωτική και καλύπτει ακόμα και προστατευόμενα έργα, όπως φωτογραφίες. Η εξαίρεση αυτή εκπληρώνει τον σκοπό της όσον αφορά στη χρήση της Deepfake τεχνολογίας, δίνοντας στον χρήστη το δικαίωμα τροφοδότησης της τεχνητής νοημοσύνης με φωτογραφίες προσώπων, αλλά μόνο ο νόμιμος χρήστης δικαιούται την επίκληση στην εξαίρεση της εξόρυξης.[309]

Τι συμβαίνει, λοιπόν, όταν από την τεράστια βιβλιοθήκη φωτογραφιών ενός διάσημου προσώπου που υπάρχει στο διαδίκτυο, κάποιος κακόβουλος χρήστης αποθηκεύσει τις φωτογραφίες αυτές με

[307] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[308] Regulating deep fakes: legal and ethical considerations, Edvinas Meskys, Paulius Jurcys, Article in Journal of Intellectual Property Law & Practice · January 2020

[309] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

σκοπό να τις εισάγει ως δεδομένα σε έναν αλγόριθμο deepfake για να δημιουργήσει μια πλαστή εικόνα ή ένα ψεύτικο βίντεο;

### Γ.2.2.3. Το δικαίωμα επί της ιδίας εικόνας

Το Deepfake αποτελεί ξεκάθαρη απόδειξη ότι η εικόνα του προσώπου είναι αντικείμενο εκμετάλλευσης και εμπορευματοποίησης. Στο Ενωσιακό δίκαιο το δικαίωμα επί της ιδίας εικόνας προσεγγίζεται και αναλύεται από την σκοπιά της προστασίας της προσωπικότητας. Αντίθετα, στην Αμερική ισχύει το λεγόμενο "δικαίωμα στην δημοσιότητα (right to publicity), με αποτέλεσμα η προστασία της εικόνας του προσώπου να καθίσταται εξαιρετικά προβληματική από την σκοπιά των Deepfakes. Στην Γερμανία αναγνωρίζεται το δικαίωμα στην εικόνα ως μορφή διανοητικής ιδιοκτησίας ήδη από το 1907. Στην Ελλάδα, όμως, δεν αναγνωρίζεται ρητά ένα ειδικό δικαίωμα στην εικόνα ως μια μορφή διανοητικής ιδιοκτησίας, αλλά βασίζεται στην προστασία της προσωπικότητας.[310]

Ως εικόνα νοείται η εξωτερική μορφή του προσώπου, η οποία το εξατομικεύει, ενώ το right of publicity έγκειται στην εξουσία οικονομικής εκμετάλλευσης στοιχείων της προσωπικότητας, όπως η εικόνα. Στο μέτρο που τα εν λόγω στοιχεία μπορεί και να έγκειται και σε πληροφορίες, ήτοι δεδομένα προσωπικού χαρακτήρα, το ζήτημα διέπεται όχι μόνον από την ΑΚ 57, αλλά και από τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων. Σύμφωνα με τη νομολογία είναι ανεπίτρεπτη η εμπορευματοποίηση της εικόνας τρίτου και γενικότερα η οικονομική εκμετάλλευση στοιχείων της προσωπικότητας άλλου χωρίς τη συναίνεσή του. [311]

Πέραν των ως άνω διατάξεων, το ΕΔΔΑ τις τελευταίες δεκαετίες ανέπτυξε πλούσια νομολογία σχετικά με το δικαίωμα επί της ίδιας εικόνας ως έκφανση του δικαιώματος προστασίας του ιδιωτικού βίου. Σύμφωνα με την απόφαση Von Hannover κατά Γερμανίας το 2004 θεμελιώνεται η ύπαρξη του δικαιώματος επί της ίδιας εικόνας ακόμα και ενός δημοσίου προσώπου ενώ στην απόφαση του 2012 προσφέρεται ένα λεπτομερές σύστημα αξιολόγησης της αναλογικότητας μεταξύ ελευθερίας έκφρασης και σεβασμού του ιδιωτικού βίου. Από τη νομολογία αυτή συνάγεται το συμπέρασμα ότι κατά κανόνα απαιτείται η συναίνεση του προσώπου ή των αντιπροσώπων του, ωστόσο η συγκατάθεση αυτή υπαναχωρεί μπροστά στο κριτήριο του δημοσίου συμφέροντος του κοινού να ενημερωθεί σε σχέση με ότι αφορά σε δημόσια πρόσωπα. Το χαρακτηριστικό αυτό ερμηνεύεται ευρέως, με αποτέλεσμα η ελευθερία έκφρασης να υπερτερεί κατά τεκμήριο του

[310] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[311] Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018

δικαιώματος επί της ίδιας εικόνας. Όμως το αντίθετο ισχύει για την εικόνα των μη δημόσιων προσώπων.[312]

## Γ.3. ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΠΡΟΣΒΟΛΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η εικόνα κατά κανόνα αποτελεί προσωπικό δεδομένο και η τεχνολογία του Deepfake εμπίπτει στον ορισμό της επεξεργασίας, αφού η τεχνολογία απαιτεί εξαρχής την αναγνώριση του προσώπου, με συνέπεια να εφαρμόζονται ο Γενικός Κανονισμός Προστασίας προσωπικών δεδομένων και οι εθνικές διατάξεις. Το γεγονός ότι οι φωτογραφίες συχνά είναι ήδη προσβάσιμες στο διαδίκτυο δεν επηρεάζει αυτό το συμπέρασμα, καθώς κάθε επεξεργασία βασίζεται σε έναν ειδικό και συγκεκριμένο σκοπό.

### Γ.3.1. Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΥΠΟ ΤΟ ΦΩΣ ΤΟΥ ΓΚΠΔ

Σύμφωνα με το άρθρο 4 περ. 1 του ΓΚΠΔ ως δεδομένα προσωπικού χαρακτήρα νοείται *«κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου».*[313]

Προσωπικό δεδομένο είναι κάθε πληροφορία που σχετίζεται με την ταυτότητα συγκεκριμένου φυσικού προσώπου. Τα προσωπικά δεδομένα διακρίνονται σε απλά, όπως το όνομα ή η κατοικία και σε ευαίσθητα, που αποτελούν τον σκληρό πυρήνα της ιδιωτικής ζωής του ατόμου στο παρόν ή στο παρελθόν ή στο μέλλον και αφορούν τη φυλή, τις πολιτικές, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, την υγεία, την ερωτική ζωή, τα γενετικά δεδομένα κ.α..[314] Ο Άρειος Πάγος έχει κρίνει ότι «για να εμπίπτει η πληροφορία[…] στην έννοια του προσωπικού δεδομένου, θα πρέπει να συνδέεται άμεσα με το υποκείμενο και τις, προσωπικού χαρακτήρα, ιδιότητες ή εκδηλώσεις αυτού».[315] Σύμφωνα με την Ομάδα προστασίας δεδομένων του άρθρου 29, Γνώμη 4/2007 «ως δεδομένα προσωπικού χαρακτήρα γίνονται δεκτά και τα ηχητικά ή οπτικά δεδομένα στο μέτρο που συνιστούν πληροφορίες για ένα φυσικό πρόσωπο.»

Κατά τους ορισμούς και του άρθρου 2 στοιχείο α΄ και γ΄ 2472/1997 και ερμηνεύοντας γραμματικά τη διάταξη, προκύπτει ότι για να είναι μια πληροφορία προσωπικό δεδομένο, πρέπει το φυσικό

---

[312] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[313] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf

[314] Προσωπικά Δεδομένα, Ευγενία Αλεξανδροπούλου Αιγυπτιάδου, Νομική Βιβλιοθήκη, 2016

[315] Βλ. ΑΠ 637/2013

πρόσωπο να μπορεί να ταυτοποιείται. Σύμφωνα με την απόφαση 41/2017 της ΑΠΔΠΧ «η δυνατότητα ταυτοποίησης ενός προσώπου πρέπει να εξετάζεται διασταλτικά καθώς η βούληση του νομοθέτη είναι να εξασφαλιστεί αποτελεσματική προστασία στο υποκείμενο των δεδομένων.» Για να προκύπτει άμεσα, το πρόσωπο πρέπει να γίνεται άμεση αναφορά σε αυτό ή έμμεσα, όπως με τη φωτογράφισή του ή με τον αριθμός δελτίου ταυτότητας κλπ.[316]

Υποκείμενο των προσωπικών δεδομένων είναι το φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα. Υπεύθυνος επεξεργασίας είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων, και συνακόλουθα φέρει και την ευθύνη για την επεξεργασία, ο οποίος οφείλει να ανταποκρίνεται σε ορισμένες νόμιμες υποχρεώσεις. Εκτελών την επεξεργασία είναι ο οποιοσδήποτε επεξεργάζεται προσωπικά δεδομένα για λογαριασμό υπεύθυνου επεξεργασίας. Τρίτος είναι κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων. Αρχείο προσωπικών δεδομένων είναι κάθε διαρθρωμένο σύνολο δεδομένων, τα οποία είναι προσιτά με γνώμονα συγκεκριμένα κριτήρια. Αποδέκτης είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, στον οποίο ανακοινώνονται ή μεταδίδονται τα δεδομένα, ανεξαρτήτως αν πρόκειται για τρίτο ή όχι.[317]

Σύμφωνα με το άρθρο 4 περ. 2 του Κανονισμού ως επεξεργασία νοείται *«κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή».*[318]

Προκειμένου να διαπιστωθεί η νομιμότητα της επεξεργασίας ακολουθείται και εδώ η δοκιμασία των τριών σταδίων: πρώτα ερευνάται αν η επεξεργασία εφαρμόζει τις αρχές επεξεργασίας, στη συνέχεια ερευνάται αν υπάρχει η συγκατάθεση του υποκειμένου και τέλος ερευνάται αν η επεξεργασία είναι νόμιμη.

Σύμφωνα με το άρθρο 5 παρ. 1 περ. α' ΓΚΠΔ «*τα δεδομένα θα πρέπει να τυγχάνουν επεξεργασίας μόνο εάν συντρέχει νόμιμος λόγος προς τούτο, και μάλιστα στο βαθμό που η επεξεργασία διεξάγεται με σύννομο, θεμιτό και διαφανή τρόπο προς τα υποκείμενα των δεδομένων.»*[319] Για να είναι νόμιμη η επεξεργασία πρέπει να θεμελιώνεται σε μία τουλάχιστον από τις προϋποθέσεις που τίθενται στο

[316] Ι.Ιγγλεζάκης Δ. Ιωάννης «Επεξεργασία δεδομένων εικόνας ή/και ήχου μέσω φωτογράφησης και βιντεοσκόπησης από δικαστικό επιμελητή κατά τη διαδικασία αναγκαστικής εκτέλεσης (γνωμοδότηση)». ΔΙΜΕΕ 10/2013 σελ. 172 επ.
[317] Προσωπικά Δεδομένα, Ευγενία Αλεξανδροπούλου Αιγυπτιάδου, Νομική Βιβλιοθήκη, 2016
[318] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
[319] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf

αρ. 6. Πιο συγκεκριμένα, θα πρέπει «*να έχει συναινέσει το υποκείμενο των δεδομένων στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.*»[320] Σύμφωνα με το α. 7 ΓΚΠΔ, η συγκατάθεση πρέπει να είναι ελεύθερη και ελευθέρως ανακληθείσα, δηλαδή το υποκείμενο των δεδομένων να έχει αληθινή ή ελεύθερη επιλογή ή να είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεση χωρίς να ζημιωθεί ανά πάσα στιγμή και σε αυτή την περίπτωση τα δεδομένα πρέπει να διαγράφονται ή να ανωνυμοποιούνται από τον υπεύθυνο επεξεργασίας.[321],[322]

Επιπλέον, η επεξεργασία είναι απαραίτητη ***α)*** *για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,* ***β)*** *για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, γ) για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, δ) για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, ε) για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.*[323]

Η επεξεργασία προσωπικών δεδομένων και κυρίως των ευαίσθητων πρέπει να εξασφαλίζει όσο το δυνατόν μικρότερη εισβολή στην ιδιωτική και οικογενειακή ζωή του υποκειμένου των δεδομένων ώστε να προστατεύεται αυτή από τη μία και από την άλλη η ελευθερία της έκφρασης, ιδίως μάλιστα όταν πρόκειται για δημοσίευση ευαίσθητων δεδομένων που αφορούν την ερωτική ζωή του υποκειμένου των δεδομένων. Σύμφωνα με την αρχή της αναλογικότητας, πρέπει να συνδέεται ο σκοπός της επεξεργασίας με τα δεδομένα, με την έννοια ότι αυτά πρέπει να είναι συναφή για την επίτευξη του σκοπού της επεξεργασίας, αφετέρου όσο το δυνατόν λιγότερα, δηλαδή τα απολύτως απαραίτητα δεδομένα.[324]

Σύμφωνα με την αρχή της καθορισμένης χρονικής διάρκειας διατήρησης των δεδομένων, τα δεδομένα αυτά πρέπει να είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (Α. 5 παρ. 1 περ. γ. ΓΚΠΔ), ενώ

[320] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
[321] Προσωπικά Δεδομένα, Ευγενία Αλεξανδροπούλου Αιγυπτιάδου, Νομική Βιβλιοθήκη, 2016
[322] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
[323] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
[324] Προσωπικά Δεδομένα, Ευγενία Αλεξανδροπούλου Αιγυπτιάδου, Νομική Βιβλιοθήκη, 2016

σύμφωνα με την αρχή της ακρίβειας τα δεδομένα πρέπει να ανταποκρίνονται στην πραγματικότητα και να είναι επίκαιρα και ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.[325]

Τέλος, μία από τις σημαντικότερες καινοτομίες είναι το δικαίωμα στη λήθη, το οποίο κατοχυρώνεται στο άρθρο 34 Ν. 4624/2019 «Δικαίωμα διαγραφής» (αντίστοιχο άρθρο 17 ΓΚΠΔ), με βάση το οποίο το υποκείμενο των δεδομένων ζητά τη διαγραφή των προσωπικών του δεδομένων, εφόσον δεν επιθυμεί πια αυτά τα δεδομένα να αποτελούν αντικείμενο επεξεργασίας, και εφόσον δεν υφίσταται νόμιμος λόγος να τα κατέχει ο υπεύθυνος επεξεργασίας. Ουσιαστικά, το δικαίωμα στη λήθη είναι το δικαίωμα κάθε προσώπου να μη γίνεται εκ νέου αντικείμενο ενδιαφέροντος για οδυνηρές ή δυσάρεστες υποθέσεις ενός κομματιού του πρότερου βίου του. Η πρακτική αναγνώριση του δικαιώματος ήρθε το 2014, με την υπόθεση Google Spain SL και Google Inc κατά Agencia Espanola de Proteccion de Datos (AEPD] και Mario Costeja Gonzalez Υπόθεση C-131/12.

## Γ.3.2. Η ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΑΡΑΒΙΑΣΕΩΝ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΔΙΑΔΟΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Το άρθρο 22 του Ν. 2472/1997 τιμωρεί προσβολές του εννόμου αγαθού της ιδιωτικής ζωής και ειδικότερα του δικαιώματος για πληροφοριακή αυτοδιάθεση, όταν πραγματοποιούνται με την χωρίς δικαίωμα επέμβαση σε αρχείο δεδομένων προσωπικού χαρακτήρα, με λήψη γνώσης αυτών, με αφαίρεση, με επεξεργασία, με μετάδοση, με ανακοίνωση, με γνωστοποίηση σε τρίτους κ.λπ.[326] Η γνωστοποίηση και δημοσίευση των δεδομένων προσωπικού χαρακτήρα αίρει την έννοια του απορρήτου, της μυστικότητας της ιδιωτικής ζωής, διότι αυτά καθίστανται προσιτά στον καθένα.[327]

Οι ποινικές κυρώσεις στο άρθρο 22 προβλέπονταν όχι γενικώς και αορίστως αλλά για συγκεκριμένες ειδικά περιγραφόμενες περιστάσεις, στις οποίες κοινό συνδετικό γνώρισμα αποτελεί η αναφορά στην τήρηση "αρχείων προσωπικών δεδομένων.[328] Προβλέπονται τρεις κατηγορίες συμπεριφορών που κρίνονται αξιόποινες, ήτοι α) παραβάσεις των υποχρεώσεων προστασίας των προσωπικών δεδομένων, β) παραβάσεις λόγω μη συμμόρφωσης με αποφάσεις της Αρχής και γ) παραβάσεις που αφορούν τη χωρίς δικαίωμα επέμβαση σε αρχείο προσωπικών δεδομένων και την τέλεση περαιτέρω πράξεων που προσβάλλουν τα προσωπικά δεδομένα. Για την αντικειμενική υπόσταση του εν λόγω εγκλήματος απαιτείται να υπάρχουν δεδομένα σε "Αρχείο", υποκείμενο των δεδομένων να είναι φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και μπορεί να ταυτοποιηθεί, επενέργεια του υπαιτίου, επέμβαση δηλαδή στο "αρχείο" και χωρίς δικαίωμα, χωρίς δηλαδή την συγκατάθεση του υποκειμένου. Υποκειμενικά απαιτείται δόλος του

[325] https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
[326] ΤρΕφΠλημΑθ 175/2014, Α' ΔΗΜΟΣΙΕΥΣΗ βάση δεδομένων Νόμος, Αρμ 2014,1740, ΔiΜΕΕ 2014,379
[327] ΤρμΕφΑθ 174/2014
[328] ΔιατΕισΠρΑθ 123/2014

υπαιτίου να προβεί στην παράνομη παρέμβαση στο αρχείο, στην περαιτέρω γνωστοποίηση σε τρίτους κ.λπ. Το ως άνω άρθρο έπαυσε να ισχύει από τις 25-5-2018 με τη θέση σε ισχύ του ΓΚΠΔ, ο οποίος δεν περιλαμβάνει ποινικές κυρώσεις, αναγνωρίζοντας στα κράτη μέλη την ευχέρεια να εξειδικεύσουν τους κανόνες τους. Σύμφωνα με το άρθρο 84 παρ. 1 του Κανονισμού και υπό τις επιφυλάξεις που τίθενται στο εν λόγω άρθρο ο Νόμος 2472/1997 καταργήθηκε. [329]

Η Ελλάδα μόλις στις 29-8-2019 θέσπισε και έθεσε σε ισχύ το νέο Ν. 4624/2019 για την προστασία προσωπικών δεδομένων, ενσωματώνοντας τις διατάξεις του ΓΚΠΔ και τυποποιώντας τα αδικήματα του άρθρου 22 του Ν 2472/1997 εκ νέου στο άρθρο 38 του νέου Νόμου 4624/2019, όπου προβλέπεται ότι: *"Όποιος, χωρίς δικαίωμα: α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών· β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει, τιμωρείται με φυλάκιση μέχρι ενός (1) έτους, εάν η πράξη δεν τιμωρείται βαρύτερα με άλλη διάταξη".*[330]

Σύμφωνα με τη σχετική αιτιολογική έκθεση, ο δράστης ενεργεί όταν τελεί τις παραπάνω πράξεις χωρίς δικαίωμα και χωρίς να του το επιτρέπει νομική διάταξη. Η χωρίς δικαίωμα επέμβαση με οποιονδήποτε τρόπο "θέτει σε κίνδυνο" το εν λόγω έννομο αγαθό, ενώ με την αντιγραφή κλπ. των δεδομένων αυτών το "βλάπτει". Αντικείμενο προσβολής με την εγκληματική πράξη της παραγράφου 1 αποτελεί το "σύστημα αρχειοθέτησης" όπως αυτό ορίζεται στο άρθρο 4 στοιχείο 6 του ΓΚΠΔ.[331]

Τέλος, τα προσωπικά δεδομένα προστατεύονται, πέρα από τις στοχευμένες ανωτέρω διατάξεις, και από άλλες συναφείς ποινικές διατάξεις, οι οποίες ενεργοποιούνται όταν η παραβίαση των προσωπικών δεδομένων θα έμενε ατιμώρητη, γιατί δεν εμπίπτει στο πραγματικό των παραπάνω ειδικών διατάξεων.

### Γ.3.3. ΠΕΡΙΠΤΩΣΕΙΣ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗ ΧΡΗΣΗ DEEPFAKES

#### Γ.3.3.1. Deep Fake Pornography

Η «εκδικητική πορνογραφία» ή αλλιώς revenge porn απασχολεί ολοένα και συχνότερα τα μέσα μαζικής ενημέρωσης, όπως επίσης και τις δικαστικές αρχές της Ελλάδας. Οι όροι «εκδικητική

[329] https://www.dpa.gr/sites/default/files/2019-10/2472_97%20%28SEPT2019%29.pdf
[330] https://www.uoi.gr/wp-content/uploads/2019/09/nomos_4624_2019.pdf
[331] https://www.dpa.gr/

πορνογραφία», «μη συναινετική πορνογραφία»[332] και «σεξουαλική κακοποίηση μέσω εικόνας»[333] περιγράφουν τη δημοσιοποίηση στο διαδίκτυο φωτογραφιών ή βίντεο με σεξουαλικό περιεχόμενο χωρίς τη συναίνεση του εικονιζόμενου προσώπου. Το ευαίσθητο αυτό οπτικό υλικό συνήθως ανταλλάσσεται αρχικά μεταξύ ερωτικών συντρόφων («sexting»), ενώ σε άλλες περιπτώσεις, οι εν λόγω εικόνες έχουν αποκτηθεί μέσω των λεγόμενων πρακτικών «upskirting» και «downblousing» (όπου ο δράστης «τραβάει» μια φωτογραφία κάτω από τη φούστα ή μέσα από τη μπλούζα του θύματος, αντίστοιχα), μέσω hacking ή εκβιασμού («sextortion»), ή μπορεί ακόμη να έχουν δημιουργηθεί με ψηφιακή επεξεργασία («pornographic photoshopping» και «deepfake videos») ή να αποτελούν προϊόν μαγνητοσκόπησης σεξουαλικών επιθέσεων.[334] Πλέον οι ιδιωτικές καταγραφές σεξουαλικών πράξεων δεν είναι απαραίτητες καθώς με την τεχνολογία deepfake κάθε χρήστης μπορεί να δημιουργήσει ένα ψεύτικο βίντεο σεξουαλικού περιεχομένου και να το διανείμει στους φίλους του ή στα κοινωνικά δίκτυα.[335]

Η μη συναινετική λήψη και κοινοποίηση προσωπικών εικόνων μπορεί να έχει σημαντικές και μακροχρόνιες επιπτώσεις στα θύματα και αναφέρεται ως κατάχρηση οικείων εικόνων = intimate images abuse. Παραβιάζει τη σεξουαλική αυτονομία, τη σωματική ιδιωτικότητα και την αξιοπρέπεια του εικονιζόμενου προσώπου. Τα θύματα της κακοποίησης εικόνας μπορεί να υποστούν σοβαρή και σημαντική βλάβη, όπως ψυχολογική βλάβη, επιδείνωση της σωματικής υγείας και οικονομικές απώλειες. Ο νόμος αναγνωρίζει ότι η κακοποίηση της εικόνας είναι επιβλαβής και άδικη. Με την πάροδο του χρόνου, αναπτύχθηκε ένα συνονθύλευμα αδικημάτων για να αντιμετωπιστεί η εξελισσόμενη φύση της κακοποίησης της οικείας εικόνας.[336]

Η δημιουργία deepfake porn video ήταν η πρώτη περίπτωση χρήσης των γεννητικών παραθετικών δικτύων και είχε ως στόχο διάσημες ηθοποιούς, όπως η Σκάρλετ Γιόχανσον ή η Έμμα Γουάτσον, των οποίων οι εικόνες τοποθετούνταν πάνω στα σώματα ατόμων που επιδίδονται σε σεξουαλικές πράξεις. Το "revenge porn" δημιουργείται και διαδίδεται ευρέως για να ταπεινώσει, να απειλήσει ή να βλάψει με άλλο τρόπο ένα άτομο, το οποίο συνήθως έχει διακόψει τη σχέση του με το άτομο - δημιουργό. Το τελευταίο διάστημα, παρατηρούμε τα βίντεο αυτά να διαδίδονται και από χάκερ ή οποιονδήποτε επιδιώκει οικονομικό κέρδος ή φήμη αντί για εκδίκηση. Το "revenge porn" σε όλες

[332] Citron, D.K. & Franks, M.A. (2014) Criminalizing Revenge Porn. Wake Forest L.Rev. 49: 345-391
[333] McGlynn, C. & Rackley, E. (2017) Image-based Sexual Abuse. Oxford Journal of Legal Studies. 37(3): 534-561
[334] McGlynn, C. & Downes, J. (2015) We Need A New Law to Combat 'Upskirting' and 'Downblousing'. Available at: https://inherentlyhuman.wordpress.com/2015/04 /15/ we-need-a-new-law-to-combat-upskirting-and-downblousing/ (Last Accessed: 28.05.2021); Citron, D.K. (2019) Sexual Privacy. Yale LJ. 128. 1870-1960 (1921 επ.); McGlynn, C., Rackley, E. & Houghton, R. (2017) Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse, Feminist Legal Studies. 25: 25-46 (32-36)
[335] DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society
[336]Intimate Image Abuse, Summary of the final report, Law Comission, Reforming the Law, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Intimate-Image-Abuse-summary-of-report-1.pdf

τις μορφές του αποτελεί μορφή παραβίασης της σεξουαλικής ιδιωτικής ζωής, μια πτυχή της σεξουαλικής ταπείνωσης και εκμετάλλευσης, της σωματικής, ψυχικής ή οικονομικής κακοποίησης ατόμων. Το revenge porn είναι αναμφισβήτητα η χειρότερη παραλλαγή των deepfakes, καθώς περιλαμβάνει ρητό περιεχόμενο χωρίς τη συγκατάθεση του θύματος και δημιουργεί το πιο ταπεινωτικό αποτέλεσμα. Η κοινωνική αντίδραση στο φαινόμενο αυτό όμως δεν ήταν τόσο εχθρική. Γενικότερα, παρόλο που το ψεύτικο βίντεο παραβιάζει την ιδιωτική ζωή και θα μπορούσε να θεωρηθεί ότι παραβιάζει τη δημόσια τάξη και είναι ανήθικο, ένας μεγάλος αριθμός της διαδικτυακής κοινότητας είναι μάλλον αδιάφορος.[337]

Διαφορετική γνώμη φαίνεται να έχει η νομοθεσία σε διάφορες χώρες παγκοσμίως. Στην Ευρώπη αρκετές χώρες πρόσθεσαν στο ποινικό τους οπλοστάσιο διατάξεις για να τιμωρήσουν αυτοτελώς την «εκδικητική πορνογραφία» ως sui generis έγκλημα που προσβάλλει το έννομο αγαθό της ιδιωτικής ζωής ή -πιο συγκεκριμένα- αυτό των προσωπικών δεδομένων. Αντίθετα, πολλές άλλες, μεταξύ των οποίων είναι και η Ελλάδα εξακολουθεί να εφαρμόζει σε τέτοιες περιπτώσεις τις διατάξεις που αφορούν ήδη υφιστάμενα αδικήματα.[338] Η Γερμανία ανήκει στις πρώτες χώρες η οποία τιμώρησε τη χωρίς άδεια δημιουργία ή μετάδοση φωτογραφιών ατόμου που βρίσκεται εντός οικίας ή δωματίου ιδιαιτέρως προστατευμένου από την κοινή θέα και την κατά αυτόν τον τρόπο παραβίαση της ερωτικής ιδιωτικότητάς του (Art. 201a StGB 2018).

