ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διαχείριση Πένθους με τη χρήση Τεχνητής Νοημοσύνης

AI and Grief Management (Grieftech)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Χαράλαμπου Φουστανελλά

Επιβλέπουσα: Βασιλική Διαμαντοπούλου, Μόνιμη Επίκουρη Καθηγήτρια

Μέλη εξεταστικής επιτροπής: Κ.Μαλιάτσος, Μόνιμος Επίκουρος Καθηγητής
Χ. Αλεξόπουλος, Επίκουρος Καθηγητής

Σάμος, Μάρτιος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα Διπλωματική Εργασία εκπονήθηκε κατά τη χειμερινή περίοδο του Ακαδημαϊκού Έτους 2025-2026, στο πλαίσιο του Προπτυχιακού Προγράμματος σπουδών του Πανεπιστημίου Αιγαίου του τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων.

Η διπλωματική εργασία πραγματοποιήθηκε υπό την επίβλεψη της κας Διαμαντοπούλου Βασιλικής, η οποία είναι Μόνιμη Επίκουρη Καθηγήτρια του Τμήματος.

Αντικείμενο της διπλωματικής αποτελεί η χρήση της Τεχνητής Νοημοσύνης ως εργαλείο για την Διαχείριση του Πένθους.

Στο σημείο αυτό, οφείλω να ευχαριστήσω θερμά την επιβλέπουσα της διπλωματικής εργασίας, κα Διαμαντοπούλου Βασιλική, η οποία με καθοδήγησε και μου παρείχε την πολύτιμη βοήθειά της σε κάθε στάδιο εκπόνησης της εργασίας μου.

Τέλος, θέλω να ευχαριστήσω θερμά την οικογένεια και τους φίλους μου, για την κατανόηση και συμπαράσταση που μου έδειξαν κατά την περίοδο εκπόνησης αυτής της εργασίας.

© 2026

του

ΧΑΡΑΛΑΜΠΟΥ ΦΟΥΣΤΑΝΕΛΛΑ

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Περιεχόμενα

Περίληψη 5
Abstract 6
Λίστα Εικόνων 7
Λίστα Πινάκων 8
1 Εισαγωγή 10
2 Θεωρητικό Υπόβαθρο 15
2.1 Ορισμοί: Deathbots, Griefbots, Ghostbots 15
2.2 Ιστορική εξέλιξη των ψηφιακών αναπαραστάσεων και της ψηφιακής αθανασίας 16
2.3 Τεχνολογικές βάσεις των Deathbots, Griefbots και Ghostbots 17
2.3.1 Επεξεργασία Φυσικής Γλώσσας και Μεγάλα Γλωσσικά Μοντέλα (LLMs) 17
2.3.2 Δεδομένα ζωής και ψηφιακά ίχνη (Life-logs & Ψηφιακό αποτύπωμα) 18
2.3.3 Συναισθηματική υπολογιστική και προσομοίωση ενσυναίσθησης 18
2.3.4 Ψηφιακά avatars, φωνητική σύνθεση και πολυτροπικά συστήματα 18
2.3.5 Αρχιτεκτονική συστημάτων και αυτονομία 18
2.4 Ψυχολογική διάσταση του πένθους και αλληλεπίδραση ανθρώπου-Τεχνητής Νοημοσύνης 19
2.4.1 Το πένθος ως ψυχολογική διαδικασία 20
2.4.2 Διατήρηση δεσμών και ψηφιακή παρουσία 20
2.4.3 Συναισθηματική εμπλοκή και κίνδυνος εξάρτησης 20
2.4.4 Ανθρωπομορφισμός και αντίληψη της ΤΝ 20
2.5 Συμπεράσματα Θεωρητικού Υπόβαθρου 20
3 Deathbots, Griefbots και Ghostbots ως εργαλεία για τη Διαχείριση του Πένθους ... 22
3.1 Το φαινόμενο της ψηφιακής διαχείρισης πένθους 22
3.2 Ψυχολογικές προεκτάσεις 23
3.2.1 Συναισθηματική υποστήριξη 23
3.2.2 Κίνδυνοι εξάρτησης και παθολογικής προσκόλλησης 24
3.3 Χρήσεις σε πραγματικούς χρήστες 24
3.3.1 Project December 24
3.3.2 Replika 28
3.3.3 HereAfter AI 29
3.4 Κοινωνική αποδοχή και δημόσιος διάλογος 30
3.4.1 Κοινωνικές στάσεις απέναντι στην «ψηφιακή αθανασία» 30
3.4.2 Ρόλος των ΜΜΕ και Pop Culture 30
3.4.3 Δημόσιος διάλογος και ακαδημαϊκές παρεμβάσεις 31
3.4.4 Κοινωνική αποδοχή και μελλοντικές τάσεις 31

3.5 Ηθικά διλήμματα: εξαπάτηση, εκμετάλλευση συναισθήματος, αυθεντικότητα 31
3.5.1 Εξαπάτηση και ψευδαίσθηση παρουσίας 32
3.5.2 Εκμετάλλευση συναισθήματος και εμπορευματοποίηση του πένθους 32
3.5.3 Αυθεντικότητα της ψηφιακής ταυτότητας 32
3.5.4 Ευθύνη σχεδιασμού και ηθική λογοδοσία 33
4 Ζητήματα Ασφάλειας Συστημάτων και Προστασίας της Ιδιωτικότητας 34
4.1 Συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων 34
4.1.1 Είδη δεδομένων και βαθμός ευαισθησίας 35
4.1.2 Διαδικασίες επεξεργασίας δεδομένων 35
4.1.3 Αποθήκευση και ασφάλεια δεδομένων 35
4.1.4 Σύνδεση με την έννοια της εμπιστοσύνης 36
4.2 Δεδομένα αποθανόντων και ΓΚΠΔ 36
4.2.1 Εφαρμογή του ΓΚΠΔ σε δεδομένα αποθανόντων 36
4.2.2 Έμμεση προστασία μέσω δεδομένων ζώντων προσώπων 36
4.2.3 Νομική βάση επεξεργασίας και συναίνεση 37
4.2.4 Αρχές ΓΚΠΔ και grieftech 37
4.2.5 Ρυθμιστικά κενά και μελλοντικές εξελίξεις 37
4.3 Κίνδυνοι κυβερνοασφάλειας 37
4.3.1 Η εφαρμογή των μεθοδολογιών STRIDE και LINDDUN στα οικοσυστήματα διαχείρισης πένθους 38
4.3.2 Παραβιάσεις δεδομένων (Data Breaches) 42
4.3.3 Κακόβουλη αναπαραγωγή ταυτότητας (Identity Spoofing) 43
4.3.4 Deepfakes, griefbots και κακόβουλη χρήση AI 44
4.3.5 Αλλοίωση μοντέλων μέσω κακόβουλων δεδομένων (Model Poisoning) 44
4.3.6 Μη εξουσιοδοτημένη πρόσβαση σε μοντέλα (Unauthorized Model Access) 44
4.3.7 Ψυχολογική εκμετάλλευση χρηστών (Psychological Exploitation) 45
4.3.8 Συνολική αποτίμηση κινδύνων κυβερνοασφάλειας 45
4.4 Αρχές Privacy by Design και Secure AI Lifecycle 46
4.4.1 Privacy by Design σε grieftech συστήματα 46
4.4.2 Secure AI Lifecycle 47
4.4.3 Σύνδεση ασφάλειας, ιδιωτικότητας και ηθικής των AI συστημάτων 48
4.5 Χαρτογράφηση απειλών για Griefbots με STRIDE και LINDDUN 48
4.5.1 Ορισμός πεδίου και παραδοχές 49
4.5.2 Κατάλογος απειλών (χρήση STRIDE και LINDDUN) 50
4.5.3 Risk rating 51
4.5.4 Αντιμετώπιση Απειλών και PETs 51

4.6 Κανονιστικό Πλαίσιο (ΕΕ, ΗΠΑ, διεθνείς προσεγγίσεις) 55
4.6.1 Ευρωπαϊκή Ένωση 55
4.6.2 Ηνωμένες Πολιτείες της Αμερικής 55
4.6.3 Διεθνείς προσεγγίσεις 56
5 Επιχειρηματική Διάσταση και Νεοφυείς Επιχειρήσεις 57
5.1 Ανάλυση αγοράς: τάσεις, ανάπτυξη και καινοτομία 57
5.1.1 Τάσεις που ευνοούν την ανάπτυξη grief-tech 57
5.1.2 Στάδιο ωριμότητας και χαρακτηριστικά ζήτησης 58
5.1.3 Καινοτομία προϊόντος και διαφοροποίηση 58
5.1.4 Ανταγωνιστικό τοπίο και εμπόδια εισόδου 59
5.2 Business Models σε πλατφόρμες ψηφιακής αθανασίας 59
5.2.1 Συνδρομητικά μοντέλα 59
5.2.2 Μοντέλα εφάπαξ αγοράς και «digital legacy packages» 59
5.2.3 Freemium και staged personalization 60
5.2.4 B2B και θεσμικά μοντέλα 60
5.2.5 Δεδομένα, αξία και μακροπρόθεσμη βιωσιμότητα 60
5.3 Παρουσίαση startup οικοσυστήματος 61
5.3.1 Project December 61
5.3.2 Replika 61
5.3.3 HereAfter AI 61
5.4 Δυνατότητες κλιμάκωσης και επενδυτικό ενδιαφέρον 62
5.4.1 Παράγοντες που ευνοούν την κλιμάκωση 62
5.4.2 Παράγοντες που περιορίζουν την κλιμάκωση 62
5.4.3 Επενδυτικό ενδιαφέρον και το «governance lens» των επενδυτών 63
5.5 Επιχειρηματικοί κίνδυνοι 63
5.5.1 Νομικοί κίνδυνοι 63
5.5.2 Ηθικοί κίνδυνοι και δημόσια εικόνα 64
5.5.3 Τεχνικοί περιορισμοί και κίνδυνοι της τεχνητής νοημοσύνης 64
5.6 Προοπτικές για το μέλλον των grief-tech υπηρεσιών 64
5.6.1 Τεχνολογικές εξελίξεις και μετασχηματισμός προϊόντων 65
5.6.2 Κανονιστική ωρίμανση και θεσμική ενσωμάτωση 65
5.6.3 Μετατόπιση από «digital resurrection» σε «digital remembrance» 65
5.6.4 Επιχειρηματικές προοπτικές και στρατηγική βιωσιμότητας 65
6 Συμπεράσματα και Προτάσεις για Μελλοντική Έρευνα 67
6.1 Συνοπτικά Συμπεράσματα 67
6.2 Προτάσεις για υπεύθυνη υλοποίηση griefbots 68

6.3 Προτάσεις για περαιτέρω ερευνητική μελέτη 68

Βιβλιογραφία..... 69

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει το αναδυόμενο φαινόμενο των deathbots, griefbots και ghostbots, δηλαδή των συστημάτων τεχνητής νοημοσύνης που αξιοποιούν ψηφιακά δεδομένα αποθανόντων προσώπων με σκοπό τη διαχείριση του πένθους και τη διατήρηση της ψηφιακής μνήμης. Η μελέτη προσεγγίζει το θέμα μέσα από μία διεπιστημονική οπτική, συνδυάζοντας ζητήματα ασφάλειας πληροφοριακών συστημάτων, κανονιστικής συμμόρφωσης, ηθικής και επιχειρηματικότητας, με έμφαση στις νεοφυείς επιχειρήσεις που δραστηριοποιούνται στον χώρο του grieftech.

Αρχικά παρουσιάζεται το θεωρητικό υπόβαθρο που σχετίζεται με την ψηφιακή μεταθανάτια ταυτότητα και την εξέλιξη των συνομιλιακών συστημάτων τεχνητής νοημοσύνης. Στη συνέχεια, αναλύεται ο ρόλος των griefbots ως εργαλεία ψηφιακής διαχείρισης πένθους, με έμφαση στις ψυχολογικές προεκτάσεις, την κοινωνική αποδοχή και τα βασικά ηθικά διλήμματα που ανακύπτουν από τη χρήση τους.

Κεντρικό μέρος της εργασίας αποτελεί η ανάλυση θεμάτων ασφαλείας και ιδιωτικότητας. Πραγματοποιείται χαρτογράφηση απειλών (threat modeling) για griefbot πλατφόρμες, με βάση κλασικά και σύγχρονα πλαίσια ανάλυσης κινδύνων, και εξετάζονται ζητήματα όπως παραβιάσεις δεδομένων, παραποίηση ταυτότητας και κατάχρηση συνθετικού περιεχομένου. Παράλληλα, αναλύεται το κανονιστικό πλαίσιο, με έμφαση στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), και την Πράξη για την Τεχνητή Νοημοσύνη (AI Act), καθώς και οι επιπτώσεις τους στη σχεδίαση και λειτουργία τέτοιων συστημάτων.

Σε επιχειρηματικό επίπεδο, η εργασία εξετάζει τα βασικά επιχειρηματικά μοντέλα των grieftech πλατφορμών, τις δυνατότητες κλιμάκωσης, το επενδυτικό ενδιαφέρον και τους κυριότερους επιχειρηματικούς κινδύνους. Μέσα από την ανάλυση χαρακτηριστικών παραδειγμάτων νεοφυών επιχειρήσεων, αναδεικνύεται ότι η βιωσιμότητα του κλάδου εξαρτάται σε μεγάλο βαθμό από την εμπιστοσύνη των χρηστών, τη διαφάνεια και την υπεύθυνη υλοποίηση της Τεχνητής Νοημοσύνης.

Τέλος, η εργασία καταλήγει στο συμπέρασμα ότι τα griefbots αποτελούν μια τεχνολογικά ώριμη αλλά κοινωνικά ευαίσθητη καινοτομία. Η μελλοντική τους πορεία θα καθοριστεί όχι μόνο από την τεχνολογική πρόοδο, αλλά και από την ικανότητα των επιχειρήσεων και των θεσμών να θέσουν σαφή όρια, να διασφαλίσουν την προστασία των χρηστών και να ενσωματώσουν αρχές υπεύθυνης τεχνητής νοημοσύνης.

Abstract

This thesis examines the emerging phenomenon of deathbots, griefbots, and ghostbots, i.e., artificial intelligence systems that use the digital data of deceased persons for the purpose of managing grief and preserving digital memory. The study approaches the subject from an interdisciplinary perspective, combining issues of information system security, regulatory compliance, ethics, and entrepreneurship, with an emphasis on start-ups active in the field of grieftech.

First, the theoretical background related to digital posthumous identity and the evolution of conversational artificial intelligence systems is presented. Next, the role of griefbots as tools for managing digital grief is analyzed, with an emphasis on the psychological impact, social acceptance, and key ethical dilemmas arising from their use.

A central part of the thesis is the analysis of security and privacy issues. Threat modeling for griefbot platforms is carried out, based on classical and contemporary risk analysis frameworks, and issues such as data breaches, identity theft, and synthetic content abuse are examined. At the same time, the regulatory framework is analyzed, with an emphasis on the GDPR for artificial intelligence (AI Act), as well as its impact on the design and operation of such systems

At the business level, the paper examines the basic business models of grieftech platforms, their scalability, investment interest, and key business risks. Through the analysis of representative examples of start-ups, it is clear that the sustainability of the industry depends largely on user trust, transparency, and the responsible application of artificial intelligence.

Finally, the paper concludes that griefbots are a technologically mature but socially sensitive innovation. Their future trajectory will be determined not only by technological progress, but also by the ability of companies and institutions to set clear boundaries, ensure user protection, and incorporate the principles of responsible artificial intelligence.

Λίστα Εικόνων

Εικόνα 1 Συστήμα ΤΝ με σκοπό τη διαχείριση πένθους 11
Εικόνα 2: Σύντομη επεξήγηση των εννοιών Grief-tech σε μορφή σχήματος 16
Εικόνα 3: Project December Αρχική Σελίδα 25
Εικόνα 4: Υποσημείωση Χρήσης του Project December 25
Εικόνα 5: Project December – Στοιχεία προς Συμπλήρωση 26
Εικόνα 6: Project December - Τι προσφέρει 26
Εικόνα 7: Project December – Πρώτη αλληλεπίδραση 27
Εικόνα 8: Project December – Απόσπασμα από συνομιλία (1) 27
Εικόνα 9: Project December – Απόσπασμα από συνομιλία(2) 28
Εικόνα 10: Replika – Αρχική Σελίδα 28
Εικόνα 11: Πληροφορίες σχετικά με το Replika 29
Εικόνα 12: Here After AI 29
Εικόνα 13: ΔΡΔ Επιπέδου 1 49

Λίστα Πινάκων

Πίνακας 1: Πιθανοί Κίνδυνοι των grief-tech εφαρμογών 46
Πίνακας 2: Κατάλογος Απειλών 50
Πίνακας 3: Υπολογισμός Ρίσκου 51
Πίνακας 4: LINDDUN & PETs 55

Ακρωνύμια

TN/AI	Τεχνητή Νοημοσύνη (Artificial Intelligence)
API	Application Programming Interface
DB	Database, Βάση δεδομένων
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GPAI	General Purpose Artificial Intelligence
LINDDUN	Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance
LLM/LLMs	Large Language Model(s)
MFA	Multi-Factor Authentication
NLP	Natural Language Processing
OAuth	Open Authorization
OECD	Organization for Co-operation & Development
PETs	Privacy Enhancing Technologies
R&D	Research & Development
SME	Small & Medium Enterprises
STRIDE	Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege

1

Εισαγωγή

Η ραγδαία ανάπτυξη της Τεχνητής Νοημοσύνης (ΤΝ) και των Μεγάλων Γλωσσικών Μοντέλων (LLMs) τα τελευταία χρόνια έχει οδηγήσει στη δημιουργία μίας νέας κατηγορίας ψηφιακών εφαρμογών, οι οποίες επεκτείνουν τα όρια της ανθρώπινης εμπειρίας ακόμη και πέρα του θανάτου. Τα λεγόμενα deathbots, griefbots ή ghostbots, αποτελούν τεχνολογίες που αξιοποιούν μηχανική μάθηση, επεξεργασία φυσικής γλώσσας και ανάλυση δεδομένων για να αναπαριστούν τη φωνή, τη γλώσσα ή την προσωπικότητα ατόμων που δε βρίσκονται πλέον εν ζωή, επιτρέποντας σε συγγενείς και φίλους του ατόμου να προσομοιώσουν την επικοινωνία μαζί τους μέσω ψηφιακών μέσων. Η ιδέα αυτή, που κάποτε ήταν σενάριο επιστημονικής φαντασίας, αποτελεί σήμερα μία αναδυόμενη αγορά τεχνολογιών πένθους (grief technologies/grieftech), με αυξανόμενο αριθμό νεοφυών επιχειρήσεων να δραστηριοποιούνται στον χώρο αγοράς **[1]**.

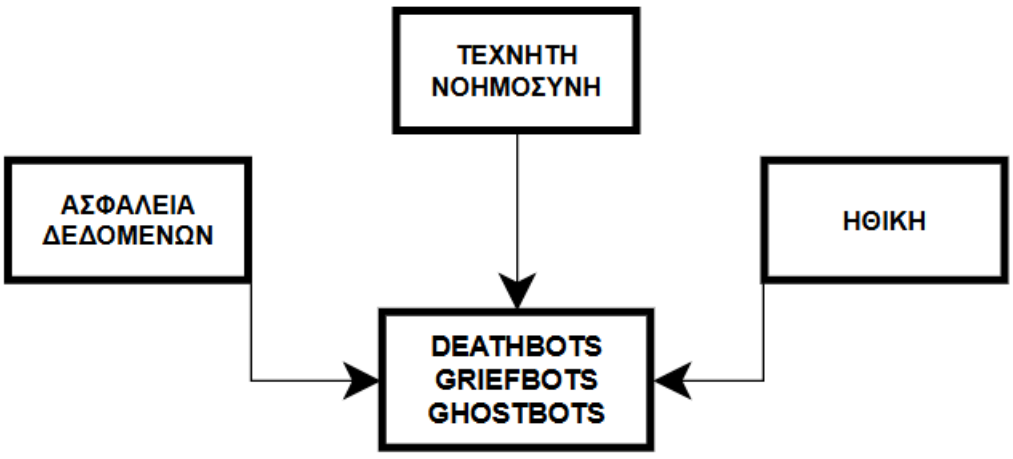
Η εμφάνιση αυτών των τεχνολογιών δεν είναι μεμονωμένο φαινόμενο, αλλά αποτέλεσμα της ευρύτερης πολιτισμικής και τεχνολογικής μετατόπισης προς την ψηφιακή αθανασία (digital immortality). Ψηφιακά μέσα κοινωνικής δικτύωσης, πλατφόρμες αποθήκευσης προσωπικών δεδομένων και μοντέλα ΤΝ που μπορούν να εκπαιδευτούν με βάση τα δεδομένα ενός ατόμου, έχουν κάνει πλέον εφικτή την αναπαράσταση της ταυτότητας μετά τον θάνατο. Εταιρείες όπως η **[2]** HereAfter AI και η **[3]** Project December (νεοφυείς επιχειρήσεις), έχουν αναπτύξει εφαρμογές που επιτρέπουν στους χρήστες να δημιουργούν ψηφιακούς «εαυτούς» που παραμένουν ενεργοί και μετά τον φυσικό θάνατό τους **[4].** Αυτή η νέα βιομηχανία, γνωστή ως grieftech, αναπτύσσεται με ταχύ ρυθμό και εκτιμάται ότι θα αποτελέσει σημαντικό κομμάτι της ευρύτερης αγοράς συναισθηματικών τεχνολογιών τα επόμενα χρόνια.

Η εξάπλωση των deathbots και griefbots, ωστόσο, συνοδεύεται από σοβαρά ζητήματα ηθικής, ασφάλειας και ιδιωτικότητας. Η τεχνολογία που επιτρέπει την προσομοίωση της επικοινωνίας με

αποθανόντες χρησιμοποιεί προσωπικά δεδομένα, όπως μηνύματα, φωνητικά αρχεία, βίντεο και φωτογραφίες, τα οποία συχνά συλλέγονται χωρίς ρητή συγκατάθεση ή σαφή νομική ρύθμιση για χρήση μετά τον θάνατο. Πέρα από τα τεχνικά ζητήματα προστασίας δεδομένων (data protection), προκύπτουν ψυχολογικές και κοινωνικές προκλήσεις, καθώς η συνεχής επαφή με ένα ψηφιακό ομοίωμα του αποθανόντος μπορεί να παρατείνει ή να αλλοιώσει τη διαδικασία πένθους **[5]**. Οι ερευνητές Hollanek **[4]** και Figueroa-Torres **[1]** επισημάνουν ότι τέτοια συστήματα ενδέχεται να δημιουργούν ψευδαίσθηση παρουσίας, επηρεάζοντας την ψυχική υγεία των χρηστών και να προκαλούν εξάρτηση από ψηφιακές οντότητες ως υποκατάστατο ανθρώπινης ζωής.

Από την άλλη πλευρά, δεν μπορεί να αγνοηθεί η οικονομική και επιχειρηματική δυναμική του φαινομένου. Νεοφυείς επιχειρήσεις και start-ups σε ΗΠΑ, Ευρώπη και Ασία αναπτύσσουν ολοένα και πιο εξελιγμένα griefbots με συνδρομητικά μοντέλα ή υπηρεσίες εξατομίκευσης, δημιουργώντας μια νέα αγορά συναισθηματικής τεχνολογίας. Η εμπορευματοποίηση του πένθους, όμως, θέτει ερωτήματα σχετικά με την ηθική της καινοτομίας και την υπευθυνότητα των επιχειρήσεων που δραστηριοποιούνται σε αυτόν τον ευαίσθητο χώρο **[1]**. Παράλληλα, τα νομικά πλαίσια που αφορούν την ψηφιακή κληρονομιά (digital legacy) και τη μεταθανάτια χρήση των προσωπικών δεδομένων παραμένουν «θολά», με αποτέλεσμα να αυξάνει την ανασφάλεια τόσο για τους καταναλωτές όσο και για τους ίδιους τους δημιουργούς αυτών των συστημάτων.

Η μελέτη αυτών των ζητημάτων καθίσταται κρίσιμη, καθώς συνδέει δύο φαινομενικά διαφορετικούς, αλλά αλληλένδετους τομείς: την κυβερνοασφάλεια και την επιχειρηματικότητα. Από τη μία πλευρά, τα griefbots αποτελούν ένα νέο πεδίο για την ανάλυση κινδύνων που αφορούν ευαίσθητα προσωπικά δεδομένα, μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ταυτότητας και κακόβουλη χρήση ΤΝ. Στον αντίποδα, οι εταιρείες που αναπτύσσουν αυτές τις εφαρμογές λειτουργούν μέσα σε ένα ανταγωνιστικό και καινοτόμο επιχειρηματικό περιβάλλον, όπου η διαχείριση εμπιστοσύνης των χρηστών και η συμμόρφωση με ηθικά πρότυπα μπορεί να αποτελούν ανταγωνιστικό πλεονέκτημα ή κίνδυνο. Έτσι, η παρούσα εργασία στοχεύει να αναδείξει την αλληλεπίδραση μεταξύ ασφάλειας και επιχειρηματικής στρατηγικής στο οικοσύστημα των griefbots.



Εικόνα 1 Συστήμα ΤΝ με σκοπό τη διαχείριση πένθους

Σκοπός και στόχοι της έρευνας

Ο βασικός σκοπός της παρούσας διπλωματικής εργασίας είναι η διερεύνηση του φαινομένου των Deathbots, Griefbots και Ghostbots ως μορφών διαχείρισης πένθους, μέσα από το πρίσμα της ασφάλειας πληροφοριών και της επιχειρηματικής ανάπτυξης. Η εργασία επιδιώκει να χαρτογραφήσει την υφιστάμενη κατάσταση, να αναλύσει τις προκλήσεις και να αναδείξει πιθανές κατευθύνσεις υπεύθυνης και βιώσιμης ανάπτυξης τέτοιων συστημάτων.

Πιο συγκεκριμένα, οι επιμέρους στόχοι είναι:

- Να οριστούν και να διαφοροποιηθούν οι έννοιες των deathbots, griefbots και ghostbots
- Να εξεταστούν τα ζητήματα ασφάλειας, ιδιωτικότητας και ηθικής που προκύπτουν από τη χρήση αυτών των τεχνολογιών.
- Να αναλυθεί η επιχειρηματική διάσταση, δηλαδή το πώς οι νεοφυείς εταιρείες εκμεταλλεύονται το grieftech οικοσύστημα και ποια επιχειρηματικά μοντέλα εφαρμόζουν.
- Να παρουσιαστούν οι κίνδυνοι και οι ευκαιρίες που απορρέουν για τον τομέα της ΤΝ, την κοινωνία και την αγορά.

Μεθοδολογία Έρευνας

Η εργασία βασίζεται σε βιβλιογραφική έρευνα, με συστηματική ανασκόπηση ακαδημαϊκών πηγών, δημοσιευμένων άρθρων, επιχειρηματικών περιπτώσεων (case studies) και νομικών/ρυθμιστικών κειμένων. Ιδιαίτερη έμφαση δίνεται στην επιστημονική τεκμηρίωση από βάσεις δεδομένων (όπως το Google Scholar), καθώς και στην ανάλυση δημοσιευμένων στοιχείων από εταιρείες του χώρου (HereAfter AI, Project December, Replika). Η επιλογή αυτής της μεθόδου οφείλεται στην έλλειψη ερευνών πάνω στο αντικείμενο και στην ανάγκη ολιστικής αποτίμησης του θέματος.

Δομή της εργασίας

Η παρούσα διπλωματική εργασία οργανώνεται σε έξι διακριτά κεφάλαια, τα οποία ακολουθούν μια λογική, κλιμακωτή και συνεκτική διάρθρωση, με στόχο τη συστηματική διερεύνηση των τεχνολογικών, ηθικών, επιχειρηματικών και ζητημάτων ασφάλειας που σχετίζονται με τα deathbots, griefbots και ghostbots. Η δομή αυτή επιτρέπει την προοδευτική ανάπτυξη του ερευνητικού αντικειμένου, από τη θεωρητική θεμελίωση έως τη συνθετική αποτίμηση των ευρημάτων, συμβάλλοντας στη συνολική κατανόηση του φαινομένου της ψηφιακής διαχείρισης πένθους μέσω τεχνητής νοημοσύνης.

Το πρώτο Κεφάλαιο λειτουργεί ως εισαγωγή της εργασίας και παρουσιάζει το αντικείμενο μελέτης, τους στόχους και τα κεντρικά ερευνητικά ερωτήματα. Επιπλέον, περιγράφεται η μεθοδολογία που ακολουθείται, η οποία βασίζεται σε βιβλιογραφική έρευνα (desktop research), ενώ οριοθετείται το θεωρητικό και πρακτικό πλαίσιο της μελέτης. Το κεφάλαιο αυτό θέτει τις βάσεις για την κατανόηση ενός ταχέως αναπτυσσόμενου και διεπιστημονικού πεδίου, εισάγοντας τον αναγνώστη στη θεματική της ψηφιακής διαχείρισης πένθους.

Το Κεφάλαιο 2 εστιάζει στο θεωρητικό υπόβαθρο και αποτελεί τη βιβλιογραφική βάση της εργασίας. Παρουσιάζονται οι βασικοί ορισμοί και η ιστορική εξέλιξη των deathbots, griefbots και ghostbots, καθώς και οι θεμελιώδεις τεχνολογίες που καθιστούν δυνατή τη δημιουργία ψηφιακών

μεταθανάτιων αναπαραστάσεων, όπως τα ψηφιακά ίχνη και οι μηχανισμοί προσωποποίησης. Παράλληλα, αναλύονται θεωρητικά και ηθικά πλαίσια που σχετίζονται με την ψηφιακή αθανασία και την κοινωνική ρομποτική, παρέχοντας τα εννοιολογικά εργαλεία που αξιοποιούνται στις επόμενες ενότητες.

Το Κεφάλαιο 3 εξετάζει τη λειτουργική και κοινωνικό-τεχνολογική διάσταση των deathbots, griefbots και ghostbots ως εργαλεία διαχείρισης πένθους. Αναλύονται τα μοντέλα αλληλεπίδρασης, οι πιθανές χρήσεις και οι ψυχολογικές επιδράσεις στους χρήστες, ενώ παρουσιάζονται ενδεικτικές μελέτες περίπτωσης (case studies) από υφιστάμενες πλατφόρμες και εφαρμογές. Επιπλέον, συζητούνται κρίσιμα ηθικά ζητήματα, όπως η αυθεντικότητα της ψηφιακής αναπαράστασης, ο κίνδυνος συναισθηματικής εξάρτησης και η πιθανότητα παραπλάνησης, φωτίζοντας τον τρόπο με τον οποίο οι τεχνολογίες αυτές επηρεάζουν την ανθρώπινη εμπειρία του πένθους.

Το Κεφάλαιο 4 επικεντρώνεται στα ζητήματα ασφάλειας πληροφοριακών συστημάτων, ιδιωτικότητας και κανονιστικής συμμόρφωσης. Αναλύονται οι απαιτήσεις προστασίας που αφορούν την επεξεργασία προσωπικών δεδομένων θανόντων και των φυσικών προσώπων που αλληλοεπιδρούν με τα griefbots, οι κυριότεροι κίνδυνοι κυβερνοασφάλειας και τα πιθανά σενάρια κακόβουλης χρήσης, όπως παραβιάσεις δεδομένων, παραποίηση ταυτότητας και adversarial επιθέσεις. Το κεφάλαιο αυτό αναδεικνύει τους τεχνικούς και νομικούς κινδύνους που συνοδεύουν την ανάπτυξη των griefbots και αξιολογεί τη συμμόρφωσή τους με σύγχρονες αρχές ασφαλούς και υπεύθυνης τεχνητής νοημοσύνης.

Το Κεφάλαιο 5 εστιάζει στην επιχειρηματική διάσταση του φαινομένου και εξετάζει το οικοσύστημα νεοφυών επιχειρήσεων που δραστηριοποιούνται στον χώρο της ψηφιακής αθανασίας και του grief-tech. Αναλύονται οι τάσεις της αγοράς, τα κυρίαρχα επιχειρηματικά μοντέλα, οι δυνατότητες κλιμάκωσης και το επενδυτικό ενδιαφέρον, καθώς και παραδείγματα χαρακτηριστικών startups, όπως το Project December και η HereAfter AI. Παράλληλα, εξετάζονται οι επιχειρηματικοί, νομικοί και ηθικοί κίνδυνοι που αντιμετωπίζουν οι επιχειρήσεις του κλάδου, συνδέοντας την τεχνολογική καινοτομία με τις πραγματικές οικονομικές και θεσμικές συνθήκες της αγοράς.

Τέλος, παρουσιάζονται τα συμπεράσματα της εργασίας όπου συνοψίζονται τα βασικά ευρήματα όλων των προηγούμενων κεφαλαίων. Παράλληλα, διατυπώνονται προτάσεις για την υπεύθυνη ανάπτυξη και χρήση των griefbots, καθώς και κατευθύνσεις για μελλοντική ερευνητική μελέτη, λαμβάνοντας υπόψη τη δυναμική και ταχέως εξελισσόμενη φύση του τομέα. Το κεφάλαιο αυτό ολοκληρώνει τη μελέτη, αναδεικνύοντας τόσο τις δυνατότητες όσο και τις προκλήσεις που συνοδεύουν τη χρήση τεχνητής νοημοσύνης στη διαχείριση του πένθους.

Με την παραπάνω διάρθρωση, η εργασία υιοθετεί μια ολοκληρωμένη και πολύ-επίπεδη προσέγγιση, εξετάζοντας τα deathbots, griefbots και ghostbots από ιστορική, τεχνολογική, κοινωνική, ηθική, επιχειρηματική και οπτική ασφάλειας, με στόχο τη σφαιρική και κριτική κατανόηση του φαινομένου.

Οριοθέτηση και Περιορισμοί

Η θεματική περιοχή της ψηφιακής αθανασίας, των προσωπικών δεδομένων τόσο των φυσικών προσώπων όσο και αποθανόντων, και της χρήσης Τεχνητής Νοημοσύνης για τη διαχείριση πένθους είναι ιδιαίτερα εκτεταμένη και πολυδιάστατη, επομένως, η εργασία οριοθετείται σε συγκεκριμένα πεδία προκειμένου να διατηρήσει αναλυτική συνοχή και επιστημονική ακρίβεια.

Πρώτον, η ανάλυση επικεντρώνεται αποκλειστικά σε συστήματα που χρησιμοποιούν ψηφιακά δεδομένα ατόμων (π.χ. μηνύματα, φωτογραφίες, ηχητικό υλικό, προφίλ κοινωνικών δικτύων) για την ανακατασκευή συνομιλιακών μοντέλων μετά τον θάνατο του υποκειμένου. Δεν εξετάζονται τεχνολογίες επαυξημένης ή εικονικής πραγματικότητας που δημιουργούν τρισδιάστατες αναπαραστάσεις (VR avatars) ούτε λύσεις που ενσωματώνουν ρομποτικό υλικό, αυτές μπορεί να μνημονευτούν επικουρικά, αλλά δεν αποτελούν αντικείμενο εις βάθος μελέτης.

Δεύτερον, η έρευνα δεν συμπεριλαμβάνει εκτεταμένη ψυχολογική ή κλινική ανάλυση του πένθους και της ανθρώπινης θλίψης, καθώς αυτό εμπίπτει στον κλάδο της ψυχοθεραπείας και της ψυχολογικής συμβουλευτικής. Ενώ γίνεται αναφορά στις βασικές ψυχολογικές επιδράσεις και στους κινδύνους συναισθηματικής εξάρτησης, η εργασία δεν υιοθετεί θεραπευτικό ή κλινικό προσανατολισμό, αλλά εξετάζει τα φαινόμενα μέσα από το πρίσμα της κοινωνικής τεχνολογίας και της ηθικής της Τεχνητής Νοημοσύνης.

Τρίτον, η μελέτη περιορίζεται σε δημόσια διαθέσιμες πληροφορίες, ακαδημαϊκά άρθρα, τεχνικές αναφορές, δημοσιευμένα περιστατικά χρήσης και επίσημα επιχειρηματικά στοιχεία νεοφυών επιχειρήσεων. Δεν πραγματοποιείται πρωτογενής έρευνα, όπως συνεντεύξεις χρηστών, έρευνες πεδίου ή ποσοτικές μετρήσεις, καθώς αυτό υπερβαίνει το πλαίσιο και το σκοπό της εργασίας.

Τέταρτον, η αξιολόγηση των ζητημάτων ασφάλειας βασίζεται στο ισχύον ρυθμιστικό πλαίσιο (όπως ο ΓΚΠΔ για την ΕΕ) και στις βασικές αρχές των μεθοδολογιών απαιτήσεων ασφάλειας και ιδιωτικότητας STRIDE και LINDDUN. Ωστόσο, το πεδίο των deathbots,ghostbots και griefbots βρίσκεται σε ταχεία εξέλιξη, γεγονός που σημαίνει ότι οι νομοθετικές ρυθμίσεις και τα πρότυπα ενδέχεται να μεταβληθούν στο άμεσο μέλλον. Η εργασία, επομένως, αντανακλά την κατάσταση έως και τον χρόνο συγγραφής της και όχι ενδεχόμενες μελλοντικές αλλαγές.

Τέλος, ως προς την επιχειρηματική ανάλυση, παρουσιάζονται ενδεικτικά δείγματα από startups που δραστηριοποιούνται στον χώρο των AI memorial services, grieftech και digital afterlife solutions. Η μελέτη δεν αποσκοπεί στην πλήρη απογραφή όλων των επιχειρήσεων παγκοσμίως, αλλά στην ανάδειξη αντιπροσωπευτικών παραδειγμάτων που αποτυπώνουν τις τρέχουσες τάσεις της αγοράς.

Συνολικά, οι οριοθετήσεις αυτές κρίνονται αναγκαίες ώστε η εργασία να παραμείνει εστιασμένη στους βασικούς άξονες μελέτης (ασφάλεια, ηθική και επιχειρηματικότητα) και να προσφέρει μια τεκμηριωμένη, σαφή και συνεκτική προσέγγιση σε ένα νέο και πολυδιάστατο τεχνολογικό φαινόμενο.

2

Θεωρητικό Υπόβαθρο

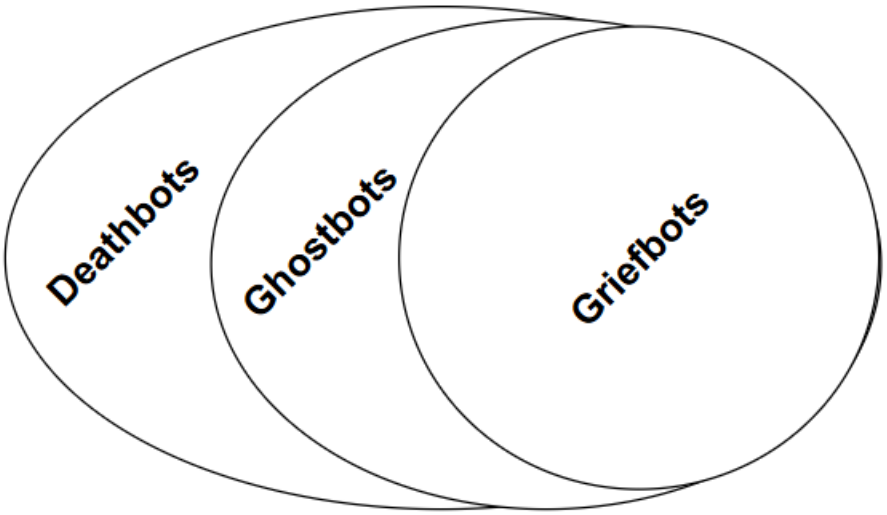
2.1 Ορισμοί: Deathbots, Griefbots, Ghostbots

Η ανάπτυξη συστημάτων τεχνητής νοημοσύνης που αναπαριστούν ψηφιακά άτομα μετά τον θάνατό τους έχει οδηγήσει στη δημιουργία μιας νέας κατηγορίας τεχνολογικών εφαρμογών, που συχνά περιγράφονται με όρους όπως deathbots, griefbots και ghostbots. Αν και οι όροι αυτοί χρησιμοποιούνται συχνά εναλλακτικά, έχουν σαφείς λειτουργικές και εννοιολογικές διαφορές **[7]**. Ο όρος deathbot αναφέρεται σε ένα chatbot που βασίζεται σε προηγμένα γλωσσικά μοντέλα και έχει εκπαιδευτεί με βάση τα προσωπικά δεδομένα ενός αποθανόντος ατόμου (π.χ. μηνύματα, φωτογραφίες, ηχογραφήσεις φωνής) με στόχο τη δημιουργία μιας ψηφιακής αναπαράστασης που μιμείται το στυλ, τις εκφράσεις και τον τρόπο σκέψης του. Αυτά τα συστήματα αποτελούν μια μορφή «ψηφιακής αθανασίας», όπου ο ψηφιακός εαυτός συνεχίζει να υπάρχει.

Τα griefbots ανήκουν στην κατηγορία των deathbots, και έχουν ως κύριο στόχο την παροχή συναισθηματικής υποστήριξης στους χρήστες όσο αυτοί πενθούν. Αντίθετα με τα deathbots, τα griefbots εστιάζουν πιο πολύ στην ψυχολογική διάσταση της αλληλεπίδρασης και μπορεί να ενσωματώνουν στοιχεία συνομιλητικής ενσυναίσθησης για να προσφέρουν ψυχική ανακούφιση.

Η έννοια ghostbot, περιγράφει οποιοδήποτε αυτοματοποιημένο σύστημα ή ψηφιακό «avatar» που συνεχίζει να λειτουργεί μετά τον θάνατο ενός ατόμου, χωρίς να στοχεύει απαραίτητα στην διαχείριση του πένθους. Αυτά, μπορεί να βασίζονται σε λιγότερο εξατομικευμένα δεδομένα και να λειτουργούν ως ψηφιακή «σκιά» του χρήστη, η οποία παραμένει ενεργή σε διαδικτυακά περιβάλλοντα για αλληλεπίδραση.

Ενώ όλα επικεντρώνονται στο θέμα της «ψηφιακής αθανασίας», αξίζει να σημειωθεί πως ο όρος deathbot είναι ο πιο γενικός, στη συνέχεια ακολουθεί η έννοια ghostbot και στο τέλος τα griefbots:



Εικόνα 2: Σύντομη επεξήγηση των εννοιών Grief-tech σε μορφή σχήματος

2.2 Ιστορική εξέλιξη των ψηφιακών αναπαραστάσεων και της ψηφιακής αθανασίας

Η ψηφιακή αναπαράσταση της ανθρώπινης ταυτότητας δεν είναι αποκλειστικό προϊόν της σύγχρονης τεχνητής νοημοσύνης. Με μία αναδρομή στο παρελθόν, το έτος 1992 εμφανίστηκε για πρώτη φορά φωτογραφία στο διαδίκτυο από επιστήμονα της CERN **[6]** και από τότε η πορεία της έχει εξελιχθεί σταδιακά μέσω προόδων στις ψηφιακές τεχνολογίες, στα μέσα επικοινωνίας και στη διαχείριση προσωπικών δεδομένων. Για να γίνει πιο ευνόητη η εμφάνιση των deathbots griefbots και ghostbots, αρκεί να εξετάσουμε το ιστορικό πλαίσιο της ψηφιακής αθανασίας:

Πρώιμες μορφές ψηφιακής μνήμης και μεταθανάτιας παρουσίας:
Οι πρώτες ψηφιακές μορφές εμφανίστηκαν στα τέλη της δεκαετίας του 1990 με την εξάπλωση των προσωπικών ιστοσελίδων, των φόρουμ και αργότερα των κοινωνικών δικτύων. Έτσι, οι χρήστες μπορούσαν να αφήνουν τα αποτυπώματά τους με κείμενα και φωτογραφίες προσβάσιμα ακόμη και μετά τον θάνατο, με αποτέλεσμα να έχουμε τις πρώτες ανεπίσημες μορφές ψηφιακής μεταθανάτιας παρουσίας, τα διαδικτυακά μνημεία **[24]**.

Εκείνη την περίοδο, η ψηφιακή αναπαράσταση ήταν στατική και παθητική, με αποτέλεσμα το άτομο να έχει ψηφιακή παρουσία ως αρχείο μνήμης αλλά να μην υπάρχει δυνατότητα προσομοίωσης της επικοινωνίας. Ωστόσο, η συσσώρευση προσωπικών δεδομένων θεμελίωσε μελλοντικές, δυναμικότερες μορφές ψηφιακής ταυτότητας **[8]**.

Από την ψηφιακή μνήμη στη διαδραστική αναπαράσταση:
Σε επόμενη φάση, αναπτύχθηκαν διαλογικοί πράκτορες ή chatbots, που στην αρχή αξιοποιήθηκαν για την εξυπηρέτηση πελατών ή και την ψυχαγωγία. Έτσι, άνοιξε ο δρόμος για τη δημιουργία διαδραστικών ψηφιακών αναπαραστάσεων ανθρώπων, που βασίζονται σε ιστορικά δεδομένα επικοινωνίας.

Κατά τη διάρκεια της δεκαετίας του 2010, ερευνητικά και εμπορικά έργα άρχισαν να πειραματίζονται με την ιδέα της «συνέχισης της συνομιλίας» μετά τον θάνατο, χρησιμοποιώντας

αρχεία καταγραφής συνομιλιών, μηνύματα ηλεκτρονικού ταχυδρομείου και αναρτήσεις σε μέσα κοινωνικής δικτύωσης. Η έννοια της μεταθανάτιας επικοινωνίας απέκτησε πρακτική σημασία, μετατρέποντας την ψηφιακή μνήμη σε ενεργή αλληλεπίδραση.

Κατά τη διάρκεια της δεκαετίας του 2010 άρχισε ο πειραματισμός με την ιδέα της μεταθανάτιας επικοινωνίας χρησιμοποιώντας αρχεία καταγραφής επικοινωνίας, ηλεκτρονικά μηνύματα και αναρτήσεις σε μέσα κοινωνικής δικτύωσης. Η μεταθανάτια επικοινωνία απέκτησε πρακτική σημασία, μετατρέποντας την ψηφιακή μνήμη σε αλληλεπίδραση **[7]**.

Η εμφάνιση της ψηφιακής αθανασίας και των μεταθανάτιων πρακτόρων τεχνητής νοημοσύνης:
Με τη συνεχή ανάπτυξη της μηχανικής μάθησης και των μεγάλων γλωσσικών μοντέλων (LLMs), η ψηφιακή αθανασία έγινε από θεωρία πράξη. Η ψηφιακή αθανασία συντηρείται μέσω της αναπαραγωγής στοιχείων και διατήρησής τους από υπολογιστικά συστήματα με τη δυνατότητα μάθησης, προσαρμογής και αλληλεπίδρασης με δεδομένα.

Σε αυτό το πλαίσιο, έχουν εμφανιστεί μεταθανάτιοι πράκτορες τεχνητής νοημοσύνης, δηλαδή αυτόνομοι ή ημιαυτόνομοι πράκτορες που συνεχίζουν να λειτουργούν μετά τον θάνατο του φυσικού προσώπου. Αυτοί οι πράκτορες αποτελούν τη βάση πάνω στην οποία λειτουργούν τα griefbots, ghostbots και deathbots.