Στην έννομη τάξη της Αγγλίας και της Ουαλίας κατέστη αξιόποινη η δημοσίευση ιδιωτικών σεξουαλικών φωτογραφιών και ταινιών, η οποία συμβαίνει χωρίς τη συναίνεση του εικονιζόμενου προσώπου και έχει σκοπό την πρόκληση ψυχικού πόνου σε αυτό (Section 33 Criminal Justice and Courts Act 2015). Το «revenge porn» ποινικοποιήθηκε ως μορφή σεξουαλικής κακοποίησης.[339] Το Ηνωμένο Βασίλειο ψήφισε νόμο κατά του πορνό εκδίκησης το 2015, όμως τα θύματα και οι ακτιβιστές προειδοποιούν εδώ και χρόνια ότι το καθεστώς δεν λειτουργεί και ασκούν πιέσεις για επανεξέταση.[340] Σύμφωνα με επίσημα στατιστικά στοιχεία που παραθέτει το Υπουργείο Δικαιοσύνης, περίπου 1 στους 14 ενήλικες στην Αγγλία και την Ουαλία αντιμετώπισαν απειλές να μοιραστούν προσωπικές εικόνες και υπήρξαν περισσότερες από 28.000 αναφορές για αποκάλυψη ιδιωτικών εικόνων σεξουαλικού περιεχομένου χωρίς συναίνεση, μεταξύ Απριλίου 2015 και

[337] Regulating deep fakes: legal and ethical considerations, Edvinas Meskys, Paulis Jurcys, Vilnius University, Article in Journal of Intellectual Property Law & Practice · January 2020

[338] Šepec, M. (2019) Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. International Journal of Cyber Criminology. 13(2): 418-438 (419, 430)

[339] Šepec, M. (2019) Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. International Journal of Cyber Criminology. 13(2): 418-438

[340] https://techcrunch.com/2022/11/25/deepfake-porn-revenge-porn-uk-law-change/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKrR_HBxBvzgVmgipoeJFrTgMd0ThrMB4GIG61hnl3qM_8N4Cav1EWgL5SauVX34uWeWKSv_E-Zc2EurkK71112II979Azo0YRxMB1wdegxoT-hS8W1gJ1PpmZPE9u6qjKfsORiFNUC7U3QLCc6p4shXmoNRgWuyNacRV18bBG9j

Δεκεμβρίου 2021.[341] Για το λόγο αυτό, το Δεκέμβριο 2022 η κυβέρνηση της Αγγλιας ανακοίνωσε τη συζήτηση νέου νομοσχεδίου, με βάση το οποίο η μη συναινετική "deepfake" πορνογραφία και το "downblousing" θα καταστούν παράνομα.[342] Οι τροποποιήσεις αντιμετωπίζουν τα "deepfakes" σε δύο τμήματα. Προτείνεται ένα εντελώς νέο άρθρο 30α, με τίτλο "Deep Fakes", το οποίο έχει ως εξής: "Όταν μια πολύ μεγάλη διαδικτυακή πλατφόρμα αντιλαμβάνεται ότι ένα κομμάτι περιεχομένου είναι μια παραγόμενη ή παραποιημένη εικόνα, ήχος ή βίντεο που μοιάζει αισθητά με υπάρχοντα πρόσωπα, αντικείμενα, τόπους ή άλλες οντότητες ή γεγονότα και εμφανίζεται ψευδώς σε ένα άτομο ως αυθεντικό ή αληθινό (βαθιά απομίμηση), ο πάροχος επισημαίνει το περιεχόμενο με τρόπο που ενημερώνει ότι το περιεχόμενο είναι μη αυθεντικό και ο οποίος είναι σαφώς ορατός για τον αποδέκτη των υπηρεσιών". Η δεύτερη τροπολογία αφορά στο υφιστάμενο άρθρο 63, το σχετικό κείμενο έχει ως εξής: "Επιπλέον, οι πολύ μεγάλες διαδικτυακές πλατφόρμες θα πρέπει να επισημαίνουν όλα τα γνωστά βαθιά πλαστά βίντεο, ήχους ή άλλα αρχεία."[343]

Εκτός Ευρώπης, παράδειγμα αποτελεί η Κίνα, όπου από την 1η Ιανουαρίου 2020 εφαρμόζεται μια νέα κυβερνητική πολιτική που αποσκοπεί στην αποτροπή της διάδοσης ψευδών ειδήσεων και παραπλανητικών βίντεο που δημιουργούνται με τη χρήση τεχνητής νοημοσύνης, γνωστά και ως deepfakes. Ο νέος κανόνας απαγορεύει τη δημοσίευση ψευδών πληροφοριών ή deepfakes στο διαδίκτυο χωρίς την κατάλληλη γνωστοποίηση ότι η εν λόγω ανάρτηση δημιουργήθηκε με τεχνολογία AI ή VR. Η μη αποκάλυψη αυτού του γεγονότος αποτελεί πλέον ποινικό αδίκημα, σύμφωνα με την κινεζική κυβέρνηση.[344]

Αντίθετα, η Ελλάδα, δεν έχει ποινικοποιήσει τη μη συναινετική πορνογραφία ή τη διάδοση ψεύτικων βίντεο, με αποτέλεσμα οι εν λόγω συμπεριφορές να τιμωρούνται βάσει των ποινικών διατάξεων του νόμου «για την προστασία των δεδομένων προσωπικού χαρακτήρα» (Ν. 4624/2019), οι οποίες -κατά την κρατούσα άποψη- προστατεύουν το έννομο αγαθό της πληροφοριακής αυτοδιάθεσης.[345]

Ενδεικτικό παράδειγμα - καθώς τέτοιες υποθέσεις απασχολούν τις δικαστικές αίθουσες στις μέρες μας αρκετά συχνά πλέον - όχι μόνο μη συναινετικής, αλλά συγκεκριμένα «εκδικητικής» πορνογραφίας αποτελεί η υπόθεση επί της οποίας απεφάνθη πρόσφατα και το Ε΄ Ποινικό Τμήμα

[341] https://www.bbc.com/news/technology-63669711
[342] https://www.theguardian.com/technology/2022/nov/24/online-safety-bill-to-return-to-parliament-next-month
[343] https://www.unite.ai/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/
[344] https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality
[345] Λαχανά Κ.-Χ. (2016) Η κατά το Ελληνικό Δίκαιο Ποινική Προστασία των Προσωπικών Δεδομένων στο Πλαίσιο της Αστυνομικής Δικαστικής Συνεργασίας σε Ποινικές Υποθέσεις: Προκλήσεις και Προοπτικές. Διατριβή επί Διδακτορία. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης-Νομική Σχολή-Τομέας Ποινικών και Εγκληματολογικών Επιστημών. (72 επ.); Γανιάρης Ν., (2020) Δεδομένα Προσωπικού Χαρακτήρα. Σε: Παύλου Στ. Κ. και Σάμιος Θ. Π. Ειδικοί Ποινικοί Νόμοι. (6η ενημέρωση). Π.Ν. Σάκκουλας.

του Αρείου Πάγου με την υπ' αριθμόν 505/2020 απόφασή του, στην περίπτωση της οποίας ο κατηγορούμενος, χρησιμοποιώντας την ψηφιακή κάμερα του κινητού του τηλεφώνου, μαγνητοσκόπησε ερωτικές του συνευρέσεις με την πολιτικώς ενάγουσα και τότε σύντροφό του, ενώ μετά τη λήξη της σχέσης τους (που έληξε με πρωτοβουλία της τελευταίας), προέβη στην ανάρτηση δύο βίντεο αντίστοιχου περιεχομένου στο διαδίκτυο, καθιστώντας το οπτικοακουστικό αυτό υλικό διαθέσιμο σε απροσδιόριστο αριθμό προσώπων. Αξίζει να σημειωθεί ότι η εγκαλούσα όχι μόνο δε συνήνεσε στη δημιουργία και στη διατήρηση των συγκεκριμένων βίντεο από τον κατηγορούμενο, αλλά αντιθέτως ρητώς απαίτησε από αυτόν τη διαγραφή τους. Κατόπιν τούτων, σε βάρος του εγκαλουμένου ασκήθηκε ποινική δίωξη για τα αδικήματα, αφενός, της χωρίς δικαίωμα διατήρησης στην κατοχή του άνευ αδείας αρχείου δεδομένων προσωπικού χαρακτήρα και ευαίσθητων προσωπικών δεδομένων κατ' εξακολούθηση (ά. 38 παρ. 1 εδ. β' του Ν. 4624/2019) και, αφετέρου, της μετάδοσης-ανακοίνωσης δεδομένων προσωπικού χαρακτήρα και ευαίσθητων προσωπικών δεδομένων (ά. 38 παρ. 2 του Ν. 4624/2019). Το Τριμελές Εφετείο Πλημμελημάτων επέβαλε στον κατηγορούμενο συνολική ποινή φυλάκισης δεκαπέντε μηνών με τριετή αναστολή, ενώ ο Άρειος Πάγος, αφού επιβεβαίωσε ότι ο άνδρας πράγματι προέβη στη δημιουργία και την επεξεργασία αρχείου ευαίσθητων προσωπικών δεδομένων χωρίς δικαίωμα και χωρίς τη συγκατάθεση της παθούσας, αναίρεσε την παραπάνω απόφαση μόνο κατά το μέρος που αφορούσε το αξιόποινο των πράξεων και την επιβληθείσα ποινή.[346]

Σύμφωνα με την Ευρωπαϊκή Σύμβαση Ανθρωπίνων Δικαιωμάτων, τα δημόσια πρόσωπα (καθώς και οι απλοί πολίτες) μπορούν να επικαλούνται το δικαίωμά τους στην ιδιωτική ζωή προκειμένου να προστατεύσουν το όνομα, την τιμή και τη φήμη τους, ακόμη και όταν επιδιώκουν ενεργά να βρεθούν στο προσκήνιο. Ωστόσο, το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων έχει επίσης αποφανθεί ότι τα δημόσια πρόσωπα πρέπει να ανέχονται μεγαλύτερη εισβολή στην ιδιωτική τους ζωή από ό,τι οι απλοί πολίτες και πρέπει να δέχονται ότι θα τους χλευάζουν και θα τους γελοιοποιούν. Η σχέση μεταξύ της ελευθερίας της έκφρασης των πολιτών και του δικαιώματος στην ιδιωτική ζωή των δημοσίων προσώπων αξιολογείται από το Δικαστήριο κατά περίπτωση. Κατά συνέπεια, υπάρχουν λίγοι γενικοί κανόνες και απαγορεύσεις σχετικά με τις εκφράσεις για δημόσια πρόσωπα. Αυτό σημαίνει ότι τα δημόσια πρόσωπα έχουν ελάχιστη ασφάλεια δικαίου όταν προσφεύγουν στο δικαστήριο για τέτοιου είδους προσβολές σε βάρος τους. Το αποτέλεσμα είναι

[346] Η Μη Συναινετική Πορνογραφία στην Ελληνική Έννομη Τάξη, Αγγελική Γιαννάκη, Δικηγόρος Αθηνών, MSc in Criminology and Criminal Justice (University of Oxford) ΜΑΪΟΣ 2021 https://theartofcrime.gr/%CE%B7-%CE%BC%CE%B7-%CF%83%CF%85%CE%BD%CE%B1%CE%B9%CE%BD%CE%B5%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CE%BF%CF%81%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5%CE%BB%CE%BB/

ότι σπάνια λαμβάνονται νομικά μέτρα, με αποτέλεσμα την ομαλοποίηση των ακραίων εκφράσεων.[347]

Υποστηρίζεται ευρέως η άποψη ότι η μη συναινετική πορνογραφία αποτελεί μορφή σεξουαλικού εγκλήματος και δεν είναι καθόλου άστοχος ο όρος «διαδικτυακός βιασμός» («cyber rape»)[348] και ο όρος «σεξουαλική κακοποίηση μέσω εικόνας» («image-based sexual abuse»). Οι συμπεριφορές αυτές αποτελούν μορφές σεξουαλικής βίας.[349] Η σεξουαλική ελευθερία δεν είναι μόνο σωματική, αλλά έχει και ψυχολογική και πνευματική πλευρά, με αποτέλεσμα η διαδικτυακή προσβολή να μπορεί επίσης να χαρακτηριστεί πράξη σεξουαλικής βίας.[350]

Ως εκ τούτου, ελλείψει ποινικής διάταξης που να προσδιορίζει με συγκεκριμένο τρόπο τις συμπεριφορές που αποτελούν ένα είδος εκδικητικής πορνογραφίας, οι δικαστικές αρχές της Ελλάδας ευλόγως προσφεύγουν στις διατάξεις που αφορούν αδικήματα κατά της ιδιωτικής ζωής και της πληροφοριακής αυτοδιάθεσης. Ωστόσο, όπως σε άλλες χώρες έτσι και στην ελληνική έννομη τάξη θα μπορούσε να προβλεφθούν νέες διατάξεις που να ποινικοποιούν ρητά και ευθέως τις πράξεις αυτές που προσβάλλουν το έννομο αγαθό της σεξουαλικής αυτοδιάθεσης.

### Γ.3.3.2. Τα deepfakes ως μορφή σάτιρας

Στο πλαίσιο που η τεχνολογία Deepfake χρησιμοποιείται κυρίως ως μορφή σάτιρας, ενδεχομένως η τεχνολογία να εμπίπτει στην έννοια της καλλιτεχνικής έκφρασης η οποία προβλέπεται στο άρθρο 85 του ΓΚΠΔ, όπου όμως απλά δίνει την ελευθεριότητα στον εθνικό νομοθέτη να ρυθμίσει όπως θέλει ο ίδιος το θέμα. Ο Έλληνας νομοθέτης, στο άρθρο 28 του Ν 4624/2019, προέβλεψε την επεξεργασία για καλλιτεχνικούς σκοπούς, σε ορισμένες περιπτώσεις, με τη ρητή συγκατάθεση του υποκειμένου. Συνεπώς, σε περιπτώσεις καλλιτεχνικής χρήσης της εικόνας για σατιρικούς λόγους, ο ΓΚΠΔ παύει να αποτελεί εμπόδιο στην ανάρτηση του βίντεο.[351]

Χαρακτηριστικό παράδειγμα αποτελούν τα video του Tom Cruise στο TikTok. Τα deepfakes έχουν προχωρήσει τόσο πολύ τα τελευταία χρόνια που υπάρχει πλέον ένας λογαριασμός στο TikTok

---

[347] DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society

[348] Citron, D.K. & Franks, M.A. (2014) Criminalizing Revenge Porn. Wake Forest L.Rev. 49: 345-391 (346-υποσημ. 10).

[349] McGlynn, C., Rackley, E. & Houghton, R. (2017) Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse, Feminist Legal Studies. 25: 25-46 (28-29); Bloom, S. (2016) No Vengeance for 'Revenge Porn' Victims: Unraveling Why This Latest Female-Centric, Intimate-Partner Offense is Still Legal, and Why We Should Criminalize It. Fordham Urb.LJ. vol. 42(1): 233-289 (278 επ.).

[350] Šepec, M. (2019) Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. International Journal of Cyber Criminology. 13(2): 418-438 (422-423); Citron, D.K. & Franks, M.A. (2014) Criminalizing Revenge Porn. Wake Forest L.Rev. 49: 345-391 (362).

[351] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

αφιερωμένος αποκλειστικά στα deepfakes του Tom Cruise. Τα βίντεο δείχνουν τον Cruise να κάνει τα πάντα, από το γκολφ μέχρι την επίδειξη ενός μαγικού κόλπου, ακόμη και σε καθημερινές καταστάσεις όπως το πλύσιμο των χεριών του. Η περιγραφή του λογαριασμού στο TikTok αναφέρει απλώς: "Παρωδία. Επίσης, νεότερος". Ο Cruise δεν είναι όμως ο μόνος ψεύτικος διάσημος με τους δικούς του ακόλουθους στο TikTok. Έκτοτε, στην πλατφόρμα έχει προστεθεί ένας ψεύτικος Keanu Reeves και πολλοί άλλοι. Ο Unreal_Keanu έχει συγκεντρώσει απίστευτα 7,4 εκατομμύρια followers, οι οποίοι φαίνεται να λατρεύουν τις αναφορές στους κινηματογραφικούς του ρόλους, το χορό του (είναι TikTok) και τα αστεία για τη ζωή με σύντροφο. Όπως και με τον Cruise παραπάνω, αυτή η συγκεκριμένη deepfake διασημότητα χρησιμοποιείται για πλάκα και δεν περνάει ως αληθινή. Όμως, παρά το χιούμορ, δείχνει τους κινδύνους που εγκυμονούν τα deepfakes για τους διάσημους. Από τη μία πλευρά, η τεχνολογία θα μπορούσε να επιτρέψει στις διασημότητες να πουλήσουν την εικόνα τους στις μάρκες χωρίς να χρειάζεται να μπουν στον κόπο να γυρίσουν ένα σποτ ή να πάνε σε μια φωτογράφηση. Αλλά από την άλλη πλευρά, έχουν ήδη υπάρξει αναφορές για ασυνείδητες μάρκες που χρησιμοποιούν deepfakes για να προωθήσουν τα προϊόντα τους χωρίς την άδεια των διασημοτήτων.[352]

Άλλο ένα παράδειγμα αποτελεί εκείνο με πρωταγωνίστρια την αποβιώσασα βασίλισσα Ελισσάβετ της Αγγλίας. Η βασίλισσα συνήθιζε κάθε χρόνο παραδοσιακά να μεταφέρει ένα δημόσιο μήνυμα τα Χριστούγεννα. Αλλά την ομιλία της τα Χριστούγεννα του 2020 ακολούθησε μια ψηφιακά δημιουργημένη απομίμηση της βασίλισσας, που προβλήθηκε από το Channel 4 και είχε τη φωνή ενός ηθοποιού, προειδοποιώντας τους τηλεθεατές να αναρωτηθούν "αν αυτό που βλέπουμε και ακούμε είναι πάντα αυτό που φαίνεται". Η ψεύτικη στο βίντεο βασίλισσα συζητά για τη μετακόμιση του πρίγκιπα Χάρι και της Μέγκαν στη Βόρεια Αμερική, λέγοντας: "Λίγα πράγματα είναι πιο πληγωτικά από το να σου λέει κάποιος ότι προτιμά την παρέα των Καναδών" Στη συνέχεια η ψεύτικη βασίλισσα παρουσίασε επίσης ένα χορευτικό πρόγραμμα Tik Tok.[353]

### Γ.3.3.3. Η εικόνα του αποθανόντος ως προσωπικό δεδομένο

Με την μαγεία της deepfake τεχνολογίας ο δημιουργός μπορεί να αναστήσει ανθρώπους που έχουν αποβιώσει και αυτή η ψηφιακή αναγέννηση διάσημων προσώπων, μέσω αυτής της τεχνολογίας, θέτει προφανώς σοβαρά ηθικά και νομικά ζητήματα στην ελληνική έννομη τάξη, καθώς η προστασία προσωπικών δεδομένων αφορά αποκλειστικά άτομα που βρίσκονται εν ζωή σύμφωνα με το Νόμο 4624/2019. Ωστόσο, σύμφωνα με την αιτιολογική σκέψη 27 *«Ο παρών κανονισμός δεν εφαρμόζεται στα δεδομένα προσωπικού χαρακτήρα θανόντων. Τα κράτη μέλη μπορούν να προβλέπουν κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα θανόντων»*. Στο πλαίσιο αυτό, κάποιες χώρες έχουν κάνει χρήση της ευχέρειας επέκτασης της προστασίας σε

[352] https://www.creativebloq.com/features/deepfake-examples
[353] https://edition.cnn.com/2020/12/25/uk/deepfake-queen-speech-christmas-intl-gbr/index.html

αποθανόντα άτομα, όπως η Δανία η οποία προβλέπει 10 χρόνια προστασίας των δεδομένων μετά τον θάνατο.

Επομένως, αν και η τεχνολογία στην περίπτωση αυτή εφαρμόζεται σε εξαιρετικές περιπτώσεις, παραμένει εφικτή η επίκληση των ποινικών κανόνων που ρυθμίζουν την προσβολή της μνήμης νεκρού. Παρομοίως, ισχύει έμμεσα και για τον αποθανόντα η προστασία επί της εικόνας μέσω της προστασίας του δικαιώματος προσωπικότητας των συγγενών του. Η νομολογία έχει κρίνει ότι *«Προσβολή της μνήμης του νεκρού, ως συνέχεια της εν ζωή προσωπικότητας του ατόμου, μπορεί να συντελεστεί, υπό την προεκτεθείσα έννοια, με κάθε τρόπο, κατά τον οποίον είναι δυνατή προσβολή και επί ζώντος ατόμου, όπως με αντίστοιχη προσβολή της τιμής, της εικόνας, του απορρήτου και της αναπαραστάσεως εν γένει της ζωής του αποθανόντος", με την λογική ότι «προστατευόμενο έννομο αγαθό δεν είναι η «μεταθανάτια» προστασία της προσωπικότητας του νεκρού, αλλά η ίδια προσωπικότητα των ως άνω προσώπων, στο μέτρο που η προσβολή της μνήμης του νεκρού προσέβαλε, λόγω του στενού συνδέσμου μεταξύ τους (συνήθως οικογενειακού) το αίσθημα σεβασμού τους προς την μνήμη του νεκρού, που αποτελεί και αυτό έκφανση της προσωπικότητάς του».*[354]

Τα deepfakes φέρνουν αυτή τη συζήτηση σε μια νέα διάσταση, τόσο από ηθική όσο και από εμπορική άποψη. Για παράδειγμα, είναι επιθυμητό και επιτρεπτό να διδάσκουν στα σχολεία ιστορικές προσωπικότητες που έχουν φύγει προ πολλού ή να ξεναγούν αποθανόντες καλλιτέχνες σε ένα μουσείο ή να εμφανίζονται σε ταινίες αποβιώσαντες ηθοποιοί ή να πρωταγωνιστεί ένας αποθανών σε ταινία με σεξουαλικό περιεχόμενο ή να εξακολουθούν να δίνουν συναυλίες οι αποβιώσαντες καλλιτέχνες;[355]

Παράδειγμα αποτελεί η επιστροφή του Σαλβαντόρ Νταλί, όταν το πρακτορείο GS&P ανέστησε τον Καταλανό καλλιτέχνη ως χαρισματικό οικοδεσπότη στο Μουσείο Νταλί στη Φλόριντα. Το Dalí Lives, που χαρακτηρίζεται ως "η τέχνη συναντά την τεχνητή νοημοσύνη", δημιουργήθηκε με τη λήψη περισσότερων από 6.000 καρέ από παλιές συνεντεύξεις βίντεο και την επεξεργασία τους μέσω 1.000 ωρών μηχανικής μάθησης, προτού επικαλυφθεί η πηγή στο πρόσωπο ενός ηθοποιού. Το κείμενο αποτελούνταν από αποσπάσματα συνεντεύξεων και επιστολών με νέα σχόλια, σχεδιασμένα για να βοηθήσουν τους επισκέπτες να κατανοήσουν τον καλλιτέχνη και να συσχετιστούν με το έργο του. Η καινοτομία αυτού του παραδείγματος deepfake είναι η διαδραστικότητά του. Συνολικά 45 λεπτά υλικού που κατανέμονται σε 125 βίντεο επιτρέπουν περισσότερους από 190.000 πιθανούς συνδυασμούς ανάλογα με τις απαντήσεις των επισκεπτών και περιλαμβάνουν ακόμη και σχόλια για τον καιρό. Τελειώνει με τον Νταλί να γυρίζει και να

[354] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[355] DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society

βγάζει μια selfie με το κοινό του. Ο Νταλί ισχυρίστηκε ότι ήταν απίθανο να πεθάνει ποτέ, και ίσως είχε δίκιο, επειδή τον επανέφερε στη ζωή για δεύτερη φορά πρόσφατα το εργαστήριο Τεχνητής Νοημοσύνης της Samsung στη Μόσχα, αυτή τη φορά εκπαιδεύοντας την Τεχνητή Νοημοσύνη σε χαρακτηριστικά του προσώπου που αποτελούν ορόσημο από μια χούφτα εικόνες αντί για τις συνήθεις χιλιάδες.