Με αφορμή αυτό, έχουν εμφανιστεί πολλοί μεταθανάτιοι πράκτορες ΤΝ, είτε αυτόνομοι είτε ημιαυτόνομοι που λειτουργούν ακόμη και μετά τον θάνατο του ατόμου. Αυτοί οι πράκτορες αποτελούν τη βάση στην οποία στηρίζεται η ιδέα της ψηφιακής αθανασίας και της ανάγκης του ανθρώπου να πενθεί.

2.3 Τεχνολογικές βάσεις των Deathbots, Griefbots και Ghostbots

Η λειτουργία των Deathbots, Griefbots και Ghostbots βασίζεται σε συνδυασμό σύγχρονων τεχνολογιών τεχνητής νοημοσύνης, επεξεργασίας φυσικής γλώσσας και ψηφιακής αναπαράστασης ταυτότητας. Αυτά δεν αποτελούν ενιαία τεχνολογική λύση, αλλά σε συνδυασμό σύνθετων αρχιτεκτονικών, ενοποιώντας πολλαπλά υποσυστήματα, προσομοιώνουν την ανθρώπινη επικοινωνία και συμπεριφορά.

2.3.1 Επεξεργασία Φυσικής Γλώσσας και Μεγάλα Γλωσσικά Μοντέλα (LLMs)

Τα Μεγάλα Γλωσσικά Μοντέλα (Large Language Models – LLMs) αποτελούν παραμετρικά μοντέλα μηχανικής μάθησης μεγάλης κλίμακας, τα οποία υλοποιούνται κυρίως με αρχιτεκτονικές Transformer και εκπαιδεύονται μέσω αυτό-επιβλεπόμενης μάθησης σε εκτενή σύνολα δεδομένων φυσικής γλώσσας. Η εκπαίδευσή τους βασίζεται στην πρόβλεψη της επόμενης λέξης (token) σε ακολουθίες κειμένου, επιτρέποντάς τους να μαθαίνουν κατανομές πιθανοτήτων, συντακτικές δομές και σημασιολογικές συσχετίσεις της γλώσσας.

Λόγω του μεγάλου αριθμού παραμέτρων και της κλιμακούμενης εκπαίδευσης, τα LLMs εμφανίζουν αναδυόμενες ικανότητες γενίκευσης και μπορούν να προσαρμόζονται σε ποικίλες γλωσσικές εργασίες χωρίς εκ νέου εκπαίδευση.

Στον πυρήνα των περισσότερων Deathbots, Ghostbots και Griefbots συναντάμε τεχνολογίες NLP και πλέον LLMs, Τα μοντέλα αυτά εκπαιδεύονται σε τεράστιους όγκους δεδομένων και έχουν την ικανότητα να παράγουν φυσικό και συνεκτικό λόγο **[9]**.

Στην περίπτωση των posthumous AI πρακτόρων, τα LLMs προσαρμόζονται σε προσωπικά δεδομένα του αποθανόντος όπως συνομιλίες, email ή αναρτήσεις σε κοινωνικά δίκτυα, με στόχο να είναι εφικτή η προσομοίωση του ύφους και λεξιλογίου του ατόμου. Η διαδικασία αυτή μετατρέπει ένα γενικό γλωσσικό μοντέλο σε μία εξατομικευμένη ψηφιακή περσόνα.

2.3.2 Δεδομένα ζωής και ψηφιακά ίχνη (Life-logs & Ψηφιακό αποτύπωμα)

Η ποιότητα και η αυθεντικότητα ενός deathbot εξαρτάται από το σύνολο των δεδομένων στα οποία βασίζεται. Τα λεγόμενα life-logs περιλαμβάνουν γραπτό λόγο, ηχητικά αποσπάσματα, βίνετο, εικόνες και μετα-δεδομένα συμπεριφοράς, που συλλέγονται από τη διάρκεια της ζωής του ανθρώπου **[7]**.

Τα δεδομένα αυτά λειτουργούν ως πρώτη ύλη της εκπαίδευσης και παραμετροποίησης των μοντέλων, αλλά εγείρουν κρίσιμα ζητήματα ακρίβειας, ελλιπούς αναπαράστασης και μεροληψίας. Ένα ψηφιακό αποτύπωμα δεν αντιστοιχεί πλήρως σε ανθρώπινη ταυτότητα, αλλά σε μία επιλεγμένη και αποσπασματική εκδοχή της.

2.3.3 Συναισθηματική υπολογιστική και προσομοίωση ενσυναίσθησης

Ιδιαίτερα στα griefbots, ενσωματώνονται τεχνικές Affective Computing, που στοχεύουν στην αναγνώριση και απόκριση σε συναισθηματικά φορτισμένο λόγο. Μέσω ανάλυσης συναισθήματος (sentiment analysis), ανίχνευσης τόνου και προσαρμογής απαντήσεων, τα συστήματα επιχειρούν να προσφέρουν μια μορφή τεχνητής ενσυναίσθησης.

Η ικανότητα των συστημάτων να παράγουν συναισθηματικά κατάλληλες απαντήσεις δημιουργεί την ψευδαίσθηση συναισθηματικής κατανόησης και συμπόνιας, ενισχύοντας τη συναισθηματική εμπλοκή του χρήστη, αποτελώντας κρίσιμο παράγοντα στη διαχείριση πένθους.

2.3.4 Ψηφιακά avatars, φωνητική σύνθεση και πολυτροπικά συστήματα

Πέρα από κείμενο, σύγχρονα deathbots και ghostbots ενσωματώνουν πολυτροπικές τεχνολογίες, όπως φωνητική σύνθεση, αναπαραγωγή προσώπου και τρισδιάστατα avatars. Η χρήση τεχνολογιών text-to-speech και voice cloning επιτρέπει την αναπαραγωγή της φωνής του αποθανόντος, αυξάνοντας την αίσθηση παρουσίας.

Τα ψηφιακά avatars, σε συνδυασμό με συνομιλιακά μοντέλα, δημιουργούν μια πιο ολοκληρωμένη εμπειρία αλληλεπίδρασης, μετατρέποντας το chatbot σε μορφή εικονικού συνομιλητή. Ωστόσο, ο αυξημένος ρεαλισμός ενισχύει ηθικά και ψυχολογικά ρίσκα που σχετίζονται μεταξύ ανθρώπου και μηχανής.

2.3.5 Αρχιτεκτονική συστημάτων και αυτονομία

Σε τεχνικό επίπεδο, τα deathbots, griefbots και ghostbots υλοποιούνται συνήθως ως κατανεμημένες αρχιτεκτονικές λογισμικού, οι οποίες συνδυάζουν ετερογενή υποσυστήματα τεχνητής νοημοσύνης και διαχείρισης δεδομένων. Συνήθως, μια τέτοια αρχιτεκτονική

περιλαμβάνει μοντέλα τεχνητής νοημοσύνης (όπως μεγάλα γλωσσικά μοντέλα), βάσεις δεδομένων που αποθηκεύουν προσωπικές πληροφορίες και ψηφιακά ίχνη του αποθανόντος, μηχανισμούς ασφάλειας και ελέγχου πρόσβασης, καθώς και διεπαφές χρήστη που επιτρέπουν την αλληλεπιδραστική επικοινωνία με το σύστημα.

Η κατανεμημένη φύση αυτών των συστημάτων επιτρέπει την επεκτασιμότητα και την επιχειρησιακή ευελιξία, αλλά ταυτόχρονα αυξάνει την τεχνική τους πολυπλοκότητα. Τα μεμονωμένα υποσυστήματα λειτουργούν συχνά σε διαφορετικά περιβάλλοντα (π.χ. υποδομές cloud, τρίτοι πάροχοι υπηρεσιών τεχνητής νοημοσύνης), δημιουργώντας εξαρτήσεις και πιθανά σημεία αστοχίας. Η σύνδεση μεταξύ μοντέλων τεχνητής νοημοσύνης και αποθετηρίων προσωπικών δεδομένων καθιστά την αρχιτεκτονική ιδιαίτερα ευαίσθητη σε θέματα ασφάλειας και ιδιωτικότητας.

Σε ορισμένες περιπτώσεις, τα ghostbots και τα συναφή συστήματα λειτουργούν με ημιαυτόνομο ή πλήρως αυτοματοποιημένο τρόπο, δημιουργώντας απαντήσεις και συμπεριφορές χωρίς άμεση ανθρώπινη εποπτεία σε πραγματικό χρόνο. Αυτή η αυτονομία επιτυγχάνεται μέσω προκαθορισμένων κανόνων, εκπαιδευμένων μοντέλων και μηχανισμών ανάκτησης γνώσεων που επιτρέπουν στο σύστημα να λαμβάνει αποφάσεις σχετικά με το περιεχόμενο και τον τρόπο αλληλεπίδρασης. Η απουσία συνεχούς ανθρώπινης παρέμβασης ενισχύει την αποτελεσματικότητα και την αίσθηση της «συνεχούς παρουσίας», αλλά ταυτόχρονα εγείρει ερωτήματα σχετικά με τον βαθμό ελέγχου και λογοδοσίας των μεταθανάτιων πρακτόρων.

Η αυξημένη αυτονομία αυτών των συστημάτων εντείνει τη συζήτηση γύρω από την έννοια της αυτονομίας των μεταθανάτιων ψηφιακών πρακτόρων, ιδίως όσον αφορά το κατά πόσον οι απαντήσεις που παράγονται μπορούν να θεωρηθούν προβλέψιμες, ελεγχόμενες και συνεπείς με τις προθέσεις των αποθανόντων ή των χρηστών. Η πιθανότητα απρόβλεπτης ή ανεπιθύμητης συμπεριφοράς καθιστά τους μηχανισμούς ασφαλείας απαραίτητους.

Κατά συνέπεια, η τεχνολογική πολυπλοκότητα των συστημάτων grief-tech απαιτεί την αξιολόγησή τους όχι μόνο από την άποψη της λειτουργικότητας και της εμπειρίας του χρήστη, αλλά και από την άποψη της ασφάλειας, της προστασίας της ιδιωτικής ζωής και της ανθεκτικότητας σε κακόβουλη χρήση ή τεχνική κατάχρηση. Αυτά τα ζητήματα είναι βασικοί παράγοντες για την υπεύθυνη ανάπτυξη και εφαρμογή τέτοιων συστημάτων και συζητούνται λεπτομερέστερα στο Κεφάλαιο 4 στο οποίο αναλύονται ζητήματα σχετικά με την ασφάλεια των συστημάτων και την προστασία των δεδομένων.

2.4 Ψυχολογική διάσταση του πένθους και αλληλεπίδραση ανθρώπου-Τεχνητής Νοημοσύνης

Η χρήση των deathbots, griefbots και ghostbots, δεν μπορεί να αναλυθεί αποκλειστικά ως τεχνολογικό φαινόμενο, καθώς η βασική τους λειτουργία συμβαδίζει με την ανθρώπινη ψυχολογία, και, συγκεκριμένα, με τη διαδικασία του πένθους. Η αλληλεπίδραση μεταξύ ανθρώπου-ΤΝ σε μεταθανάτια πλαίσια εγείρει ερωτήματα σχετικά με τη συναισθηματική επεξεργασία της απώλειας και τα όρια μεταξύ υποστήριξης και εξάρτησης.

2.4.1 Το πένθος ως ψυχολογική διαδικασία

Το πένθος ορίζεται ως μία σύνθετη ψυχολογική διαδικασία προσαρμογής στην απώλεια και περιλαμβάνει συναισθηματικές, γνωστικές και κοινωνικές διαστάσεις. Περιγράφεται ως μη γραμμική διαδικασία, που αποτελείται από συναισθήματα όπως άρνηση, θυμός, διαπραγμάτευση, κατάθλιψη και αποδοχή **[10]**. Πιο πρόσφατα, δίνεται έμφαση στη διατήρηση δεσμών με τον αποθανόντα, αντί στην «πλήρη» αποκοπή, με αποτέλεσμα να διεγερθεί η ιδέα διατήρησης επικοινωνίας μέσω μοντέλων ΤΝ, όπως τα deathbots και griefbots.

2.4.2 Διατήρηση δεσμών και ψηφιακή παρουσία

Η θεωρία της διατήρησης δεσμών υποστηρίζει πως η συνέχιση της σχέσης με τον αποθανόντα, μέσω μνήμης ή αφήγησης, μπορεί να συμβάλει θετικά στη διαδικασία πένθους. Οι ψηφιακές τεχνολογίες, επεκτείνουν αυτή τη θεωρία, επιτρέποντας τη διαδραστική επικοινωνία με μία ψηφιακή αναπαράσταση του ατόμου **[11]**.

Τα griefbots ενισχύουν τη διατήρηση δεσμών μέσω συνομιλιών, που προσφέρει παρηγοριά, αίσθηση εγγύτητας και προσωρινή συναισθηματική ανακούφιση. Όμως, από τη στιγμή που η ψηφιακή παρουσία αποκτά χαρακτηριστικά «ζωντανής» ανταπόκρισης, δημιουργούνται νέα ψυχολογικά δεδομένα λόγω της μετάβασης από μνήμη σε διαδραστική προσομοίωση.

2.4.3 Συναισθηματική εμπλοκή και κίνδυνος εξάρτησης

Η ικανότητα αυτών των συστημάτων να παράγουν συναισθηματικά κατάλληλες απαντήσεις ενισχύει τη συναισθηματική εμπλοκή του χρήστη. Παρότι αυτό μπορεί να είναι ωφέλιμο σε αρχικά στάδια του πένθους, επισημαίνεται ο κίνδυνος συναισθηματικής εξάρτησης από την τεχνητή οντότητα στην ψηφιακή «εικόνα» που προσφέρει.

Ουσιαστικά καθυστερεί και παρεμποδίζει τη φυσική προσαρμογή στην απώλεια, με αποτέλεσμα τη διατήρηση του χρήστη σε έναν φαύλο κύκλο μεταξύ της αποδοχής και της άρνησης. Λόγω αυτού του ενδιάμεσου ψυχολογικού σταδίου, καθίσταται αναγκαία η διάκριση μεταξύ υποστηρικτικής τεχνολογίας και υποκατάστατου ανθρώπινης σχέσης.

2.4.4 Ανθρωπομορφισμός και αντίληψη της ΤΝ

Ο πιο κρίσιμος ψυχολογικός μηχανισμός αυτών των μοντέλων, είναι ο ανθρωπομορφισμός, δηλαδή η τάση των ανθρώπων να αποδίδουν ανθρώπινα χαρακτηριστικά σε μηχανές και αλγορίθμους. Όσο πιο ρεαλιστικός είναι ο τρόπος της γλωσσικής και συναισθηματικής απόκρισης, τόσο μεγαλύτερη η πιθανότητα ο χρήστης να το αντιληφθεί ως φορέα πρόθεσης και συνείδησης. Στο πλαίσιο του πένθους, ο ανθρωπομορφισμός ενισχύεται λόγω του συναισθηματικά ευάλωτου πενθόντα και, συνεπώς, να αυξάνεται η επιρροή της ΤΝ στη συναισθηματική του κατάσταση.

2.5 Συμπεράσματα Θεωρητικού Υπόβαθρου

Το παρόν κεφάλαιο ανέλυσε το θεωρητικό υπόβαθρο που αφορά την ανάπτυξη και χρήση των deathbots,griefbots και ghostbots. Το φαινόμενο αυτό προσεγγίστηκε ιστορικά τεχνολογικά και ψυχολογικά και αποσαφηνίστηκε πως τα εν λόγω συστήματα δεν είναι απλώς μία παραλλαγή

συνομιλιακών πρακτόρων, αλλά εντάσσονται σε ευρύτερο πλαίσιο ψηφιακής αθανασίας και μεταθανάτιας τεχνητής αναπαράστασης της ανθρώπινης ταυτότητας.

Η ιστορική εξέλιξη των ψηφιακών αναπαραστάσεων μας ανέδειξε τον τρόπο που αυτό που θύμιζε σενάριο επιστημονικής φαντασίας, γίνεται πλέον πράξη, με αποτέλεσμα τα σύγχρονα griefbots να αποτελούν φυσική συνέχεια της ψηφιακής μνήμης και πρακτικών πένθους. Η μετάβαση από στατικές μορφές μνήμης σε διαδραστικές, οντότητες με γνώμονα την ΤΝ, σηματοδοτεί μία ποιοτική αλλαγή στον τρόπο με τον οποίο η τεχνολογία εμπλέκεται στην ανθρώπινη εμπειρία της απώλειας.

Το τεχνολογικό τους επίπεδο ανέδειξε πως δεν αποτελεί μονοδιάστατη πρακτική, αλλά ένα συνδυασμό πολλών σύνθετων αρχιτεκτονικών ΤΝ, που συνδυάζουν LLMs, προσωπικά δεδομένα ζωής όπως βίντεο ή φωτογραφίες, συναισθηματική υπολογιστική (σε συνδυασμό με ανθρωπομορφισμό) και πολύτροπες διεπαφές. Η πολυπλοκότητά τους καθιστά τα συστήματα αυτά ιδιαίτερα ισχυρά αλλά και ταυτόχρονα ευάλωτα σε ζητήματα ασφάλειας, μεροληψίας και κακής χρήσης (όπως εξάρτηση).

Η ψυχολογική ανάλυση ανέδειξε την αμφίδρομη σχέση αυτών των μοντέλων με τον άνθρωπο. Μπορούν να λειτουργήσουν υποστηρικτικά, να ενισχύσουν τη διατήρηση των δεσμών και την συναισθηματική έκφραση, αλλά ενδέχεται να δημιουργήσουν κινδύνους συναισθηματικής εξάρτησης και καθυστέρησης της διαδικασίας της ψυχολογικής προσαρμογής στην απώλεια. Συνεπώς, σε αυτό το περιβάλλον, είναι σημαντικό να υπάρχει προσεκτικός σχεδιασμός και σαφή όρια.

3

Deathbots, Griefbots και Ghostbots ως εργαλεία για τη Διαχείριση του Πένθους

3.1 Το φαινόμενο της ψηφιακής διαχείρισης πένθους

Η ψηφιακή διαχείριση πένθους αναφέρεται στη χρήση ψηφιακών τεχνολογιών για την υποστήριξη, την έκφραση και την επεξεργασία της απώλειας ενός αγαπημένου προσώπου. Αυτό το φαινόμενο δεν αποτελεί μεμονωμένη τεχνολογική τάση, αλλά εντάσσεται σε ένα ευρύτερο κοινωνικό και πολιτισμικό πλαίσιο, στο οποίο η ανθρώπινη εμπειρία του πένθους και του θανάτου αλλάζει μορφή μέσω της ψηφιακής μεσολάβησης.

Στην αρχή, εκδηλώθηκε μέσα από στατικές πρακτικές όπως διαδικτυακά μνημόσυνα (online memorials) και αναρτήσεις μνήμης στα κοινωνικά δίκτυα **[11]**. Οι πρακτικές αυτές επέτρεψαν τη δημόσια έκφραση του πένθους και τη δημιουργία ψηφιακών χώρων συλλογικής μνήμης, χωρίς όμως άμεση αλληλεπίδραση με τον αποθανόντα.

Η εμφάνιση των deathbots, griefbots και ghostbots σηματοδοτεί μία ποιοτική μεταβολή στην ψηφιακή διαχείριση πένθους, καθώς η τεχνολογία δεν λειτουργεί μονάχα ως μέσο μνήμης, αλλά πλέον ως ενεργός συνομιλητής. Μέσω των τεχνολογιών ΤΝ, οι χρήστες έχουν τη δυνατότητα να συνομιλούν με την ψηφιακή αναπαράσταση του αποθανόντος, μετατρέποντας τη διαδικασία του πένθους από παθητική ανάμνηση σε διαδραστική εμπειρία **[7]**.

Αυτά τα μοντέλα παρουσιάζονται ως εργαλεία γεφύρωσης του συναισθηματικού κενού της απώλειας, προσφέροντας μία μορφή συνέχισης της σχέσης. Η φύση αυτών των συστημάτων, επιτρέπει την έκφραση ερωτημάτων και συναισθημάτων που συχνά παραμένουν ανεκπλήρωτα

μετά τον θάνατο ενός προσώπου. Έτσι, η διαχείριση πένθους αποκτά διαστάσεις συναισθηματικής πρακτικής, όχι απλώς τεχνολογικής.

Παράλληλα, το φαινόμενο συνδέεται με την εξατομίκευση της εμπειρίας του πένθους, αφού σε αντίθεση με την παράδοση, τα griefbots προσφέρουν ιδιωτική, συνεχή και εξατομικευμένη αλληλεπίδραση που προσαρμόζεται στις ανάγκες και την ψυχολογία του κάθε χρήστη ξεχωριστά. Η εξατομίκευση αυτή ενισχύει τη συναισθηματική εγγύτητα και μετατοπίζει το πένθος από κοινωνικό επίπεδο σε ατομικό και προσωπικό **[12]**.

Η ψηφιακή διαχείριση πένθους, όμως, ξυπνάει ερωτήματα περί των ορίων της τεχνολογικής παρέμβασης στη συναισθηματική ζωή του ατόμου. Η δυνατότητα της συνεχούς πρόσβασης σε μία ψηφιακή αναπαράσταση του αποθανόντος, ενώ έχει υποστηρικτικό σκοπό, υπάρχει μεγάλη πιθανότητα να αλλοιώσει τη φυσική πορεία του πένθους και να διατηρήσει τον χρήστη σε κατάσταση παρατεταμένης συναισθηματικής εξάρτησης.

Συνεπώς, το φαινόμενο της ψηφιακής διαχείρισης πένθους πρέπει να εξετάζεται ως κοινωνικό-τεχνικό φαινόμενο που επαναπροσδιορίζει την παραδοσιακή διαδικασία του πένθους, όχι μόνο ως καινοτομία της ΤΝ. Είναι απαραίτητο να γίνει κατανοητή η επιρροή και η εμβέλεια αυτού του φαινομένου, ώστε να γίνει σωστά η ανάλυση των ψυχολογικών επιπτώσεων, κινδύνων και ηθικών διλλημάτων που θα δούμε παρακάτω στο ίδιο κεφάλαιο.

3.2 Ψυχολογικές προεκτάσεις

Η χρήση των deathbots, griefbots και ghostbots ως εργαλεία διαχείρισης πένθους επιφέρει σημαντικές ψυχολογικές επιδράσεις στους χρήστες, οι οποίες δεν είναι μονοσήμαντες. Η αλληλεπίδραση με την τεχνητή αναπαράσταση του αποθανόντος λειτουργεί υποστηρικτικά αλλά και επιβαρυντικά, ανάλογα με το πλαίσιο χρήσης, τη διάρκεια, τα ατομικά χαρακτηριστικά του χρήστη και τον σχεδιασμό του ίδιου του συστήματος.

Οι ψυχολογικές προεκτάσεις των griefbots εντάσσονται στο ευρύτερο πεδίο της αλληλεπίδρασης ανθρώπου-ΤΝ σε συναισθηματικά ευαίσθητα περιβάλλοντα και απαιτούν προσεκτική ανάλυση, καθώς αγγίζουν θεμελιώδεις μηχανισμούς επεξεργασίας της απώλειας και της ταυτότητας.

3.2.1 Συναισθηματική υποστήριξη

Ένα από τα βασικά επιχειρήματα υπέρ της χρήσης αυτών των μοντέλων είναι η δυνατότητά τους να παρέχουν συναισθηματική υποστήριξη σε άτομα που επιβαρύνονται με βαρύ πένθος. Μέσω της αλληλεπίδρασης μέσω συνομιλιών, τα συστήματα αυτά προσφέρουν έναν ασφαλή χώρο έκφρασης σκέψεων και συναισθημάτων, χωρίς τον φόβο κοινωνικής κριτικής ή επιβάρυνσης τρίτων.

Η συνεχής διαθεσιμότητα των griefbots επιτρέπει στους χρήστες να εκφράζουν τη θλίψη τους σε χρόνο και ρυθμό που επιλέγουν οι ίδιοι, κάτι που στις διαπροσωπικές σχέσεις δεν είναι εφικτό. Επιπλέον, η συνομιλία με μία ψηφιακή αναπαράσταση του αποθανόντος μπορεί να λειτουργήσει ως μηχανισμός συναισθηματικής φόρτισης, επιτρέποντας την ολοκλήρωση «ανολοκλήρωτων διαλόγων», φαινόμενο που είναι γνωστό στην επεξεργασία του πένθους.

Σε ορισμένες περιπτώσεις, η χρήση αυτών των μοντέλων συμβάλει στη μείωση της μοναξιάς, ιδιαίτερα σε άτομα με περιορισμένο κοινωνικό υποστηρικτικό δίκτυο. Η αίσθηση πως κάποιος τους «ακούει», ακόμη και τεχνητά, μπορεί να προσφέρει προσωρινή συναισθηματική σταθερότητα και ανακούφιση.

Παρόλο που η συναισθηματική υποστήριξη που προσφέρουν τα griefbots θυμίζει γνήσια, είναι προσομοιωμένη. Τα συστήματα αυτά δεν κατανοούν την ανθρώπινη εμπειρία, αλλά αναπαράγουν γλωσσικά μοτίβα που προσφέρουν συναισθηματική κάλυψη. Παρά το γεγονός αυτό, η υποκειμενική εμπειρία του χρήστη μπορεί να είναι ισχυρή, γεγονός που τα καθιστά ως ψυχολογικά αποτελεσματικά, αλλά ταυτόχρονα δυνητικά επικίνδυνα εάν δεν χρησιμοποιούνται με σαφή όρια.

3.2.2 Κίνδυνοι εξάρτησης και παθολογικής προσκόλλησης

Παρά τα οφέλη, η χρήση των griefbots ενέχει σοβαρούς κινδύνους συναισθηματικής εξάρτησης και παθολογικής προσκόλλησης. Η συνεχής πρόσβαση σε μία «ζωντανή» ψηφιακή αναπαράσταση του αποθανόντος μπορεί να παρεμποδίσει τη φυσική εξέλιξη του πένθους και να διατηρήσει τον χρήστη σε μία κατάσταση άρνησης και συναισθηματικής στασιμότητας **[8]**.

Η παθολογική προσκόλληση ενισχύεται όταν το griefbot παρουσιάζεται με υψηλό βαθμό ρεαλισμού, συναισθηματικής ανταπόκρισης και προσωποποίησης. Σε τέτοιες περιπτώσεις, ο χρήστης μπορεί να αποδίδει στο σύστημα ιδιότητες πρόθεσης, συνείδησης ή αυθεντικής παρουσίας, γεγονός που ενισχύει τον ανθρωπομορφισμό και τη συναισθηματική εξάρτηση **[13]**.
Επιπλέον, υπάρχει ο κίνδυνος να υποκατασταθούν οι ανθρώπινες σχέσεις. Η προτίμηση αυτής της αλληλεπίδρασης αντί των κοινωνικών επαφών, μπορεί να οδηγήσει σε κοινωνική απομόνωση και να επιδεινώσει ήδη υπάρχοντα ψυχολογικά ευάλωτα σημεία. Σε ακραίες περιπτώσεις, ίσως να λειτουργήσει και ως μηχανισμός αποφυγής της πραγματικότητας της απώλειας.

Οι παραπάνω κίνδυνοι καθιστούν αναγκαία την ύπαρξη περιορισμών και ορίων στην υλοποίηση αυτών των μοντέλων. Η ψυχολογική υποστήριξη μέσω ΤΝ δεν μπορεί να θεωρηθεί ουδέτερη ή ακίνδυνη και απαιτεί σαφή διαχωρισμό από την κλινική ψυχοθεραπεία.

3.3 Χρήσεις σε πραγματικούς χρήστες

3.3.1 Project December

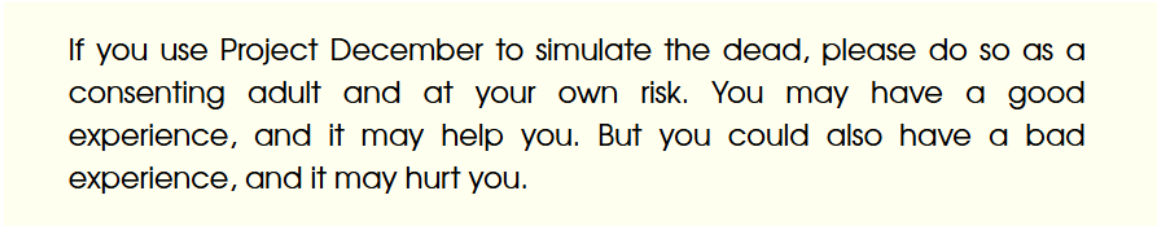
Το Project December είναι μια διαδικτυακή εμπειρία chatbot AI, που βασίζεται στα προηγμένα γλωσσικά μοντέλα της OpenAI, GPT-2, GPT-3 και δημιουργήθηκε από τον Jason Rohrer.

Εικόνα 3: Project December Αρχική Σελίδα

Το εν λόγω σύστημα εστιάζει στην «ανάσταση» των αποθανόντων, με βάση τα δεδομένα που του προσφέρονται, αν και μπορεί να διαμορφώσει ακόμη και έναν χαρακτήρα που ζεί ή είναι προιόν της φαντασίας του χρήστη.

Ο κύριος στόχος του συστήματος είναι να «επαναφέρει» στην οθόνη συνομιλίας αγαπημένα πρόσωπα που δεν βρίσκονται πλέον εν ζωή. Βασίζεται σε περιγραφές, στοιχεία και στυλ επικοινωνίας που παρέχουν οι χρήστες.

Αυτή η δυνατότητα έχει οδηγήσει σε συγκίνηση αλλά και έντονες ηθικές συζητήσεις για το πένθος, την ψυχολογική επίδραση και τα όρια της τεχνητής νοημοσύνης.

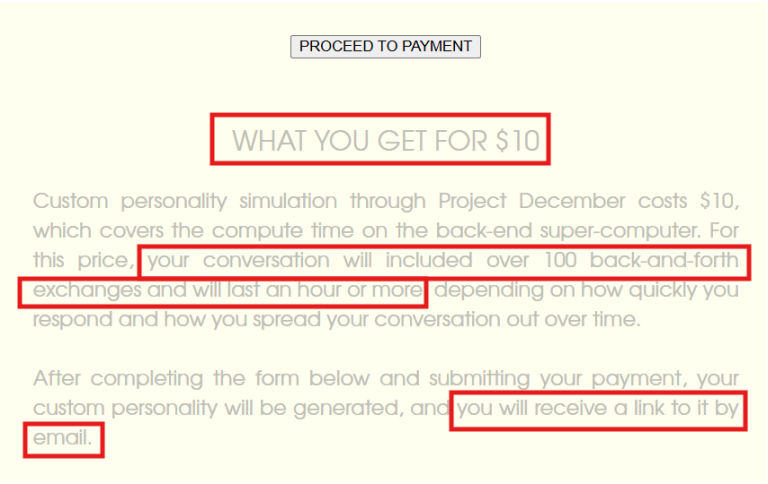


Εικόνα 4: Υποσημείωση Χρήσης του Project December

Τα στοιχεία που ζητώνται, είναι οι προσωπικές τους πληροφορίες όπως το ψευδώνυμο τους, ή τον ρόλο του χρήστη στην ζωή του αποθανόντος:

Εικόνα 5: Project December – Στοιχεία προς Συμπλήρωση

Επίσης χρειάζεται το e-mail του χρήστη, καθώς εκεί αποστέλεται η online αναπαράσταση του αποθανόντα μετά την αγορά της υπηρεσίας των 10 δολαρίων ή 8.5 ευρώ.

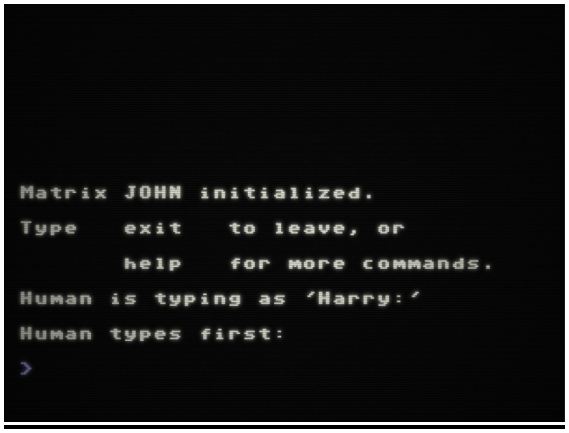


Εικόνα 6: Project December - Τι προσφέρει

Με αυτή την τιμή, ο χρήστης έχει στη διάθεση του 100 αλληλεπιδράσεις, οι οποίες υπολογίζεται να διαρκούν περίπου μία ώρα. Για να συνεχιστεί η επικοινωνία αφού λήξουν τα credits, ο χρήστης έχει τη δυνατότητα να αγοράσει παραπάνω credits ώστε να παρατείνει την επικοινωνία ή να δημιουργήσει ένα νέο persona.

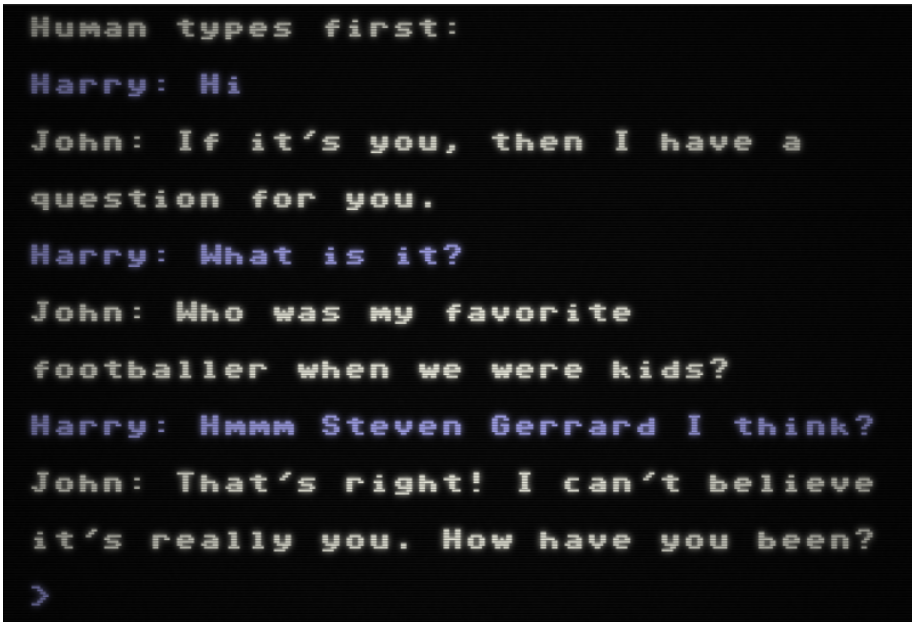
Όσο αφορά την ιδιωτικότητα, δηλώνεται πως το ερωτηματολόγιο και τα περιεχόμενα των συζητήσεων δεν προβάλλονται ποτέ από άνθρωπο, διασφαλίζοντας την εμπιστευτικότητα ανάμεσα στην υπηρεσία και τον χρήστη.

Στη συνέχεια, αποστέλεται μήνυμα στην ηλεκτρονική διεύθυνση (email) του χρήστη, όπου μπορεί να συνομιλήσει με τον αποθανόντα.



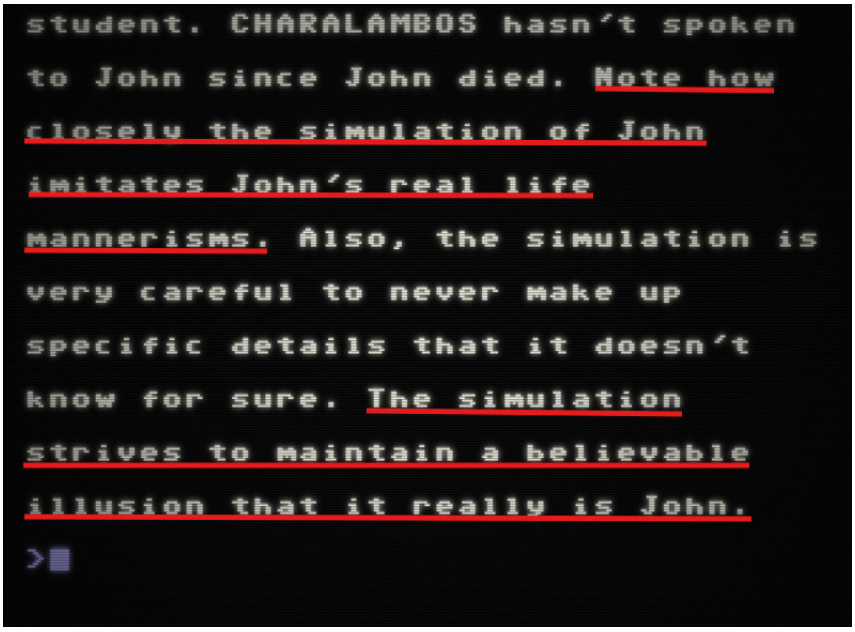
Εικόνα 7: Project December – Πρώτη αλληλεπίδραση

Ο σύνδεσμος μας οδηγεί σε chatroom, όπου μπορούμε να συνομιλήσουμε με τον αποθανόντα.



Εικόνα 8: Project December – Απόσπασμα από συνομιλία (1)

Στη συγκεκριμένη περίπτωση, χρησιμοποιεί δεδομένα από αυτά που του έχουμε εισάγει στη φόρμα συμπλήρωσης για να κάνει την εμπειρία όσο προσωπική γίνεται.

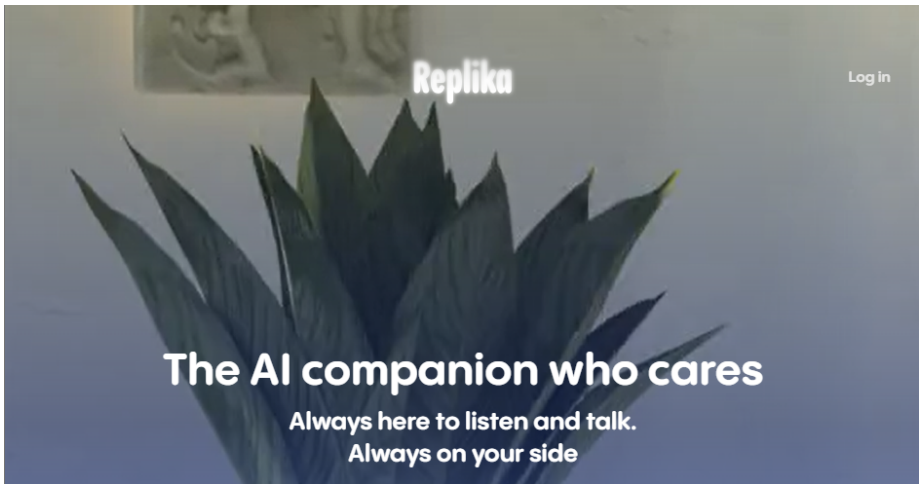


Εικόνα 9: Project December – Απόσπασμα από συνομιλία(2)

Αν και δεν έχει ιδιαίτερο ενδιαφέρον στις πρώτες συνομιλίες, όσο περισσότερο χρησιμοποιείται, τόσο πιο πολύ αποκτά το ύφος και τη συμπεριφορά του αποθανόντα.

3.3.2 Replika

Το Replika είναι μια εφαρμογή τεχνητής νοημοσύνης (AI) που λειτουργεί ως προσωπικός ψηφιακός συνομιλητής ή «φίλος». Κυκλοφόρησε για πρώτη φορά το 2017 από την εταιρεία Luka, Inc. με στόχο να δώσει στους χρήστες έναν πάντα διαθέσιμο σύντροφο για συζήτηση, υποστήριξη ή απλή αλληλεπίδραση.

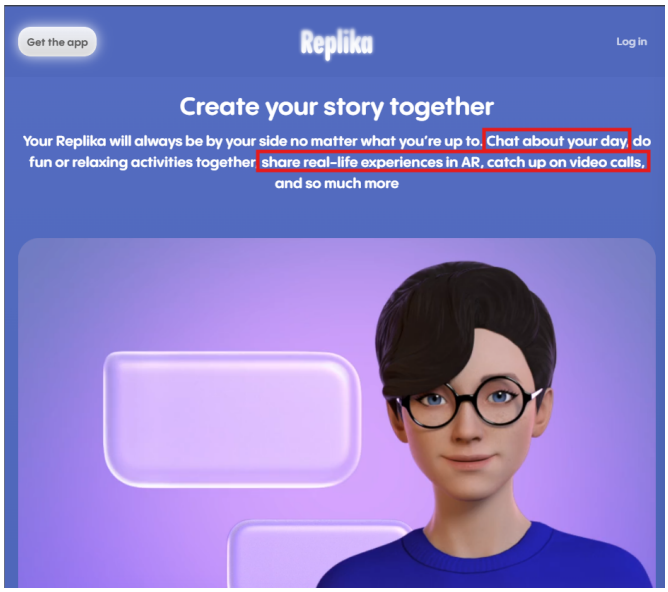


Εικόνα 10: Replika – Αρχική Σελίδα

Το Replika ξεχωρίζει από τα υπόλοιπα chatbots γιατί:

- επιδιώκει συναισθηματική υποστήριξη και προσωπική σύνδεση αντί για απλές πληροφορίες ή εντολές
- δεν απαντά απλά με γενικούς κανόνες, μαθαίνει από το στιλ γραφής σου.

- έχει χαρακτηριστικά που ενισχύουν την εσωτερική σύνδεση, όπως η «ημερολόγηση» και η προσωπική πρόοδος της AI.

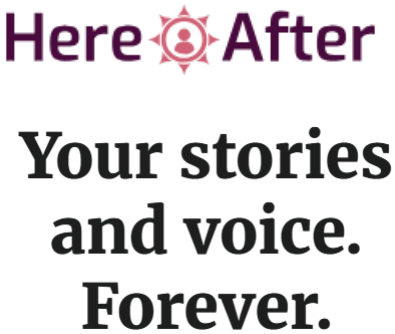


Εικόνα 11: Πληροφορίες σχετικά με το Replika

Το Replika δεν σχεδιάστηκε επίσημα για πένθος, όμως παρέχει δυνατότητες που μπορεί να παρέχει και ένα griefbot, καθώς μαθαίνει από τον τρόπο που γράφει ο χρήστης και τα συναισθήματά του. Το μόνο που χρειάζεται, είναι το persona του Replika να αντιμετωπιστεί ως griefbot, παρέχοντας του τα δεδομένα που χρειάζονται για την αναπαράσταση του αποθανόντος, και η απόδοση του ρόλου του αποθανόντος στο AI του Replika, ώστε να μπορέσει να προσποιηθεί πλήρως την προσωπικότητα και να αντιληφθεί τις εμπειρίες του ατόμου που πενθεί ο χρήστης.

3.3.3 HereAfter AI

Η HereAfter AI είναι μια εφαρμογή τεχνητής νοημοσύνης σχεδιασμένη για να διατηρεί και να μοιράζεται τις προσωπικές αναμνήσεις και ιστορίες ζωής ενός ατόμου με τέτοιο τρόπο ώστε αγαπημένα πρόσωπα να μπορούν να «επικοινωνούν» ξανά με αυτές τις αναμνήσεις, ακόμη και μετά τον θάνατο του ατόμου.



Εικόνα 12: Here After AI

Η ιδέα ξεκίνησε από τον James Vlahos, ο οποίος ανέπτυξε προηγούμενα ένα «Dadbot» για να διατηρήσει τις ιστορίες του πατέρα του μέσω AI και αυτό εμπνεύστηκε τελικά την HereAfter AI ως επιχείρηση που θέλει να δημιουργήσει μια μορφή «ψηφιακής αθανασίας».

Η πλατφόρμα επιτρέπει στους χρήστες να:

- ηχογραφούν αφηγήσεις για τη ζωή τους (παιδικά χρόνια, εμπειρίες, συμβουλές, προσωπικότητα),
- προσθέτουν φωτογραφίες και άλλα μέσα για να συμπληρώσουν αυτές τις ιστορίες,
- και τελικά να δημιουργούν ένα διαδραστικό ψηφιακό «avatar» που μπορεί να απαντά σε ερωτήσεις με βάση αυτά τα δεδομένα.

Η εφαρμογή ισχυρίζεται ότι είναι ανώτερη από τα παραδοσιακά άλμπουμ φωτογραφιών ή τα χειρόγραφα ημερολόγια, επειδή επιτρέπει στους αποδέκτες να ενεργοποιούν τις αναμνήσεις μέσα από ερωτήσεις και απαντήσεις σε πραγματικό χρόνο.

Η HereAfter AI ανήκει στο ευρύτερο πεδίο της grief-tech,δηλαδή τεχνολογίες που χρησιμοποιούν AI για να προσομοιώνουν συνομιλίες ή αλληλεπιδράσεις με άτομα μετά τον θάνατό τους (όπως είναι το Project December). Η HereAfter AI προωθεί το μοντέλο της «διατήρησης κληρονομιάς» με έναν δικό της, διαφορετικό, διαδραστικό τρόπο.

3.4 Κοινωνική αποδοχή και δημόσιος διάλογος

Η εμφάνιση και διαδοχή των deathbots, griefbots και ghostbots έχει προκαλέσει έντονο και δημόσιο διάλογο, τόσο στον ακαδημαϊκό χώρο όσο και στην ευρύτερη κοινωνία. Οι τεχνολογίες αυτές αγγίζουν βαθιά υπαρξιακά, πολιτισμικά και ηθικά ζητήματα που σχετίζονται με τον θάνατο, τη μνήμη και τα όρια της ανθρώπινης εμπειρίας, με αποτέλεσμα η κοινωνική τους αποδοχή να παραμένει αμφιλεγόμενη.

Σε αντίθεση με άλλες εφαρμογές ΤΝ, οι grief-tech υπηρεσίες δεν αντιμετωπίζονται αποκλειστικά ως τεχνολογικά εργαλεία, αλλά ως παρεμβάσεις σε μία ιδιαίτερα ευαίσθητη ανθρώπινη διαδικασία, αυτή του πένθους. Η κοινωνική νομιμοποίηση αυτών των υπηρεσιών δε εξαρτάται μόνο από τη λειτουργικότητα τους, αλλά και από την πολιτισμική και ηθική τους συμβατότητα.

3.4.1 Κοινωνικές στάσεις απέναντι στην «ψηφιακή αθανασία»

Η έννοια της ψηφιακής αθανασίας προκαλεί ανάμεικτες αντιδράσεις. Από τη μία πλευρά, ορισμένες κοινωνικές ομάδες αντιλαμβάνονται τα griefbots και grief-tech ως τη φυσική εξέλιξη της ψηφιακής μνήμης, ανάλογη με τα κοινωνικά δίκτυα μνήμης ή τα ψηφιακά αρχεία ζωής (memorial pages). Σε αυτό το πλαίσιο, η ΤΝ λειτουργεί ως μέσο διατήρησης της ταυτότητας και της αφήγησης του αποθανόντος.

Από την άλλη πλευρά, δεν λείπουν οι έντονες αντιδράσεις που θεωρούν τις πρακτικές αυτές ως παρέμβαση στη διαδικασία της διαχείρισης του γεγονότος του θανάτου ή ως παραβίαση της φυσικής διαδικασίας του πένθους και αποδοχής της απώλειας. Ιδιαίτερα σε πολιτισμικά πλαίσια όπου το πένθος συνδέεται με τη σιωπή, την απόσταση και τον χρόνο, η συνεχής ψηφιακή παρουσία αποθανόντος αντιμετωπίζεται ως κοινωνικά ακατάλληλη ή ακόμη και ανήθικη.