## Γ.4. ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΔΥΣΦΗΜΗΣΗΣ

Τα εγκλήματα κατά της τιμής σήμερα παίζουν σημαντικό ρόλο για την προστασία της προσωπικότητας στα μέσα κοινωνικής δικτύωσης. Καθώς τα fake news περιέχουν την ψευδή πληροφορία για κάποιο γεγονός, σημαντική θέση έχει η συκοφαντική δυσφήμηση.[356]

Η τεχνολογία deepfake μπορεί να αποτελέσει έγκλημα κατά της τιμής, αφού βασίζεται σε ένα ψέμα, διότι με την ανταλλαγή προσώπου υπονοείται ότι το άτομο συμμετείχε με τη βούλησή του στο βίντεο, ενώ στην πραγματικότητα αυτό δεν συνέβη ποτέ. Συνεπώς, στην περίπτωση κακόβουλης χρήσης στοιχειοθετούνται τα εγκλήματα των άρθρων 362, 363 και 367 ΠΚ, με την καθοδήγηση όμως του Ευρωπαϊκού Δικαστηρίου του Ανθρώπου (ΕΔΔΑ) σχετικά με την ελευθερία της έκφρασης.[357]

Σύμφωνα με το άρθρο 362 του νέου Ποινικού Κώδικα, *«Όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση έως ένα έτος ή χρηματική ποινή. Αν η πράξη τελέστηκε δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως τρία έτη ή χρηματική ποινή.»*[358]

Δυσφήμηση είναι ο ισχυρισμός ή διάδοση γεγονότος ενώπιον τρίτου, με οποιονδήποτε τρόπο για άλλον που μπορεί να βλάψει την τιμή και την υπόληψή του, δηλ. το καλό όνομα που έχει ο παθών στην κοινωνία. Ισχυρισμός είναι η ανακοίνωση του δράστη, ενώ διάδοση υπάρχει, όταν ο δράστης μεταδίδει ανακοίνωση που έγινε από άλλον. Η διάδοση μπορεί να γίνει και μέσω του διαδικτύου, οπότε τόπος τέλεσης είναι όλη η Επικράτεια κατά το άρθρο 5 παρ. 3 (βλ. ΑΠ 2083/17 ΤΝΠ ΔΣΑ).[359]

---

[356] Ποινική ευθύνη ενδιάμεσων παρόχων, ιδίως φορέων μέσων κοινωνικής δικτύωσης, για fake news και προσβολές της τιμής στο διαδίκτυο (υπό το νέο Ποινικό Κώδικα), Ιωάννης Μοροζίνης, Δικηγόρος, ΔΝ, Εντεταλμένος Διδάσκων Νομικής Σχολής ΔΠΘ, σελ. 107 σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 95

[357] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[358] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/

[359] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1046

Γεγονός είναι κάθε συγκεκριμένο περιστατικό του πραγματικού κόσμου, κατάσταση, σχέση ή συμπεριφορά, που αναφέρεται στο παρελθόν ή το παρόν, υποπίπτει στις αισθήσεις και είναι δεκτικό απόδειξης, καθώς και αντίκειται στην ηθική και την ευπρέπεια.[360],[361] Δεν είναι όμως γεγονός η έκφραση αξιολογικών κρίσεων, συμπεράσματα και προγνώσεις.[362],[363]

Προστατευόμενο αγαθό είναι η τιμή ή η υπόληψη του προσώπου. «Τιμή» είναι η εκτίμηση που απολαμβάνει το άτομο στην κοινωνία, με βάση την ηθική αξία που έχει συνεπεία εκπληρώσεως απ' αυτό των ηθικών και νομικών κανόνων, ενώ «υπόληψη» είναι το αγαθό όνομα, η εκτίμηση που απολαμβάνει το άτομο στην κοινωνία με βάση την κοινωνική αξία του συνεπεία των ιδιοτήτων και ικανοτήτων που έχει για την εκπλήρωση των ιδιαιτέρων κοινωνικών του έργων ή του επαγγέλματός του (ΑΠ 1100/16, 1180/13, 486/11 ΤΝΠ ΔΣΑ). Το ισχυριζόμενο ή διαδιδόμενο πρέπει να είναι πρόσφορο, δηλ. ικανό να βλάψει την τιμή ή την υπόληψη του παθόντος. Τούτο θα κριθεί κατά τρόπο αντικειμενικό.[364]

Για την υποκειμενική υπόσταση του εγκλήματος απαιτείται δόλος που θεμελιώνεται στη γνώση του δράστη ότι το γεγονός που διαδίδει ή ισχυρίζεται μπορεί να βλάψει την τιμή ή την υπόληψη άλλου και τη θέληση να ισχυριστεί ενώπιον τρίτου ή να διαδώσει το βλαπτικό αυτό γεγονός αρκεί δε και ενδεχόμενος δόλος.[365]

Η απλή δυσφήμηση στη βασική της μορφη τιμωρείται με φυλάκιση έως 1 έτος ή χρηματική ποινή. Αν ο υπαίτιος όμως τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως 3 έτη ή χρηματική ποινή. Δημόσια τελείται η πράξη, όταν είναι δυνατό να υποπέσει στην αντίληψη αόριστου αριθμού προσώπων, σε ιδιωτικό ή δημόσιο χώρο, ασχέτως αν πράγματι την αντελήφθησαν τρίτοι, αρκεί να υπάρχει η δυνατότητα να γίνει αντιληπτή.[366]

Σύμφωνα με το άρθρο 363 του νέου Ποινικού Κώδικα, *«Αν στην περίπτωση του προηγούμενου άρθρου, το γεγονός είναι ψευδές και ο υπαίτιος γνώριζε ότι αυτό είναι ψευδές τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή και αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου, με φυλάκιση τουλάχιστον έξι μηνών και χρηματική ποινή.»*[367]

Η αναλήθεια του δυσφημιστικού γεγονότος αποτελεί την ειδοποιό διαφορά της συκοφαντικής από την (απλή) δυσφήμηση, ισχύει όμως και σ' αυτήν την περίπτωση η επιβαρυντική περίσταση

[360] ΑΠ 1100/2016, 1184/2014, 1180/2013 κ.α. σε Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1046
[361] www.areiospagos.gr
[362] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1047
[363] www.areiospagos.gr
[364] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1049
[365] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1049
[366] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1049
[367] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/

τελέσεώς του δημόσια ή μέσω του διαδικτύου (βλ. ΑιτΕκθ του νέου ΠΚ). Όπως και στο αδίκημα απλής δυσφήμησης, έτσι και για τη συκοφαντική απαιτείται ισχυρισμός ή διάδοση γεγονότος για άλλον που μπορεί να βλάψει την τιμή και την υπόληψή του. [368]

Το γεγονός πρέπει να είναι ψευδές αντικειμενικώς. Αν το γεγονός είναι αληθινό, τελείται απλή δυσφήμηση. Αν δεν αποδεικνύεται ότι το γεγονός είναι ψευδές, καταλειπομενων αμφιβολιών για την αλήθεια ή αναλήθεια τούτου, δεν στοιχειοθετείται το έγκλημα της συκοφαντικής δυσφήμησης. Για την υποκειμενική υπόσταση απαιτείται δόλος σκοπού, που συνίσταται στη γνώση του δράστη, ότι το γεγονός αυτό είναι ψευδές και μπορεί να βλάψει την τιμή και την υπόληψη του άλλου και αφετέρου, στη θέληση αυτού να ισχυριστεί ή διαδώσει ενώπιον τρίτου το γεγονός αυτό.[369]

Η συκοφαντική δυσφήμηση στη βασική της μορφή τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή και αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου, με φυλάκιση τουλάχιστον έξι μηνών και χρηματική ποινή. Δημόσια τελείται η πράξη, όταν είναι δυνατό να υποπέσει στην αντίληψη αόριστου αριθμού προσώπων, σε ιδιωτικό ή δημόσιο χώρο, ασχέτως αν πράγματι την αντελήφθησαν τρίτοι, αρκεί να υπήρχε η δυνατότητα να γίνει αντιληπτή.[370]

Τέλος, σύμφωνα με το άρθρο 367 ΠΚ, *«1. Δεν αποτελούν άδικη πράξη: α) οι δυσμενείς κρίσεις για επιστημονικές, καλλιτεχνικές ή επαγγελματικές εργασίες, β) οι δυσμενείς εκφράσεις που περιέχονται σε έγγραφο δημόσιας αρχής για αντικείμενα που ανάγονται στον κύκλο της υπηρεσίας της, γ) οι εκδηλώσεις που γίνονται για την εκτέλεση νόμιμων καθηκόντων, την άσκηση νόμιμης εξουσίας ή για τη διαφύλαξη (προστασία) δικαιώματος ή από άλλο δικαιολογημένο ενδιαφέρον και δ) σε ανάλογες περιπτώσεις. 2. Η προηγούμενη διάταξη δεν εφαρμόζεται: α) όταν οι παραπάνω κρίσεις και εκδηλώσεις περιέχουν τα συστατικά στοιχεία της πράξης του άρθρου 363 και β) αν από τον τρόπο που πραγματοποιήθηκε ή από τις περιστάσεις υπό τις οποίες τελέστηκε ή δυσφήμηση προκύπτει σκοπός εξύβρισης.»*[371]

Ως δικαιολογημένο ενδιαφέρον νοείται η επιδίωξη σκοπού (δημόσιου ή ιδιωτικού, ηθικής ή υλικής φύσεως), ο οποίος αναγνωρίζεται από το δίκαιο ως άξιος προστασίας.[372] Βασική προϋπόθεση αποτελεί το ότι η προσβολή της τιμής ήταν εύλογη και αναγκαία για την προστασία του συμφέροντος του δράστη.[373]

---

[368] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1050-1051
[369] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1052
[370] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 1051-1053
[371] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/
[372] ΑΠ 73/2002 ΠοινΔικ 2002, 582, ΑΠ 451/2000 ΠοινΧρ Ν', 921
[373] ΑΠ 406/2013 ΝΟΜΟΣ, ΑΠ 871/2007 ποινχρ Α Π, 671/2005 ποινχρ ΝΕ , 1006, ΑΠ 169/2002 ποινχρ ΝΒ', 888, ΑΠ 1147/1998 ποινχρ Μθ', 665, 1678/1994 ΜΕ', 47

Επομένως, ένα κριτήριο για να χαρακτηριστεί η χρήση της τεχνολογίας deepfake ως δυσφημιστική είναι αν στρέφεται κατά δημόσιου ή μη προσώπου. Ωστόσο, μεγαλύτερο ρόλο παίζει ο σκοπός της δημοσίευσης, καθώς δεν μπορεί σε όλες τις περιπτώσεις η ελευθερία της έκφρασης να υπερισχύει το συμφέρον προστασίας της τιμής και της υπόληψης του προσώπου. Για παράδειγμα, ένα ψεύτικο βίντεο πορνογραφικού περιεχομένου με πρωταγωνιστή το πρόσωπο μιας διάσημης ηθοποιού αλλά το σώμα ενός ηθοποιού της βιομηχανίας πορνογραφικού υλικού, δεν θεωρείται, κατά τη γνώμη της γράφουσας, αντικείμενο δημοσίου συμφέροντος του κοινού να ενημερωθεί σχετικά. Αφού το συγκεκριμένο βίντεο προσβάλλει σε κάθε περίπτωση την τιμή και την υπόληψη του προσώπου που θίγει και δεν μπορεί να υπερτερεί καμία ελευθερία έκφρασης, ούτε μπορεί να χαρακτηριστεί ως σάτιρα, ούτε μορφή καλλιτεχνικής έκφρασης.

Απόφαση σταθμό αποτελεί η πολύ πρόσφατη απόφαση του Τριμελούς Πλημμελειοδικείου Αθηνών σχετικά με την υπόθεση Chatpic. Ο δράστης καταδικάστηκε σε ποινή φυλάκισης δύο ετών για παραβίαση των διατάξεων περί προσωπικών δεδομένων αλλά και για συκοφαντική δυσφήμιση για διαδικτυακό βιασμό και σεξουαλική κακοποίηση στην πλατφόρμα CHATPIC. Πρόκειται για γυμνές φωτογραφίες του θύματος που είχε ανεβάσει ο κατηγορούμενος στο εν λόγω site, χωρίς φυσικά τη συγκατάθεσή της και χωρίς η ίδια να το γνωρίζει. Με την απόφαση αυτή για πρώτη φορά τιμωρήθηκε δράστης αυτού του εγκλήματος και για την προσβολή της προσωπικότητας του θύματος, αφού μέχρι τώρα, δικάζονταν μόνο για τα προσωπικά δεδομένα. Σήμερα, το δικαστήριο δέχθηκε ότι η δημοσίευση ερωτικών φωτογραφιών της κοπέλας, χωρίς τη συναίνεσή της, αποτελεί προσβολή της προσωπικότητας της, την συκοφαντεί και πλήττει την υπόληψή της.

### Γ.5. ΤΟ DEEPFAKE ΩΣ ΡΑΤΣΙΣΤΙΚΟ ΚΑΙ ΞΕΝΟΦΟΒΙΚΟ ΥΛΙΚΟ

Ως «ρατσιστικό και ξενοφοβικό υλικό» ορίζεται σύμφωνα με το άρθρο 2 παρ. 1 του Πρόσθετου Πρωτοκόλλου της Σύμβασης της Βουδαπέστης *«κάθε γραπτό υλικό, εικόνα ή άλλη έκφραση ιδεών ή θεωριών που υποστηρίζουν, προάγουν ή υποδαυλίζουν το μίσος τις διακρίσεις ή την βία κατά κάποιου ατόμου ή ομάδας ατόμων με βάση την φυλή, το χρώμα, την καταγωγή, την εθνική ή την εθνοτική προέλευση, καθώς και την θρησκεία, εάν αυτή χρησιμοποιείται ως πρόσχημα για κάποιον από τους ανωτέρω παράγοντες»*.[374] Θύματα των εν λόγω εγκλημάτων μίσους είναι πρόσωπα που έχουν ως χαρακτηριστικό ότι ανήκουν σε μια εξατομικευμένη ομάδα που διακρίνεται με βάση κάποιο χαρακτηριστικό, όπως το χρώμα, την καταγωγή ή τη θρησκεία.[375]

[374] https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

[375] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 114

### Γ.5.1 Εγκλήματα εκφοράς ρατσιστικού λόγου μέσω του διαδικτύου

Ο Ν 927/1979 περί κολασμού πράξεων ή ενεργειών αποσκοπουσών εις φυλετικάς διακρίσεις αποτελεί τον πιο σημαντικό νόμο για το ρατσισμό, ο οποίος όμως δύσκολα έχει εφαρμοστεί για τον ρατσισμό καθώς η διατύπωσή του παρουσιάζει σημαντικά προβλήματα στην εφαρμογή του. Για το λόγο αυτό, ψηφίστηκε ο Ν 4285/2014, ο οποίος αντικατέστησε πλήρως τον Ν 927/1979, διαμορφώνοντας ένα νέο πλαίσιο αντιμετώπισης του φαινομένου.[376]

Ο Έλληνας νομοθέτης με το άρθρο 1 του Ν 4285/2014 τυποποίησε μεταξύ άλλων και την τέλεση του εγκλήματος μέσω του διαδικτύου. Κυριότερες μεταβολές που επήλθαν στη διατύπωση του άρθρου 1 του Ν 929/1987 είναι α) η διεύρυνση του αριθμού των διακρίσεων και β) η αναφορά περισσότερων τρόπων τέλεσης του εγκλήματος.[377]

Έτσι η υποκίνηση βίας ή μίσους μέσω του διαδικτύου (άρθρο 1 παρ. 1-3 του Ν 927/1979) τελείται με προτροπή: α) σε πράξη που αντικειμενικά είναι πρόσφορη να προκαλέσει διακρίσεις, μίσος ή βία κατά προσώπου ή ομάδας προσώπων που προσδιορίζονται με βάση τα αναφερόμενα στη διάταξη ιδιαίτερα χαρακτηριστικά, κατά τρόπο αντικειμενικά πρόσφορο να προκαλέσει κίνδυνο για τη δημόσια τάξη που ενέχει ούτως ή άλλως απειλή για τη ζωή, την ελευθερία ή τη σωματική ακεραιότητα των ως άνω προσώπων (άρθρο 1 παρ. 1) και β) σε διάπραξη φθοράς ή βλάβης πραγμάτων, εφόσον αυτά χρησιμοποιούνταν από τις παραπάνω ομάδες ή πρόσωπα, κατά τρόπο αντικειμενικά πρόσφορο να προκαλέσει κίνδυνο για τη δημόσια τάξη (άρθρο 1 παρ. 2).[378] , [379]

Αντίστοιχα, σύμφωνα με το άρθρο 2 τυποποιήθηκε μεταξύ άλλων και η τέλεση του εγκλήματος της δημόσιας επιδοκιμασίας ή άρνησης εγκλημάτων μέσω του διαδικτύου, όπου αξιόποινη θεωρείται και η μέσω του διαδικτύου επιδοκιμασία, η κακόβουλη άρνηση της ύπαρξης, ο ευτελισμός της σοβαρότητας γενοκτονιών, εγκλημάτων πολέμου, του Ολοκαυτώματος και των ναζιστικών εγκλημάτων που έχουν αναγνωριστεί, όταν η συμπεριφορά αυτή εκδηλώνεται σε βάρος προσώπων ή ομάδας που προσδιορίζεται με βάση τη φυλή, το χρώμα, τη θρησκεία, τις γενεαλογικές καταβολές, την εθνική ή εθνοτική καταγωγή, το σεξουαλικό προσανατολισμό, την ταυτότητα φύλου, χαρακτηριστικά φύλου ή την αναπηρία και σωρευτικά όταν η συμπεριφορά

---

[376] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 114

[377] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 115

[378] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 116

[379] https://www.kodiko.gr/nomothesia/document/307515/nomos-927-1979

αυτή εκδηλώνεται κατά τρόπο που μπορεί να υποκινήσει βία ή μίσος ή ενέχει απειλητικό ή υβριστικό χαρακτήρα κατά μιας τέτοιας ομάδας ή μέλους της. Πρόκειται κατ' ουσίαν για περιπτώσεις έμμεσης προτροπής στις πράξεις του άρθρου 1 του ίδιου νόμου.[380]

Έχουν εκφραστεί πολλές απόψεις για το έννομο αγαθό που προστατεύει ο νόμος. Τα ρατσιστικά εγκλήματα προσβάλλουν τη δημόσια τάξη αφού προκαλούν όχι μόνο ανησυχίες και τρόμο στους πολίτες για την επιβολή της έννομης τάξης και για την υποχρέωση της πολιτείας να τηρηθεί ο σεβασμός στην ανθρώπινη αξιοπρέπεια και στα ανθρώπινα δικαιώματα. Για το λόγο αυτό, παράλληλα, με την προσβολή της δημόσιας τάξης προσβάλλεται κι ένα σύνολο ατομικών αγαθών της ανθρώπινης αξιοπρέπειας, της ζωής, της υγείας, προσωπικής ελευθερίας (παρ. 1) και της ιδιοκτησίας (παρ. 2), διότι αν διακινδυνεύσουν μαζικά τα παραπάνω προσωπικά έννομα αγαθά, τότε διακινδυνεύει κατ' ουσίαν και η δημόσια τάξη.

### Γ.5.2. Εγκλήματα με ρατσιστικά χαρακτηριστικά που τελούνται μέσω διαδικτύου

Το άρθρο 21 του Ν 4356/2015, αντικατέστησε το άρθρο 81Α ΠΚ που είχε προστεθεί στον ΠΚ με το άρθρο 10 του Ν 4285/2014, και το εν λόγω άρθρο έλαβε νέο τίτλο «Έγκλημα με ρατσιστικά χαρακτηριστικά» και προβλέπει γενικά επαυξημένα πλαίσια απειλούμενης ποινής, κατά περίπτωση «αν από τις περιστάσεις προκύπτει ότι έχει τελεστεί έγκλημα κατά παθόντος, η επιλογή του οποίου έγινε λόγω των χαρακτηριστικών φυλής, χρώματος, εθνικής ή εθνοτικής καταγωγής γενεαλογικών καταβολών, θρησκείας, αναπηρίας, σεξουαλικού προσανατολισμού, ταυτότητας ή χαρακτηριστικών φύλου», συνοδευόμενο πλέον από γενική επαύξηση του κατώτατου ορίου μετατροπής της ποινής κατ' άρθρο 82 παρ. 3 ΠΚ. Με τη νέα διατύπωση από τη δυσαπόδεικτη διάγνωση του κινήτρου του μίσους, το κέντρο βάρους μετατίθεται στο κριτήριο επιλογής του θύματος, με βάση τα ειδικά χαρακτηριστικά του, μεταβολή που έχει επισημανθεί ως θετική από την επιστήμη. Ο νομοθέτης είναι ιδιαίτερα προστατευτικός απέναντι στον παθόντα, φροντίζοντας να καλύψει κάθε κίνητρο του δράστη που στρέφεται κατά του θύματος και αφορά χαρακτηριστικά του τελευταίου.[381]

Τα deepfakes ως επί το πλείστον δεν σχετίζονται με πολιτική παραπληροφόρηση ή με χιουμοριστικό υλικό, αλλά με την πορνογραφία. Περίπου το 95% των deepfakes που θα συναντήσει κανείς στο διαδίκτυο είναι πορνογραφικού υλικό και δημιουργείται στο πλαίσιο του revenge porn. Ξεκίνησε με πιο δημοφιλείς «στόχους» όπως η Νάταλι Πόρτμαν, η Σκάρλετ

[380] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 116

[381] Ιδιαιτερότητες στην ποινική αντιμετώπιση του ρατσισμού που εκδηλώνονται μέσω του διαδικτύου, Χρήστος Νάιντος, Αντιεισαγγελέας Πρωτοδικών, Ειδικός Επιστήμονας Νομικής Σχολής ΔΠΘ, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η 2023, σελ. 118

Τζόχανσον και άλλες διάσημες. Όμως υπήρξε τρομακτική άνοδος της χρήσης deepfakes ως πορνογραφικό υλικό προξενώντας έντονες ανησυχίες για το μέλλον, με μια ισχυρή δόση σεξισμού, αφού ο μεγαλύτερος αριθμός των παραπλανητικών βίντεο χρησιμοποιείται για παρενόχληση, εξευτελισμό ή ακόμα και εκβιασμό γυναικών.[382] Τα βίντεο με πορνογραφικό περιεχόμενο δημιουργημένα με την τεχνολογία deepfake είναι στην πραγματικότητα κατά κύριο λόγο μια συνέπεια της ασέβειας προς τις γυναίκες και της αντικειμενοποίησης του γυναικείου σώματος που είναι ανεξέλεγκτη εκτός σύνδεσης και σίγουρα στο διαδίκτυο.

Τον Σεπτέμβριο 2021 το Ευρωπαϊκό Κοινοβούλιο ψήφισε υπέρ μιας νομοθετικής πρωτοβουλίας που απαιτεί ειδική νομοθεσία για την αντιμετώπιση όλων των μορφών έμφυλης βίας και διακρίσεων λόγω φύλου (κατά γυναικών και κοριτσιών, αλλά και κατά ατόμων LGBTIQ+), είτε εντός είτε εκτός διαδικτύου. Η έμφυλη βία μαστίζει στις μέρες μας. Στην κορυφή του μπορεί να βρίσκεται ακόμη και η αφαίρεση της ζωής – γυναικοκτονίες (όχι φυσικά μέσω διαδικτύου), καθώς πολλές φορές περιστατικά έμφυλης βίας μέσω ψηφιακών μέσων αποτελούν το προστάδιο για την τέλεση πράξεων έμφυλης βίας και στην πραγματική ζωή. Για παράδειγμα, πριν λίγα χρόνια η φοιτήτρια Λίνα Κοεμτζή πήδηξε από τον 9ο όροφο των φοιτητικών εστίων στην Θεσσαλονίκη, καθώς δεν άντεξε και δεν μπόρεσε να διαχειριστεί τις απειλές που δεχόταν έπειτα από την παράνομη δημοσίευση οπτικοακουστικού υλικού με ερωτικό περιεχόμενο στο οποίο απεικονιζόταν. Μπορούμε να φανταστούμε πλέον με τα όπλα που η τεχνολογία προσφέρει πως τα deepfakes μπορούν να χρησιμοποιηθούν για να προωθήσουν την έμφυλη βια ως μορφή σεξιστικής ρητορικής μίσους.

### Γ.6. ΤΟ DEEPFAKE ΩΣ ΜΕΣΟ ΕΚΦΟΒΙΣΜΟΥ - ΕΚΒΙΑΣΜΟΥ

Σύμφωνα με το άρθρο 385 του νΠΚ *«1. Όποιος, εκτός από τις περιπτώσεις του άρθρου 380, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, εξαναγκάζει κάποιον με βία ή απειλή σε πράξη, παράλειψη ή ανοχή από την οποία επέρχεται ζημία στην περιουσία του εξαναγκαζομένου ή άλλου τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή. 2. Αν η πράξη της προηγούμενης παραγράφου τελέστηκε με σωματική βία εναντίον προσώπου ή με απειλές ενωμένες με επικείμενο κίνδυνο σώματος ή ζωής επιβάλλεται κάθειρξη και χρηματική ποινή. Αν από την πράξη επήλθε ο θάνατος κάποιου προσώπου ή βαριά σωματική βλάβη ή αν η πράξη εκτελέστηκε με ιδιαίτερη σκληρότητα εναντίον προσώπου, επιβάλλεται κάθειρξη ισόβια ή πρόσκαιρη τουλάχιστον δέκα ετών και χρηματική ποινή. 3. Η εκβίαση τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή αν ο υπαίτιος μεταχειρίστηκε βία ή απειλή βλάβης της επιχείρησης, του επαγγέλματος, του λειτουργήματος ή άλλης δραστηριότητας που ασκεί ο εξαναγκαζόμενος ή άλλος ή προσφέρθηκε να παρέχει ή παρέχει προστασία για την αποτροπή πρόκλησης τέτοιας βλάβης*

[382] https://www.kathimerini.gr/society/561629566/vathainei-i-pligi-toy-revenge-porn-ayxisi-66-stis-kataggelies-to-2021/

*από τρίτον. Αν την παραπάνω πράξη τέλεσε πρόσωπο που διαπράττει τέτοιες πράξεις κατ' επάγγελμα, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή.»*[383]

Για τη θεμελίωση του εγκλήματος πρέπει να υπάρχει καταρχήν εξαναγκασμός κάποιου με βία ή με απειλή. Εξαναγκασμός είναι η επιβολή συμπεριφοράς μη ηθελημένης από τον παθόντα, δηλ. ο εξαναγκασμός έγκειται στην άσκηση βίας ή απειλής, που μπορούν να συνυπάρχουν ή να ασκηθούν διαδοχικώς, διά της οποίας περιάγεται ο άλλος σε τρόμο ή ανησυχία, στρέφεται δε η βία ή απειλή κατά της ελευθερίας της περιουσιακής διάθεσης,[384] με το σκοπό να καμφθεί η θέληση του εξαναγκαζομένου και να οδηγηθεί είτε ο ίδιος είτε άλλος σε πράξη, παράλειψη ή ανοχή, μετά από επηρεασμό και αφού εξουδετερωθεί η ελεύθερη βούλησή του, ουσιαστικά πειθαναγκαζόμενος να υποκύψει και να αποδεχθεί ακουσίως τις προτάσεις, ενώ η επαπειλούμενη εις βάρος του ενέργεια δεν απαιτείται να είναι παράνομη και τούτο διότι εκβίαση συνιστά όχι αυτή καθ' εαυτή η άσκηση εξουσίας ή δικαιώματος, αλλά η απειλή άσκησής τους προς επίτευξη του σκοπού που αναφέρεται στο άρθρο. [385],[386]

Ως βία νοείται κάθε μορφής βία (vis absoluta ή vis compulsiva στην § 1) και όχι μόνο σωματική που είναι ικανή να αποκλείσει το αυτοπροαίρετο της απόφασης του εξαναγκαζόμενου. Ως απειλή νοείται κάθε συμπεριφορά που συνιστά παρούσα πρόκληση κακού και είναι προορισμένη και πρόσφορη κατά την αντίληψη του δράστη να υπερνικήσει την αντίσταση που ο εξαναγκαζόμενος είτε έχει προβάλει, είτε αναμένεται να προβάλει. Η απειλή μπορεί να είναι ρητή και άμεση, να έχει διατυπωθεί προφορικώς ή εγγράφως, ή και εμμέσως να έχει μεταβιβαστεί και με άλλον, αρκεί να είναι ικανή να αποκλείσει το αυτοπροαίρετο της αποφάσεως του εξαναγκαζόμενου. Η απειλή μπορεί να στρέφεται κατά οποιουδήποτε έννομου αγαθού του παθόντος, όχι μόνο της ζωής ή της σωματικής ακεραιότητας, αλλά και της προσωπικης ελευθερίας της περιουσίας, της τιμής κ.λπ.[387]

Η περιουσιακή ζημία του εξαναγκαζόμενου πρέπει να προκληθεί διά της εκβίασης, πράγμα που σημαίνει ότι ο εξαναγκασμός πρέπει να υπάρχει και κατά το χρόνο που το θύμα ενδίδει και να επέδρασε η βία ή απειλή στο σχηματισμό της βούλησής του, αδιάφορο αν ο δράστης είχε αποφασίσει να πραγματοποιήσει την απειλή ή αν ήταν ή όχι πραγματοποιήσιμη. Όσον αφορά δε στην υποκειμενική υπόσταση, απαιτείται δόλος που περιλαμβάνει τη γνώση, έστω και με την έννοια του ενδεχόμενου δόλου (της αμφιβολίας) ότι με την ασκούμενη βία ή απειλή περιάγεται το παθητικό υποκείμενο σε καταναγκαστική κατάσταση και τη θέληση του δράστη να εξαναγκάσει τον παθόντα σε πράξη, παράλειψη ή ανοχή, από την οποία επέρχεται ζημία στην περιουσία αυτού του ίδιου ή άλλου (βασικός δόλος) και επί πλέον σκοπός του δράστη να αποκομίσει ο ίδιος ή άλλος

[383] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/
[384] https://www.karagiannislawfirm.gr/news/plastografia-kakoyrghmatikh
[385] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 3011
[386] ΑΠ 604/2021, www.areiospagos.gr
[387] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ 3012

παράνομο περιουσιακό όφελος (υπερχειλής δόλος), ανεξαρτήτως επίτευξης ή μη του οφέλους.[388],[389]

### Γ.6.1 Cyberbullying: Έννοια – Μέσα και Τρόποι εκδήλωσης αυτού

Το Cyberbullying μαστίζει στις μέρες και παρά τη θέσπιση των νέων διατάξεων του Ποινικού Κώδικα δεν προβλέφθηκε πάραυτα ρητή διάταξη που να αναφέρεται στη συμπεριφορά εκφοβιμού στο διαδίκτυο, για να τιμωρείται ο δράστης τέτοιων εγκλημάτων. Ένας πιθανός ορισμός που μπορεί να προσδιορίσει τι είναι ο διαδικτυακός εκφοβισμός είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, Tablets, κινητών τηλεφώνων). Ο θύτης μπορεί να είναι ανώνυμος και απουσιάζει η προσωπική επαφή με το θύμα, γεγονός που κάνει τον δράστη ισχυρότερο. Το θύμα βλάπτεται στον προσωπικό του χώρου, αφού όλα γίνονται μέσω ενός ηλεκτρονικού υπολογιστή.[390], [391]

Τα μέσα που χρησιμοποιούνται για τον εκφοβισμό μέσω διαδικτύου είναι το ηλεκτρονικό ταχυδρομείο (e-mail), τα γραπτά μηνύματα (sms), τα μέσα κοινωνικής δικτύωσης (social media), τα δωμάτια επικοινωνίας (chat rooms), τα ιστολόγια (blogs), τα διαδικτυακά παιχνίδια (internet games).[392]

Επιπλέον, σχετικά με τον τρόπο εκδήλωσης αυτού, οι δράστες χρησιμοποιούν τις νέες τεχνολογίες για να απειλήσουν, να παρενοχλήσουν, να δυσφημήσουν, να εκβιάσουν, να εκφοβίσουν και να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους σε μερικές περιπτώσεις. Μερικές από τις πιο συνηθισμένες μεθόδους είναι η αποστολή κειμένων - μηνυμάτων, e-mail με προσβλητικό περιεχόμενο (σε instant messengers ή chatrooms), η κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες κ.λπ..[393]

Η σεξουαλική εκβίαση [sextortion] είναι συχνό φαινόμενο στις μέρες μας και συντρέχει όταν ο δράστης εκβιάζει το θύμα με προσωπικό ή οικονομικό κίνητρο και πάλι με την δημοσίευση προσωπικών/σεξουαλικών εικόνων ή βίντεο. Πολύ συχνά μάλιστα μπορεί να πάρει την μορφή της

---

[388] Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022, σελ. 3023
[389] InLaw.gr
[390] https://www.sciencedirect.com/science/article/abs/pii/S0747563212002154
[391] https://socialpolicy.gr/2015/09/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1.html
[392] https://youngpeople.gr/cyber-bullying-%CE%AD%CE%BD%CE%B1%CF%82-%CE%B5%CE%BA%CF%86%CE%BF%CE%B2%CE%B9%CF%83%CE%BC%CF%8C%CF%82-%CE%B4%CE%AF%CF%87%CF%89%CF%82-%CF%8C%CF%81%CE%B9%CE%B1/
[393] https://www.proquest.com/openview/df7b85db5268ac4d18d07478e8fe197f/1.pdf?pq-origsite=gscholar&cbl=25066

απάτης σεξουαλικής εκβίασης [sexrtotion scam], όπου ο δράστης αποστέλλει μαζικά μηνύματα στο θύμα ότι δήθεν θα αποκαλύψει ευαίσθητο υλικό που το απεικονίζει εάν δεν καταθέσει το Χ οικονομικό ποσό σε τραπεζικό λογαριασμό που του αποστέλλει.

Το σημαντικό πλέον στις περιπτώσεις αυτές είναι ότι ο θύτης δεν χρειάζεται να έχει έρθει σε πραγματική επαφή και επικοινωνία με το θύμα, αφού μέσω των λογαριασμών του θύματος στα μέσα κοινωνικής δικτύωσης και χρησιμοποιώντας ως δεδομένα τις φωτογραφίες που έχει αναρτήσει μπορεί να δημιουργήσει απαγορευμένο υλικό, το οποίο μπορεί στη συνέχεια να χρησιμοποιήσει με σκοπό να εκβιάσει το θύμα, ώστε να έχει ο δράστης οικονομικό όφελος.

## Γ.7. ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΑΠΑΤΗΣ

Σύμφωνα με το άρθρο 386 ΠΚ «*1. Όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή. 2. Αν η απάτη στρέφεται άμεσα κατά του νομικού προσώπου του ελληνικού δημοσίου, των νομικών προσώπων δημοσίου δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και η ζημιά που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Η πράξη αυτή παραγράφεται μετά είκοσι (20) έτη.».*[394]

Το έγκλημα της απάτης στρέφεται αποκλειστικά κατά της περιουσίας[395], η οποία προστατεύεται ως σύνολο.[396] Κρατούσα στη θεωρία είναι η νομική-οικονομική θεωρία, κατά την οποία στην περιουσία ανήκουν όλα τα αγαθά ενός προσώπου, που έχουν οικονομική αξία και μπορούν να αποτιμηθούν σε χρήμα, εφόσον δεν αποδοκιμάζονται από την έννομη τάξη.[397] Στη νομολογία φαίνεται να επικρατεί η οικονομική θεωρία, κατά την οποία στην περιουσία υπάγονται όλα τα αγαθά ενός προσώπου που μπορούν να αποτιμηθούν σε χρήμα, έχουν δηλαδή οικονομική αξία.[398]

[394] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/
[395] πάγια νομολογία βλ. ενδ. ΑΠ 556/2020 ΤΝΠ QUALEX, ΑΠ 1759/2016 ΠοινΧρ 2018, 108 με παρατ. Βαθιώτη, ΣυμβΑΠ 324/2007 ποινχρ 2008, 45
[396] Μυλωνόπουλος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, 2006, 439
[397] Σπινέλλης, ΠΔ, ΕιδΜερ, τ.Β' 1985, 97, Μυλωνόπουλος, ό.π., 373 επ., Αποστολιδου, Απάτη - Η πλάνη ως αποτέλεσμα πράξης εξαπάτησης και η περιουσιακή διάθεση στο έγκλημα της απάτης, 2000, 119 επ.
[398] βλ. ενδ. ΑΠ 1470/2019 ποινχρ 2019, 665, ΑΠ 735/2017 ΠοινΧρ 2018, 751, ΑΠ 1759/2016 ποινχρ 2018, 108, ΑΠ 196/2015 ΠοινΔικ 2017, 45 με παρατ. Μπαλτά = ΠοινΧρ 2017, 274, ΑΠ 972/2014 ποινχρ 2015, 97, ΑΠ 389/2014 ποινχρ 2015, 176

Η απάτη είναι πλημμέλημα στο εδ. α' της παρ. 1 του άρθρου 386 ΠΚ και κακούργημα στο εδ. β' της παρ. 1 και στην παρ. 2, έγκλημα κοινό, αφού μπορεί να τελεστεί από τον οποιονδήποτε, υπαλλακτικώς μικτό,[399] αφού οι περισσότεροι τρόποι εξαπάτησης μπορούν να εναλλαχθούν ή να σωρευθούν στο ίδιο υλικό αντικείμενο, χωρίς να τελεί ο δράστης περισσότερα εγκλήματα, εφόσον προσβάλλεται η ίδια μονάδα του εννόμου αγαθού, έγκλημα υπερχειλούς υποκειμενικής υπόστασης ή σκοπού, έγκλημα χαρακτηριζόμενο από αλληλεπίδραση μεταξύ δράστη και θύματος, έγκλημα βλάβης του εννόμου αγαθού της περιουσίας και ειδικότερα αυτοβλάβης του θύματος, αποτελέσματος συνδεδεμένου με ειδική συμπεριφορά, αφού πρέπει η παραπλάνηση του θύματος να προκλήθηκε μόνον με τους περιγραφόμενους στη διάταξη τρόπους, περιουσιακής μετάθεσης ή περιουσιακής μετατόπισης κατά παρεμφερή ορολογία.[400]

Η αντικειμενική υπόσταση του εγκλήματος της απάτης περιλαμβάνει α) την πράξη εξαπάτησης, που έγκειται στην εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή στην αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, β) την πλάνη που δημιουργήθηκε στο θύμα, ως παραγωγός αιτία της πράξης εξαπάτησης, η οποία δεν αναγράφεται ρητά στο νόμο, αλλά συνάγεται ερμηνευτικά από τη λέξη «πείθοντας», γ) την περιουσιακή διάθεση του θύματος, που συνίσταται σε πράξη, παράλειψη ή ανοχή, με την οποία επενεργεί άμεσα στην περιουσία αυτού ή άλλου και η οποία πρέπει να προκλήθηκε αιτιωδώς από την πλάνη που του προκάλεσε ο δράστης, δ) τη βλάβη, ξένης κατά το αστικό δίκαιο, περιουσίας του θύματος ή άλλου, που πρέπει να αντιστοιχεί στο περιουσιακό όφελος που σκόπευε ο δράστης της απάτης και να τελεί σε αιτιώδη σύνδεσμο με την απατηλή συμπεριφορά και την εξαιτίας αυτής πλάνη του διαθέτοντος. Στην αντικειμενική υπόσταση εξετάζεται και ε) ο αντικειμενικός αιτιώδης σύνδεσμος μεταξύ όλων των προαναφερόμενων στοιχείων, όπως και στ) η υλική αντιστοιχία μεταξύ του επιδιωκόμενου περιουσιακού οφέλους και της προκληθείσας περιουσιακής ζημίας.[401]

Η υποκειμενική υπόσταση του εγκλήματος της απάτης περιλαμβάνει α) τον δόλο (αρκούντως του ενδεχόμενου) ως προς όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, εκτός από την πράξη εξαπάτησης που απαιτεί αναγκαίο άμεσο δόλο, δηλαδή γνώση του ψευδούς περιεχομένου της παράστασης κ.λπ. και β) τον σκοπό του δράστη να αποκομίσει παράνομο

[399] πάγια νομολογία βλ. ΟλΑΠ 1/2020 ΠοινΔικ 2020, 708 = ποινχρ 2020, 499, ΑΠ 825/2020 ΤΝΠ QUALEX, ΑΠ 457/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX (αναιρ.), ΟλΑΠ 3/2019 ΠοινΔικ 2019, 594 = ποινχρ 2019, 424, ΑΠ 1232/2019 ΤΝΠ QUALEX, ΑΠ 983/2018 ΠειρΝομ 2018, 250 = ποινχρ 2019, 197

[400] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη, σελ. 3058-3059

[401] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη, σελ. 3059

περιουσιακό όφελος άμεσα από τη βλάβη της περιουσίας του θύματος ή άλλου (έγκλημα υπερχειλούς υποκειμενικής υπόστασης).[402]

Η παραπλάνηση του θύματος επιτυγχάνεται με τρεις, υπαλλακτικά μικτούς, τρόπους (παράσταση, απόκρυψη, παρασιώπηση), που κατατείνουν σε ένα και το αυτό έγκλημα και διαφέρουν εννοιολογικά μεταξύ τους. Ειδικότερα, οι δύο πρώτοι συνιστούν περιπτώσεις θετικής απατηλής συμπεριφοράς, ενώ εκείνος της αθέμιτης παρασιώπησης αληθινών γεγονότων, συνιστά περίπτωση απατηλής συμπεριφοράς, τελούμενης με παράλειψη, δηλαδή με την παράλειψη ανακοίνωσης αληθινών γεγονότων, για τα οποία υπήρχε υποχρέωση ανακοίνωσης από τον νόμο, τη σύμβαση ή προηγούμενη συμπεριφορά του υπαιτίου.[403] Ο δράστης μπορεί να χρησιμοποιεί παράλληλα ή διαδοχικά όλους τους τρόπους διάπραξης της απάτης, ιδίως με συνεχιζόμενες ψευδείς παραστάσεις, που επαναλαμβάνονται μέχρι να καλλιεργηθεί στο εξαπατώμενο πρόσωπο η επιδιωκόμενη πλάνη με την απόσπαση της εμπιστοσύνης του.[404] Η πράξη εξαπάτησης μπορεί να γίνει με οποιονδήποτε τρόπο, με έγγραφο ή προφορικά, ρητά ή σιωπηλά, δηλαδή να συνάγεται από τη συμπεριφορά του δράστη[405] και απαιτεί επικοινωνία μεταξύ δράστη και θύματος. Έχει όμως νομολογηθεί ότι πρέπει η ψευδής παράσταση να απευθύνεται σε συγκεκριμένα πρόσωπα, χωρίς όμως να είναι απαραίτητη και η προσωπική επικοινωνία δράστη και θυμάτων.[406] Ο δράστης τελικά κατάφερε, με τις παραπλανητικές του μεθόδους, να προκαλέσει πλάνη σε ατομικώς προσδιορισμένα άτομα, τα οποία και αυτοζημιώθηκαν εξαιτίας της παραπλανητικής του συμπεριφοράς. Συνεπώς, όταν η παραπλανητική ενέργεια του δράστη (είτε συνίσταται σε παράσταση ψευδούς γεγονότος ως αληθινού είτε σε αθέμιτη απόκρυψη είτε σε αθέμιτη παρασιώπηση αληθινού γεγονότος) οδήγησε αιτιωδώς ένα πρόσωπο σε περιουσιακή διάθεση επιζήμια για την περιουσία αυτού ή άλλου και πληρούται η ειδική υπόσταση της απάτης, δεν νοείται σε μεταγενέστερους χρόνους η τέλεση νέας παραπλανητικής ενέργειας κατά αυτού του ίδιου προσώπου με άλλον τρόπο τέλεσης από τους υπαλλακτικά τρεις προβλεπόμενους.[407]

Σύμφωνα με πάγια νομολογία, ως γεγονότα κατά την έννοια του άρθρου 386 ΠΚ νοούνται τα πραγματικά περιστατικά, δηλαδή τα συμβεβηκότα του εξωτερικού κόσμου, που απεικονίζουν την

---

[402] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 3059

[403] βλ. ενδ. ΑΠ 825/2020 ΤΝΠ QUALEX, ΑΠ 651/2020 ΤΝΠ QUALEX, ΑΠ 556/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX κλπ

[404] ΑΠ 2030/2019 ΤΝΠ QUALEX, ΑΠ 1377/2019 ΤΝΠ QUALEX κ.α.

[405] ενδ. ΑΠ 556/2020 ΤΝΠ QUALEX, ΑΠ 569/2012 ΠοινΧΡ 2012, 678

[406] ΑΠ 1874/2019 ΤΝΠ QUALEX, ΑΠ 201/2010 ΠοινΔικ 2010, 1261 = ΠοινΧρ 2011

[407] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 3061-3062

πραγματικότητα, τα οποία ανάγονται στο παρελθόν ή στο παρόν[408] και πρέπει να έχουν συμβεί το αργότερο μέχρι τον χρόνο έναρξης της παραπλανητικής συμπεριφοράς του δράστη.[409] Τα γεγονότα μπορεί να αναφέρονται στην προσωπική κατάσταση, όπως είναι η ηλικία και η ταυτότητα, στη φερεγγυότητα, στο επάγγελμα, στις έννομες στη νομική κατάσταση του πράγματος και στο κύρος ή την ισχύ δικαιοπραξιών.[410] Γίνεται δεκτό κατά πάγια νομολογία ότι οι απλές υποσχέσεις ή συμβατικές υποχρεώσεις μπορεί να θεμελιώνουν το έγκλημα της απάτης, εάν συνοδεύονται ταυτόχρονα από άλλες παραστάσεις ψευδών γεγονότων, που αναφέρονται στο παρελθόν ή στο παρόν, κατά τέτοιο τρόπο ώστε να δημιουργούν την εντύπωση μελλοντικής εκπλήρωσής τους με βάση την εμφανιζόμενη ήδη στο παρόν ψευδή πραγματική κατάσταση από τον δράστη, που είχε εξαρχής ειλημμένη την πρόθεση να μην εκπληρώσει την υποχρέωσή του.[411]

Ως παράσταση ψευδών γεγονότων νοείται η ανακοίνωση σε κάποιον μιας σκέψης ή η βεβαίωση ή ο ισχυρισμός σχετικά με ένα γεγονός.[412] Η παράσταση μπορεί να αφορά οποιαδήποτε ανακοίνωση, δήλωση διαβεβαίωση ή ισχυρισμό, στον οποίο υπάρχει ανακριβής παρουσίαση ή απεικόνιση της πραγματικότητας. Μπορεί να είναι ρητή ή να συνάγεται συμπερασματικά από τη συμπεριφορά του δράστη[413], μπορεί να γίνεται με λόγια ή έργα ή ενδεικτικές πράξεις ή να προκύπτει από την όλη στάση του δράστη, χωρίς να είναι ανάγκη να συνοδεύεται από δόλια τεχνάσματα και μηχανοραφίες, αρκεί να είναι ικανή να παραπλανήσει αυτόν προς τον οποίο γίνεται ή κατ' άλλη ορολογία να είναι πρόσφορη να παραπλανήσει τον παθόντα για να προβεί στην περιουσιακή διάθεση.[414]

Η αθέμιτη απόκρυψη της αλήθειας συνιστά θετική συμπεριφορά με την οποία ο παραπλανώμενος εμποδίζεται να πληροφορηθεί την αλήθεια. Διαφέρει από την απάτη με παρασιώπηση, διότι η απόκρυψη έχει ως προϋπόθεση και άλλη αθέμιτη ενέργεια με θετική πράξη του δράστη, σύγχρονη ή συγκαλυπτική της αλήθειας.[415]

Κατά πάγια νομολογία, συνιστά αθέμιτη παρασιώπηση η παράλειψη ανακοίνωσης αληθινών γεγονότων, όταν από τον νόμο ή τη σύμβαση ή από προηγούμενη ενέργεια του δράστη υπάρχει υποχρέωση ανακοίνωσή τους κατ' άρθρο 15 ΠΚ.[416]

---

[408] ενδ. ΑΠ 651/2020 ΤΝΠ QUALEX, ΑΠ 128/2018 ΠοινΔικ 2018, 1126 = ΠοινΧρ 2019, 217, Συμβ ΑΠ 1074/2018 ΠειρΝομ 2018, 254 = ΠοινΧρ 2019, 199, ΑΠ 310/2016 ΠοινΧρ 2017, 670
[409] ΑΠ 735/2017 ΠοινΧρ 2018, 751, ΑΠ 1759/2016 ΠοινΧρ 2018, 108
[410] ΑΠ 112/2019 ΤΝΠ QUALEX, ΑΠ 569/2012 ΠοινΧρ 2012, 678
[411] ΟλΑΠ 1/2020 ΠοινΔικ 2020, 708 = ΠοινΧρ 2020, 499, ΑΠ 773/2020 areiospagos.gr, ΑΠ 651/2020 ΤΝΠ QUALEX, ΑΠ 514/2020 ΤΝΠ QUALEX, ΑΠ 457/2020 ΤΝΠ QUALEX κ.α.
[412] ΟλΑΠ 1585/1984 ΠοινΧρ 1985, 496
[413] ΑΠ 107/2020 ΤΝΠ QUALEX (αναιρ.), ΟλΑπ 1/2020 ΠοινΔικ 2020, 708 = ΠοινΧρ 2020, 499, ΟλΑπ 3/2019 ΠοινΔικ 2019, 594 = ΠοινΧρ 2019, 424 κ.α.
[414] ΑΠ 874/2019 ΤΝΠ QUALEX κ.α.
[415] ΑΠ 1924/1997 ΠοινΧρ 1998, 648, ΣυμβΑΠ 1925/1997 ΠοινΧρ 1998, 651 κ.α.
[416] βλ. ενδ. ΟλΑΠ 1/2020 ΠοινΔικ 2020, 708= ΠοινΧρ 2020, 499, ΟλαΑΠ 3/2019 ΠοινΔικ 2019 κ.α.

Πλάνη είναι κάθε παράσταση στη συνείδηση του διαθέτοντας ως προς συγκεκριμένο πραγματικό περιστατικό, που δεν ανταποκρίνεται στην πραγματικότητα. Πλάνη είναι η διάσταση μεταξύ της βούλησης και της δήλωσης βούλησης.[417] Η παραπλάνηση του θύματος δύναται να προκληθεί μόνο με κάποιον από τους τρόπους που ρητά αναφέρονται στη διάταξη (παράσταση ψευδών γεγονότων, απόκρυψη ή αποσιώπηση αληθινών) και όχι από οποιαδήποτε άλλη αιτία.[418]

Όσον αφορά στην περιουσιακή διάθεση πρέπει να προσδιορίζεται ποια πράξη, παράλειψη ή ανοχή, η οποία συνιστά περιουσιακή διάθεση, τέλεσε ο παραπλανημένος, ως συνέπεια της προκληθείσας από τον δράστη πλάνης, ελλείποντος δε του στοιχείου αυτού λείπει και ο αντικειμενικός αιτιώδης σύνδεσμος μεταξύ της πράξης εξαπάτησης, της πλάνης του διαθέτοντος, της περιουσιακής διάθεσης και της βλάβης, οπότε δεν υφίσταται απάτη.[419] Ως περιουσία νοείται το σύνολο των οικονομικών αγαθών του προσώπου που έχουν χρηματική αξία ή κατ' άλλη παρεμφερή διατύπωση, το σύνολο των περιουσιακών αγαθών ενός προσώπου που έχουν αποτιμητή σε χρήμα αξία.[420] Βλάβη της περιουσίας είναι η μείωσή της, δηλαδή η επί έλαττον διαφορά μεταξύ της χρηματικής αξίας την οποία είχε πριν την περιουσιακή διάθεση που προκλήθηκε με την απατηλή συμπεριφορά και εκείνης που απέμεινε μετά από αυτήν.[421]

Από την παράσταση ψευδών γεγονότων ως αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών, πρέπει ως παραγωγό αιτία, να παραπλανήθηκε κάποιος και να προέβη στην επιζήμια για τον ίδιο ή άλλον πράξη, παράλειψη ή ανοχή.[422] Έπειτα, η βλάβη της ξένης περιουσίας πρέπει να τελεί σε αιτιώδη σύνδεσμο με τις παραπλανητικές ενέργειες ή παραλείψεις του δράστη και την πλάνη εκείνου που προέβη στην περιουσιακή διάθεση.[423] Όπως αναφέρεται και στην υπ' αρ. 1/2020 ΑΠ *«Πρέπει δηλαδή να υπάρχει αιτιώδης σύνδεσμος μεταξύ της απατηλής συμπεριφοράς και της πλάνης που προκλήθηκε από αυτήν, καθώς και μεταξύ της πλάνης αυτής και της περιουσιακής βλάβης, η οποία πρέπει να είναι το άμεσο, αναγκαίο και αποκλειστικό αποτέλεσμα της πλάνης και της εξαιτίας αυτής πράξης, παράλειψης ή ανοχής, στην οποία προέβη εκείνος που πλανήθηκε από την απατηλή συμπεριφορά του δράστη.»*[424]

---

[417] ΑΠ 131/2020 ΤΝΠ QUALEX, ΑΠ 568/2020 ΤΝΠ QUALEX, ΑΠ 1331/2019 ΤΝΠ QUALEX

[418] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 3074-3075

[419] ΑΠ 743/2012 ΠοινΧρ 2013, 604 = ΤΝΠ QUALEX (αναιρ.), ΑΠ 211/2008 ΠοινΧρ 2009, 38

[420] ΑΠ 457/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX, ΑΠ 2332/2019 ΤΝΠ QUALEX κ.α.

[421] ΑΠ 107/2020 ΤΝΠ QUALEX, ΑΠ 457/2020 ΤΝΠ QUALEX, ΑΠ 2332/2019 ΤΝΠ QUALEX κ.α.

[422] βλ. ενδ. ΑΠ 825/2020 ΤΝΠ QUALEX, ΑΠ 774/2020 ΤΝΠ QUALEX, ΑΠ 527/2020 ΤΝΠ QUALEX, ΑΠ 457/2020 ΤΝΠ QUALEX, ΑΠ 131/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX, ΑΠ 1470/2019 ΠοινΧρ 2019, 665, ΑΠ 178/2019 ΤΝΠ QUALEX κ.α.

[423] βλ. ενδ. ΑΠ 825/2020 ΤΝΠ QUALEX, ΑΠ 527/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX, ΑΠ 128/2018 ΠοινΔικ 2018, 1126 = ΠοινΧρ 2019, 217 κ.α.

[424] βλ. ενδ. ΟλΑΠ 1/2020, 708 = ΠοινΧρ 2020, 499, ΑΠ 651/2020 ΤΝΠ QUALEX, ΑΠ 107/2020 ΤΝΠ QUALEX κ.α.