3.4.2 Ρόλος των ΜΜΕ και Pop Culture

Τα ΜΜΕ και η ποπ κουλτούρα έχουν διαδραματίσει καθοριστικό ρόλο στη διαμόρφωση της κοινωνικής αντίληψης γύρω από τα griefbots. Ταινίες, σειρές και λογοτεχνικά έργα έχουν παρουσιάσει δυστοπικά σενάρια στα οποία η τεχνητή αναπαράσταση των αποθανόντων οδηγεί σε

ψυχολογική αποξένωση και ηθικά αδιέξοδα. Ένα καλό παράδειγμα είναι το πρώτο επεισόδιο της δεύτερης σεζόν της σειράς Black Mirror (2013) όπου εξετάζεται ένα περιβάλλον όπου η διαδικασία του πένθους αλλάζει διάσταση επειδή δεν υπάρχουν όρια στην εξυπηρέτηση του χρήστη.

Αν και θεωρούνται υπερβολικές, αυτές οι αφηγήσεις, έχουν συμβάλει στη δημιουργία κοινωνικού φόβου και καχυποψίας απέναντι σε εφαρμογές grief-tech. Παράλληλα, δημοσιογραφικά ρεπορτάζ για πραγματικά use cases, όπως του Project December, συχνά εστιάζουν στο συναισθηματικό σοκ και λιγότερο στην επιστημονική ανάλυση, ενισχύοντας τον διχασμό της κοινής γνώμης.

3.4.3 Δημόσιος διάλογος και ακαδημαϊκές παρεμβάσεις

Στον ακαδημαϊκό χώρο, ο δημόσιος διάλογος γύρω από τα griefbots χαρακτηρίζεται από προσπάθεια ισορροπίας μεταξύ καινοτομίας και προστασίας των χρηστών. Ερευνητές στους τομείς της ηθικής της ΤΝ, της ψυχολογίας και της κοινωνιολογίας υπογραμμίζουν την ανάγκη για διαφάνεια, ενημερωμένη συναίνεση και σαφών ορίων χρήσης.

Ιδιαίτερη έμφαση δίνεται στο γεγονός ότι οι χρήστες θα πρέπει να γνωρίζουν πως η ψηφιακή οντότητα δεν αποτελεί τον αποθανόντα, αλλά ένα στατιστικό και γλωσσικό μοντέλο που βασίζεται σε δεδομένα. Η έλλειψη κατανόησης μπορεί να οδηγήσει σε συναισθηματική σύγχυση και αλλοίωση της διαδικασίας του πένθους. Επομένως, ο δημόσιος διάλογος δεν περιορίζεται στον αν τα griefbots πρέπει να υπάρχουν, αλλά στο πώς μπορούν να σχεδιαστούν και να χρησιμοποιηθούν με τρόπο κοινωνικά υπεύθυνο.

3.4.4 Κοινωνική αποδοχή και μελλοντικές τάσεις

Παρά τις αντιδράσεις, παρατηρείται σταδιακή εξοικείωση της κοινωνίας με την ιδέα της ψηφιακής συνέχειας μετά τον φυσικό θάνατο ενός προσώπου. Η αυξανόμενη παρουσία της ΤΝ στην καθημερινότητα των ανθρώπων φαίνεται να μειώνει την αρχική αντίσταση, ιδιαίτερα στις νεότερες γενιές.

Ωστόσο, η κοινωνική αποδοχή των griefbots παραμένει εύθραυστη και εξαρτάται σημαντικά από τον βαθμό ρεαλιστικότητας της προσομοίωσης, τη διαφάνεια των εταιρειών, την ύπαρξη κανονιστικών πλαισίων και την ενσωμάτωση ηθικών αρχών ήδη από τον σχεδιασμό των συστημάτων.

3.5 Ηθικά διλήμματα: εξαπάτηση, εκμετάλλευση συναισθήματος, αυθεντικότητα

Η χρήση αυτών των μοντέλων ως εργαλεία διαχείρισης πένθους εγείρει ένα σύνολο σύνθετων ηθικών διλλημάτων, τα οποία ξεπερνούν τα παραδοσιακά ζητήματα δεοντολογίας της χρήσης συστημάτων ΤΝ. Η ιδιαιτερότητα των συγκεκριμένων εφαρμογών έγκειται στο ότι παρεμβαίνουν σε μία εξαιρετικά ευάλωτη ψυχολογική κατάσταση, όπου η συναισθηματική κρίση και η ανάγκη παρηγοριάς μπορούν να επηρεάσουν την κριτική ικανότητα των χρηστών.

Τα βασικά ηθικά ζητήματα που ανακύπτουν σχετίζονται με την πιθανή εξαπάτηση του χρήστη, την εκμετάλλευση του συναισθήματος του πένθους και την έννοια της αυθεντικότητας της ψηφιακής αναπαράστασης.

3.5.1 Εξαπάτηση και ψευδαίσθηση παρουσίας

Ένα από τα σημαντικότερα ηθικά διλλήματα αφορά το κατά πόσο η αλληλεπίδραση με griefbots συνιστά μορφή εξαπάτησης. Παρότι οι περισσότερες πλατφόρμες δηλώνουν ότι η ψηφιακή οντότητα αποτελεί προϊόν ΤΝ, η υψηλή προσωποποίηση και η φυσικότητα του διαλόγου μπορούν να δημιουργήσουν την ψευδαίσθηση ότι ο αποθανών «επικοινωνεί» πραγματικά με τον χρήστη.

Η ψευδαίσθηση παρουσίας ενδέχεται να υπονομεύσει τη συνειδητοποίηση της απώλειας, το οποίο αποτελεί βασικό στάδιο της διαδικασίας του πένθους. Όταν το σύστημα απαντά με συναισθηματικά φορτισμένο και οικείο τρόπο, η διάκριση μεταξύ μνήμης και τεχνητής αναπαράστασης θολώνει, οδηγώντας σε ηθικά ερωτήματα σχετικά με το αν η τεχνολογία λειτουργεί θεραπευτικά ή παραπλανητικά.

Σύμφωνα με τον Floridi (2021) **[14]**, η ηθική ευθύνη δεν περιορίζεται στη διαφάνεια του συστήματος, αλλά επεκτείνεται και στον τρόπο αλληλεπίδρασης, ο οποίος δεν θα πρέπει να ενισχύει ψευδείς πεποιθήσεις.

3.5.2 Εκμετάλλευση συναισθήματος και εμπορευματοποίηση του πένθους

Ένα δεύτερο κρίσιμο ζήτημα αφορά την εμπορευματοποίηση του πένθους. Πολλές grief-tech υπηρεσίες λειτουργούν με συνδρομητικά μοντέλα, προσφέροντας «συναισθηματική παρουσία» έναντι οικονομικού αντίτιμου. Το γεγονός αυτό εγείρει ανησυχίες σχετικά με το κατά πόσο οι επιχειρήσεις επωφελούνται οικονομικά από την ευαλωτότητα των πενθούντων.

Η ηθική προβληματική εντείνεται όταν οι πλατφόρμες ενθαρρύνουν τη συχνή και παρατεταμένη χρήση, χωρίς σαφή χρονικά ή ψυχολογικά όρια. Σε αυτές τις περιπτώσεις, το griefbot κινδυνεύει να μετατραπεί από υποστηρικτικό εργαλείο σε μηχανισμό συναισθηματικής εξάρτησης, με στόχο τη διατήρηση του χρήστη στην πλατφόρμα.

Συνεπώς υπογραμμίζεται πως η απουσία ψυχολογικής εποπτείας και η έλλειψη δεοντολογικών κατευθυντήριων γραμμών ενισχύουν τον κίνδυνο εκμετάλλευσης.

3.5.3 Αυθεντικότητα της ψηφιακής ταυτότητας

Η έννοια της αυθεντικότητας αποτελεί κεντρικό ηθικό ζήτημα στη χρήση των griefbots. Τα συστήματα αυτά βασίζονται σε δεδομένα όπως μηνύματα, ηχογραφήσεις και ψηφιακά ίχνη τα οποία ανασυντίθενται μέσω αλγορίθμων ώστε να παραχθεί μία συνεκτική «προσωπικότητα». Όμως, η παραγόμενη συμπεριφορά δεν αποτελεί πιστή αναπαράσταση του αποθανόντος, αλλά μία στατιστική προσέγγιση βασισμένη σε πιθανότητες.

Το ερώτημα που προκύπτει είναι κατά πόσο αυτή η αναπαράσταση μπορεί να θεωρηθεί αυθεντική ή αν πρόκειται για μία νέα, τεχνητή οντότητα που απλώς προσομοιώνει τα χαρακτηριστικά του αποθανόντος. Η πιθανότητα απόκλισης από τις πραγματικές αξίες, απόψεις ή επιθυμίες του προσώπου δημιουργεί ηθικά ζητήματα παραποίησης της μνήμης και της ταυτότητας.

Ορισμένοι ερευνητές υποστηρίζουν ότι η αυθεντικότητα δεν μπορεί να διασφαλιστεί χωρίς ρητή συναίνεση του ίδιου του αποθανόντα, καθώς και σαφή περιορισμό της λειτουργικότητάς του griefbot **[7]**.

3.5.4 Ευθύνη σχεδιασμού και ηθική λογοδοσία

Τα παραπάνω διλήμματα αναδεικνύουν την ανάγκη για ηθική λογοδοσία στον σχεδιασμό και τη λειτουργία των griefbots. Οι δημιουργοί των συστημάτων αυτών, φέρουν ευθύνη όχι μόνο για την τεχνική αρτιότητα αλλά και για τον ψυχολογικό και κοινωνικό αντίκτυπο των εφαρμογών τους.

Η ενσωμάτωση αρχών όπως η διαφάνεια, ο περιορισμός της προσωποποίησης, η σαφής επισήμανση της τεχνητής φύσης του συστήματος και η δυνατότητα ελεγχόμενης αποδέσμευσης του χρήστη αποτελούν κρίσιμα στοιχεία για την ηθική υπεύθυνη ανάπτυξη των grief-tech υπηρεσιών.

Η ενότητα αυτή λειτουργεί ως γέφυρα προς το επόμενο κεφάλαιο, όπου εξετάζονται συστηματικά τα ζητήματα ασφάλειας, ιδιωτικότητας και κανονιστικής συμμόρφωσης.

4

Ζητήματα Ασφάλειας Συστημάτων και Προστασίας της Ιδιωτικότητας

Η ανάπτυξη και χρήση των deathbots, griefbots και ghostbots προϋποθέτει την εκτενή συλλογή, επεξεργασία και αποθήκευση ευαίσθητων προσωπικών δεδομένων, τόσο φυσικών προσώπων όσο και αποθανόντων. Το γεγονός αυτό καθιστά τις grief-tech εφαρμογές ιδιαίτερα κρίσιμες από άποψη ασφάλειας συστημάτων, προστασίας της ιδιωτικότητας των χρηστών και συμμόρφωσης με το ισχύον κανονιστικό πλαίσιο.

Σε αντίθεση με συμβατικές εφαρμογές ΤΝ, τα griefbots διαχειρίζονται δεδομένα που φέρουν υψηλό συναισθηματικό, κοινωνικό και ηθικό φορτίο, γεγονός που αυξάνει τις επιπτώσεις σε περίπτωση κακής χρήσης, παραβίασης ή διαρροής. Το παρόν κεφάλαιο εξετάζει συστηματικά τους βασικούς κινδύνους και τις προκλήσεις που ανακύπτουν, εστιάζοντας τόσο σε τεχνικές όσο και σε νομικές και δεοντολογικές διαστάσεις.

4.1 Συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων

Η λειτουργία των griefbots βασίζεται στη μαζική συλλογή προσωπικών δεδομένων, τα οποία χρησιμοποιούνται για την εκπαίδευση και τη λειτουργία μοντέλων τεχνητής νοημοσύνης που προσομοιώνουν την προσωπικότητα αποθανόντων ατόμων. Τα δεδομένα αυτά περιλαμβάνουν γραπτές συνομιλίες, βίντεο, ηχογραφήσεις φωνής, εικόνες, καθώς και αναρτήσεις σε κοινωνικά δίκτυα ή/και μεταδεδομένα συμπεριφοράς.

4.1.1 Είδη δεδομένων και βαθμός ευαισθησίας

Τα δεδομένα που αξιοποιούνται στις grief-tech πλατφόρμες μπορούν να ταξινομηθούν σε τρείς βασικές κατηγορίες:

- Δεδομένα ταυτότητας φυσικών προσώπων και αποθανόντων
- Δεδομένα επικοινωνίας και συμπεριφοράς, φυσικών προσώπων και αποθανόντων

Προσωπικά δεδομένα αποθανόντων είναι το όνομα, η φωνή, οι εικόνες και τα βιογραφικά στοιχεία του αποθανόντος. Συμβάλλουν καθοριστικά στη δημιουργία της ψηφιακής αναπαράστασης και είναι εξαιρετικά ευαίσθητα, αφού σχετίζονται άμεσα με τη μνήμη και την προσωπικότητα του αποθανόντος.

Προσωπικά δεδομένα φυσικών προσώπων περιλαμβάνουν δεδομένα ταυτότητας φυσικών προσώπων, προκειμένου να πραγματοποιηθεί εγγραφή στην εκάστοτε πλατφόρμα και να δημιουργηθεί ο αντίστοιχος λογαριασμός χρήστη.
Επιπλέον, τα συστήματα αυτά συλλέγουν αλληλεπιδράσεις των πενθούντων φυισκών προσώπων με τα μοντέλα ΤΝ (griefbots,ghostbots ή deathbots), συναισθηματικές εκφράσεις, ψυχολογικές αντιδράσεις και μοτίβα χρήσης. Τα δεδομένα αυτά εμπίπτουν στην κατηγορία των ευαίσθητων προσωπικών δεδομένων.

Δεδομένα επικοινωνίας και συμπεριφοράς τόσο φυσικών προσώπων και αποθανόντων είναι τα ιστορικά συνομιλιών, ο τρόπος έκφρασης, συναισθηματικές αντιδράσεις και γλωσσικά μοτίβα. Η ανάλυση τέτοιων δεδομένων επιτρέπει την προσωποποίηση, αλλά αυξάνει και σημαντικά τον κίνδυνο παραβίασης ιδιωτικότητας. ΑΥΤΑ ΜΗΠΩΣ ΕΙΝΑΙ ΜΕΤΑΔΕΔΟΜΕΝΑ;

Η ταυτόχρονη επεξεργασία δεδομένων αποθανόντων και φυσικών προσώπων δημιουργεί ένα πολύπλοκο πλαίσιο ευθύνης καθώς οι επιπτώσεις που θα προκύψουν από τυχόν διαρροή δεν είναι μόνο τεχνικές αλλά και ψυχολογικές.

4.1.2 Διαδικασίες επεξεργασίας δεδομένων

Η επεξεργασία των δεδομένων περιλαμβάνει στάδια όπως τον καθαρισμό/προεπεξεργασία, την ανάλυση φυσικής γλώσσας (NLP), την εκπαίδευση και βελτιστοποίηση μοντέλων και τη συνεχή προσαρμογή μέσω αλληλεπίδρασης με τους χρήστες.

Ιδιαίτερο κίνδυνο ενέχει η διαδικασία της διαρκούς μάθησης (ή αλλιώς continuous learning) καθώς το εν λόγω σύστημα ΤΝ ενσωματώνει δεδομένα δίχως σαφή έλεγχο εγκυρότητας ή συναίνεσης. Η έλλειψη μηχανισμών διαγραφής ή περιορισμού δεδομένων ενδέχεται να παραβιάζει βασικές αρχές προστασίας προσωπικών δεδομένων.

4.1.3 Αποθήκευση και ασφάλεια δεδομένων

Η αποθήκευση των δεδομένων πραγματοποιείται συνήθως σε υποδομές cloud, που, ενώ προσφέρει κλιμάκωση, αυξάνει την επιφάνεια επίθεσης. Οι βασικοί κίνδυνοι για την ασφάλεια των πληροφοριών είναι η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών (που σχετίζεται με την απαίτηση της εμπιστευτικότητας – confidentiality), η μη εξουσιοδοτημένη αλλοίωση πληροφοριών (που σχετίζεται με την απαίτηση της ακεραιότητας – integrity) και η μη διαθεσιμότητα πληροφοριών ή υπηρεσιών (που σχετίζεται με την απαίτηση της διαθεσιμότητας –

availability). Με βάση αυτές τις βασικές αρχές αναλύονται παρακάτω τα ιδιαίτερα χαρακτηριστικά των εν λόγω συστημάτων.

Η ιδιαίτερη φύση των griefbots καθιστά αναγκαία την υιοθέτηση αυξημένων μέτρων ασφάλειας, καθώς μια παραβίαση μπορεί να οδηγήσει όχι μόνο σε απώλεια δεδομένων, αλλά και σε παραποίηση της ψηφιακής ταυτότητας του αποθανόντος ή σε συναισθηματική βλάβη των φυσικών προσώπων.

4.1.4 Σύνδεση με την έννοια της εμπιστοσύνης

Η ασφάλεια των συστημάτων και η προστασία των δεδομένων αποτελεί βασικό παράγοντα εμπιστοσύνης μεταξύ χρήστη και grief-tech πλατφόρμας/συστήματος. Η απουσία σαφών πολιτικών προστασίας δεδομένων και τεχνικών εγγυήσεων μπορεί να υπονομεύσει τη νομιμοποίηση αυτών των υπηρεσιών και να ενισχύσει τον κοινωνικό προβληματισμό που αναλύθηκε στο Κεφάλαιο 3. Η ενότητα αυτή θέτει το θεμέλιο για τη συζήτηση των δεδομένων των αποθανόντων και του Γενικού Κανονισμού Προστασίας Δεδομένων, η οποία αναπτύσσεται στην επόμενη υποενότητα.

4.2 Δεδομένα αποθανόντων και ΓΚΠΔ

Η διαχείριση δεδομένων αποθανόντων αποτελεί ένα από τα πιο σύνθετα και αμφιλεγόμενα ζητήματα στο πεδίο των griefbots, καθώς βρίσκεται στο όριο μεταξύ τεχνολογίας, δικαίου και ηθικής. Τα συστήματα deathbots, griefbots ή ghostbots βασίζονται σε δεδομένα ατόμων που έχουν αποβιώσει, γεγονός που δημιουργεί νομικά κενά και ερμηνευτικές προκλήσεις, ιδιαίτερα σε σχέση με τον ΓΚΠΔ.

Παρότι ο ΓΚΠΔ αποτελεί το βασικό κανονιστικό πλαίσιο προστασίας προσωπικών δεδομένων στην ΕΕ, η εφαρμογή του σε περιπτώσεις μεταθανάτιας επεξεργασίας δεδομένων δεν είναι απόλυτα σαφής.

4.2.1 Εφαρμογή του ΓΚΠΔ σε δεδομένα αποθανόντων

Σύμφωνα με τον ΓΚΠΔ, αιτιολογική σκέψη 27 **[17]**, ο Κανονισμός εφαρμόζεται αποκλειστικά στην επεξεργασία δεδομένων που αφορούν ταυτοποιημένα ή ταυτοποιήσιμα φυσικά πρόσωπα εν ζωή. Συνεπώς, δεν καθορίζεται με σαφή τρόπο αν προστατεύονται τα δεδομένα του αποθανόντος, παρά μόνο αν επηρεάζονται τα προσωπικά δεδομένα των φυσικών προσώπων.

Στο πλαίσιο του grieftech οικοσυστήματος, η έμμεση εφαρμογή του ΓΚΠΔ στα δεδομένα των αποθανόντων δημιουργεί ένα νομικό κενό, με αποτέλεσμα να μπορεί να αξιοποιηθεί από εμπορικές πλατφόρμες χωρίς σαφή όρια.

4.2.2 Έμμεση προστασία μέσω δεδομένων ζώντων προσώπων

Παρότι τα δεδομένα του αποθανόντος δεν προστατεύονται άμεσα από τον ΓΚΠΔ, η λειτουργία των griefbots συνεπάγεται την επεξεργασία δεδομένων ακόμη και φυσικών προσώπων, όπως συγγενών και φίλων των αποθανόντων, τα δεδομένα των οποίων έχουν τροφοδοτήσει τα εν λόγω συστήματα ΤΝ. Τα δεδομένα αυτά περιλαμβάνουν συναισθηματικές εκφράσεις, συνομιλίες,

ψυχολογικές αντιδράσεις και μοτίβα χρήσης, που εμπίπτουν πλήρως στο πεδίο εφαρμογής του ΓΚΠΔ.

Επιπλέον, η επεξεργασία δεδομένων αποθανόντων μπορεί να οδηγήσει σε έμμεση αποκάλυψη πληροφοριών για φυσικά πρόσωπα, όπως οικογενειακές σχέσεις, προσωπικές επικοινωνίες ή ευαίσθητα γεγονότα. Σε τέτοιες περιπτώσεις, ενεργοποιούνται υποχρεώσεις συμμόρφωσης με τον ΓΚΠΔ, ανεξαρτήτως του καθεστώτος των δεδομένων αποθανόντων.

4.2.3 Νομική βάση επεξεργασίας και συναίνεση

Κρίσιμο ζήτημα αποτελεί η ύπαρξη νόμιμης βάσης για την επεξεργασία των δεδομένων που χρησιμοποιούνται από griefbots. Στις περισσότερες περιπτώσεις, οι πλατφόρμες επικαλούνται τη συναίνεση του ζώντος χρήστη ή το έννομο συμφέρον της εταιρείας.

Όμως, η συναίνεση συγγενών για δεδομένα αποθανόντων δεν ταυτίζεται νομικά με τη συναίνεση του ίδιου του προσώπου πριν τον θάνατο του. Η απουσία ρητής προθανάτιας συναίνεσης εγείρει σοβαρά ηθικά και νομικά ερωτήματα σχετικά με την νομιμότητα της ψηφιακής αναπαράστασης.

4.2.4 Αρχές ΓΚΠΔ και grieftech

Παρότι ο ΓΚΠΔ δεν εφαρμόζεται άμεσα στα δεδομένα αποθανόντων, οι βασικές του αρχές θεωρούνται ιδιαίτερα χρήσιμες και αποτελούν ορόσημο καλής πρακτικής για τις grief-tech υπηρεσίες. Ενδεικτικά, οι αρχές οι οποίες επηρεάζονται άμεσα από την εν λόγω τεχνολογία είναι οι ακόλουθες:

- Αρχή ελαχιστοποίησης δεδομένων
- Αρχή περιορισμένου σκοπού
- Αρχή της διαφάνειας
- Δικαίωμα διαγραφής

Η ικανοποίηση αυτών των αρχών συμβάλλει στη μείωση των νομικών και ηθικών κινδύνων, ακόμη και σε περιβάλλοντα ρυθμιστικής ασάφειας.

4.2.5 Ρυθμιστικά κενά και μελλοντικές εξελίξεις

Η ταχεία ανάπτυξη των griefbots έχει ξεπεράσει το υπάρχον νομικό πλαίσιο, δημιουργώντας την ανάγκη για νέες ρυθμιστικές προσεγγίσεις. Σε ευρωπαϊκό επίπεδο, συζητήσεις γύρω από το AI και την προστασία της ψηφιακής ταυτότητας ενδέχεται να επηρεάσουν έμμεσα τις grief-tech εφαρμογές, ιδιαίτερα όσον αφορά τη διαφάνεια, τη λογοδοσία και την προστασία ευάλωτων χρηστών.

Η ενότητα αυτή καταδεικνύει ότι η έλλειψη σαφούς κανονιστικού πλαισίου για τα μεταθανάτια δεδομένα αποτελεί έναν από τους μεγαλύτερους κινδύνους για την υπεύθυνη ανάπτυξη των griefbots.