Η υποκειμενική υπόσταση του εγκλήματος της απάτης περιλαμβάνει α) τον δόλο, αρκούντος του ενδεχόμενου ως προς όλα τα στοιχεία της αντικειμενικής υπόστασης του εγκλήματος, εκτός από την πράξη εξαπάτησης που απαιτεί άμεσο αναγκαίο δόλο και β) τον σκοπό του δράστη να αποκομίσει παράνομο περιουσιακό όφελος από τη βλάβη της περιουσίας του θύματος ή άλλου, αδιάφορα αν τελικά επιτευχθεί το όφελος.[425]

Στοιχειοθετείται απάτη σε βαθμό κακουργήματος τιμωρούμενη με κάθειρξη έως δέκα έτη και χρηματική ποινή, όταν η ζημία που προκλήθηκε από την απάτη υπερβαίνει συνολικά το ποσό των 120.000 ευρώ. Προϋποθέτει η διάταξη ότι έχουν πληρωθεί όλα τα στοιχεία της αντικειμενικής και υποκειμενικής υπόστασης του βασικού αδικήματος της παρ. 1 και η πράξη ανάγεται σε κακούργημα εξαιτίας του ύψους της ζημίας.[426]

Η απάτη, που στρέφεται άμεσα κατά του ελληνικού δημοσίου, των ΟΤΑ και των ΝΠΔΔ, εφόσον η ζημία που προκλήθηκε υπερβαίνει συνολικά τις 120.000 ευρώ, τυποποιείται στο άρθρο 386 παρ. 2 ΠΚ και συνιστά ιδιαίτερα διακεκριμένη μορφή απάτης, τιμωρούμενη με κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες. Για να εφαρμοστεί το άρθρο 386 παρ. 2 ΠΚ, πρέπει να συντρέχουν όλα τα αντικειμενικά και υποκειμενικά στοιχεία του βασικού εγκλήματος της απάτης της παρ. 1, δηλαδή ο δράστης πρέπει εν γνώσει του να τέλεσε μια πράξη παραπλάνησης (παράσταση ψευδών γεγονότων, αθέμιτη απόκρυψη αληθινών, παρασιώπηση αληθινών), η οποία πρέπει να προκάλεσε αιτιωδώς πλάνη σε άλλον, εξαιτίας της οποίας προέβη σε περιουσιακή διάθεση, η οποία αιτιωδώς πρέπει να προκάλεσε βλάβη στην περιουσία του δημοσίου κλπ. Από υποκειμενικής πλευράς, απαιτείται επιπλέον του δόλου, που πρέπει να καλύπτει όλα τα στοιχεία της αντικειμενικής υπόστασης και της γνώσης του ψεύδους των γεγονότων, ο δράστης να σκοπεύει να αποκομίσει αυτός ή άλλος, από την πράξη του, παράνομο περιουσιακό όφελος, που να προέρχεται από την περιουσία του δημοσίου κλπ. συνιστώστας την αντίστροφη όψη της ζημίας, χωρίς να απαιτείται και ο προσπορισμός αυτού του οφέλους. Επίσης, απαιτείται η πράξη της απάτης να στρέφεται άμεσα κατά του ελληνικού δημοσίου, του ΟΤΑ ή του ΝΠΔΔ, όπως ρητά ορίζει η παρ. 2 του άρθρου 386 νέου ΠΚ.[427]

Χαρακτηριστικό παράδειγμα απάτης deepfake αποτελεί το γεγονός που έλαβε χώρα τον Μάρτιο του 2019, όπου η Wall Street Journal ανέφερε ότι μια βρετανική εταιρεία ενέργειας εξαπατήθηκε κατά 250.000 ευρώ μέσω της χρήσης deepfake audio. Η εταιρεία παραμένει ανώνυμη, αλλά οι

[425] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 3091

[426] ΣυμβΠλημΑθ 2992/2016 ΠοινΧρ 2017, 309

[427] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 3100

ασφαλιστές της μοιράστηκαν τα γεγονότα με τη Wall Street Journal, υποστηρίζοντας ότι οι απατεώνες χρησιμοποίησαν τεχνητή νοημοσύνη για να μιμηθούν τη φωνή του Γερμανού διευθύνοντος συμβούλου της εταιρείας. Χρησιμοποιώντας αυτή τη φωνή, κάλεσαν έναν ανώτερο υπάλληλο και του ζήτησαν να μεταφέρει αμέσως 250.000 ευρώ στο λογαριασμό ενός υποτιθέμενου προμηθευτή ενέργειας. Ο εργαζόμενος θεώρησε ότι επρόκειτο για ένα ασυνήθιστο αίτημα, αλλά συμμορφώθηκε επειδή πίστευε ότι μιλούσε με το αφεντικό του. Ο συναγερμός σήμανε μόνο όταν του ζητήθηκε να στείλει άλλα 250.000 ευρώ. Μέχρι να εμπλακούν οι τράπεζες και οι αρχές, τα χρήματα είχαν εξαφανιστεί και τα ίχνη είχαν χαθεί. Για να το πετύχουν αυτό, οι δράστες συγκέντρωσαν προσωπικά δεδομένα για να εκπαιδεύσουν τους αλγόριθμους τεχνητής νοημοσύνης. Στην περίπτωση αυτή, τα δεδομένα εκπαίδευσης θα ήταν η φωνή του Γερμανού διευθύνοντος συμβούλου. Δεδομένης της εξέχουσας θέσης του, αυτό θα μπορούσε να είναι δημόσια διαθέσιμο και εύκολα προσβάσιμο. Ίσως είχε κάνει μια ομιλία που βρισκόταν στον ιστότοπο της εταιρείας, στο YouTube ή στο LinkedIn. Ίσως παρουσιάστηκε σε ηχητικό ή βιντεοσκοπημένο υλικό στα μέσα κοινωνικής δικτύωσης, όπως μια συνέντευξη σε ένα ειδησεογραφικό κανάλι. Ίσως εμφανίστηκε κάπου στα μέσα κοινωνικής δικτύωσης με την προσωπική του ιδιότητα. Ακόμη και αν ο διευθύνων σύμβουλος δεν είχε αναρτήσει τίποτα ο ίδιος, μπορεί να έχει αναρτηθεί από κάποιον άλλον. Με τη δυνατότητα κλοπής της φωνής και της εικόνας κάποιου, η απάτη μέσω μιμήσεων έχει ενισχυθεί. Εντός τεσσάρων μηνών από την υπόθεση που έγινε πρωτοσέλιδο τον Μάρτιο του 2019, η εταιρεία κυβερνοασφάλειας Symantec ανέφερε ότι τρεις άλλες εταιρείες είχαν πέσει θύματα παρόμοιων παγίδων, με την Al να χρησιμοποιείται για να κλωνοποιεί φωνές και να καλεί ανώτερους οικονομικούς υπαλλήλους ζητώντας επείγουσες μεταφορές χρημάτων. Η Symantec δεν αποκάλυψε τα ονόματα των επιχειρήσεων, αλλά επιβεβαίωσε ότι χάθηκαν εκατομμύρια δολάρια.[428]

Όμως, φυσικά, δεν είναι μόνο οι εταιρείες που πρέπει να ανησυχούν, καθώς ήδη δέχονται επιθέσεις και μεμονωμένα άτομα. Τα deepfakes μπορούν να εξαπατήσουν ιδιώτες, από τη διείσδυση στις ηλεκτρονικές τραπεζικές συναλλαγές μέχρι τους απατεώνες που παριστάνουν τα μέλη της οικογένειας ή έναν φίλο που βρίσκεται σε κίνδυνο. Οι ηλικιωμένοι και οι ευάλωτες ομάδες αποτελούσαν παραδοσιακά στόχους ατομικής απάτης, καθώς υποτίθεται ότι είναι ευκολότερο να εξαπατηθούν.

### Γ.8. ΤΑ DEEPFAKES ΩΣ ΜΕΣΟ ΠΛΑΣΤΟΓΡΑΦΙΑΣ

Σύμφωνα με το άρθρο 216 του νέου ΠΚ *"1. Όποιος καταρτίζει πλαστό ή νοθεύει έγγραφο με σκοπό να παραπλανήσει με τη χρήση του άλλον σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες τιμωρείται με φυλάκιση και χρηματική ποινή. 2. Με την ίδια ποινή τιμωρείται όποιος για τον παραπάνω σκοπό εν γνώσει χρησιμοποιεί πλαστό ή νοθευμένο έγγραφο. 3. Αν ο υπαίτιος των*

[428] Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020, σελ. 149

*πράξεων των παρ. 1 και 2 σκόπευε να προσπορίσει στον εαυτό του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται: α) εάν το συνολικό όφελος ή η συνολική ζημία είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή, β) εάν το συνολικό όφελος ή η συνολική ζημία υπερβαίνει τις εκατόν είκοσι χιλιάδες (120.000) ευρώ, με κάθειρξη έως δέκα (10) έτη και χρηματική ποινή. 4. Αν οι πράξεις των παρ. 1 και 2 στρέφονται άμεσα κατά του νομικού προσώπου του ελληνικού Δημοσίου, των νομικών προσώπων Δημοσίου Δικαίου ή των οργανισμών τοπικής αυτοδιοίκησης και το συνολικό περιουσιακό όφελος ή η συνολική ζημία υπερβαίνει συνολικά τις εκατόν είκοσι χιλιάδες (120.000) ευρώ, επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες (1.000) ημερήσιες μονάδες. Οι πράξεις αυτές παραγράφονται μετά είκοσι (20) έτη.».*[429]

Στο άρθρο αυτό τυποποιείται το έγκλημα της πλαστογραφίας και της χρήσης πλαστού σε βαθμό πλημμελήματος και κακουργήματος. Έννομο αγαθό της συγκεκριμένης διάταξης είναι η αποδεικτική ακεραιότητα του «υπομνήματος», η γνησιότητα του εγγράφου, ως κοινωνικού αγαθού και η διάταξη προστατεύει την ασφάλεια και την ακεραιότητα των έγγραφων συναλλαγών.[430] Η πλαστογραφία είναι έγκλημα κοινό, δηλαδή μπορεί να τελεστεί από οποιονδήποτε, τυπικό, σωρευτικά μικτό, δυνητικής διακινδύνευσης, στιγμιαίο, γνήσιο ενέργειας που δεν μπορεί να τελεστεί με παράλειψη.[431]

Στο άρθρο 216 ΠΚ τυποποιούνται σε βαθμό πλημμελήματος η πλαστογραφία της παρ. 1 που τιμωρείται με φυλάκιση και χρηματική ποινή και στην παρ. 2 η χρήση πλαστού εγγράφου που τιμωρείται με την ίδια ποινή. Στην παρ. 3 τυποποιείται η πλαστογραφία σε βαθμό κακουργήματος με περιουσιακό όφελος ή ζημία, που υπερβαίνει τις 120.000 ευρώ και τιμωρείται με κάθειρξη έως δέκα έτη και χρηματική ποινή και στην παρ. 4 η πλαστογραφία σε βάρος του ελληνικού δημοσίου ή ΝΠΔΔ ή ΟΤΑ, με συνολικό όφελος ή ζημία που υπερβαίνει 120.000€ και τιμωρείται με κάθειρξη τουλάχιστον δέκα ετων και χρηματική ποινή έως 1000 ημερήσιες μονάδες.[432]

Δράστης της πλαστογραφίας μπορεί να είναι ο οποιοσδήποτε, ενώ υλικό αντικείμενο της πλαστογραφίας είναι το έγγραφο. Η έννοια του εγγράφου προσδιορίζεται αυθεντικά στο άρθρο 13 στοιχ. γ' ΠΚ. Υλικό αντικείμενο της πλαστογραφίας μπορεί να αποτελέσει τόσο το ιδιωτικό όσο και το δημόσιο έγγραφο, αφού ο νόμος δεν διακρίνει. Έγγραφα συνιστουν τα επικυρωμένα και ανεπικύρωτα φωτοαντίγραφα άλλων εγγράφων, το telefax, το telex, το e-mail, οι ιστοσελίδες, η

[429] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/, https://www.lawspot.gr/
[430] ΑΠ Ολ 1/2018 ΠοινΧρ 2018, 514, ΑΠ 1150/2019 ΝΟΜΟΣ, ΑΠ 537/2019 ΝΟΜΟΣ, ΑΠ 367/2019 ΝΟΜΟΣ, ΑΠ 940/2017 ΝΟΜΟΣ, ΑΠ 729/2017 ΝΟΜΟΣ κ.λπ.
[431] ΑΠ 940/2017 ΝΟΜΟΣ, ΑΠ 232/2017 ΝΟΜΟΣ, ΑΠ 2325/2009 ΠοινΧρ 2010, 271 (με παρατ. Παπούλια), ΑΠ 1536/2008 ΠοινΧρ 2009, 545, ΣυμβΑΠ 1393/2008 ΠοινΧρ 2009, 523, ΣυμβΑΠ 35/2008 ΠοινΧρ 2008, 834, ΑΠ 1103/2007 ΠοινΧρ 2008, 328, ΣυμβΑΠ 759/1999 ΠοινΧρ 2000, 324, ΣυμβΑΠ 769/2003 ΠοινΧρ 2004, 150
[432] Νομοθεσία - Δικηγόρος - Δικαστήρια - Νομικά Νέα - Νομικά Blogs | Lawspot

ψηφιακή υπογραφή κ.α.[433] Το έγγραφο πρέπει να μπορεί αντικειμενικά, δηλαδή να είναι πρόσφορο να παραπλανήσει άλλον όταν αυτό χρησιμοποιείται για κάποιο γεγονός που μπορεί να έχει έννομες συνέπειες.[434] Ενώ όμως σε αντικειμενικό επίπεδο αρκεί το έγγραφο να μπορεί να δημιουργήσει πλάνη σχετικά με οποιοδήποτε γεγονός το οποίο ενδέχεται να έχει έννομες συνέπειες, σε υποκειμενικό επίπεδο πρέπει να αποδεικνύεται ότι ο δράστης απέβλεπε στην επιτυχή παραπλάνηση άλλου μέσω της πλαστότητας και την επίτευξη μέσω αυτής συγκεκριμένων έννομων συνεπειών. Αν επομένως οι ίδιες έννομες συνέπειες θα επέρχονταν ούτως ή άλλως με τον ίδιο ακριβώς τρόπο, ακόμη και χωρίς το πλαστό μέρος του εγγράφου, το έγκλημα της πλαστογραφίας δεν τελείται.[435]

Η νόθευση διαφέρει από την κατάρτιση πλαστού αφού στη νόθευση απαιτείται υλική επέμβαση σε ήδη υπάρχον έγγραφο, του οποίου μεταβάλλεται το περιεχόμενο σε ορισμένα σημεία[436], ενώ κατάρτιση πλαστού συμβαίνει όταν εξαρχής δημιουργείται έγγραφο, το οποίο προέρχεται από τρίτο πρόσωπο.[437] Νόθευση εγγράφου συνιστά η αλλοίωση της έννοιας ενός εγγράφου που έχει ήδη καταρτιστεί, όταν μεταβάλλεται το περιεχόμενό του, το οποίο μπορεί να γίνει με προσθήκη ή εξάλειψη ή και με τους δύο τρόπους, αλλά και όταν περιορίζεται το περιεχόμενο με αποτέλεσμα τη μεταβολή της αποδεικτικής του ισχύς.[438] Για να υπάρχει νόθευση εγγράφου θα πρέπει η μεταβολή της έννοιας του να επηρεάζει ή να ματαιώνει το περιεχόμενο της αποδεικτικής του δύναμης και η επελθούσα αλλοίωση του περιεχομένου του να έχει αντικειμενικά έννομες συνέπειες.[439]

Η κατάρτιση πλαστού και η νόθευση εγγράφου (άρθρο 216 παρ. 1 ΠΚ) απαιτεί τουλάχιστον ενδεχόμενο δόλο ως προς όλα τα στοιχεία της αντικειμενικής υπόστασης και επιπλέον σκοπό του δράστη να παραπλανήσει άλλον σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες και να θέλει την κατάρτιση ή τη νόθευσή του. Επειδή η πλαστογραφία είναι έγκλημα υπερχειλούς υποκειμενικής υπόστασης (ή σκοπού), εκείνος που καταρτίζει πλαστό ή νοθεύει έγγραφο πρέπει να έχει σκοπό την παραπλάνηση άλλου μέσω της χρήσης του πλαστού ή νοθευμένου εγγράφου. Ο σκοπός της παραπλάνησης δεν είναι απαραίτητο να κατευθύνεται σε παραπλάνηση εκείνου ενώπιον του οποίου γίνεται η χρήση του εγγράφου, αλλά μπορεί να κατευθύνεται σε παραπλάνηση τρίτου, ακόμη και μη προκαθορισμένου προσώπου. Δεν απαιτείται επομένως ταυτότητα του

[433] ΑΠ 367/2019 ΝΟΜΟΣ, ΑΠ 697/2017 ΝΟΜΟΣ, Παύλου, Υπερ 1991, 301, Ανδρουλάκης, 785, ΑΠ 471/2017 ΝΟΜΟΣ
[434] ΑΠ Ολ 1/2018 Ποινχρ 2018,514, ΑΠ 1150/2019 ΝΟΜΟΣ, ΑΠ 163/2019 ΝΟΜΟΣ, ΑΠ 584/2015 ΝΟΜΟΣ, InLaw.gr
[435] Συμεωνίδου-Καστανίδου, Παρατ. στην αντίθ. ΔΙατΕισΕφθεσ 305/2005, ΠοινΔικ 2006, 1000
[436] ΑΠ 1113/2009 ΠοινΔικ 2010, 283, ΑΠ 1536/2008 ΠοινΧρ 2009, 545, ΣυμβΑΠ 1393/2008 ΠοινΧρ 2009, 523, ΑΠ 415/2007 ΠοινΧρ 2008, 66, ΣυμβΑΠ 759/1999 ΠοινΧρ 2000, 324
[437] ΑΠ 217/2003 ΠοινΧρ 2003, 929
[438] ΑΠ 902/2017 ΠοινΧρ 2019, 124, ΑΠ 729/2017 ΝΟΜΟΣ, ΣυμβΑΠ 35/2008 ΠοινΧρ 2008, 834 κ.α.
[439] ΑΠ 445/1992 ΠοινΧρ 1992, 541, ΑΠ 1072/1988 ΠονΧρ 1989, 985

προσώπου ενώπιον του οποίου κατά τον σκοπό του δράστη πρόκειται να χρησιμοποιηθεί το πλαστό ή νοθευμένο έγγραφο με το πρόσωπο εκείνου που σκοπείται να παραπλανηθεί.[440]

Από την άλλη, δράστης του εγκλήματος εδώ μπορεί να είναι οποιοσδήποτε. Αντικειμενικά, είναι απαιτητή η χρησιμοποίηση του πλαστού ή νοθευμένου εγγράφου, που σκοπεί την παραπλάνηση άλλου για γεγονός που έχει έννομες συνέπειες. Κατά πάγια νομολογία, η χρήση του πλαστού ή νοθευμένου εγγράφου στοιχειοθετείται αντικειμενικά όταν ο δράστης καταστήσει προσιτό το έγγραφο αυτό στον μέλλοντα να παραπλανηθεί από το περιεχόμενό του τρίτο, μεταφέροντας το έγγραφο στον κύκλο της κυριαρχίας του τρίτου και δίνοντάς του τη δυνατότητα να μάθει το περιεχόμενο, χωρίς να είναι απαραίτητο να λάβει πραγματική γνώση ή ακόμα και να παραπλανηθεί.[441] Χρήση πλαστού ή νοθευμένου εγγράφου υπάρχει όταν χρησιμοποιηθεί το έγγραφο κατά οποιονδήποτε τρόπο, άμεσα ή έμμεσα, με άλλο πρόσωπο, το οποίο τελεί σε καλή πίστη ως προς την πλαστότητα του εγγράφου[442] ή από παρένθετο πρόσωπο που αγνοεί την πλαστότητα.

Στην υποκειμενική υπόσταση απαιτείται δόλος που συνίσταται στην ενέργεια του δράστη και στη γνώση του ότι το έγγραφο που χρησιμοποιεί είναι πλαστό ή νοθευμένο. Επιπλέον, απαιτείται και σκοπός του υπαιτίου να παραπλανήσει με τη χρήση του εγγράφου αυτού άλλον για γεγονός που μπορεί να έχει έννομες συνέπειες, οι οποίες αναφέρονται στη δημιουργία, κατάργηση ή μεταβίβαση δικαιώματος προστατευόμενου από τον νόμο, άσχετα από το αν επι ή παραπλάνηση.[443] Το έγκλημα της χρήσης πλαστού ή νοθευμένου εγγράφου προϋποθέτει ότι ο δράστης γνωρίζει πλήρως ότι το έγγραφο που χρησιμοποιεί είναι πλαστό ή νοθευμένο, χωρίς να απαιτείται να γνωρίζει το πρόσωπο του πλαστογράφου, το οποίο μπορεί να του είναι και άγνωστο.[444]

Η χρήση πλαστού ή νοθευμένου εγγράφου προσλαμβάνει κακουργηματικό χαρακτήρα όταν, επιπλέον της γνώσης της πλαστότητας του εγγράφου και του σκοπού παραπλάνησης άλλου σχετικά με γεγονός που μπορεί να έχει έννομες συνέπειες, ο δράστης είτε α) σκοπεύει με τη χρήση να προσπορίσει στον εαυτό του ή άλλον, με βλάβη τρίτου, παράνομο περιουσιακό όφελος ή να βλάψει άλλον, εφόσον το όφελος ή η βλάβη που επιδιώχθηκε υπερβαίνει το ποσό των 120.000 ευρώ, χωρίς να ενδιαφέρει αν επιτεύχθηκε ή όχι η εξαπάτηση και το περιουσιακό όφελος ή βλάβη του άλλου. Για τη στοιχειοθέτηση της κακουργηματικής πλαστογραφίας απαιτείται καταρχήν να

[440] ΑΠ 729/2017 ΝΟΜΟΙ ΑΠ 317/2015 ΠοινΔικ 2016, 282, Μαγκάκης, 346
[441] ΑΠ 228/2019 ΝΟΜΟΣ, ΑΠ 1125/2017 ΝΟΜΟΣ, ΑΠ 902/2017 ΠοινΧρ 2019, 124 κλπ
[442] ΑΠ 1150/2019 ΝΟΜΟΣ, ΑΠ 819/2019 ΝΟΜΟΣ, ΑΠ 1051/2017 ΝΟΜΟΣ, ΑΠ 420/2018 ποινχρ 2019, 193
[443] ΑΠ 1098/2017 ποινχρ 2018, 387, ΑΠ 1051/2017 ΝΟΜΟΣ, ΑΠ 729/2017 ΝΟΜΟΣ, ΑΠ 471/2017 ΝΟΜΟΣ, ΑΠ 313/2017 ΝΟΜΟΣ, ΑΠ 1774/2008 ποινχρ 2009, 712, ΑΠ 1491/2006 ποινχρ 2007, 640, ΑΠ 2132/2005 ποινχρ 2006, 597
[444] ΑΠ 652/2013 ΠοινΧρ 2014, 113, ΑΠ 1034/2007 ΠοινΧρ 2007, 694, ΑΠ 1445/1984 ΠοινΧρ 1985, 457, ΑΠ 1051/2017 ΝΟΜΟΣ

συντρέχουν όλα τα στοιχεία της παραγράφου 1 ή 2 του άρθρου 216 ΠΚ και επιπλέον απαιτείται σκοπός του δράστη να προσπορίσει από την πράξη του περιουσιακό όφελος με ταυτόχρονη τη βλάβη τρίτου και το συνολικό όφελος ή αντίστοιχα η συνολική ζημία να ξεπερνούν τις 120.000€.