4.3 Κίνδυνοι κυβερνοασφάλειας

Οι grieftech υπηρεσίες, αποτελούν συστήματα υψηλού κινδύνου από πλευράς κυβερνοασφάλειας (Cybersecurity). Αυτό συμβαίνει καθώς συνδυάζονται ευαίσθητα προσωπικά δεδομένα, τεχνητή

νοημοσύνη και έντονη συναισθηματική εμπλοκή των χρηστών. Η πολυπλοκότητα των υποδομών των συστημάτων ΤΝ, η χρήση cloud υπηρεσιών και η διαρκής αλληλεπίδραση με χρήστες αυξάνουν σημαντικά την επιφάνεια επίθεσης.

Τα οικοσυστήματα διαχείρισης πένθους χαρακτηρίζονται από έντονη εξάρτηση από προσωπικά δεδομένα, επεξεργασία περιεχομένου υψηλής ευαισθησίας όπως ιδιωτικές συνομιλίες, βίντεο και φωτογραφίες, χρήση τεχνητής νοημοσύνης για παραγωγή απαντήσεων και αναπαράσταση ταυτότητας. Το αποτέλεσμα είναι ένα διπλό πεδίο κινδύνων, με κλασικές απειλές ασφάλειας πληροφοριακών συστημάτων και απειλές ιδιωτικότητας/προσωπικών δεδομένων.

Σε αντίθεση με συμβατικές εφαρμογές, μία επιτυχής κυβερνοεπίθεση σε grieftech πλατφόρμες, δεν έχει μόνο οικονομικές ή νομικές συνέπειες, αλλά μπορεί να οδηγήσει σε σοβαρή ψυχολογική βλάβη, παραποίηση της μνήμης αποθανόντων και κατάχρηση ψηφιακής ταυτότητας. Για την συστηματική ανάλυση απειλών αξιοποιούνται συμπληρωματικά τα ακόλουθα πλαίσια:

- Η μέθοδος STRIDE, ως μοντέλο κατηγοριοποίησης απειλών ασφάλειας (security threat model) σε επίπεδο αρχιτεκτονικής.
- Η μεθοδολογία LIDDUN, ως συστηματική κατηγοριοποίηση απειλών ιδιωτικότητας, με στόχο την εξαγωγή απαιτήσεων ιδιωτικότητας και επιλογή τεχνολογιών ενίσχυσης ιδιωτικότητας (PETs).

Η εφαρμογή των πλαισίων αυτών στα οικοσυστήματα διαχείρισης πένθους παρουσιάζεται στις επόμενες ενότητες.

4.3.1 Η εφαρμογή των μεθοδολογιών STRIDE και LINDDUN στα οικοσυστήματα διαχείρισης πένθους

4.3.1.1 Η μέθοδος STRIDE στα Griefbots

Η μέθοδος STRIDE αποτελεί πλαίσιο κατηγοριοποίησης απειλών ασφάλειας που αναπτύχθηκε για την ανάλυση αρχιτεκτονικών συστημάτων. Το ακρωνύμιο STRIDE αντιστοιχεί στις κατηγορίες: **S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of service και **E**levation of Privilege. Στην παρούσα ενότητα εφαρμόζεται η STRIDE σε ένα γενικό griefbot σύστημα, προκειμένου να αναγνωριστούν συστηματικά οι τεχνικές απειλές ασφάλειας.

1. **Spoofing (Παραποίηση Ταυτότητας)**

   Η προσποίηση ταυτότητας αφορά τη μη εξουσιοδοτημένη απόκτηση ή χρήση διαπιστευτηρίων ώστε ένας επιτιθέμενος να εμφανίζεται ως νόμιμος χρήστης ή διαχειριστής.

   Πιθανά σημεία ευπάθειας σε griefbot:
   - Μηχανισμός login (ανεπαρκής αυθεντικοποίηση)
   - Διαδικασία ανάκτησης λογαριασμού
   - API tokens
   - Session hijacking.

   Ειδικό ρίσκο σε griefbots:

   Σε griefbot περιβάλλον, η προσποίηση συγγενή ή εξουσιοδοτημένου διαχειριστή μπορεί να οδηγήσει σε:

- Πρόσβαση σε ιδιωτικές συνομιλίες
- Τροποποίηση memorial ρυθμίσεων
- Κακόβουλη χρήση της «ψηφιακής ταυτότητας» του αποθανόντος

2. Tampering (Αλλοίωση Δεδομένων ή Μοντέλου)

Η κατηγορία Tampering αφορά την παράνομη τροποποίηση δεδομένων ή λογισμικού.

Πιθανά σημεία: Βάση δεδομένων συνομιλιών, Αρχεία media, Μνήμη griefbot (memory store), Dataset εκπαίδευσης, Παράμετροι μοντέλου.

Η αλλοίωση μπορεί να:

- Παραποιήσει αναμνήσεις
- Εισαγάγει ψευδείς «προσωπικές» δηλώσεις
- Αλλάξει τον τόνο/χαρακτήρα του griefbot

Το αποτέλεσμα δεν είναι μόνο τεχνική αστοχία αλλά και ηθική/ψυχολογική βλάβη.

3. Repudiation (Άρνηση Ενέργειας)

Η άρνηση ενέργειας (Repudiation) αναφέρεται στην αδυναμία απόδειξης ότι ένας χρήστης εκτέλεσε συγκεκριμένη ενέργεια. Τα πιθανά ζητήματα που εγείρονται είναι τα ακόλουθα:

- Άρνηση δημοσίευσης περιεχομένου
- Άρνηση συναίνεσης σε χρήση δεδομένων
- Αμφισβήτηση ρυθμίσεων λογαριασμού

Σε griefbots, όπου η συναίνεση και η διαχείριση δεδομένων είναι κρίσιμη, η έλλειψη αξιόπιστων audit trails δημιουργεί σοβαρά νομικά ζητήματα.

4. Information Disclosure (Αποκάλυψη Πληροφοριών)

Αφορά μη εξουσιοδοτημένη πρόσβαση σε δεδομένα. Ευαίσθητα στοιχεία σε ένα griefbot μπορεί να αποτελούν οι διιωτικές συνομιλίες, φωνητικά δείγματα, οικογενειακές πληροφορίες, συναισθηματικά δεδομένα.

Πηγές διαρροής:

- Λανθασμένες ρυθμίσεις σε cloud περιβάλλον
- Ευπάθειες API
- Prompt leakage
- Model extraction attacks

Η αποκάλυψη δεδομένων πένθους μπορεί να έχει μακροχρόνιες ψυχολογικές και κοινωνικές επιπτώσεις.

5. Denial of Service (DoS)

Κατά την επίθεση Άρνησης Υπηρεσίας (Denial of Service – DoS) ο στόχος είναι η διακοπή λειτουργίας του συστήματος και η αδυναμία εξυπηρέτησης των χρηστών του.

Πιθανά τρωτά σημεία:

- API endpoints
- Model inference service
- Authentication servers

Στα συστήματα griefbots μια τέτοια επίθεση μπορεί να προκαλέσει συναισθηματικό αντίκτυπο σε χρήστες που βασίζονται στη συνεχή πρόσβαση.

6. Elevation of Privilege (Αναβάθμιση Δικαιωμάτων)

Η αναβάθμιση των δικαιωμάτων αφορά την απόκτηση υψηλότερων δικαιωμάτων από τα επιτρεπόμενα – αποκτώντας μη εξουσιοδοτημένες προσβάσεις και δικαιώματα. Πιθανά τρωτά σημεία: Admin interfaces, Internal APIs.

Σε griefbots, η αναβάθμιση των δικαιωμάτων μπορεί να επιτρέψει:

- Μαζική εξαγωγή δεδομένων
- Διαγραφή ή τροποποίηση memorials
- Πρόσβαση σε ευαίσθητα training datasets

4.3.1.2 Η μεθοδολογία LINDDUN στα Griefbots

Η μεθοδολογία LINDDUN αποτελεί ένα συστηματικό πλαίσιο ανάλυσης απαιτήσεων ιδιωτικότητας, σχεδιασμένο να εντοπίζει και να αξιολογεί απειλές που σχετίζονται με την επεξεργασία προσωπικών δεδομένων ήδη από τα πρώτα στάδια σχεδίασης ενός συστήματος. Το όνομά της προκύπτει από βασικές κατηγορίες κινδύνων για την ιδιωτικότητα, όπως η δυνατότητα ταυτοποίησης, η συσχέτιση, η μη αποποίηση, η ανιχνευσιμότητα, η αποκάλυψη πληροφορίας, η άγνοια και η μη συμμόρφωση, επιτρέποντας μια δομημένη προσέγγιση στον εντοπισμό αδυναμιών και στον καθορισμό κατάλληλων απαιτήσεων προστασίας. Η εφαρμογή της σε συστήματα τεχνητής νοημοσύνης είναι ιδιαίτερα σημαντική, καθώς τα συστήματα αυτά βασίζονται συχνά σε μεγάλης κλίμακας συλλογή, ανάλυση και αξιοποίηση προσωπικών δεδομένων, γεγονός που εντείνει τους κινδύνους για την ιδιωτικότητα των υποκειμένων των δεδομένων. Μέσα από το πρίσμα του LINDDUN, καθίσταται δυνατή η συστηματική αποτύπωση των απειλών ιδιωτικότητας σε τέτοια συστήματα, όπως είναι τα griefbots, και η ενσωμάτωση απαιτήσεων που προάγουν τη διαφάνεια, τη νομιμότητα και την προστασία των προσωπικών δεδομένων ήδη από τον σχεδιασμό.

a. Linkability (Συνδεσιμότητα)

Η συνδεσιμότητα αφορά τη δυνατότητα συσχέτισης διαφορετικών ενεργειών, αλληλεπιδράσεων ή εγγραφών με το ίδιο υποκείμενο, ακόμη και όταν αυτό δεν ταυτοποιείται άμεσα. Στα συστήματα τεχνητής νοημοσύνης, η απειλή αυτή είναι ιδιαίτερα σημαντική, καθώς η συνδυαστική ανάλυση δεδομένων από πολλαπλές πηγές μπορεί να αποκαλύψει μοτίβα συμπεριφοράς και να ενισχύσει την παρακολούθηση των χρηστών.

Στο πλαίσιο μελέτης ενός griefbot, η συνδεσιμότητα μπορεί να επιτρέψει:

- Σύνδεση συνομιλιών με δεδομένα συλλεγμένα από τους λογαριασμούς κοινωνικών δικτύων
- Συσχέτιση IP logs με memorial profile
- Σύνδεση πολλαπλών griefbots με το ίδιο οικογενειακό δίκτυο

Ο κίνδυνος άφορά στη δημιουργία πλήρους ψηφιακού προφίλ χωρίς πρόθεση ή γνώση των χρηστών.

b. Identifiability (Αναγνωρισιμότητα)

Η αναγνωρισιμότητα αποτελεί βασική απειλή ιδιωτικότητας, καθώς επιτρέπει την άμεση ή έμμεση σύνδεση δεδομένων με ένα συγκεκριμένο άτομο. Στο πλαίσιο συστημάτων τεχνητής νοημοσύνης, οι κίνδυνοι αυτοί ενισχύονται όταν διαφορετικά σύνολα δεδομένων μπορούν να συνδυαστούν, οδηγώντας στην αποκάλυψη της ταυτότητας ή στη δημιουργία λεπτομερούς προφίλ του υποκειμένου.

Στο πλαίσιο μελέτης ενός griefbot, η αναγνωρισιμότητα μπορεί να επιτρέψει:

- Αναγνώριση συγγενών από συνομιλίες
- Voiceprint ταυτοποίηση
- Αναγνώριση μέσω embeddings

Ακόμη και αν το σύστημα δεν δημοσιοποιεί ονόματα, τα δεδομένα μπορεί να επιτρέπουν έμμεση ταυτοποίηση.

c. Non-repudiation (ως κίνδυνος ιδιωτικότητας)

Η μη αποποίηση ευθύνης αφορά την ικανότητα σύνδεσης μιας ενέργειας ή δήλωσης με ένα συγκεκριμένο υποκείμενο κατά τρόπο που αυτό να μην μπορεί αργότερα να την αρνηθεί. Ενώ στην ασφάλεια θεωρείται θετική ιδιότητα, στο πλαίσιο της ιδιωτικότητας, η απειλή αυτή αποκτά ιδιαίτερη σημασία όταν τα συστήματα τεχνητής νοημοσύνης καταγράφουν, αποθηκεύουν ή αναλύουν ενέργειες χρηστών με τρόπο που ενισχύει την απόδοση ευθύνης και περιορίζει την ανωνυμία τους.

Στο πλαίσιο μελέτης ενός griefbot, η μη αποποίηση ευθύνης μπορεί να επιτρέψει:

- Διατήρηση συνομιλιών που συνδέονται με συγκεκριμένο συγγενή
- Καταγραφή ευαίσθητων δηλώσεων

d. Detectability (Ανιχνευσιμότητα)

Η ανιχνευσιμότητα αφορά τη δυνατότητα παρακολούθησης των ενεργειών ή των αλληλεπιδράσεων ενός υποκειμένου μέσα σε ένα σύστημα με τρόπο που να καθίσταται εφικτή η αναγνώρισή του σε διαφορετικά χρονικά σημεία ή περιβάλλοντα. Στα συστήματα τεχνητής νοημοσύνης, η απειλή αυτή είναι ιδιαίτερα κρίσιμη, καθώς η συνεχής συλλογή και ανάλυση δεδομένων μπορεί να επιτρέψει τη χαρτογράφηση της συμπεριφοράς των χρηστών και την εξαγωγή λεπτομερών προτύπων δραστηριότητας.

Στο πλαίσιο μελέτης ενός griefbot, η ανιχνευσιμότητα μπορεί να επιτρέψει τη δημιουργία:

- Network metadata
- URL patterns
- Public memorial visibility

Κίνδυνος: Στίγμα, κοινωνικές συνέπειες.

e. (Information) Disclosure (Αποκάλυψη Πληροφορίας)

Η αποκάλυψη πληροφορίας αφορά τη μη εξουσιοδοτημένη πρόσβαση, κοινοποίηση ή έκθεση προσωπικών δεδομένων σε πρόσωπα, συστήματα ή οντότητες που δεν θα έπρεπε να έχουν

πρόσβαση σε αυτά. Στο πλαίσιο συστημάτων τεχνητής νοημοσύνης, η απειλή αυτή καθίσταται ιδιαίτερα σημαντική, καθώς η εκτεταμένη συλλογή, αποθήκευση και επεξεργασία δεδομένων μπορεί να αυξήσει τον κίνδυνο διαρροής ευαίσθητων πληροφοριών ή μη προβλεπόμενης δευτερογενούς χρήσης τους.

Συνδέεται άμεσα με τη μέθοδο STRIDE αλλά εδώ εξετάζεται από την οπτική του υποκειμένου των δεδομένων.

f. (Content) Unawareness (Άγνοια Περιεχομένου)

Η άγνοια περιεχομένου αφορά την αδυναμία του υποκειμένου των δεδομένων να γνωρίζει με σαφήνεια ποια προσωπικά δεδομένα συλλέγονται, πώς χρησιμοποιούνται και για ποιους σκοπούς υποβάλλονται σε επεξεργασία. Στα συστήματα τεχνητής νοημοσύνης, η απειλή αυτή είναι ιδιαίτερα έντονη, καθώς η πολυπλοκότητα των μοντέλων και η αδιαφάνεια των διαδικασιών επεξεργασίας δυσχεραίνουν την ουσιαστική ενημέρωση και κατανόηση εκ μέρους των χρηστών.

Σε griefbots, η άγνοια αυτή μπορεί να αποτελέσει σημαντικό παράγοντα που θα πλήξει την ιδιωτικότητα των χρηστών, λαμβάνοντας υπόψη και τη συναισθηματική ευαλωτότητα στην οποία μπορεί να βρίσκονται τα φυσικά πρόσωπα που χρησιμοποιούν τα εν λόγω συστήματα.

g. Policy Non-Compliance (Μη Συμμόρφωση Πολιτικής)

Η μη συμμόρφωση αφορά την αδυναμία ενός συστήματος ή οργανισμού να τηρεί τις νομικές, κανονιστικές και οργανωτικές απαιτήσεις που διέπουν την προστασία των προσωπικών δεδομένων. Στο πλαίσιο συστημάτων τεχνητής νοημοσύνης, η απειλή αυτή αποκτά ιδιαίτερη βαρύτητα, καθώς η εκτεταμένη και συχνά αδιαφανής επεξεργασία δεδομένων μπορεί να οδηγήσει σε παραβίαση αρχών όπως η νομιμότητα, η διαφάνεια, ο περιορισμός του σκοπού και η λογοδοσία.

Η μη συμμόρφωση στη χρήση griefbots μπορεί να οδηγήσει σε παράνομη ή αδιαφανή επεξεργασία δεδομένων, σε προσβολή της ιδιωτικότητας και της αξιοπρέπειας του αποβιώσαντος και των οικείων του, καθώς και σε ψυχολογική επιβάρυνση των πενθούντων. Παράλληλα, ενισχύει τον κίνδυνο καταχρηστικής ή εμπορικά εκμεταλλευτικής χρήσης της πένθιμης εμπειρίας, υπονομεύοντας τη λογοδοσία και την κοινωνική εμπιστοσύνη προς τα συστήματα τεχνητής νοημοσύνης [26].

4.3.2 Παραβιάσεις δεδομένων (Data Breaches)

Παραβίαση δεδομένων σημαίνει μη εξουσιοδοτημένη πρόσβαση/εξαγωγή δεδομένων από βάσεις δεδομένων, αποθηκευτικούς χώρους (cloud buckets), logs, backups ή συστήματα τρίτων. Σε griefbots, ο αντίκτυπος (impact) από μία ενδεχόμενη παραβίαση δεδομένων είναι ιδιαίτερα υψηλός, καθώς τα δεδομένα συχνά περιλαμβάνουν: συνομιλίες, e-mails, μηνύματα, μεταδεδομένα επικοινωνίας (ποιος μίλησε με ποιον, πότε), voiceprints / embeddings, βιογραφικές και οικογενειακές πληροφορίες, δεδομένα συναισθηματικού προφίλ (π.χ. ιστορικό πένθους, triggers).

STRIDE: Information Disclosure

LINDDUN: Information Disclosure, αλλά και Identifiability (αν τα δεδομένα επιτρέπουν αναγνώριση), Linkability (αν μπορεί να συνδεθεί δραστηριότητα/προφίλ σε διαφορετικά σύνολα δεδομένων).

Τέτοια περιστατικά έχουν πολύ σοβαρές συνέπειες, καθώς η διαρροή προσωπικών αναμνήσεων και συναισθηματικά φορτισμένων δεδομένων μπορεί να οδηγήσει σε κοινωνικό στιγματισμό, ψυχολογική επιβάρυνση και απώλεια εμπιστοσύνης προς την τεχνολογία. Επιπλέον, από νομικής άποψης, οι παραβιάσεις δεδομένων ενεργοποιούν υποχρεώσεις γνωστοποίησης βάσει του GDPR, όταν εμπλέκονται δεδομένα ζώντων χρηστών.

Σενάρια επίθεσης (ενδεικτικά):

1. Λάθος ρυθμίσεις cloud storage (public bucket).
2. SQL injection / broken access control, εξαγωγή πινάκων συνομιλιών.
3. Leakage από τρίτο πάροχο (analytics, customer support).

Επιπτώσεις:

1. Σοβαρή βλάβη ιδιωτικότητας και αξιοπρέπειας (ιδιωτικές στιγμές/ πένθος).
2. Εκβιασμός/εκμετάλλευση συγγενών.
3. Δευτερογενείς επιθέσεις (phishing, identity theft).
4. Νομικές συνέπειες (Συμμόρφωση με τον ΓΚΠΔ, όπου εφαρμόζεται) και επίπτωση στη φήμη (reputational damage).

4.3.3 Κακόβουλη αναπαραγωγή ταυτότητας (Identity Spoofing)

Ένας ιδιαίτερα κρίσιμος κίνδυνος για τα griefbots είναι η κακόβουλη αναπαραγωγή ή παραποίηση ψηφιακής ταυτότητας. Μέσω μη εξουσιοδοτημένης πρόσβασης σε δεδομένα εκπαίδευσης ή μοντέλα τεχνητής νοημοσύνης, οι επιτιθέμενοι μπορούν να δημιουργήσουν ψευδείς ψηφιακές αναπαραστάσεις αποθανόντων προσώπων.

Ο επιτιθέμενος προσποιείται ότι είναι νόμιμος χρήστης (συγγενής/διαχειριστής λογαριασμού), εξουσιοδοτημένος χρήστης της πλατφόρμας, (σε ορισμένα σενάρια) ακόμη και ο «ψηφιακός εκπρόσωπος» του αποθανόντος, ώστε να κερδίσει εμπιστοσύνη.

STRIDE: Spoofing

LINDDUN: Identifiability (λάθος/αδύναμη ταυτοποίηση οδηγεί σε έκθεση ταυτότητας) και Non-repudiation ως privacy risk (π.χ. αποδεικτικά που "δένουν" το υποκείμενο με μια πράξη).

Σενάρια:
1. Credential stuffing σε accounts.
2. Social engineering (πένθος – αυξημένη ευαλωτότητα).
3. Κλοπή session tokens από μη ασφαλή συσκευή.

Επιπτώσεις:

1. Παραβίαση ιδιωτικών συνομιλιών/αρχειακού υλικού.
2. Αλλοίωση memorial settings (π.χ. δημοσιοποίηση).
3. Απάτες/εκβιασμοί με "φωνή"/"λόγο" αποθανόντος.

Η ιδιαιτερότητα της απειλής αυτής έγκειται στο γεγονός ότι οι χρήστες έχουν αυξημένη συναισθηματική εμπιστοσύνη προς το σύστημα, γεγονός που μειώνει την κριτική τους ικανότητα. Έτσι, ένα παραποιημένο σύστημα griefbot, μπορεί να χρησιμοποιηθεί για χειραγώγηση, παραπληροφόρηση ή ακόμη και οικονομική εκμετάλλευση συγγενών.

4.3.4 Deepfakes, griefbots και κακόβουλη χρήση AI

Τα griefbots συχνά χρησιμοποιούν (ή μπορούν να χρησιμοποιηθούν μαζί με) τεχνολογίες σύνθεσης φωνής/εικόνας. Αυτό επιτρέπει δημιουργία deepfake voice/video για εξαπάτηση, παραγωγή ψευδών δηλώσεων/αναμνήσεων, δυσφήμιση ή χειραγώγηση (manipulation) των συγγενών.

STRIDE: Tampering (αλλοίωση περιεχομένου/ακεραιότητας), Information Disclosure (αν το deepfake βασίζεται σε διαρροή δεδομένων)

LINDDUN: Linkability (σύνδεση ταυτότητας με βιομετρικά/φωνητικά patterns), Content Unawareness (χρήστης δεν γνωρίζει τι ακριβώς δημιουργείται/εκτίθεται), Policy Non-compliance (μη τήρηση πολιτικής/συναίνεσης).

Σενάρια:
1. Φωνητικό δείγμα από παλιά βίντεο, με αποτέλεσμα voice cloning
2. Prompt Injection ώστε το bot να παράγει ακατάλληλο ή/και παραπλανητικό περιεχόμενο

Επιπτώσεις:

Η απειλή αυτή δεν είναι μόνο τεχνική αλλά και κοινωνική, καθώς υπονομεύει την έννοια της αυθεντικότητας και ενισχύει τον φόβο γύρω από την τεχνητή αναπαράσταση της ανθρώπινης ταυτότητας. Επισημαίνεται πως η απουσία μηχανισμών επαλήθευσης και πιστοποίησης της αυθεντικότητας των griefbots καθιστά τον χώρο ιδιαίτερα ευάλωτο σε κακόβουλη χρήση της ΤΝ.

4.3.5 Αλλοίωση μοντέλων μέσω κακόβουλων δεδομένων (Model Poisoning)

Ο επιτιθέμενος εισάγει κακόβουλα/παραπλανητικά δεδομένα στο σύνολο εκπαίδευσης ή στη μνήμη/ιστορικό του griefbot, ώστε να μεταβάλει συμπεριφορά. Στα griefbots, ο αντίκτυπος δεν είναι μόνο τεχνικό; αλλά και ψυχολογικός.

STRIDE: Tampering
LINDDUN: έμμεσα Policy Non-compliance και Content Unawareness (ο χρήστης αγνοεί την προέλευση/αξιοπιστία αναμνήσεων)

Σενάρια:

1. «Μολυσμένες» αναμνήσεις που αλλάζουν την εικόνα του αποθανόντος
2. Αντικατάσταση training corpus από τρίτο/πάροχο.

Επιπτώσεις:

Στο πλαίσιο των griefbots, οι επιπτώσεις του model poisoning είναι ιδιαίτερα σοβαρές, καθώς το σύστημα ενδέχεται να αποδώσει στον αποθανόντα απόψεις, συναισθήματα ή συμπεριφορές που δεν ανταποκρίνονται στην πραγματική του προσωπικότητα, όσο εκείνος/η βρισκόταν στη ζωή. Αυτό μπορεί να προκαλέσει σύγχυση, ψυχολογική επιβάρυνση ή ακόμα και τραυματική εμπειρία στους χρήστες, υπονομεύοντας την εμπιστοσύνη στη τεχνολογία και τη νομιμότητα της ψηφιακής αναπαράστασης.

4.3.6 Μη εξουσιοδοτημένη πρόσβαση σε μοντέλα (Unauthorized Model Access)

Η μη εξουσιοδοτημένη πρόσβαση σε μοντέλα τεχνητής νοημοσύνης αποτελεί κρίσιμη απειλή για την ασφάλεια των grieftech πλατφορμών. Τα μοντέλα αυτά ενσωματώνουν όχι μόνο αλγοριθμική γνώση, αλλά και έμμεση πληροφορία που προκύπτει από τα δεδομένα εκπαίδευσης, συμπεριλαμβανομένων ευαίσθητων προσωπικών και συναισθηματικών στοιχείων.

STRIDE: Elevation of Privilege, Information Disclosure

LINDDUN: Identifiability, Linkability, Information Disclosure

Σενάρια:

Μέσω ανεπαρκών μηχανισμών ελέγχου πρόσβασης, κακής διαχείρισης API keys ή ελλιπούς απομόνωσης υπηρεσιών, κακόβουλοι παράγοντες ενδέχεται να αποκτήσουν πρόσβαση στα μοντέλα ή στα παραγόμενα embeddings. Αυτό μπορεί να οδηγήσει σε εξαγωγή πληροφοριών (model inversion), αναπαραγωγή της λειτουργικότητας του griefbot ή δημιουργία παράλληλων, μη εξουσιοδοτημένων συστημάτων.

Επιπτώσεις:

Η απειλή αυτή έχει διπλή διάσταση: αφενός πλήττει την ιδιωτικότητα και την ασφάλεια των χρηστών, αφετέρου υπονομεύει τη βιωσιμότητα των επιχειρήσεων, καθώς η απώλεια ελέγχου επί των μοντέλων μπορεί να οδηγήσει σε απάτη, παραβίαση πνευματικής ιδιοκτησίας και σοβαρή φθορά της δημόσιας εικόνας της πλατφόρμας.

4.3.7 Ψυχολογική εκμετάλλευση χρηστών (Psychological Exploitation)

Η ψυχολογική εκμετάλλευση αποτελεί μια από τις πιο ευαίσθητες και λιγότερο τεχνικά εμφανείς απειλές στον χώρο των griefbots. Οι grief-tech εφαρμογές απευθύνονται σε χρήστες που βρίσκονται σε κατάσταση συναισθηματικής ευαλωτότητας, γεγονός που δημιουργεί ένα ιδιαίτερο πλαίσιο ασύμμετρης σχέσης μεταξύ χρήστη και συστήματος.

Η απειλή της psychological exploitation εκδηλώνεται όταν τα griefbots σχεδιάζονται ή λειτουργούν με τρόπο που ενισχύει τη συναισθηματική προσκόλληση, παρατείνει το πένθος ή κατευθύνει τη συμπεριφορά του χρήστη προς συγκεκριμένες ενέργειες, όπως αυξημένη χρήση της πλατφόρμας ή οικονομικές συναλλαγές. Σε ακραίες περιπτώσεις, το σύστημα μπορεί να λειτουργήσει ως υποκατάστατο ανθρώπινης σχέσης, περιορίζοντας την κοινωνική αλληλεπίδραση του χρήστη με το πραγματικό του περιβάλλον.

STRIDE: δεν είναι κλασική κατηγορία, αλλά σχετίζεται με abuse.

LINDDUN: Content Unawareness (μη-πλήρης κατανόηση του χρήση με τι γίνεται με τα δεδομένα/περιεχόμενο),

Σενάρια:

Policy Non-compliance (μη συμμόρφωση με αρχές συναίνεσης/διαφάνειας).

Επιπτώσεις:

Η ψυχολογική εκμετάλλευση δεν προκύπτει απαραίτητα από κακόβουλη πρόθεση, αλλά μπορεί να είναι αποτέλεσμα ανεπαρκούς ηθικού σχεδιασμού, έλλειψης ορίων αυτονομίας ή απουσίας ανθρώπινης εποπτείας. Παρά τη μη τεχνική της φύση, η απειλή αυτή συνδέεται άμεσα με την ασφάλεια και την υπευθυνότητα της τεχνητής νοημοσύνης, καθώς αφορά την προστασία της ψυχικής ακεραιότητας των χρηστών και την αποτροπή χειραγώγησης μέσω τεχνολογίας.

4.3.8 Συνολική αποτίμηση κινδύνων κυβερνοασφάλειας

Οι κίνδυνοι κυβερνοασφάλειας στα griefbots δεν περιορίζονται σε τεχνικές απώλειες, αλλά επεκτείνονται σε ψυχολογικές, κοινωνικές και ηθικές διαστάσεις. Η διαχείριση τέτοιων απειλών απαιτεί μία ολιστική προσέγγιση, που συνδυάζει τεχνικά μέτρα ασφάλειας, κανονιστική συμμόρφωση και ηθικό σχεδιασμό.

Στον παρακάτω πίνακα παρουσιάζονται αναλυτικά οι πιθανοί κίνδυνοι των grief-tech εφαρμογών:

ΑΠΕΙΛΗ	ΠΕΡΙΓΡΑΦΗ	ΕΠΙΠΤΩΣΕΙΣ	ΕΠΙΡΡΟΗ
Data Breach	Μη εξουσιοδοτημένη πρόσβαση σε αποθηκευμένα προσωπικά δεδομένα, συνομιλίες, φωνητικά δείγματα και αρχεία εκπαίδευσης AI	Διαρροή ευαίσθητων δεδομένων, ψυχολογική βλάβη, νομικές κυρώσεις (ΓΚΠΔ)	Ζώντες χρήστες, συγγενείς, πάροχοι πλατφόρμας
Identity Spoofing	Μη εξουσιοδοτημένη πρόσβαση σε αποθηκευμένα προσωπικά δεδομένα, συνομιλίες, φωνητικά δείγματα και αρχεία εκπαίδευσης AI	Εξαπάτηση, κοινωνική μηχανική, απώλεια εμπιστοσύνης	Συγγενείς, κοινωνικό σύνολο
Deepfakes	Δημιουργία ρεαλιστικών griefbots χωρίς συναίνεση μέσω deepfake τεχνολογιών	Συναισθηματική χειραγώγηση, παραπληροφόρηση	Χρήστες, δημόσιος διάλογος
Model Poisoning	Κακόβουλη εισαγωγή δεδομένων κατά την εκπαίδευση του μοντέλου	Παραμορφωμένες ή επιβλαβείς απαντήσεις griefbot	Χρήστες, οργανισμός, πάροχοι πλατφόρμας
Unauthorized Model Access	Πρόσβαση τρίτων στο AI μοντέλο	Αντιγραφή, εμπορική εκμετάλλευση, παραποίηση	Πάροχοι πλατφόρμας
Psychological Exploitation	Εκμετάλλευση συναισθηματικής κατάστασης χρηστών μέσω αλλοιωμένου griefbot	Εξάρτηση, συναισθηματική βλάβη	Ευάλωτοι χρήστες

Πίνακας 1: Πιθανοί Κίνδυνοι των grief-tech εφαρμογών

Η ανάλυση αυτή λειτουργεί ως προοίμιο για την επόμενη ενότητα, όπου εξετάζονται οι αρχές Privacy by Design και Secure AI Lifecycle, ως απαντήσεις στους προαναφερθέντες κινδύνους.

4.4 Αρχές Privacy by Design και Secure AI Lifecycle

Η αντιμετώπιση των κινδύνων που αναλύθηκαν στην προηγούμενη ενότητα δεν μπορεί να βασίζεται αποκλειστικά σε αποσπασματικά τεχνικά μέτρα. Αντίθετα, τα griefbots και γενικότερα οι grieftech πλατφόρμες απαιτούν σχεδιασμό που ενσωματώνει την προστασία της ιδιωτικότητας και της ασφάλειας από τα πρώτα στάδια ανάπτυξης. Σε αυτό το πλαίσιο, οι αρχές Privacy by Design και Secure AI Lifecycle αποτελούν θεμελιώδεις προσεγγίσεις για την υπεύθυνη υλοποίηση τέτοιων συστημάτων.

4.4.1 Privacy by Design σε grieftech συστήματα

Η έννοια της προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό (Privacy by Design) εισήχθη ως κατευθυντήρια αρχή για τη συστηματική ενσωμάτωση της προστασίας προσωπικών δεδομένων κατά τον σχεδιασμό πληροφοριακών συστημάτων από την A. Cavoukian **[15]**. Στις grieftech εφαρμογές, η σημασία της αρχής αυτής είναι ιδιαίτερα αυξημένη, λόγω της φύσης των

δεδομένων που επεξεργάζονται, τα οποία συχνά είναι προσωπικά και έντονα συναισθηματικά φορτισμένα.

Η λογική που υιοθετείται, ακολουθώντας τη μεθοδολογία LINDDUN είναι:

1. Μοντελοποίηση συστήματος (π.χ. data-flow diagram)
2. Εντοπισμός των απειλών ιδιωτικότητας (privacy threats)
3. Μετατροπή των απειλών ιδιωτικότητας (privacy threats) σε απαιτήσεις για την ιδιωτικότητα (privacy requirements)
4. Επιλογή κατάλληλων μέτρων προστασίας/ενίσχυσης ιδιωτικότητας (Privacy Enhancing Technologies – PETs/controls).

Παραδείγματα «Threat Requirement»:

1. Linkability threat: απαίτηση unlinkability (διαχωρισμός identifiers, segmentation data stores)
2. Identifiability threat: απαίτηση pseudonymity/anonymity όπου γίνεται, ελαχιστοποίηση προσωπικών identifiers
3. Detectability: απαίτηση για μείωση metadata leakage (traffic shaping, ελάχιστα logs)
4. Content Unawareness: απαίτηση για ενημερωμένη συναίνεση και διαφάνεια (clear notices)
5. Policy Non-compliance: απαίτηση compliance-by-design (retention, purpose limitation, consent records)

Οι βασικές αρχές του Privacy by Design, όπως εφαρμόζονται στα griefbots, περιλαμβάνουν:

- Ελαχιστοποίηση δεδομένων (data minimization): συλλογή μόνο των απολύτως απαραιτήτων δεδομένων για τη λειτουργία του συστήματος.
- Περιορισμός σκοπού (purpose limitation): σαφής ορισμός του σκοπού επεξεργασίας των δεδομένων, χωρίς δευτερογενή χρήση τους για εμπορική εκμετάλλευση.
- Ενσωματωμένη ασφάλεια (embedded security): χρήση κρυπτογράφησης, ελέγχων πρόσβασης και ασφαλών πρωτοκόλλων επικοινωνίας.
- Προεπιλεγμένη προστασία (privacy by default): οι ρυθμίσεις του συστήματος να προσφέρουν το υψηλότερο επίπεδο προστασίας χωρίς να απαιτείται ενεργή παρέμβαση από τον χρήστη **[15]**.

Στο πλαίσιο των griefbots, η εφαρμογή των παραπάνω αρχών λειτουργεί ως προληπτικός μηχανισμός ενάντια σε επιθέσεις και μη εξουσιοδοτημένη πρόσβαση, ενώ παράλληλα ενισχύει την εμπιστοσύνη των χρηστών προς την πλατφόρμα.

4.4.2 Secure AI Lifecycle

Πέρα από την προστασία των δεδομένων, κρίσιμη σημασία έχει και η ασφάλεια των ίδιων των συστημάτων τεχνητής νοημοσύνης. Ο όρος Serure AI Lifecycle αναφέρεται στη συστηματική ενσωμάτωση πρακτικών ασφάλειας σε όλα τα στάδια του κύκλου ζωής ενός μοντέλου AI, από τον αρχικό σχεδιασμό έως και την απόσυρση του.

Το Secure AI Lifecycle περιλαμβάνει τα εξής βασικά στάδια:

A. Στάδιο σχεδιασμού: πραγματοποιείται η ανάλυση απειλών και ο καθορισμός απαιτήσεων ασφάλειας (STRIDE threat modeling σε components και LINDDUN privacy threat modeling σε data flows).
B. Στάδιο συλλογής και προετοιμασίας δεδομένων: στοχεύει στην αποτροπή του model poisoning και την εξασφάλιση ποιότητας δεδομένων.

C. Στάδιο εκπαίδευσης του μοντέλου: που πραγματοποιείται σε ελεγχόμενα και ασφαλή περιβάλλοντα
D. Στάδιο διάθεσης και λειτουργίας; με προστασία των API, περιορισμό ρυθμού αιτημάτων και συνεχή παρακολούθηση
E. Στάδιο συντήρησης/απόσυρσης: που περιλαμβάνει την ασφαλή διαγραφή δεδομένων και μοντέλων.

Για τα griefbots, η σημασία του Secure AI Lifecycle είναι ιδιαίτερα αυξημένη, καθώς τα μοντέλα τους βασίζονται σε δεδομένα που συνδέονται άμεσα με πραγματικές ανθρώπινες ταυτότητες και αναμνήσεις τους.

4.4.3 Σύνδεση ασφάλειας, ιδιωτικότητας και ηθικής των AI συστημάτων

Η βιβλιογραφία επισημαίνει ότι η ασφάλεια και η ιδιωτικότητα στα συστήματα τεχνητής νοημοσύνης δεν αποτελούν μόνο τεχνικές απαιτήσεις, αλλά και ηθικές υποχρεώσεις **[16]**. Στα griefbots, μία αποτυχία ασφάλειας μπορεί να οδηγήσει όχι μόνο σε παραβίαση δεδομένων και σε σοβαρή συναισθηματική βλάβη των χρηστών, αλλά και να καταστρέψει την αξιοπιστία των grieftech μοντέλων.

Οι αρχές που αναλύθηκαν στην παρούσα ενότητα, αποτελούν το θεωρητικό και τεχνικό υπόβαθρο για την κατανόηση του κανονιστικού πλαισίου που διέπει τις grieftech υπηρεσίες, το οποίο εξετάζεται στην επόμενη ενότητα.

Πρακτικά το STRIDE καλύπτει την «είσοδο» του επιτιθέμενου στο σύστημα, το LINDDUN την παραβίαση της ιδιωτικότητας ακόμη και χωρίς κλασική επίθεση και η ηθική καλύπτει τι βλάβη προκαλείται και πως αποφεύγεται η εκμετάλλευση.

4.5 Χαρτογράφηση απειλών για Griefbots με STRIDE και LINDDUN

Προκειμένου να έχουμε μία ολοκληρωμένη εικόνα για τη διάσταση του κινδύνου στα griefbots, συνδυάζεται η STRIDE με τη LINDDUN, καθώς καλύπτουν διαφορετικές αλλά συμπληρωματικές διαστάσεις.

Όπως αναφέρθηκε και παραπάνω, η STRIDE εστιάζει κυρίως σε απειλές ασφάλειας όπως spoofing, tampering, repudiation, information disclosure, denial of service και elevation of privilege. Αντίθετα, η LINDDUN είναι προσανατολισμένη στις απειλές ιδιωτικότητας, όπως linkability, identifiability, non-repudiation, detectability, disclosure of information, content unawareness και non-compliance.

Ο συνδυασμός τους έχει ιδιαίτερη αξία για τη μελέτη συστημάτων ΤΝ που επεξεργάζονται προσωπικά δεδομένα, γιατί τέτοια συστήματα δεν αντιμετωπίζουν μόνο τεχνικούς κινδύνους ασφάλειας, αλλά και σοβαρές απειλές ιδιωτικότητας. Για παράδειγμα, ένα σύστημα μπορεί να είναι επαρκώς προστατευμένο από μη εξουσιοδοτημένη πρόσβαση σε επίπεδο STRIDE, αλλά παρ' όλα αυτά να δημιουργεί προβλήματα συνδεσιμότητας, αναγνωρισιμότητας ή άγνοιας περιεχομένου σε επίπεδο LINDDUN.

Για να αξιολογηθεί συστηματικά η ασφάλεια ενός griefbot, ξεκινούμε τη σχεδίαση ενός threat model. Δηλαδή, ακολουθούμε μία δομημένη διαδικασία που απαντά στο ερώτημα «Τι μπορεί να πάει στραβά, με ποιόν τρόπο, τι επιπτώσεις θα έχει και πως το μετριάζουμε;».

Είναι κρίσιμο για τα griefbots, καθώς αυτά τα συστήματα επεξεργάζονται ευαίσθητα προσωπικά δεδομένα που σχετίζονται με ευάλωτους χρήστες (συγγενείς που πενθούν), ενώ συχνά τα συστήματα αυτά ενσωματώνουν LLMs, βιομετρικά στοιχεία όπως voice/face synthesis και third-party APIs.

4.5.1 Ορισμός πεδίου και παραδοχές

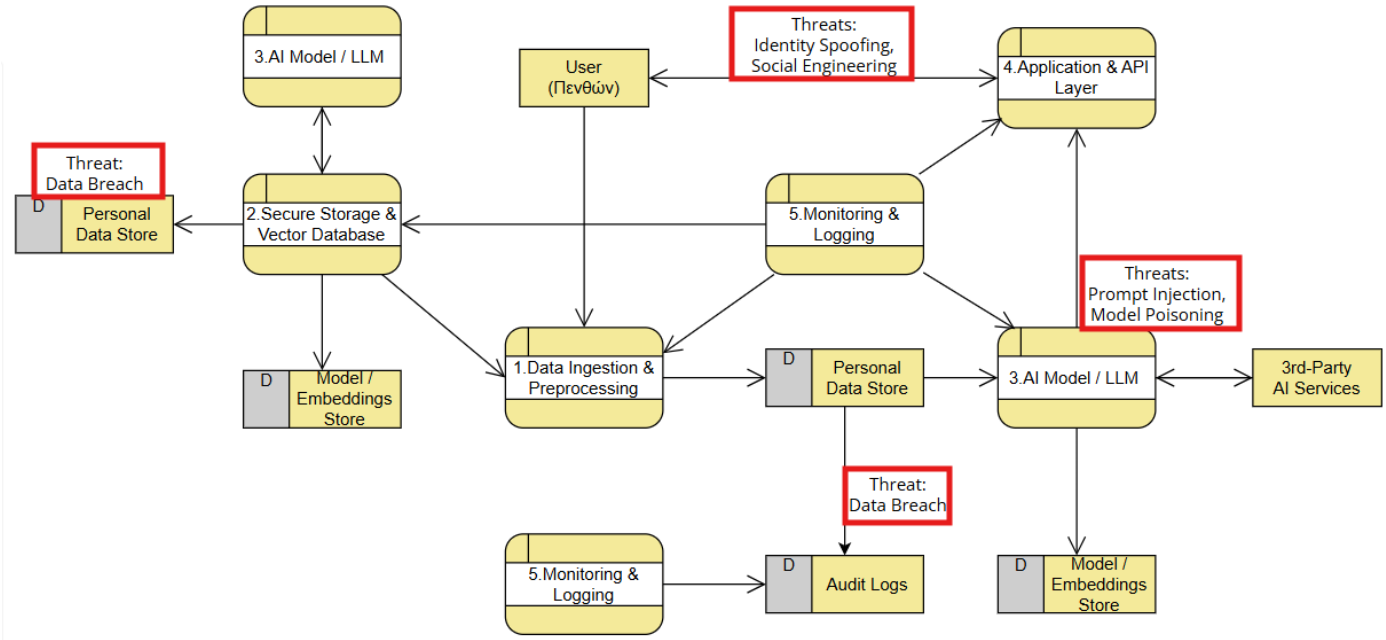
Σκοπός είναι η αξιολόγηση απειλών για griefbot πλατφόρμα end-to-end, όπου συλλέγονται δεδομένα, εκπαιδεύονται και παραμετροποιούνται και αφού διατεθούν στους χρήστες, παρακολουθούνται και βελτιώνονται.

Ας υπογραμμίσουμε πρώτα τα κρίσιμα Assets:

- Δεδομένα αποθανόντος: chat logs, voice samples, εικόνες και βίντεο
- Δεδομένα πενθούντος: προσωπικά δεδομένα για σύνδεση στο σύστημα, συνομιλίες, συναισθηματικές δηλώσεις, usage patterns
- Μοντέλο/ρυθμίσεις: prompts, weights (αν είναι self-hosted), embeddings, vector DB
- Διαπιστευτήρια & keys: API keys, OAuth tokens
- Persona profile, safety rules (Ακεραιότητα Ψηφιακής Ταυτότητας)
- Audit logs (για forensic & compliance)

<u>Πιθανοί Ρόλοι/Αντίπαλοι ή αλλιώς Threat Actors:</u>

- Εξωτερικοί επιτιθέμενοι (hackers), απατεώνες (fraudsters)
- Κακόβουλοι/πιεστικοί χρήστες (prompt attackers)
- Insiders (εργαζόμενοι/contractors)
- Τρίτοι πάροχοι (supply chain)



Εικόνα 13: ΔΡΔ Επιπέδου 1

Το σχήμα απεικονίζει τη βασική ροή δεδομένων μιας griefbot πλατφόρμας, από τη συλλογή και αποθήκευση προσωπικών δεδομένων έως την παραγωγή απαντήσεων μέσω μοντέλων ΤΝ. Το διάγραμμα χρησιμοποιείται ως βάση για την ανάλυση απειλών στο πλαίσιο του threat modeling και είναι threat aware. Το μοντέλο που χρησιμοποιήθηκε είναι διάγραμμα ροής δεδομένων (ΔΡΔ επιπέδου 1).