Για να θεμελιωθεί κακούργημα του άρθρου 216 παρ. 3 ΠΚ αντικειμενικά είναι απαιτητό να καταρτίζεται εξαρχής πλαστό έγγραφο ή να νοθεύεται αυτό. Για την πλήρωση της υποκειμενικής υπόστασης χρειάζεται δόλος του δράστη, που προκύπτει από τη γνώση και τη θέληση του δράστη να πράξει και σκοπός του με τη χρήση του πλαστού εγγράφου να παραπλανήσει άλλον για γεγονός που μπορεί να έχει έννομες συνέπειες. Πρέπει, επιπροσθέτως, ο δράστης να επιδιώκει να κερδίσει ή ο ίδιος ή κάποιος άλλος περιουσιακό όφελος βλάπτοντας τρίτον, εφόσον το συνολικό όφελος ή η συνολική ζημία ξεπερνούν τις 120.000 ευρώ.[445]

Ως περιουσιακό όφελος νοείται κάθε καλυτέρευση της περιουσιακής κατάστασης του δράστη ή άλλου υπέρ του οποίου πράττει, η οποία συντελείται με την αύξηση της περιουσίας του ωφελούμενου ή προσπόριση άλλων ωφελημάτων οικονομικού χαρακτήρα ή με την αποφυγή της μείωσης της περιουσίας του με βλάβη άλλου, η οποία αρκεί και μόνη για τη θεμελίωση της πλαστογραφίας σε βαθμό κακουργήματος, αν το όφελος ή η βλάβη υπερβαίνουν το ποσό των 120.000 ευρώ.[446] Για τη στοιχειοθέτηση της κακουργηματικής πλαστογραφίας, απαιτείται το σκοπούμενο περιουσιακό όφελος να επιδιώκεται να πραγματωθεί από τον υπαίτιο «βλάπτοντας» τρίτον, δηλαδή με βλάβη τρίτου. Το περιουσιακό όφελος θα πρέπει να προέρχεται από εκείνον που υφίσταται τη βλάβη, απαιτείται δηλαδή στην κακουργηματική πλαστογραφία ένα είδος υλικής αντιστοιχίας μεταξύ προκληθείσης βλάβης και επιδιωχθέντος οφέλους, όπως στην απάτη.[447]

Τέλος, κατά την παράγραφο 4 του αρ. 216 ΠΚ, η πλαστογραφία και η χρήση πλαστού, που στρέφεται άμεσα κατά του ελληνικού δημοσίου, των ΟΤΑ και των ΝΠΔΔ, εφόσον το συνολικό επιδιωκόμενο περιουσιακό όφελος ή η συνολική ζημία υπερβαίνει συνολικά τις 120.000 ευρώ τιμωρείται με κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες. Για να εφαρμοστεί το άρθρο 216 παρ. 4 ΠΚ, πρέπει να συντρέχουν όλα τα αντικειμενικά και υποκειμενικά στοιχεία των εγκλημάτων της παρ. 1 ή 2. [448]

Άξιο αναφοράς είναι και το άρθρο 217 ΠΚ σύμφωνα με το οποίο *«1. Όποιος με σκοπό να διευκολύνει την άμεση συντήρηση, την κίνηση ή την κοινωνική πρόοδο αυτού του ίδιου ή άλλου*

[445] ΣυμβΑΠ 701/2009 ποινχρ 2010, 186, ΣυμβΑΠ 2247/2008 ποινχρ 2009, 128, ΑΠ 1816/2003 ΠΟΙνΔικ 2004, 515, ΣυμβΑΠ 1131/2002 ποινχρ 2003, 401, ΣυμβΑΠ 184/2002 ποινχρ 2002, 898
[446] ΑΠ Ολ 3/2008 ΠοινΧρ 2008, 404, ΑΠ 573/2019 ΝΟΜΟΣ, ΑΠ 420/2018 193, ΑΠ 232/2017 ΝΟΜΟΣ, ΣυμβΑΠ 195/2007 ποινχρ 2007, 1006, ΣυμβΑΠ 3648/2003 ποινΧρ 2004, 64, ΣυμβΑΠ 1855/2001 ΠΛΟΥ 2001, 2073, ΣυμβΑΠ 725/2000 ποινχρ 2001, 59, ΣυμβΑΠ 1389/1997 ΠοινΧρ 1998, 480, ΣυμβΠλημθεσ 1195/2016 ΠοινΔικ 2017, 290, ΣυμβΠλημΑθ 774/2007 2008, 751
[447] Παπαδαμάκης, 75, Μυλωνόπουλος, Υπομνήματα, 100-101, ΣυμβΠλημΑθ 774/2007 ΠοινΔικ 2008, 705 = ΠοινΧρ 2008, 751
[448] www.lawspot.gr

*καταρτίζει πλαστό ή νοθεύει πιστοποιητικό ή μαρτυρικό ή άλλο έγγραφο που κατά προορισμό χρησιμεύει για τέτοιους σκοπούς ή εν γνώσει του χρησιμοποιεί τέτοιο πλαστό ή νοθευμένο έγγραφο τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας. 2. Με την ίδια ποινή τιμωρείται όποιος χρησιμοποιεί για τον ίδιο σκοπό τέτοιο έγγραφο, που είναι γνήσιο, είχε εκδοθεί όμως για άλλον. 3. Με φυλάκιση τιμωρείται όποιος καταρτίζει πλαστό ή νοθεύει πτυχίο ή κάθε πιστοποιητικό γνώσεων ή δεξιοτήτων, ή νοθεύει γνήσιο ή κάνει χρήση αυτών, με σκοπό να καταλάβει θέση εργασίας ή να διεκδικήσει βαθμολογική ή μισθολογική προαγωγή στον δημόσιο ή τον ιδιωτικό τομέα.»*[449]

Στο άρθρο αυτό, προστατευόμενο έννομο αγαθό είναι η ασφάλεια των συναλλαγών που πετυχαίνεται με την ασφάλεια της γνησιότητας των πιστοποιητικών και μαρτυρικών. Στο άρθρο 217 ΠΚ τυποποιούνται οι ακόλουθες αξιόποινες πράξεις: Α. Η πλαστογραφία ή η χρήση πλαστού ή η νόθευση πιστοποιητικού κ.λπ. (άρθρο 217 παρ. 1 ΠΚ), Β. η χρήση γνήσιου πιστοποιητικού ή μαρτυρικού τρίτου προσώπου (άρθρο 217 παρ. 2 ΠΚ) και Γ. η πλαστογραφία ή χρήση πλαστού ή νοθευμένου πτυχίου κ.λπ (άρθρο 217 παρ. 3 ΠΚ).

Στην παράγραφο 1 δράστης του εγκλήματος μπορεί να είναι οποιοσδήποτε. Υλικό αντικείμενο του εγκλήματος είναι πιστοποιητικό ή μαρτυρικό ή άλλο έγγραφο που μπορεί να διευκολύνει την άμεση συντήρηση, την κίνηση ή την κοινωνική πρόοδο του ίδιου του δράστη ή άλλου.[450] Τα πιστοποιητικά και τα μαρτυρικά υπάγονται στη γενική έννοια του εγγράφου του άρθρου 13 στοιχ. γ' ΠΚ. Για την πλήρωση της υποκειμενικής υπόστασης της κατάρτισης πλαστού πιστοποιητικού ή νόθευσης γνησίου απαιτείται δόλος, που περιλαμβάνει τη γνώση και τη θέληση των πραγματικών περιστατικών και σκοπός του δράστη προς διευκόλυνση την άμεση συντήρηση, την κίνηση ή την κοινωνική πρόοδο αυτού ή άλλου κάνοντας χρήση του πλαστού ή νοθευμένου πιστοποιητικού ή μαρτυρικού. Κίνηση είναι η μετάβαση από τόπο σε τόπο, άμεση συντήρηση είναι η εξεύρεση πόρων και κοινωνική πρόοδος είναι η επαγγελματική ή κοινωνική ένταξη ή εξέλιξη προς το καλύτερο.[451], [452]

Παρατηρούμε ότι και μόνο από τις λέξεις πλαστογραφία και deepfake υπάρχει το κοινό συνθετικό πλαστό = fake = ψεύτικο. Τα deepfakes μπορούν να αποτελέσουν αντικείμενο πλαστογραφίας με σκοπό να εξαπατήσουν τον αποδέκτη τους προκειμένου ο δράστης να επωφεληθεί είτε οικονομικά, είτε να μπορέσει να μετακινηθεί, είτε να προσληφθεί σε κάποια θέση.

[449] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/, https://www.lawspot.gr/
[450] Βλ. Βάση Δεδομένων ΝΟΜΟΣ, https://lawdb.intrasoftnet.com/, https://www.lawspot.gr/
[451] Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη σελ. 1428-1430
[452] https://efotopoulou.gr/plastografia-pistopiitikon-ke-martirikon-217-pk/

Τα διαβατήρια γίνονται όλο και πιο δύσκολα πλαστά με τα σύγχρονα μέτρα πρόληψης της απάτης. Τα συνθετικά μέσα και οι ψηφιακά επεξεργασμένες εικόνες προσώπου αποτελούν μια νέα προσέγγιση για την πλαστογραφία εγγράφων. Χρησιμοποιώντας διάφορες μεθόδους και εργαλεία, είναι δυνατόν να συνδυαστούν, ή να μορφοποιηθούν, τα πρόσωπα του ατόμου στο οποίο ανήκει στην πραγματικότητα το διαβατήριο και του ατόμου ή των ατόμων που θέλουν να αποκτήσουν παράνομα διαβατήριο. Η μέθοδος αυτή μπορεί να αυξήσει την πιθανότητα η φωτογραφία σε ένα πλαστό έγγραφο να περάσει από οποιονδήποτε έλεγχο ταυτότητας, συμπεριλαμβανομένων εκείνων που χρησιμοποιούν αυτοματοποιημένα μέσα (συστήματα αναγνώρισης προσώπου). Αυτό το είδος της προσέγγισης της πλαστογραφίας και απάτης μαζί μπορεί να εφαρμοστεί σε κάθε άλλο τύπο ψηφιακού ελέγχου ταυτότητας που απαιτεί οπτικό έλεγχο ταυτότητας. Υπονομεύει σε μεγάλο βαθμό τις διαδικασίες επαλήθευσης ταυτότητας, καθώς δεν υπάρχει αξιόπιστος τρόπος εντοπισμού αυτού του είδους της επίθεσης. Η πλαστογραφία με έγγραφα διευκολύνει άλλα εγκλήματα, όπως η παράνομη μετανάστευση, η εμπορία ανθρώπων, η πώληση διαφόρων παράνομων αγαθών και η τρομοκρατία, καθώς οι δράστες χρησιμοποιούν συχνά πλαστές ταυτότητες για να ταξιδέψουν στις τοποθεσίες προορισμού τους. Η τεχνολογία Deepfake ενδέχεται να ενισχύσει τον κίνδυνο προηγμένης πλαστογραφίας εγγράφων από ομάδες οργανωμένου εγκλήματος.[453]

## Δ. ΤΑ DEEPFAKES ΩΣ ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ ΣΤΗ ΔΙΚΑΣΤΗΡΙΑΚΗ ΠΡΑΚΤΙΚΗ

Ένας τελευταίος κίνδυνος σε σχέση με τα Deepfakes αποτελεί η χρήση τους ως αποδεικτικό μέσο με σκοπό την αλλοίωση απόδειξης. Εύλογα γεννάται το ερώτημα κατά πόσο είναι πλέον πειστικά ως αποδεικτικά στοιχεία οπτικοακουστικά μέσα, την στιγμή που είναι δυνατή τόσο εύκολα η αλλοίωση τους. Μια τέτοια δραστηριότητα χαρακτηρίζεται ως πλαστογραφία (νόθευση) και απάτη στο δικαστήριο.[454]

Όταν ο δράστης, σε οποιαδήποτε δίκη, στο πλαίσιο της οποίας ο δικαστής οφείλει να ελέγξει την ουσιαστική βασιμότητα των ισχυρισμών των διαδίκων, με την προβολή ψευδούς ισχυρισμού και την εν γνώσει του προσκόμιση ψευδών αποδεικτικών μέσων λ.χ. πλαστών εγγράφων ή γνήσιων μεν αλλά με αναληθές περιεχόμενο ή καταθέσεων ψευδομαρτύρων, πετυχαίνει να παραπλανήσει το δικαστήριο και αυτό να εκδώσει οριστική απόφαση, η οποία επιφέρει βλάβη της περιουσίας του αντιδίκου του δράστη ή τρίτου τελεί το αδίκημα της απάτης σε δικαστήριο.[455]

---

[453] Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu

[454] Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

[455] βλ. ενδ. ΑΠ 568/2020 ΤΝΠ QUALEX, ΣυμβΑΠ 1306/2019 ΤΝΠ QUALEX, ΑΠ 735/2017 ΠοινΧρ 2018, 751, ΑΠ 816/2015 ΠοινΧρ 2016, 518, ΑΠ 1019/2014 ΠοινΧρ 2015, 674 κ.α.

Σύμφωνα με το άρθρο 177 του Κώδικα Ποινικής Δικονομίας προβλέπεται η αρχής της ηθικής απόδειξης, σύμφωνα με την οποία οι δικαστές πρέπει να αποφασίζουν «σύμφωνα με την πεποίθησή τους, ακολουθώντας τη συνείδησή τους και να οδηγούνται από την απροσωπόληπτη κρίση που είναι αποτέλεσμα συζητήσεων και αφορούν στην αλήθεια των πραγματικών γεγονότων, την αξιοπιστία των μαρτύρων και την αξία των άλλων αποδείξεων».

Σήμερα, τα μέσα κοινωνικής δικτύωσης διαδραματίζουν ενεργό ρόλο στη διεξαγωγή μιας έρευνας. Πολλοί αστυνομικοί μπορούν εύκολα να βρουν ένα ένοχο άτομο από μια φωτογραφία που μπορεί να βρεθεί στους λογαριασμούς του στα μέσα κοινωνικής δικτύωσης. Εάν ένας τρομοκράτης δημοσιεύσει ένα βίντεο στο YouTube που εκφράζει τον τρόπο με τον οποίο διαπράττει ένα έγκλημα, οι ερευνητές μπορούν εύκολα να βρουν την ταυτότητά του. Επιπλέον, λόγω των εξελίξεων στην τεχνολογία, τα μέσα κοινωνικής δικτύωσης χρησιμοποιούνται σήμερα ως πρόσθετα αποδεικτικά στοιχεία στο δικαστήριο για τη δημιουργία υποστηρικτικών άλλοθι και την παροχή σημαντικών πληροφοριών που αφορούν τις δικαστικές υποθέσεις. Η συλλογή κοινωνικών δεδομένων διαδραματίζει ολοένα και πιο πολύτιμο ρόλο στη διαδικασία συλλογής αποδεικτικών στοιχείων. Αλλά πόσο αξιόπιστες είναι αυτές οι θεμελιωμένες εικόνες και βίντεο; Τι γίνεται αν κάποιος ανταλλάξει το πρόσωπο ενός ατόμου με άλλα σε αυτές τις εικόνες ή τα βίντεο;[456]

Ως ψηφιακά πειστήρια νοούνται τα δεδομένα (ευρήματα) που είναι σε ψηφιακή μορφή, των οποίων ο εντοπισμός, η εξαγωγή και η ερμηνεία συμβαίνει κατά τη διαδικασία ψηφιακής σήμανσης (digital forensics). Χρησιμοποιούνται δε επιστημονικά αποδεκτές μεθόδους, με σκοπό τα δεδομένα αυτά να γίνουν χρήσιμα στη δικονομική πρακτική. Λόγω της ψηφιακής τους μορφής τα δεδομένα είναι εξαιρετικά εύθραυστα και τούτο οφείλεται στον τρόπο με τον οποίο αποθηκεύονται, επεξεργάζονται και αποθηκεύονται.[457]

Η δικαστική αίθουσα είναι ένας μικρόκοσμος της κοινωνίας γενικά.[458] Λόγω της χειραγώγησης εικόνας, ήχου και βίντεο, πρέπει να ληφθεί σοβαρά υπόψη η ευπάθεια των ψηφιακών δεδομένων, αφού ως γνωστόν πλέον οι παραποιημένες εικόνες, ο ήχος και τα βίντεο θα μπορούσαν να παρουσιαστούν ως ψευδή στοιχεία και να οδηγήσουν σε άδικες καταδίκες. Τα δεδομένα μπορούν

[456] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792

[457] Ψηφιακά Πειστήρια, Βασίλης Κάτος, Bournemouth University, UK, σε Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Συγγραφείς: Γκύζης Δ., Δαγκλής Ν., Δαλακούρας Θ., Δανιήλ Γ., Κιούπης Δ., Ναζίρης Γ., Νούσκαλης Γ., Παπαθανασίου Α., Νάιντος Χ., Καργόπουλος Α.-Ι., Κάτος Β., Κουδελή Μ., Μοροζίνης Ι., Σαββίδης Ν. Έκδοση: Νομική Βιβλιοθήκη, 2η 2023, σελ. 64-65

[458] Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140

να γίνουν λανθασμένα δεκτά ως αποδεικτικά στοιχεία, γι' αυτό απαιτούνται επιβεβαιωτικά στοιχεία για να αποδειχθεί ότι τα ψηφιακά δεδομένα δεν έχουν παραποιηθεί.[459]

Οι εικόνες, οι ήχοι και τα βίντεο πρέπει να πιστοποιούνται πριν παρουσιαστούν ως αποδεικτικά στοιχεία σε ένα δικαστήριο- ωστόσο, η μέθοδος αυτή δυσχεραίνεται από την παρουσία των Generative Adversarial Networks. Οι δικαστικές αίθουσες έχουν επίσης επηρεαστεί από αυτές τις εξελίξεις στη συλλογή και το χειρισμό των αποδεικτικών στοιχείων. Τα ψηφιακά αποδεικτικά στοιχεία περιλαμβάνουν, μεταξύ άλλων, μηνύματα ηλεκτρονικού ταχυδρομείου, φωτογραφίες, βίντεο, κείμενα, αναρτήσεις στο Facebook, πληροφορίες που προέρχονται από ιστότοπους κ.λπ. Σύντομα θα είναι μεγάλο εμπόδιο για τα δικαστήρια να διακρίνουν τα γνήσια αποδεικτικά στοιχεία από τις βαθιές απομιμήσεις, καθώς τα προγράμματα λογισμικού και το εκπαιδευτικό υλικό για την κατασκευή βαθιών απομιμήσεων συνεχίζουν να βελτιώνονται με αυτόν τον ρυθμό.[460]

Ως αναπόφευκτη συνέπεια της ευρείας χρήσης της τεχνολογίας, δεν είναι δύσκολο να προβλέψουμε ότι στο εγγύς μέλλον θα δούμε περισσότερα deepfakes στις αίθουσες των δικαστηρίων.[461] Τα deepfakes μπορούν να προκύψουν στο πλαίσιο της αποδεικτικής διαδικασίας με διάφορους τρόπους. Ένας διάδικος μπορεί να κατασκευάσει ένα βίντεο ειδικά για τους σκοπούς της δίκης, προκειμένου να προσπαθήσει να επικρατήσει. Ή ένας διάδικος μπορεί να συναντήσει ένα deepfake βίντεο που έχει φτιάξει κάποιος άλλος και να επιθυμεί να το εισαγάγει ως αποδεικτικό στοιχείο, χωρίς να αντιλαμβάνεται ότι είναι ψεύτικο. Ψεύτικα βίντεο μπορεί να καταλήξουν (είτε τυχαία είτε κακόβουλα) σε αρχεία που ιστορικά θεωρούνται αξιόπιστα, όπως αυτά των ειδησεογραφικών πρακτορείων. Εάν η παρουσία τους δεν γίνει αντιληπτή από τον θεματοφύλακα των αρχείων αυτών, υπάρχει ο κίνδυνος ο θεματοφύλακας να εγγυηθεί άθελά του για ένα ψεύτικο έγγραφο όταν κληθεί να επικυρώσει αποδεικτικά στοιχεία σε μια δικαστική διαδικασία.

Σε μια πρόσφατη υπόθεση επιμέλειας παιδιού στο Ηνωμένο Βασίλειο, η μητέρα του παιδιού είχε εισαγάγει ένα παραποιημένο αρχείο ήχου στα αποδεικτικά στοιχεία. Για να στηρίξει τον ισχυρισμό της ότι ο πατέρας ήταν πολύ βίαιος για να του επιτραπεί η πρόσβαση στα παιδιά τους, είχε "χρησιμοποιήσει λογισμικό και διαδικτυακά σεμινάρια για να φτιάξει ένα αληθοφανές αρχείο ήχου", το οποίο ακουγόταν σαν ηχογράφηση του πατέρα που την απειλούσε σε ένα τηλεφώνημα. Μετά από εξέταση από εμπειρογνώμονα, διαπιστώθηκε ότι η ηχογράφηση είχε παραποιηθεί για να συμπεριλάβει λέξεις που δεν χρησιμοποιήθηκαν από τον πατέρα. Η ίδια η μητέρα

[459] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
[460] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
[461] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792

χρησιμοποίησε ένα πρόγραμμα λογισμικού και διαδικτυακά σεμινάρια για να συνθέσει ένα αληθοφανές αρχείο ήχου. Η υπόθεση αποτελεί ένα καλό παράδειγμα για το τι είδους προβλήματα περιμένουν τα δικαστήρια. Όπως καταδεικνύει η υπόθεση, δεν χρειάζεται να είναι κανείς ειδικός για να χειριστεί ψηφιακά αποδεικτικά στοιχεία, διότι ακόμη και ένας απλός άνθρωπος μπορεί να δημιουργήσει DeepFakes παρακολουθώντας μερικά σεμινάρια ή χρησιμοποιώντας έτοιμα προγράμματα.[462],[463]

Για να διασφαλιστεί τουλάχιστον κάποια βασική πιθανότητα ότι ένα αποδεικτικό στοιχείο "είναι αυτό που ισχυρίζεται ότι είναι", τα δικαστήρια έχουν από καιρό επιβάλει απαιτήσεις επικύρωσης των στοιχείων αυτών, είτε πρόκειται για χειρόγραφα ή δακτυλογραφημένα έγγραφα, κινηματογραφικές ή ψηφιακές φωτογραφίες, ταινίες, βιντεοκασέτες ή ψηφιακά βίντεο. Εάν ένα έγγραφο δεν μπορεί να επικυρωθεί ικανοποιητικά από τον εισηγητή του, δεν θα γίνεται δεκτό ως αποδεικτικό στοιχείο.[464]

Τα δικαστήρια αντιμετωπίζουν την επικύρωση βίντεο όπως αντιμετωπίζουν τις φωτογραφίες. Και τα δύο "συνήθως πιστοποιούνται με το να αποδεικνύεται ότι αποτελούν δίκαιη και ακριβή αναπαράσταση της απεικονιζόμενης σκηνής". Ο ρόλος του μάρτυρα είναι καθοριστικός αφού μπορεί -αλλά δεν είναι απαραίτητο- να είναι το πρόσωπο που τράβηξε τη φωτογραφία ή το βίντεο, μπορεί επίσης να είναι κάποιος που είδε το γεγονός που καταγράφεται ή που με άλλο τρόπο "είναι σε θέση να δώσει κάποια ένδειξη για το πότε, πού και υπό ποιες συνθήκες τραβήχτηκε το βίντεο και ότι αυτό απεικονίζει με ακρίβεια το θέμα που απεικονίζεται.[465]

Ως αποτελεσματικότερη λύση, τα δικαστήρια μπορούν να χρησιμοποιήσουν πιο εξελιγμένα εργαλεία που χρησιμοποιούν τεχνητή νοημοσύνη (AI) για να εντοπίζουν τα χειραγωγημένα αποδεικτικά στοιχεία, τα λεγόμενα DeepFakes, από τα γνήσια αποδεικτικά στοιχεία.[466] Με την ανάπτυξη συστημάτων εντοπισμού πλαστογραφιών με τεχνητή νοημοσύνη, οι εμπειρογνώμονες ψηφιακής εγκληματολογίας είναι έτοιμοι να διαδραματίσουν σημαντικό ρόλο στις δικαστικές μάχες για την αυθεντικοποίηση υποτιθέμενων πλαστογραφιών.[467] Κατά συνέπεια, η σημασία της ψηφιακής εγκληματολογίας και των εργαλείων τεχνητής νοημοσύνης για την ανίχνευση

[462] Patrick Ryan, 'Deepfake' Audio Evidence Used in UK Court to Discredit Dubai Dad, THE NATIONAL (Feb. 8, 2020), https://www.thenational.ae/uae/courts/deepfake-audio-evidenceused-in-uk-court-to-discredit-dubai-dad-1.97576
[463] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
[464] Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140
[465] Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140
[466] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
[467] Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140

απομιμήσεων από γνήσια αποδεικτικά στοιχεία έχει γίνει πιο σημαντική από ποτέ. Τα δικαστήρια πρέπει να χρησιμοποιήσουν την ΤΝ εναντίον της ΤΝ για να επιτύχουν καλύτερα αποτελέσματα όσον αφορά την αυθεντικοποίηση των αποδεικτικών στοιχείων. Μπορεί να χρειαστεί χρόνος για να γίνουν αποδεκτά από τα δικαστήρια τα εργαλεία πιστοποίησης βίντεο που κυκλοφορούν τώρα στην αγορά ή οι τεχνικές ανίχνευσης ψεύτικων βίντεο που αναπτύσσονται σε ακαδημαϊκά και εταιρικά ερευνητικά εργαστήρια ως βάση για την κατάθεση εμπειρογνωμόνων. [468]

Τα deepfakes θα κάνουν σύντομα τη δουλειά των δικηγόρων και των δικαστών πιο δύσκολη. Θα περιπλέξουν τις συνήθεις διαδικασίες δίκης και μπορεί να δώσουν στα δικαστήρια λόγο να επανεξετάσουν τη συνεχιζόμενη επάρκεια των υφιστάμενων κανόνων και προτύπων που διέπουν τα ψηφιακά αποδεικτικά στοιχεία. Οι δικηγόροι θα πρέπει να επιδεικνύουν μεγαλύτερη επιμέλεια στην επαλήθευση της γνησιότητας των αποδεικτικών στοιχείων βίντεο. Η πιστοποίηση της γνησιότητας των βίντεο κατά των υποψιών για βαθιά πλαστογραφία θα παρατείνει τη δικαστική διαμάχη και θα αυξήσει το κόστος μέσω της πρόσθετης επιμέλειας για την επαλήθευση της γνησιότητας εγγράφων (καθυστερώντας ή παρατείνοντας έτσι τη δίκη), των αυξημένων δαπανών για λαϊκούς και εμπειρογνώμονες μάρτυρες. Καθώς η τεχνολογία deepfake βελτιώνεται και γίνεται όλο και πιο δύσκολο να ξεχωρίσει κανείς τι είναι αληθινό, τα αποδεικτικά βίντεο μπορεί να χάσουν τη συνήθη αξιοπιστία τους.[469]

## IV. ΕΠΙΛΟΓΟΣ - ΣΥΜΠΕΡΑΣΜΑ

Η τεχνολογία στις μέρες μας έχει καταφέρει να δημιουργήσει μια νέα πραγματικότητα. Οι ζωές μας και η καθημερινότητα μας περιστρέφεται μόνο γύρω από την τεχνολογία και τις δυνατότητες που αυτή μας παρέχει. Χωρίς αυτήν, τις ηλεκτρονικές συσκευές, το ίντερνετ, το διαδίκτυο των πραγμάτων, τις έξυπνες συσκευές και όλες τις εφαρμογές και υπηρεσίες που μας παρέχονται δεν νομίζω ότι μπορούμε να φανταστούμε τη ζωή μας. Αδιαμφισβήτητα η ζυγαριά της τεχνολογίας γέρνει με μεγάλη διαφορά προς τις θετικές επιπτώσεις που την χαρακτηρίζουν, αφού τα οφέλη είναι πολλά για όλους τους τομείς της καθημερινής ζωής.

Ωστόσο, τα τεχνολογικά επιτεύγματα και οι νέες τεχνολογίες, και ειδικά ο τρόπος και η ταχύτητα με τα οποία εξαπλώνονται μπορεί να προκαλέσει μεγάλες αναταραχές και ανησυχίες στην κοινωνία. Πολύ εύκολα μια τεχνολογία, όπως αυτή των deepfakes, μπορεί να αναπτυχθεί ραγδαία και με τα μέσα και τα εργαλεία που μας παρέχει σήμερα η τεχνητή νοημοσύνη να βελτιώνεται συνεχώς. Στην αρχή τις περισσότερες φορές μια τεχνολογία δημιουργείται με καλό σκοπό για να παρέχει οφέλη στην κοινωνία, τι συμβαίνει όμως όταν βρεθεί κάποιος κακόβουλος χρήστης και

[468] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
[469] A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792

χρησιμοποιήσει αυτή την τεχνολογία για να προκαλέσει βλάβη σε άλλον; Γιατί ως γνωστόν στην αρχή επικρατεί ο ενθουσιασμός για κάτι καινούργιο και συναρπαστικό που θα αλλάξει τις ζωές μας, όμως πόσο εύκολα αυτός ο ενθουσιασμός μπορεί να δώσει τη θέση του στο φόβο και στην ανησυχία, αφού ότι εξελίσσεται ποτέ δεν έχει μόνο θετικά αποτελέσματα;

Όπως ήδη αναφέρθηκε, τα deepfakes μπορεί να πρωτοεμφανίστηκαν ως όρος πολύ πρόσφατα, το 2017 με τη δημοσίευση του χρήστη στο reddit, η τεχνολογία αυτή όμως δεν είναι καινούργια. Οι περισσότεροι δεν γνώριζαν την ύπαρξή της και πως αυτή λειτουργεί, είτε γιατί ακόμα δεν είχε διαδοθεί - δεν είχε γίνει "viral" - είτε γιατί ακόμα η τεχνολογία και η χρήση της φαινόταν δύσκολη για να αναπαραχθεί. Καθώς πλέον η τεχνολογία αποτελεί ανοιχτό κώδικα και είναι προσβάσιμη σε όλους τους χρήστες του διαδικτύου παγκοσμίως, ο αλγόριθμος των deepfakes μόνο να βελτιώνεται μπορεί, με αποτέλεσμα σε λίγο καιρό να μην μπορούμε να ξεχωρίσουμε το ψεύτικο από το αληθινό.

Πολλοί άνθρωποι ακόμα και στις μέρες μας δέχονται και πιστεύουν με μεγάλη ευκολία ειδήσεις και γεγονότα και ενστερνίζονται απόψεις, χωρίς να διασταυρώνουν την πηγή της είδησης, χωρίς να αναρωτιούνται αν αυτό που βλέπουν, που διαβάζουν ή ακούν είναι αλήθεια. Η δύναμη των social media είναι τεράστια και η παραπληροφόρηση είναι μάστιγα των καιρών μας.

Στην εποχή μας οι περισσότεροι χρήστες του διαδικτύου γνωρίζουν την ύπαρξη των DeepFakes. Οι πλατφόρμες κοινωνικής δικτύωσης κάνουν τα deepfakes πιο προσιτά και συμβάλλουν στη διάδοσή τους παγκοσμίως. Η αντίληψη των ανθρώπων για τα deepfakes μπορεί από τη μια να συμβάλλει στην επαγρύπνησή μας ώστε να μην πιστεύουμε τόσο εύκολα αυτό που βλέπουμε και να επαληθεύουμε την πηγή της ενημέρωσής μας. Από την άλλη όμως τα deepfakes μπορεί να προκαλέσουν μεγάλη αναταραχή και να επιφέρουν αρνητικές συνέπειες σε άτομα ή ομάδες.

Αν και τα deepfakes χρησιμοποιούνται καθημερινά για λόγους αναψυχής και σάτιρας, οι αρνητικές επιδράσεις στην κοινωνία είναι πλείστες και η χρήση των deepfakes μπορεί να επιφέρει τρομακτικά αποτελέσματα. Από όλα όσα αναφέρθηκαν καθίσταται σαφές ότι οι κίνδυνοι της τεχνολογίας deepfake ξεπερνούν πλέον σε φύση και σοβαρότητα τα πιθανά οφέλη. Οι ειδικοί τονίζουν ότι ο εκδημοκρατισμός της τεχνολογίας deepfake μπορεί να οδηγήσει σε πληθώρα ψεύτικων ειδήσεων, παραποιημένων φωτογραφιών και βίντεο που θα είναι σχεδόν αδύνατο να ξεχωρίσει κανείς το γεγονός από τη μυθοπλασία.

Υποστηρίζεται η άποψη ότι η ίδια η τεχνολογία Deepfake είναι ουδέτερη, ότι δηλαδή από μόνη της δεν χαρακτηρίζεται ούτε καλή ούτε κακή, αλλά τη διαφορά τελικά κάνει ο τρόπος που οι άνθρωποι χρησιμοποιούν αυτήν την τεχνολογία. Αυτή η κατανόηση της τεχνολογίας μπορεί να συνοψίζεται στο δόγμα που υιοθετείται στις Ηνωμένες Πολιτείες Αμερικής: τα όπλα δεν σκοτώνουν ανθρώπους, οι άνθρωποι σκοτώνουν ανθρώπους. Από την άλλη, υποστηρίζεται και η

άποψη ότι μια τεχνολογία δεν είναι ποτέ ουδέτερη, καθώς αυτή σχεδιάζεται και αναπτύσσεται πάντα με συγκεκριμένο σκοπό.

Όταν μια τεχνολογία αφορά όλους τους τομείς της καθημερινότητας και εξελίσσεται ραγδαία, πρέπει και η νομική επιστήμη να αναπτύσσεται παράλληλα, ώστε να προβλέπονται ειδικοί κανόνες, νόμοι και διατάξεις που θα ρυθμίζουν μια εγκληματική συμπεριφορά σχετιζόμενη με διακίνηση υλικού που προέρχεται από την τεχνολογία deepfake. Δεν είναι η ίδια η τεχνολογία που πρέπει να ρυθμίζεται, αλλά οι επιβλαβείς σκοποί για τους οποίους χρησιμοποιούνται σε συγκεκριμένες περιπτώσεις.

Καθώς τα deepfakes μπορούν να αποτελέσουν το μέσο για την τέλεση διαφόρων ποινικών αδικημάτων, εγείρονται διάφορα ερωτήματα νομικής και ηθικής φύσεως. Τι μέτρα, λοιπόν, πρέπει να ληφθούν για να αντιμετωπιστεί λοιπόν το φαινόμενο της κακόβουλης χρήσης των feepfakes;

Πρώτη και κύρια λύση αποτελεί η θέσπιση ειδικής νομοθεσίας σχετικά με το φαινόμενο αυτό. Όμως θα μπορούσε να σκεφτεί κανείς ότι είναι δύσκολο να οριστεί για κάθε τεχνολογία νομοθετικό πλαίσιο, αφού ένας πολύ εξειδικευμένος ορισμός που θα χαρακτηρίζει ως έγκλημα κάποιον συγκεκριμένο τρόπο χρήσης της τεχνολογίας, αφήνει πολύ μεγάλο περιθώριο για ανεπιθύμητες εφαρμογές ή για τεχνικές που τροποποιούνται κατά τρόπο ώστε να μην εμπίπτουν στο συγκεκριμένο ορισμό. Από την άλλη ένας πιο γενικευμένος κανόνας μπορεί να επηρεάσει αρνητικά τις χρήσιμες τεχνολογίες ή τις περιπτώσεις θετικής χρήσης τους.

Από την άλλη πλευρά, η τεχνολογία εξελίσσεται με τόσο ταχείς ρυθμούς, έτσι ώστε οι ειδικοί νομικοί κανόνες για την τεχνολογία να ξεπεραστούν γρήγορα. Δεύτερη λύση, λοιπόν, αποτελεί η αναδιαμόρφωση των ήδη υφιστάμενων νομικών διατάξεων που δεν εμφανίζονται συμβατές με τις προκλήσεις της σύγχρονης ψηφιακής κοινωνίας. Το ουσιαστικό ποινικό δίκαιο εφαρμόζεται στις περισσότερες επιβλαβείς περιπτώσεις χρήσης των deepfakes, όπως ήδη αναφέραμε και ανωτέρω, όταν για παράδειγμα χρησιμοποιούνται για την κλοπή ταυτότητας, την απάτη ή τη διανομή πορνογραφικού υλικού χωρίς συναίνεση. Όμως είναι αυτό αρκετό;

Οι νέες τεχνολογίες όπως τα deepfakes και η εγκληματική τους πλευρά θα μπορούσαν να αποτελέσουν και στην ελληνική έννομη τάξη, όπως και στις χώρες που ποινικοποίησαν το revenge porn και τα deepfakes, το έναυσμα ενός ιδιαιτέρως ενδιαφέροντος και εποικοδομητικού διαλόγου περί του βαθμού στον οποίο οι ήδη υφιστάμενες αξιόποινες πράξεις ταιριάζουν στον χαρακτήρα της παράνομης διακίνησης υλικού deepfake, όπως επίσης και περί της επάρκειας αυτών όσον αφορά στην πρόληψη και στην εν γένει ποινική μεταχείριση αυτής της τεχνολογίας.

Κατά τη γνώμη της γράφουσας, οι πολίτες χαρακτηρίζονται από άγνοια για κάθε καινούργια τεχνολογία και για τους τρόπους χρήσης της. Τις περισσότερες φορές αγνοούν ότι τα δεδομένα τους μπορεί να συλλέγονται ή να χρησιμοποιούνται χωρίς τη συναίνεσή τους. Μπορούν εύκολα

λόγω της άγνοιας τους να εξαπατηθούν και να μην αντιληφθούν ότι υφίστανται κάποιο είδος προσβολής ή ότι θυματοποιούνται. Επιπλέον, ειδικά στην ελληνική έννομη τάξη, οι πολίτες δυστυχώς δεν είναι τόσο καλά ενημερωμένοι όσο θα έπρεπε να είναι. Δεν νιώθουν την υποχρέωση να ενημερωθούν για νέες νομοθετικές ρυθμίσεις, για τις τροποποιήσεις που επέρχονται στις ήδη υφιστάμενες διατάξεις του ουσιαστικού ποινικού δικαίου, με αποτέλεσμα να μην αντιλαμβάνονται ότι μια ενέργειά τους ή μια συμπεριφορά τους είναι παράνομη, κακοποιητική και προσβλητική σε βάρος άλλου ατόμου.

Για το σκοπό αυτό ίσως να έπρεπε να εισαχθεί μια νέα ποινική διάταξη, η οποία θα μπορούσε ενδεχομένως να περιγράφει πότε η χρήση των deepfakes θεωρείται εγγενώς επιβλαβής και πότε η διάταξη αυτή μπορεί να εφαρμοστεί. Η διάταξη αυτή θα έχει στόχο να ευαισθητοποιήσει τους πολίτες μιας χώρας, να τους ενημερώσει για την κακόβουλη χρήση της τεχνολογίας, να λειτουργήσει ως μέτρο πρόληψης και αποφυγής τέλεσης τέτοιων εγκλημάτων και επιπλέον να προστατεύσει τα θύματα με την άμεση ποινικοποίηση της παράνομης συμπεριφοράς και της τιμωρίας του δράστη.

Πρόβλημα αποτελεί επίσης ο διασυνοριακός χαρακτήρας των τεχνολογιών που βασίζονται στα δεδομένα, με αποτέλεσμα τα μέρη (δράστης και θύμα) να υπόκεινται συχνά σε πολλαπλά νομικά καθεστώτα. Είναι δύσκολη η εφαρμογή νομικών κανόνων όταν μέρη της εγκληματικής συμπεριφοράς μπορεί να βρίσκονται σε πολλές χώρες ταυτόχρονα. Για παράδειγμα, ο δράστης μπορεί να βρίσκεται στην Αμερική αλλά το θύμα στην Ελλάδα, ή μπορεί τα δεδομένα να αναρτώνται σε κάποια πλατφόρμα η έδρα της οποίας να βρίσκεται στην Ασία, ή μπορεί να εμπλέκεται ένας ιστός ατόμων που βρίσκονται ταυτόχρονα σε διαφορετικές χώρες αλλά συνεργάζονται μεταξύ τους και φέρουν παράλληλη ευθύνη για το αποτέλεσμα της πράξης τους. Επιπλέον, είναι συχνά εύκολο να παρακαμφθούν οι κανόνες μιας συγκεκριμένης δικαιοδοσίας, για παράδειγμα με τη χρήση σύνδεσης VPN, όταν ο δράστης χρησιμοποιεί σύνδεση VPN, ώστε να μην αναγνωρίζεται ο τόπος στον οποίο βρίσκεται. Ίσως κρίνεται σκόπιμη η συνεργασία των χωρών και των αρχών - αστυνομικών και δικαστικών - προκειμένου να δοθεί λύση στο πιο νομικό καθεστώς πρέπει να εφαρμοστεί. Κυρίως όσον αφορά στα κράτη μέλη της ευρωπαϊκής ένωσης, τα πράγματα μπορούν να γίνουν πιο εύκολα, εάν δοθεί η οδηγία στα κράτη μέλη να ποινικοποιήσουν το ίδιο μια εγκληματική συμπεριφορά σχετιζόμενη με deepfakes.

Το ίδιο πνεύμα συνεργασίας πρέπει να επιδείξουν και οι διαμεσολαβητές του διαδικτύου κυρίως για να διαπιστωθεί η ταυτότητα του δράστη, οι οποίοι όμως δεν είναι πάντα πρόθυμοι να συνεργαστούν (χωρίς δικαστική εντολή) λόγω των συμφερόντων προστασίας της ιδιωτικής ζωής του ατόμου που ανήρτησε το υλικό.

Η απαγόρευση της παραγωγής τεχνολογίας deepfake φαίνεται δύσκολο να εφαρμοστεί, μόνο και μόνο επειδή η τεχνολογία αναπτύσσεται σε όλο τον κόσμο και μια τέτοια απαγόρευση θα ήταν

αδύνατο να διατηρηθεί. Μια επιλογή θα μπορούσε να είναι η απαγόρευση των παρόχων να πωλούν ή να διαθέτουν τεχνολογία ή εφαρμογές deepfake στους καταναλωτές. Ωστόσο, και αυτή η επιλογή εγείρει πολλά ερωτήματα. Μια τέτοια απαγόρευση θα αφορούσε όλα τα μέρη σε όλο τον κόσμο ή μόνο τα μεγάλα καταστήματα εφαρμογών και τους παρόχους υπηρεσιών; Πώς θα οριστεί/οριοθετηθεί η τεχνολογία deepfake και ο ορισμός θα περιλαμβάνει αναφορά σε συγκεκριμένες τεχνολογίες (π.χ. GAN) ή γενικότερα σε τεχνολογία που επιτρέπει τη χειραγώγηση υλικού;

Εναλλακτικά, αντί να μπλοκαριστεί η παραγωγή ή η χρήση τεχνολογιών deepfake, θα μπορούσαν να αναπτυχθούν κανόνες που θα επιβάλλουν την υποχρέωση εκ των προτέρων ελέγχου της νομιμότητας προτού το περιεχόμενο διανεμηθεί μεταξύ φίλων ή τεθεί στο διαδίκτυο. Και πάλι, το ερώτημα είναι ποιός φέρει ένα τέτοιο βάρος: οι πιο προφανείς υποψήφιοι θα ήταν οι πάροχοι υπηρεσιών διαδικτύου που φιλοξενούν ή διανέμουν τα "βαριά πλαστά". Όλο και περισσότερες υπηρεσίες και ιστότοποι απαγορεύουν ήδη (ορισμένες μορφές) deepfakes από τις πλατφόρμες τους, όπως γίνεται σαφές στους Όρους και Προϋποθέσεις τους. Θα μπορούσε να επιβληθεί ειδική υποχρέωση στους παρόχους να χρησιμοποιούν τεχνολογίες ανίχνευσης ψευδών στοιχείων. Αυτές οι τεχνικές δεν θα φιλτράρουν όλα τα deepfakes, αλλά σε κάθε περίπτωση ένα σημαντικό μέρος τους.

Ωστόσο, και πάλι ανακύπτουν διάφορα ζητήματα. Πρώτον, στην περίπτωση που ένα σύστημα ανίχνευσης υποδεικνύει ότι το υλικό θα μπορούσε να είναι πλαστό, τότε μια εταιρεία θα πρέπει να αποκλείει αυτόματα το εν λόγω περιεχόμενο ή τελικά να επιτρέπει ορισμένες βαθιές απομιμήσεις; Και στην περίπτωση που ισχύει το δεύτερο, θα πρέπει ο νομοθέτης να παράσχει περαιτέρω διευκρινίσεις σχετικά με το τι είδους deepfakes επιτρέπονται ή όχι, ή αυτό επαφίεται στους παρόχους, με πιθανή συνέπεια να εφαρμόζουν οι διάφοροι πάροχοι διαφορετικά σύνολα κανόνων;

Επιπλέον, αν το περισσότερο υλικό που κυκλοφορεί είναι παραποιημένο, τόσο από άποψη χρόνου όσο και πόρων, θα είναι πρακτικά αδύνατο για τα μέσα ενημέρωσης να ελέγχουν συστηματικά όλο το περιεχόμενο για την αυθεντικότητα, να αξιολογούν ακριβώς τι έχει παραποιηθεί σε ένα βίντεο/μια φωτογραφία/κ.λπ. και σε ποιο βαθμό αυτό είναι σχετικό με την είδηση.

Ίσως, η ανθρώπινη συμμετοχή/αξιολόγηση να είναι αναπόφευκτη και αυτό μπορεί να επιφέρει σημαντική οικονομική επιβάρυνση στις εταιρείες. Όπως συνέβη και με την εταιρεία Google, η οποία έπρεπε να επενδύσει σημαντικά για να χειριστεί όλα τα αιτήματα για το δικαίωμα στη λήθη. Έτσι και στην περίπτωση αυτή, οι εκ των προτέρων έλεγχοι νομιμότητας των δημοσιευμένων φωτογραφιών και βίντεο θα μπορούσαν δυνητικά να διενεργούνται και από την Αρχή Προστασίας Δεδομένων (ΑΠΔ). Για το σκοπό αυτό, οι πολίτες θα πρέπει να υποβάλλουν το deepfake ή τη συγκεκριμένη εφαρμογή τους στην ΑΠΔΠΧ πριν τη διανομή ή τη δημοσίευσή τους- η ΑΠΔΠΧ θα μπορεί στη συνέχεια να ελέγχει το περιεχόμενο ως προς τη συμμόρφωση με τον ΓΚΠΔ.

Ωστόσο, δεν είναι βέβαιο αν όλοι οι πολίτες θα συμμορφωθούν πραγματικά με μια τέτοια υποχρέωση, αν αυτή εισαχθεί, και είναι εξίσου αβέβαιο αν η ΑΠΔΠΧ διαθέτει το ανθρώπινο δυναμικό (ή τη βούληση) για να ελέγξει όλα τα deepfakes για συμμόρφωση με τον ΓΚΠΔ.

Το ίδιο πρέπει να συμβεί και στον δικαστικό μηχανισμό, όταν εισάγονται στη δίκη ψηφιακά πειστήρια, για τα οποία οπωσδήποτε πρέπει να επικυρώνεται η αξιοπιστία τους. Μια λύση θα μπορούσε να αποτελέσει η διενέργεια πραγματογνωμοσύνης, με το διορισμό ειδικευμένου ατόμου από κατάλογο πραγματογνωμόνων που θα μπορούσε να διαμορφωθεί. Ωστόσο, και σε αυτή την περίπτωση, όλες αυτές οι διαδικασίες εκτός από χρονοβόρες χαρακτηρίζονται και από το μεγάλο κόστος τους, με αποτέλεσμα ο διάδικος που αμφισβητεί το υλικό να βαρύνεται με μεγάλα έξοδα και να υπάρχουν μεγάλες καθυστερήσεις στην απονομή της δικαιοσύνης.

Επιπρόσθετα των ποινικών διατάξεων, της συνεργασίας των αρχών και των παρόχων, θα μπορούσε να ξεκινήσει μια εκστρατεία ευαισθητοποίησης. Όπως τα μέσα κοινωνικής δικτύωσης συμβάλλουν στη διάδοση πλαστών βίντεο, έτσι μπορούν να συμβάλλουν και στην αποτροπή της κακόβουλης χρήσης τους. Μια δημόσια εκστρατεία θα μπορούσε να αναδείξει νέα ή υφιστάμενα ηθικά και νομικά πρότυπα για τη χρήση της τεχνολογίας deepfake.

Για παράδειγμα, θα μπορούσε να γίνει σαφές στο ανδρικό φύλο, ότι η παραγωγή και η διανομή ψευδούς πορνογραφικού υλικού είναι απαράδεκτη και παράνομη. Από την άλλη, θα μπορούσαν να επισημανθούν οι θετικές εφαρμογές της τεχνολογίας deepfake. Επιπλέον, η προσοχή θα μπορούσε να στραφεί στις δυνατότητες των θυμάτων να προστατευτούν από τα deepfakes. Ειδικά οι γυναίκες θα μπορούσαν να ενημερωθούν για τις δυνατότητες απομάκρυνσης των "deepfakes" και τις νομικές ενέργειες. Ωστόσο, αυτό ίσως να επιφέρει μια "κατηγοριοποίηση των θυμάτων" και την ιδιωτικοποίηση ενός κοινωνικού προβλήματος, καθιστώντας τις γυναίκες-θύματα υπεύθυνες για την απομάκρυνση του επιβλαβούς περιεχομένου. Ίσως, όμως, η προσοχή να πρέπει να δοθεί στην ύπαρξη των deepfakes και του χειραγωγημένου περιεχομένου εν γένει. Οι δημοσιογράφοι και οι δικαστές θα πρέπει να έχουν επίγνωση του πόσο ρεαλιστικό μπορεί να φαίνεται το παραποιημένο υλικό και οι πολίτες μπορούν να προειδοποιούνται για επικίνδυνο ψευδές υλικό, για παράδειγμα, υποδεικνύοντας ως πρότυπο ότι μια πηγή δεν είναι πηγή, όταν βλέπουν εντυπωσιακές ειδήσεις ή τους ζητείται να μεταφέρουν χρήματα σε συγγενείς.

Άξιο αναφοράς, αποτελεί και οι τρόποι προστασίας των θυμάτων, αφού υπάρχουν εξαιρετικά πολλές αμφιβολίες αν τα θύματα των deepfakes τελικά προστατεύονται αποτελεσματικά. Σε αυτό συμβάλλουν πολλοί παράγοντες, όπως ο διασυνοριακός χαρακτήρας των δεδομένων, η έλλειψη αποτελεσματικής συνεργασίας των παρόχων ή η εφαρμογή πολλαπλών νομικών καθεστώτων.

Για παράδειγμα, στην περίπτωση διακίνησης ενός ψεύτικο βίντεο πορνογραφικού περιεχομένου χωρίς τη συγκατάθεση του θύματος - πρωταγωνιστή του βίντεο. Ας υποθέσουμε ότι το θύμα

βρίσκεται στην Ελλάδα και η αρχή δίωξης ηλεκτρονικού εγκλήματος δώσει ρητή εντολή στις πλατφόρμες να κατεβάσουν το επίμαχο βίντεο και να απαγορεύσουν στους χρήστες να το αναρτήσουν οπουδήποτε ξανά. Τι συμβαίνει όμως με τους χρήστες των ίδιων κοινωνικών πλατφορμών σε άλλη χώρα, για τους οποίους δεν ισχύει η ίδια απαγόρευση; Επιπλέον, αφού τα δεδομένα διακινούνται παγκοσμίως, και κάθε χώρα έχει τον δικό της τρόπο αντιμετώπισης, τι θα συμβεί αν σε κάποια χώρα η συμπεριφορά αυτή δεν θεωρείται αξιόποινη; Τη λύση ίσως να δώσει η συνεργασία των αρχών και των παρόχων σε όλες τις χώρες, όμως αυτό μπορεί να πει κανείς ότι είναι αντικειμενικά δύσκολο, τα προβλήματα που πρέπει να ξεπεραστούν για να συνεννοηθούν παγκοσμίως οι πάροχοι είναι μεγάλα και το κυριότερο πρόβλημα που θα ανακύψει είναι το κόστος.

Ζήτημα επίσης αποτελεί το γεγονός της ύπαρξης του υπολογιστικού νέφους. Μπορεί να απαγορευθεί η ανάρτηση του επίμαχου βίντεο στις πλατφόρμες του διαδικτύου, μπορεί τα υλικά αντικείμενα που ανήκουν στον δράστη, όπως το κινητό τηλέφωνο, το λάπτοπ ή ένα μέσο αποθήκευσης usb να κατασχεθούν και το παράνομο υλικό που είναι αποθηκευμένο σε αυτά να διαγραφεί μόνιμα. Τι συμβαίνει όμως όταν ο δράστης έχει αποθηκεύσει το παράνομο υλικό και σε κάποια πλατφόρμα υπολογιστικού νέφους, στην οποία έχει πρόσβαση μόνο ο ίδιος με τους προσωπικούς του κωδικούς και κανένας άλλος, με αποτέλεσμα το βίντεο να κοινοποιηθεί ξανά σε μια νέα και διαφορετική πλατφόρμα στο ίντερνετ, η οποία μπορεί να δημιουργηθεί εκ των υστέρων; Μπορεί επομένως κανείς να φανταστεί το τεράστιο πρόβλημα που δημιουργείται για το θύμα, αφού το τελευταίο θα ζει με το άγχος, την ανησυχία και τη φοβία ότι τα δεδομένα που τον αφορούν και ο δράστης προέβη σε παράνομη διακίνησή τους, θα μπορεί να γίνει λήψη τους από το νέφος του δράστη και να καταστούν διαθέσιμα ξανά στο αναρίθμητο κοινό του διαδικτύου. Μια λύση για να προστατευτούν τα δικαιώματα της προσωπικότητας του θύματος, είναι με την καταδικαστική απόφαση για τον δράστη για την παράνομη διακίνηση του deepfake υλικού, να διατάσσεται ταυτόχρονα και η οριστική διαγραφή του προσωπικού λογαριασμού νέφους του δράστη, έτσι ώστε να μην υπάρχει καμία δυνατότητα πρόσβασής του σε αυτόν.

Τέλος, ζήτημα ανακύπτει και πάλι στο κατά πόσο προστατεύεται το θύμα και αποκαθίσταται η φήμη του, καθώς κάποιος χρήστης του διαδικτύου μπορεί να έχει προλάβει όχι απλά να δει το παράνομο υλικό, αλλά να το έχει αποθηκεύσει στο κινητό του ή στον υπολογιστή του, να το έχει προωθήσει σε κάποιον διαδικτυακό του φίλο σε κάποιο μέσο ανταλλαγής μηνυμάτων με υψηλή κρυπτογράφηση, όπως το whatapp, το viber ή το messenger και το βίντεο αυτό να παραμένει εκεί μόνιμα αποθηκευμένο χωρίς κάποιος άλλος να έχει πρόσβαση σε αυτό.

Κρίνεται επομένως επιβεβλημένη τόσο η σωστή ενημέρωση και ευαισθητοποίηση των πολιτών για το νέο φαινόμενο deepfakes, όσο και η ποινικοποίηση της παράνομης χρήσης τους με σκοπό την άμεση τιμώρηση του δράστη, την προστασία των θυμάτων και την αποκατάσταση της έννομης τάξης με την ορθή απονομή της δικαιοσύνης, ενώ καθίσταται απαραίτητη και η συνεργασία μεταξύ

των αρμόδιων αρχών (δικαστικών – κυβερνητικών – διεθνών οργανισμών) και των παρόχων - διαμεσολαβητών δικτύου με σκοπό τη δημιουργία ενός νέου προστατευτικού μανδύα για όλα εκείνα τα πρόσωπα, φυσικά ή νομικά, που πέφτουν θύματα της τεχνολογίας deepfake. Δεν είναι αρκετή η καταδίκη του κατηγορουμένου για την παράνομη διακίνηση υλικού deepfake αλλά κρίνεται απαραίτητο να εξασφαλιστεί στο ακέραιο η προστασία του θύματος, των δεδομένων του και της προσωπικότητάς του με τη μόνιμη διαγραφή όλων εκείνων των δεδομένων, έτσι ώστε να μην αποφευχθεί ο κίνδυνος τα παράνομα δεδομένα να εμφανιστούν ξανά στο μέλλον, με επιβλαβείς για το θύμα τους συνέπειες.

## V. ΒΙΒΛΙΟΓΡΑΦΙΑ

### ΒΙΒΛΙΑ


- Schick N. Deepfakes : The Coming Infocalypse. First U.S. ed. New York: Twelve; 2020
- DeepFake Technology: Complete Guide to Deep Fakes, Politics and Social Media, Nobert Young, Amazon Digital Services LLC - KDP Print US, 2019
- Τεχνητή Νοημοσύνη, Ι. Βλαχάβας, Π. Κεφαλάς, Ν. Βασιλειάδης, Φ. Κόκκορας, Η. Σακελλαρίου, Δ΄Έκδοση - Ιούνιος 2020, Εκδόσεις Πανεπιστημίου Μακεδονίας
- Stuart Russell, Peter Norvig, "Τεχνητή Νοημοσύνη - Μια Σύγχρονη Προσέγγιση", 2η Αμερικανική Έκδοση, Κλειδάριθμος, 2004
- Ηλεκτρονικό Έγκλημα, Ουσιαστικές και Δικονομικές όψεις, Επιμέλεια: Θεοχάρης Δαλακούρας, Νομική Βιβλιοθήκη, 2η έκδοση 2023
- Ο νέος Ποινικός Κώδικας, Ερμηνεία κατ' άρθρο του Ν. 4619/2019, Επιμέλεια: Χαραλαμπάκης Αριστοτέλης, Συγγραφείς: Αθανασίου Χ., Αναστασοπούλου Ι., Αποστολίδου Α., Βαθιώτης Κ., Βρυνιώτης Π., Δανιήλ Γ., Διονυσοπούλου Α., Καμπέρου Ε., Κοσμάτος Κ., κ.α., Τόμος 2ος, έκδοση 2020, Νομική Βιβλιοθήκη
- Ποινικός Κώδικας, Μιχαήλ Μαργαρίτης / Άντα Μαργαρίτη, Εκδόσεις Π.Ν. Σάκκουλας 2022
- Δίκαιο Πνευματικής Ιδιοκτησίας, Κωνσταντίνος Χριστοδούλου, Καθηγητής Νομικής Σχολής Αθηνών, Εκδόσεις Νομική Βιβλιοθήκη, 2018
- Προσωπικά Δεδομένα, Ευγενία Αλεξανδροπούλου Αιγυπτιάδου, Νομική Βιβλιοθήκη, 2016
- Λαχανά Κ.-Χ. (2016) Η κατά το Ελληνικό Δίκαιο Ποινική Προστασία των Προσωπικών Δεδομένων στο Πλαίσιο της Αστυνομικής Δικαστικής Συνεργασίας σε Ποινικές Υποθέσεις: Προκλήσεις και Προοπτικές. Διατριβή επί Διδακτορία. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης-Νομική Σχολή-Τομέας Ποινικών και Εγκληματολογικών Επιστημών. (72 επ.); Γανιάρης Ν., (2020) Δεδομένα Προσωπικού Χαρακτήρα. Σε: Παύλου Στ. Κ. και Σάμιος Θ. Π. Ειδικοί Ποινικοί Νόμοι. (6η ενημέρωση). Π.Ν. Σάκκουλας.
- Μυλωνόπουλος, Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, 2006, 439
- Σπινέλλης, ΠΔ, ΕιδΜερ, τ.Β' 1985, 97, Μυλωνόπουλος, ό.π., 373 επ., Αποστολιδου, Απάτη - Η πλάνη ως αποτέλεσμα πράξης εξαπάτησης και η περιουσιακή διάθεση στο έγκλημα της απάτης, 2000, 119 επ.


### ΠΕΡΙΟΔΙΚΑ


- Deepfake, μια νομική προσέγγιση, Philippe Jougleux, Αναπληρωτής Καθηγητής, Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου, έτος 2020, δημοσίευση στο περιοδικο ΔΙΤΕ, τεύχος 3/2020, εκδόσεις Νομική Βιβλιοθήκη

- Ι. Ιγγλεζάκης Δ. Ιωάννης «Επεξεργασία δεδομένων εικόνας ή/και ήχου μέσω φωτογράφησης και βιντεοσκόπησης από δικαστικό επιμελητή κατά τη διαδικασία αναγκαστικής εκτέλεσης (γνωμοδότηση)». ΔΙΜΕΕ 10/2013 σελ. 172 επ.
- Άρθρα και αποφάσεις σε Ποινική Δικαιοσύνη και Ποινικά Χρονικά

**ΙΣΤΟΣΕΛΙΔΕΣ**

- https://www.esdi.gr/nex/images/stories/pdf/epimorfosi/2021/milosi_2021.pdf
- Machine Learning - Μηχανική μάθηση - τι είναι; _ CSC - Computer Science Center., Διαθέσιμο: https://www.csc.com.gr/machine-learning%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%BC%CE%AC%CE%B8%CE%B7%CF%83%CE%B7-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9/
- 10 Amazing Examples Of How Deep Learning AI Is Used In Practice. Διαθέσιμο: https://www.forbes.com/sites/bernardmarr/2018/08/20/10-amazing-examples-of-how-deep-learning-ai-isused-in-practice/?sh=12f48535f98a
- Τι είναι η Υπολογιστική Νοημοσύνη; - IEEE Computational Intelligence Society. Διαθέσιμο: https://cis.ieee.org/about/what-is-ci
- http://repfiles.kallipos.gr/html_books/93/04a-main.html
- Overview of GAN Structure | Generative Adversarial Networks | Google Developers https://developers.google.com/machine-learning/gan/gan_structure
- Auto-Encoder: What Is It? And What Is It Used For? (Part 1) | by Will Badr | Towards Data Science https://towardsdatascience.com/auto-encoder-what-is-it-and-what-is-it-used-for-part-1-3e5c6f017726
- Dave Lee, Matter of fact-checkers: Is Facebook winning the fake news war?, BBC News, 02 Απριλίου 2019, (https://www.bbc.com/news/technology-47779782)
- Harry Cockburn, Trump calls Fox 'fake news' for citing unfavorable 2020 election polls, The Independent, 19 Ιουνίου 2019, https://www.independent.co.uk/news/world/americas/uspolitics/trump-fox-news-poll-fake-news-joe-biden-2020-election-us-a8963786.html
- http://www.aereurope.org/wpcontent/uploads/2018/10/CodeofPracticeonDisinformation.pdf
- https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037847559&categorieLien=id&fbclid=IwAR1bXQ7K6gnVGUJN4SkTsfMFTX8BCyG-P123bLVmfWz8KXRShGEGmMttluw
- https://techcrunch.com/2020/05/14/france-passes-law-forcing-onlineplatforms-to-delete-hate-speech-content-within-24-hours/?guccounter=2
- https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm)
- https://www.lawspot.gr/nomika-nea/fake-news-tropopoieitai-i-diataxi-toy-poinikoy-kodika-gia-ti-diaspora-pseydon-eidiseon
- https://youtu.be/HG_NZpkttXE
- Intimate Image Abuse, Summary of the final report, Law Comission, Reforming the Law, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Intimate-Image-Abuse-summary-of-report-1.pdf
- https://techcrunch.com/2022/11/25/deepfake-porn-revenge-porn-uk-law-change/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKrR_HBxBvzgVmgipoeJFrTgMd0ThrMB4GIG61hnl3qM_8N4Cav1EWgL5SauVX34uWeWKSv_E-Zc2EurkK71112II979Azo0YRxMB1wdegxoT-hS8W1gJ1PpmZPE9u6qjKfsORiFNUC7U3QLCc6p4shXmoNRgWuyNacRV18bBG9j
- https://www.bbc.com/news/technology-63669711

- https://www.theguardian.com/technology/2022/nov/24/online-safety-bill-to-return-to-parliament-next-month
- https://www.unite.ai/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/
- https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality
- Η Μη Συναινετική Πορνογραφία στην Ελληνική Έννομη Τάξη, Αγγελική Γιαννάκη, Δικηγόρος Αθηνών, MSc in Criminology and Criminal Justice (University of Oxford) ΜΑΪΟΣ 2021 https://theartofcrime.gr/%CE%B7-%CE%BC%CE%B7-%CF%83%CF%85%CE%BD%CE%B1%CE%B9%CE%BD%CE%B5%CF%84%CE%B9%CE%BA%CE%AE-%CF%80%CE%BF%CF%81%CE%BD%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5%CE%BB%CE%BB/
- https://www.creativebloq.com/features/deepfake-examples
- https://edition.cnn.com/2020/12/25/uk/deepfake-queen-speech-christmas-intl-gbr/index.html
- https://www.sciencedirect.com/science/article/abs/pii/S0747563212002154
- https://youngpeople.gr/cyber-bullying-%CE%AD%CE%BD%CE%B1%CF%82-%CE%B5%CE%BA%CF%86%CE%BF%CE%B2%CE%B9%CF%83%CE%BC%CF%8C%CF%82-%CE%B4%CE%AF%CF%87%CF%89%CF%82-%CF%8C%CF%81%CE%B9%CE%B1/
- https://www.proquest.com/openview/df7b85db5268ac4d18d07478e8fe197f/1.pdf?pq-origsite=gscholar&cbl=25066
- Patrick Ryan, 'Deepfake' Audio Evidence Used in UK Court to Discredit Dubai Dad, THE NATIONAL (Feb. 8, 2020), https://www.thenational.ae/uae/courts/deepfake-audio-evidenceused-in-uk-court-to-discredit-dubai-dad-1.97576
- https://www.lawspot.gr/nomika-nea/psifiaki-edafikotita-topos-telesis-egklimatos-meso-diadiktyoy
- https://efotopoulou.gr/plastografia-pistopiitikon-ke-martirikon-217-pk/
- https://socialpolicy.gr/2015/09/%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1.html
- https://www.karagiannislawfirm.gr/news/plastografia-kakoyrghmatikh
- https://www.kathimerini.gr/society/561629566/vathainei-i-pligi-toy-revenge-porn-ayxisi-66-stis-kataggelies-to-2021/
- https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0
- https://www.dpa.gr/sites/default/files/2019-10/2472_97%20%28SEPT2019%29.pdf
- https://www.uoi.gr/wp-content/uploads/2019/09/nomos_4624_2019.pdf
- https://www.dpa.gr/
- https://www.uoi.gr/wp-content/uploads/2019/01/kanonismos-gdpr1.pdf
- https://opi.gr/vivliothiki/2121-1993
- https://www.lawspot.gr/nomika-nea/fake-news-tropopoieitai-i-diataxi-toy-poinikoy-kodika-gia-ti-diaspora-pseydon-eidiseon
- https://www.lawspot.gr/nomika-nea/psifiaki-edafikotita-topos-telesis-egklimatos-meso-diadiktyoy

**ΠΗΓΕΣ ΓΙΑ ΝΟΜΟΛΟΓΙΑ**

- https://www.qualex.gr/el-GR/syntheti-anazitisi/search?advst=gnl&cpage=1&search=jougleux&sms=true&r1=1&oti1=true&ote1=true&

itemsperpage=30&acc=false&ln=false&frc=false&tp=def&sy1=0&nr1=0&oti2=true&ote2=true&r2=1&cdalt=false

- https://lawdb.intrasoftnet.com/
- https://www.lawspot.gr/
- https://www.sakkoulas-online.gr
- https://www.dpa.gr
- https://eur-lex.europa.eu
- https://www.dsanet.gr
- https://lawdb.intrasoftnet.com
- https://www.qualex.gr/el-GR
- https://www.crimetimes.gr
- http://www.areiospagos.gr
- InLaw.gr
- https://www.kodiko.gr/nomothesia/document/307515/nomos-927-1979

**ΑΡΘΡΟΓΡΑΦΙΑ**


- Brij B. Gupta, Krishna Yadav, Imran Razzak, Konstantinos Psannis, Arcangelo Castiglione, Xiaojun Chang,, A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment, Computer Communications, Volume 175, 2021, Pages 47-57,ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2021.04.023
- Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B. Gupta, An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT Smart City Framework, Future Generation Computer Systems, Volume 83, 2018, Pages 619-628, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.04.039
- Andreas P. Plageras, Kostas E. Psannis, Christos Stergiou, Haoxiang Wang, B.B. Gupta, Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings, Future Generation Computer Systems, Volume 82, 2018, Pages 349-357, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.09.082.
- V. Memos and K.E. Psannis, NFV-based Scheme for Effective Protection against Bot Attacks in AI-enabled IoT, IEEE Internet of Things Magazine, 2022.
- Androniki Sapountzi, Kostas E. Psannis, Social networking data analysis tools & challenges, Future Generation Computer Systems, Volume 86, 2018, Pages 893-913, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.10.019.
- V. Memos, and K. Psannis, "Artificial Intelligence ANTi-Attack System (AIANTAS) for IoT Cyberspace: An Upcoming Cloud-based Security Architecture for Police Authorities", 4th World Symposium on Communication Engineering (WSCE 2021) & 9th International Conference on Information, Communication and Networks (ICICN 2021), University of Macedonia (Greece), Shaanxi Normal University (Xi'an, China), November 2021
- Kolagati, Santosh & Priyadharshini, Thenuga & v, Mary Anita Rajam. (2022). Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights. 2. 100054. 10.1016/j.jjimei.2021.100054
- Facing Reality? Law enforcement and the challenge of deepfakes, An observatory report from the Europol Innovation Lab, Luxembourg: Publications Office of the European Union, 2022 © European Union Agency for Law Enforcement Cooperation, 2022, www.europol.europa.eu
- Ahmed Seddik, Yassine Maleh, Ghada M. El Banby, Ashraf A.M. Khalaf, Fathi E. Abd El-Samie, Brij B Gupta, Konstantinos Psannis, Ahmed A. Abd El-Latif, AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities, Technological Forecasting and

Social Change, Volume 177, 2022, 121555, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2022.121555

- Shad HS, Rizvee MM, Roza NT, Hoq SMA, Monirujjaman Khan M, Singh A, Zaguia A, Bourouis S. Comparative Analysis of Deepfake Image Detection Method Using Convolutional Neural Network. Comput Intell Neurosci. 2021 Dec 16;2021:3111676. doi: 10.1155/2021/3111676. PMID: 34956345; PMCID: PMC8702341
- The Creation and Detection of Deepfakes: A Survey. By: MIRSKY, YISROEL; LEE, WENKE. ACM Computing Surveys. Jan2021, Vol. 54 Issue 1, p1-41. 41p. 2 Color Photographs, 8 Diagrams, 4 Charts, 1 Graph. DOI: 10.1145/3425780. , Database: Business Source Complete
- Christos Stergiou, Kostas E. Psannis, Brij B. Gupta, Yutaka Ishibashi, Security, privacy & efficiency of sustainable Cloud Computing for Big Data & IoT, Sustainable Computing: Informatics and Systems, Volume 19, 2018, Pages 174-184, ISSN 2210-5379, https://doi.org/10.1016/j.suscom.2018.06.003.
- C. L. Stergiou, K. E. Psannis and B. B. Gupta, "IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5164-5171, 1 April1, 2021, doi: 10.1109/JIOT.2020.3033131.
- Stergiou, C., Psannis, K.E. Efficient and secure BIG data delivery in Cloud Computing. Multimed Tools Appl 76, 22803–22822 (2017). https://doi.org/10.1007/s11042-017-4590-4
- Gamage, Dilrukshi & Ghasiya, Piyush & Bonagiri, Vamshi & Whiting, Mark & Sasahara, Kazutoshi. (2022). Are Deepfakes Concerning? Analyzing Conversations of Deepfakes on Reddit and Exploring Societal Implications. 10.1145/3491102.3517446.
- Nguyen, Thanh Thi, et al. "Deep learning for deepfakes creation and detection." arXiv preprint arXiv:1909.11573 1 (2019)
- Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2022). InFeMo: Flexible Big Data Management Through a Federated Cloud System. In ACM Transactions on Internet Technology (Vol. 22, Issue 2, pp. 1–22). Association for Computing Machinery (ACM). https://doi.org/10.1145/3426972
- Christos Stergiou and Kostas E. Psannis, Recent advances delivered by mobile cloud computing and Internet of Things for Big data applications: A Survey, International Journal of Network Management, doi: 10.1002/nem.1930 May 2016
- Vasileios A. Memos, Georgios Minopoulos, Konstantinos Stergiou, and Kostas E. Psannis, “Internet-of-Things-Enabled Infrastructure Against Infectious Diseases”, Vol. 4, No. 2, pp. 20-25, IEEE Internet of Things Magazine, June 2021, https://doi.org/10.1109/IOTM.0001.2100023
- Georgios M. Minopoulos, Vasileios A. Memos, Christos L. Stergiou, Konstantinos D. Stergiou, Andreas P. Plageras, Maria P. Koidou, and Konstantinos E. Psannis, “Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System,” Applied Sciences, Vol. 12, No. 12, pp. 58-59, June 2022, https://doi.org/10.3390/app12125859
- K. D. Stergiou, G. M. Minopoulos, V. A. Memos, C. L. Stergiou, M. P. Koidou, and K. E. Psannis, “A Machine Learning-Based Model for Epidemic Forecasting and Faster Drug Discovery,” Applied Sciences, vol. 12, no. 21, p. 10766, Oct. 2022, doi: 10.3390/app122110766
- V. Memos, K.E. Psannis, Z. Lv, A Secure Network Model against Bot Attacks in Edge-enabled Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 2022 doi:10.1109/TII.2022.3162837
- Nielsen, Michael A. Neural networks and deep learning. Vol. 2018. San Francisco, CA: Determination press, 2015
- Ongsulee, Pariwat. "Artificial intelligence, machine learning and deep learning." 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE). IEEE, 2017

- Bhavsar, Hetal, and Amit Ganatra. "A comparative study of training algorithms for supervised machine learning." International Journal of Soft Computing and Engineering (IJSCE) 2.4 (2012): 2231-2307
- Engelbrecht, Andries P. Computational intelligence: an introduction. John Wiley & Sons, 2007
- Aggarwal, Charu C. Neural networks and deep learning. Springer,, 2018
- Kriegeskorte, Nikolaus, and Tal Golan. "Neural network models and deep learning." Current Biology 29.7 (2019): R231-R236.
- Anthony, Martin, and Peter L. Bartlett. Neural network learning: Theoretical foundations. Cambridge university press, 2009.
- Wang, Sun-Chong. "Artificial neural network." Interdisciplinary computing in java programming. Springer, Boston, MA, 2003. 81-100
- Canziani, Alfredo, Adam Paszke, and Eugenio Culurciello. "An analysis of deep neural network models for practical applications." arXiv preprint arXiv:1605.07678 (2016)
- Zheng, Shuai, Abhinav Vishnu, and Chris Ding. "Accelerating deep learning with shrinkage and recall." 2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2016.
- Reed, Russell, and Robert J. MarksII. Neural smithing: supervised learning in feedforward artificial neural networks. Mit Press, 1999
- Vamvoudakis, Kyriakos G., Frank L. Lewis, and Draguna Vrabie. "Reinforcement Learning with Applications in Automation Decision and Feedback Control." Handbook on Computational Intelligence: Volume 1: Fuzzy Logic, Systems, Artificial Neural Networks, and Learning Systems. 2016. 401-439
- Bornholdt, Stefan, and Torsten Röhl. "Self-organized critical neural networks." Physical Review E 67.6 (2003): 066118
- Kanal, Laveen N. "Perceptron." Encyclopedia of Computer Science. 2003. 1383-1385.
- M. k. Alsmadi, K. B. Omar, S. A. Noah and I. Almarashdah, "Performance Comparison of Multi-layer Perceptron (Back Propagation, Delta Rule and Perceptron) algorithms in Neural Networks," 2009 IEEE International Advance Computing Conference, 2009, pp. 296-299, doi: 10.1109/IADCC.2009.4809024.
- Almeida, Luis B. "Backpropagation in perceptrons with feedback." Neural computers. Springer, Berlin, Heidelberg, 1989. 199-208
- O'Shea, Keiron, and Ryan Nash. "An introduction to convolutional neural networks." arXiv preprint arXiv:1511.08458 (2015).
- Kalchbrenner, Nal, Edward Grefenstette, and Phil Blunsom. "A convolutional neural network for modelling sentences." arXiv preprint arXiv:1404.2188 (2014)
- Chaudhari, Poonam, and Himanshu Agarwal. "Progressive review towards deep learning techniques." Proceedings of the International Conference on Data Engineering and Communication Technology. Springer, Singapore, 2017
- U. Côté-Allard et al., "Deep Learning for Electromyographic Hand Gesture Signal Classification Using Transfer Learning," in IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 27, no. 4, pp. 760-771, April 2019, doi: 10.1109/TNSRE.2019.2896269.
- Maghrebi, Houssem, Thibault Portigliatti, and Emmanuel Prouff. "Breaking cryptographic implementations using deep learning techniques." International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, Cham, 2016
- Baldi, Pierre. "Autoencoders, unsupervised learning, and deep architectures." Proceedings of ICML workshop on unsupervised and transfer learning. 2012.

- Lerch S, Polsterer KL. Convolutional autoencoders for spatially-informed ensemble post-processing. 2022. Accessed May 22, 2022.
- Kong Q, Chiang A, Aguiar AC, Fernández-Godino MG, Myers SC, Lucas DD. Deep Convolutional Autoencoders as Generic Feature Extractors in Seismological Applications. 2021. Accessed May 22, 2022
- Alessandri, Luca, et al. "Sparsely-Connected Autoencoder (SCA) for single cell RNAseq data mining." bioRxiv (2020).
- Nag S. Lookahead optimizer improves the performance of Convolutional Autoencoders for reconstruction of natural images. 2020. Accessed May 22, 2022.
- Manakov, Ilja, Markus Rohm, and Volker Tresp. "Walking the Tightrope: investigation of the Convolutional Autoencoder Bottleneck." arXiv preprint arXiv:1911.07460 (2019)
- J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann, Deepfakes: Trick or treat?, Business Horizons, 63 (2) (2020), pp. 135-146, https://www.sciencedirect.com/science/article/abs/pii/S0007681319301600
- Singh, Simranjeet, Rajneesh Sharma, and Alan F. Smeaton. "Using GANs to Synthesise Minimum Training Data for Deepfake Generation." arXiv preprint arXiv:2011.05421 (2020)
- Borji, Ali. "Pros and cons of gan evaluation measures." Computer Vision and Image Understanding 179 (2019): 41-65
- Asad Malik, Minoru Kuribayashi, Sani M. Abdullahi, Ahmad Neyaz Khan. DeepFake Detection for Human Face Images and Videos: A Survey. IEEE Access. 2022;10:18757-18775. doi:10.1109/ACCESS.2022.3151186
- Kim, Hyeongwoo, et al. "Deep video portraits." ACM Transactions on Graphics (TOG) 37.4 (2018): 1-14
- Mescheder, Lars, Sebastian Nowozin, and Andreas Geiger. "Adversarial variational bayes: Unifying variational autoencoders and generative adversarial networks." arXiv preprint arXiv:1701.04722 (2017)
- Li, Kai, et al. "A data-driven approach for facial expression synthesis in video." 2012 IEEE Conference on Computer Vision and Pattern Recognition. IEEE, 2012
- Malik, M. Kuribayashi, S. M. Abdullahi and A. N. Khan, "DeepFake Detection for Human Face Images and Videos: A Survey," in IEEE Access, vol. 10, pp. 18757-18775, 2022, doi: 10.1109/ACCESS.2022.3151186.
- Γ. Ζέκος, Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο, 2022, σ. 97 = sakkoulas-online
- DEEPFAKES: Summary, The legal challenges of a synthetic society, Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, November 2021, Tilburg Institute for Law, Technology, and Society
- Regulating deep fakes: legal and ethical considerations, Edvinas Meskys, Paulius Jurcys, Article in Journal of Intellectual Property Law & Practice · January 2020
- Citron, D.K. & Franks, M.A. (2014) Criminalizing Revenge Porn. Wake Forest L.Rev. 49: 345-391
- McGlynn, C. & Rackley, E. (2017) Image-based Sexual Abuse. Oxford Journal of Legal Studies. 37(3): 534-561
- McGlynn, C. & Downes, J. (2015) We Need A New Law to Combat 'Upskirting' and 'Downblousing'. Available at: https://inherentlyhuman.wordpress.com/2015/04 /15/ we-need-a-new-law-to-combat-upskirting-and-downblousing/ (Last Accessed: 28.05.2021); Citron, D.K. (2019) Sexual Privacy. Yale LJ. 128. 1870-1960 (1921 επ.)

- Šepec, M. (2019) Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence. International Journal of Cyber Criminology. 13(2): 418-438 (419, 430)
- McGlynn, C., Rackley, E. & Houghton, R. (2017) Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse, Feminist Legal Studies. 25: 25-46 (28-29); Bloom, S. (2016) No Vengeance for 'Revenge Porn' Victims: Unraveling Why This Latest Female-Centric, Intimate-Partner Offense is Still Legal, and Why We Should Criminalize It. Fordham Urb.LJ. vol. 42(1): 233-289 (278 επ.).
- A Survey of Deep Fake Detection for Trial Courts, Naciye Celebi, Qingzhong Liu, Muhammed Karatoprak, Cornell University, arXiv:2205.15792 [cs.CV], https://doi.org/10.48550/arXiv.2205.15792
- Pfefferkorn, Riana, 'Deepfakes' in the Courtroom (October 1, 2020). Boston University Public Interest Law Journal, Vol. 29, No. 2, 2020, Available at SSRN: https://ssrn.com/abstract=4321140

**Κυρώσεις για λογοκλοπή**

Η λογοκλοπή είναι ένα πολύ σοβαρό παράπτωμα. Με απόφαση με το άρθ. 7.2 του Κανονισμού «σε περιπτώσεις λογοκλοπής ή παράλειψης αναφοράς στη μεταπτυχιακή Διπλωματική Εργασία, η ελάχιστη κύρωση, μετά από απόφαση της ΕΔΕ, είναι η υποχρέωση του φοιτητή να επιλέξει άλλον επιβλέποντα καθηγητή με διαφορετικό θέμα Διπλωματικής και να επαναλάβει το τρίτο εξάμηνο με ανάλογες πρόσθετες οικονομικές υποχρεώσεις, ενώ μέγιστη κύρωση μπορεί να είναι η οριστική διαγραφή του από το Πρόγραμμα. Εάν έχει ήδη αποφοιτήσει, ανακαλείται το Μεταπτυχιακό Δίπλωμα Ειδίκευσης και προωθείται το θέμα στο Δικαστικό Γραφείο του Πανεπιστημίου για την έναρξη των ανάλογων νομικών διαδικασιών».