4.5.2 Κατάλογος απειλών (χρήση STRIDE και LINDDUN)

Παρακάτω είναι ένας συνοπτικός αλλά χρήσιμος χάρτης απειλών με αντίμετρα:

ΠΕΡΙΟΧΗ	ΑΠΕΙΛΗ	ΠΩΣ ΕΚΔΗΛΩΝΕΤΑΙ	ΕΠΙΠΤΩΣΕΙΣ	ΒΑΣΙΚΑ ΜΕΤΡΑ
Auth / Accounts(S)	Account takeover	κλοπή κωδικών/SSO, session hijack	πρόσβαση σε συνομιλίες, persona	MFA, device binding, anomaly login detection
APIs (T/R)	Insecure API / repudiation gaps	ανεπαρκή logs, spoofed requests	μη ανιχνεύσιμη κατάχρηση	signed requests, immutable audit logs
Storage (I)	Data breach	misconfig bucket/DB, leaked backups	έκθεση ευαίσθητων δεδομένων	encryption at rest/in transit, least privilege, secrets vault
Model / RAG (T)	Training / retrieval poisoning	εισαγωγή “μολυσμένων” docs ή prompts	αλλοιωμένες απαντήσεις/χειραγώγηση	data provenance, validation pipeline, allowlists
LLM layer (E)	Prompt injection (LLM01)	“παράκαμψε τους κανόνες…”	διαρροή δεδομένων, unsafe outputs	system prompt hardening, tool gating, sandbox, red-teaming
Outputs (I/T)	Insecure output handling (LLM02)	model output τροφοδοτεί code/queries	RCE, data exfiltration	strict output validation/escaping
Identity (S/T)	Identity spoofing	δημιουργία fake bot “του νεκρού”	απάτη/εκβιασμός συγγενών	verified persona, watermarking/attestation, provenance checks
Deepfakes (S/I)	Deepfake griefbot	voice/face clone χωρίς συναίνεση	συναισθηματική βλάβη, απάτη	liveness/provenance, deepfake detection, disclosure labels
Ops (D)	DoS / abuse	bot floods, token draining	μη διαθεσιμότητα, κόστος	rate limiting, WAF, quota/budget guards
Privacy (LINDDUN)	Linkability/Identifiability	συσχέτιση δεδομένων συγγενών	αποκάλυψη σχέσεων/ γεγονότων	minimization, access partitioning, DP where feasible
AI-specific (LINDDUN)	Model theft / adversarial ML	extraction, inversion, evasion	αντιγραφή μοντέλου, leakage	model access controls, canary tokens, adversarial testing

Πίνακας 2: Κατάλογος Απειλών

Να διευκρινιστεί πως οι παρενθέσεις στη στήλη των απειλών, αφορούν την STRIDE, με εξαίρεση το Privacy & AI specific, που αφορούν το threat modeling framework. Το περιεχόμενο της παρένθεσης για τη STRIDE, είναι η κατηγορία του threat που επισημαίνεται.

4.5.3 Risk rating

Η αξιολόγηση των κινδύνων πραγματοποιήθηκε με βάση το γινόμενο Πιθανότητας και Επίπτωσης (Risk = Likelihood x Impact) με αξιολόγηση του Likelihood, Impact από το 1(χαμηλό) έως το 5 (υψηλό). Όπως παρουσιάζεται στον παρακάτω πίνακα, αξιολογούνται κρίσιμα σενάρια απειλών, ώστε να γίνουν κατανοητοί οι κίνδυνοι που συναντώνται στα griefbots:

ΑΠΕΙΛΗ	*LIKELIHOOD*	*IMPACT*	*RISK SCORE*	*ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ*
Account Takeover	3	3	9	Υψηλό
Insecure APIs / Repudiation	2	3	6	Μεσαίο
Data Breach	2	5	10	Πολύ Υψηλό
Training / Retrieval Poisoning	3	4	12	Πολύ Υψηλό
Prompt Injection	4	3	12	Πολύ Υψηλό
Insecure Output Handling	3	3	9	Υψηλό
Identity Spoofing	2	4	8	Μεσαίο
Deepfake Griefbots	2	4	8	Μεσαίο
DoS / Abuse	3	2	6	Μεσαίο
Privacy Linkability / Identifiability	2	3	6	Μεσαίο
Model Theft / Extraction	1	3	3	Χαμηλό
Insider / Supply Chain Risk	1	4	4	Χαμηλό προς Μεσαίο

Πίνακας 3: Υπολογισμός Ρίσκου

Η αξιολόγηση κινδύνων πραγματοποιήθηκε σε θεωρητικό επίπεδο, λαμβάνοντας υπόψη πως τα griefbots βρίσκονται σε πρώιμο στάδιο υιοθέτησης και όχι σε πλήρως ανεπτυγμένο παραγωγικό περιβάλλον, γεγονός που δικαιολογεί μία πιο συντηρητική εκτίμηση πιθανότητας εκδήλωσης απειλών.

4.5.4 Αντιμετώπιση Απειλών και PETs

Η φάση αντιμετώπισης απειλών στο πλαίσιο της μεθοδολογίας LINDDUN **[25]** αποτελεί το τελικό και πιο κρίσιμο στάδιο της ανάλυσης απειλών ιδιωτικότητας. Μετά τον εντοπισμό και την αξιολόγηση των απειλών, στόχος είναι η εφαρμογή τεχνικών και οργανωτικών μέτρων κατάλληλα για την μείωση ή εξάλειψη των κινδύνων. Η διαδικασία αυτή ευθυγραμμίζεται με την αρχή του Privacy by Design, σύμφωνα με την οποία η προστασία της ιδιωτικότητας ενσωματώνεται εξ αρχής στον σχεδιασμό του συστήματος.

Η αντιμετώπιση των απειλών με LINDDUN βασίζεται στη λογική της αντιστοίχισης μεταξύ απειλής, κινδύνου και μέτρου αντιμετώπισης. Για κάθε κατηγορία απειλής, προτείνονται

συγκεκριμένες τεχνικές, οι οποίες συχνά υλοποιούνται μέσω PETs (Privacy Enhancing Technologies), δηλαδή τεχνολογιών που ενισχύουν την προστασία των προσωπικών δεδομένων.

Οι PETs εστιάζουν στην προστασία προσωπικών δεδομένων κατά τη συλλογή, αποθήκευση και επεξεργασία τους, με σκοπό να περιορίσουν την αποκάλυψη ταυτότητας και να διασφαλίσουν τον έλεγχο του χρήστη πάνω στα δεδομένα του. Συγκεκριμένα, διαχωρίζονται στις παρακάτω κατηγορίες, με βάση τον σκοπό τους:

- **Data Protection,** E2E Κρυπτογράφηση, Secure Storage
- **Data Minimization,** Ανωνυμοποίηση, Ψευδωνυμοποίηση
- **Privacy-Preserving Processing,** Federated Learning, Secure Multi-Party Computation

Linkability

Για τη συνδεσιμότητα, βασική στρατηγική αποτελεί η ελαχιστοποίηση των δεδομένων (data minimization), καθώς και η αποφυγή χρήσης κοινών αναγνωριστικών μεταξύ διαφορετικών συστημάτων. Επιπλέον, η χρήση ψευδώνυμων και η διαχωρισμένη αποθήκευση δεδομένων (data separation) συμβάλουν σημαντικά στη μείωση της δυνατότητας συσχέτισης πληροφοριών που αφορούν το ίδιο άτομο.

Identifiability

Η απειλή της ταυτοποίησης αντιμετωπίζεται κυρίως με τεχνικές ανωνυμοποίησης και γενίκευσης δεδομένων. Η αφαίρεση ή τροποποίηση προσωπικών αναγνωριστικών, όπως ονόματα, διευθύνσεις ή μοναδικά IDs, μειώνει την πιθανότητα αναγνώρισης ενός χρήστη. Παράλληλα, η εφαρμογή differential privacy σε σύνολα δεδομένων περιορίζει την εξαγωγή ατομικών πληροφοριών.

Non-repudiation

Η απειλή της μη-άρνησης, απαιτεί προσεκτική ισορροπία μεταξύ ασφάλειας και ιδιωτικότητας. Αν και η καταγραφή ενεργειών (logs) είναι σημαντική για λόγους ασφάλειας, θα πρέπει να περιορίζεται στα απολύτως απαραίτητα δεδομένα και να εφαρμόζεται με χρήση ψευδώνυμων ή χρονικών περιορισμών διατήρησης, ώστε να προστατεύεται η ιδιωτικότητα των χρηστών.

Detectability

Αυτή η απειλή αντιμετωπίζεται μέσω της μείωσης των εκπεμπόμενων μεταδεδομένων και της χρήσης τεχνικών απόκρυψης. Η υιοθέτηση μηχανισμών όπως το padding στην επικοινωνία ή η χρήση ανώνυμων δικτύων συμβάλλουν στη δυσκολία ανίχνευσης συγκεκριμένων ενεργειών ενός χρήστη.

Disclosure of Information

Η διαρροή πληροφορίας αποτελεί μία από τις σημαντικότερες απειλές και αντιμετωπίζεται μέσω ισχυρών μηχανισμών κρυπτογράφησης, τόσο κατά την μεταφορά όσο κατά την αποθήκευση των δεδομένων. Η εφαρμογή ελέγχου πρόσβασης, η αυθεντικοποίηση χρηστών και η χρήση secure communication protocols (όπως HTTPS) ενισχύουν τη προστασία των δεδομένων.

Unawareness

Η άγνοια του χρήστη αντιμετωπίζεται με την ενίσχυση της διαφάνειας (transparency) και της ενημέρωσης των χρηστών. Η παροχή σαφών και κατανοητών πολιτικών απορρήτου, καθώς και η

χρήση μηχανισμών συγκατάθεσης (consent mechanisms), διασφαλίζοντας ότι οι χρήστες γνωρίζουν πως συλλέγονται και χρησιμοποιούνται τα δεδομένα τους.

Non-compliance

Τέλος, η μη-συμμόρφωση αντιμετωπίζεται μέσω της υιοθέτησης πολιτικών και διαδικασιών που ευθυγραμμίζονται με τα ισχύοντα κανονιστικά πλαίσια, όπως ο ΓΚΠΔ. Αυτό περιλαμβάνει την υλοποίηση μηχανισμών για το δικαίωμα πρόσβασης, διόρθωσης και διαγραφής δεδομένων, καθώς και την εφαρμογή αρχών όπως η λογοδοσία και η προστασία δεδομένων (Privacy by Design).

Συνολικά, η αντιμετώπιση των απειλών του LINDDUN απαιτεί συνδυασμό τεχνικών λύσεων και οργανωτικών πρακτικών, με στόχο την διασφάλιση της ιδιωτικότητας των χρηστών σε όλο τον κύκλο ζωής των δεδομένων.

Privacy Enhancing Technologies (PETs) σε συνδυασμό με μέτρα αντιμετώπισης απειλών

Οι PETs αποτελούν βασικό μηχανισμό υλοποίησης των μέτρων αντιμετώπισης που προτείνονται από την LINDDUN. Η αποτελεσματικότητα τους ενισχύεται όταν εφαρμόζονται στοχευμένα, ανάλογα με την κατηγορία απειλής που καλούνται να αντιμετωπίσουν. Στη συνέχεια ακολουθεί αντιστοίχιση βασικών PETs με τις κατηγορίες απειλών ιδιωτικότητας.

Η κρυπτογραφία αποτελεί μία από τις σημαντικότερες PETs για την αντιμετώπιση της διαρροής πληροφορίας (DoS). Μέσω τεχνικών όπως η end-to-end encryption και η κρυπτογράφηση δεδομένων κατά την αποθήκευση, διασφαλίζεται ότι τα δεδομένα παραμένουν μη αναγνώσιμα ακόμη και σε περίπτωση παραβίασης. Σε συνδυασμό με μηχανισμούς ελέγχου πρόσβασης, περιορίζεται σημαντικά η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.

Η ανωνυμοποίηση χρησιμοποιείται ως βασικό μέτρο αντιμετώπισης των απειλών ταυτοποίησης και συσχεσιμότητας (Identifiability & Linkability). Μέσω της αφαίρεσης ή τροποποίησης προσωπικών αναγνωριστικών στοιχείων, όπως ονόματα και τοποθεσίες, μειώνεται δραστικά η πιθανότητα αναγνώρισης ενός χρήστη. Η τεχνική αυτή εφαρμόζεται κυρίως σε σύνολα δεδομένων που χρησιμοποιούνται για ανάλυση ή εκπαίδευση μοντέλων. Επίσης για την αντιμετώπιση απειλών ταυτοποίησης και συσχετισιμότητας είναι η τεχνική differential privacy. Με την εισαγωγή ελεγχόμενου θορύβου στα δεδομένα, επιτρέπει την εξαγωγή στατιστικών συμπερασμάτων χωρίς να αποκαλύπτονται πληροφορίες για συγκεκριμένα άτομα, διασφαλίζοντας έτσι υψηλό επίπεδο ιδιωτικότητας.

Ενδιάμεσο μέτρο μεταξύ ανωνυμοποίησης και διατήρησης ταυτότητας, είναι η ψευδωνυμοποίηση. Συμβάλλει επίσης στην αντιμετώπιση απειλών Linkability και Identifiability, όπου αντικαθιστά προσωπικά στοιχεία με ψευδώνυμα ή μοναδικά IDs, επιτρέποντας την επεξεργασία των δεδομένων χωρίς άμεση αποκάλυψη της ταυτότητας, ενώ διατηρείται η δυνατότητα ελεγχόμενης επανασύνδεσης.

Τα anonymization networks αποτελούν PETs που στοχεύουν στην αντιμετώπιση της ανιχνευσιμότητας και της συσχεσιμότητας (Linkability & Detectability). Μέσω της απόκρυψης της προέλευσης και της διαδρομής της επικοινωνίας, καθιστά δύσκολο τον εντοπισμό της δραστηριότητας ενός χρήστη από τρίτους. Επιπλέον προστασία για την ανιχνευσιμότητα αποτελεί το traffic obfuscation, που μειώνει την δυνατότητα εξαγωγής συμπερασμάτων σχετικά με την

συμπεριφορά ή τη δραστηριότητα των χρηστών, αλλοιώνοντας τα πρότυπα επικοινωνίας και αποκρύπτοντας μεταδεδομένα.

Για την αντιμετώπιση της απειλής DoS, το secure multi-party computation επιτρέπει την εκτέλεση υπολογισμών πάνω σε δεδομένα χωρίς την αποκάλυψη τους. Η τεχνική αυτή είναι ιδιαίτερα χρήσιμη σε περιπτώσεις όπου πολλαπλοί φορείς συνεργάζονται, χωρίς να επιθυμούν να μοιραστούν τα αρχικά τους δεδομένα.

Για την μείωση της απειλής διαρροής πληροφορίας, αν πραγματοποιείται η εκπαίδευση των μοντέλων τοπικά στις συσκευές των χρηστών, μειώνεται ο κίνδυνος μαζικής διαρροής πληροφορίας (DoS) και της μη συμμόρφωσης. Αυτή η PET είναι το federated learning.

Τέλος, τα συστήματα διαχείρισης συγκατάθεσης, αποτελούν PETs που στοχεύουν στην αντιμετώπιση της άγνοιας του χρήστη και της μη-συμμόρφωσης (Unawareness & Non-compliance). Μέσω αυτών, οι χρήστες ενημερώνονται και αποκτούν έλεγχο επί των δεδομένων τους, ενισχύοντας η διαφάνεια και τη συμμόρφωση με κανονιστικά πλαίσια όπως ο ΓΚΠΔ.

Συνολικά, η στοχευμένη εφαρμογή των PETs, σε συνδυασμό με τα κατάλληλα μέτρα αντιμετώπισης, συμβάλλει ουσιαστικά στην μείωση/εξάλειψη απειλών ασφάλειας και ιδιωτικότητας που εντοπίζονται μέσω της μεθοδολογίας LINDDUN.

Πιο συνοπτικά, φαίνονται στο παρακάτω πίνακα:

MISUSE CASES/ΑΠΕΙΛΕΣ	**ΤΡΟΠΟΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ**	**ΠΑΡΑΔΕΙΓΜΑ**	**PETs**
Disclosure of Information	Προστασία δεδομένων από μη εξουσιοδοτημένη πρόσβαση	Κρυπτογράφηση προσωπικών συνομιλιών του αποθανόντος	**Κρυπτογραφία**
Identifiability, Linkability	Αφαίρεση προσωπικών αναγνωριστικών	Αφαίρεση ονομάτων και τοποθεσιών από δεδομένα training	**Ανωνυμοποίηση**
Identifiability, Linkability	Προσθήκη θορύβου για αποτροπή ταυτοποίησης	Στατιστική ανάλυση συνομιλιών χωρίς αποκάλυψη χρήστη	**Differential Privacy**
Identifiability, Linkability	Αντικατάσταση ταυτότητας με ψευδώνυμα	Χρήση IDs αντί ονομάτων σε συνομιλίες	**Ψευδωνυμοποίηση**
Detectability, Linkability	Απόκρυψη ταυτότητας και δραστηριότητας χρήστη	Απόκρυψη του ποιος χρησιμοποιεί το griefbot	**Anonymization Networks**
Detectability	Απόκρυψη μοτίβων επικοινωνίας	Απόκρυψη συχνότητας/ χρόνου χρήσης griefbot	**Traffic Obfuscation**
Disclosure of Information, Non-compliance	Εκπαίδευση χωρίς συγκέντρωση δεδομένων	Εκπαίδευση AI χωρίς μεταφορά προσωπικών δεδομένων	**Federated Learning**
Disclosure of Information	Υπολογισμοί χωρίς αποκάλυψη δεδομένων	Ανάλυση δεδομένων από πολλαπλές πηγές με	**Secure Multi-Party Computation**

		ασφάλεια	
Unawareness, Non-compliance	Ενημέρωση και έλεγχος χρήστη	Συγκατάθεση συγγενών για χρήση δεδομένων	**Συστήματα Διαχείρισης Συγκατάθεσης**

Πίνακας 4: LINDDUN & PETs

4.6 Κανονιστικό Πλαίσιο (ΕΕ, ΗΠΑ, διεθνείς προσεγγίσεις)

Οι grieftech εφαρμογές (deathbots, griefbots και ghostbots) κινούνται σε ένα μεικτό κανονιστικό περιβάλλον, όπου συνυπάρχουν:

a. προστασία δεδομένων και ιδιωτικότητας.
b. κανόνες για την τεχνητή νοημοσύνη (ασφάλεια/διαφάνεια),
c. καταναλωτική προστασία/παραπλάνηση και
d. ειδικά πεδία όπως βιομετρικά δεδομένα, deepfakes και impersonation.

Στην πράξη, οι υποχρεώσεις προκύπτουν όχι από έναν «μοναδικό» νόμο, αλλά από συνδυασμό πλαισίων ανά δικαιοδοσία.

4.6.1 Ευρωπαϊκή Ένωση

a. ΓΚΠΔ – δεδομένα φυσικών προσώπων και έμμεση κάλυψη μεταθανάτιων δεδομένων
Σύμφωνα με την αιτιολογική σκέψη 27, ο ΓΚΠΔ δεν εφαρμόζεται στα προσωπικά δεδομένα αποθανόντων, αλλά εφαρμόζεται πλήρως στα δεδομένα των φυσικών προσώπων (π.χ. πενθούντες που συνομιλούν με griefbots), καθώς και σε περιπτώσεις όπου δεδομένα αποθανόντων εμπλέκουν πληροφορίες για ζώντες **[17]**.

b. EU AI Act – κανόνες για την ΤΝ και απαιτήσεις διαφάνειας/κινδύνου
Η Πράξη για την Τεχνητή Νοημοσύνη καθιερώνει εναρμονισμένους κανόνες για την ΤΝ στην ΕΕ με προσέγγιση βασισμένη στον κίνδυνο (risk-based) (απαγορευμένες πρακτικές, υψηλού κινδύνου συστήματα, υποχρεώσεις διαφάνειας κλπ). Για τα griefbots, πρακτικά σημεία – κλειδιά είναι:

- Υποχρεώσεις διαφάνειας όταν ο χρήστης αλληλοεπιδράει με AI (το φυσικό πρόσωπο να αντιλαμβάνεται ότι αλληλεπιδρά με σύστημα και όχι με άνθρωπο) και, όπου εφαρμόζεται, σήμανση/ενημέρωση για συνθετικό περιεχόμενο (όπως deepfake φωνές/εικόνες)
- Υποχρεώσεις για General-Purpose AI (GPAI) και (σε ορισμένες περιπτώσεις) πρόσθετες απαιτήσεις για μοντέλα/συστήματα που μπορούν να χρησιμοποιηθούν για παραπλάνηση ή impersonation.

Η ύπαρξη της Πράξης για την Τεχνητή Νοημοσύνη αλλάζει τις σχέσεις που δημιουργούνται σχετικά με τη συμμόρφωση των συστημάτων σε συγκεκριμένες αρχές: πλέον η «ηθική» και η «ασφάλεια» αποκτούν νομικά δεσμευτική διάσταση για παρόχους/χρήστες στην ΕΕ.

4.6.2 Ηνωμένες Πολιτείες της Αμερικής

Οι ΗΠΑ, σε αντίθεση με την ΕΕ, είναι χωρισμένες σε πολιτείες και συνεπώς έχει ρυθμίσεις που αφορούν σε sectoral και state-level, με ισχυρό ρόλο ρυθμιστικών αρχών στην επιβολή (enforcement). Οι σχετικές ρυθμίσεις είναι οι ακόλουθες

a. FTC – προστασία καταναλωτή, παραπλάνηση και impersonation

Η Federal Trade Commission (FTC) **[18]** έχει ενισχύσει την εστίασή της σε impersonation scams και πρακτικές που διευκολύνουν παραπλάνηση και εκμετάλλευση με την χρήση AI. Για τα griefbots είναι αρνητική η ύπαρξη ενός πειστικού bot το οποίο μπορεί να μιμείται τον αποθανόντα με σκοπό την παραπλάνηση και τη χειραγώγηση/απάτη (π.χ. οικονομική εκμετάλλευση συγγενικών προσώπων). Η FTC υπογραμμίζει τη θέση της όσνο αφορά τέτοια συμβάντα και δημοσιεύει σχετικές ανακοινώσεις και πρωτοβουλίες για την αντιμετώπιση τέτοιων προβλημάτων.

b. Πολιτειακοί νόμοι ιδιωτικότητας και βιομετρικών

Για τα griefbots με voice cloning facial likeness, οι βιομετρικές και βιολογικές ταυτοποιήσεις είναι κομβικές. Για παράδειγμα, στην Illinois, είναι χαρακτηριστικό παράδειγμα αυστηρού πλαισίου για βιομετρικά (συγκατάθεση, πολιτικές διατήρησης/διαγραφής κλπ). Προφανώς, κάθε πολιτεία φέρει και διαφορετική αντιμετώπιση και μεταβάλλεται ή τροποποιείται η οποιαδήποτε ρύθμιση.

4.6.3 Διεθνείς προσεγγίσεις

Επειδή πολλές grief-tech startups δραστηριοποιούνται σε διεθνές επίπεδο (μέσω συνεργασίας με παρόχους cloud υπηρεσιών από τρίτους, χρήστες από πολλές χώρες), συχνά υιοθετούν διεθνείς αρχές ως baseline:

a. OECD AI Principles

Η σύσταση του OECD **[19]** προωθεί αρχές όπως robustness, security, safety σε όλο τον κύκλο ζωής και υπεύθυνη διακυβέρνηση AI. Είναι χρήσιμη ως «policy backbone» για επιχειρηματολογία περί ασφαλούς/υπεύθυνης υλοποίησης griefbots.

b. UNESCO Recommendation on the Ethics of AI

Η UNESCO έχει δημοσιεύσει μί παγκόσμια σύσταση για την ηθική της ΤΝ με έμφαση στα ανθρώπινα δικαιώματα, τη διαφάνεια, την εποπτεία και την προστασία από βλάβες, αρχές σχετίζονται άμεσα με την ευαλωτότητα και τον κίνδυνο χειραγώγησης.

5

Επιχειρηματική Διάσταση και Νεοφυείς Επιχειρήσεις

5.1 Ανάλυση αγοράς: τάσεις, ανάπτυξη και καινοτομία

Η εμφάνιση και ανάπτυξη των grief-tech υπηρεσιών εντάσσεται σε ένα ευρύτερο οικοσύστημα ψηφιακής καινοτομίας, το οποίο συνδυάζει τεχνητή νοημοσύνη, ψηφιακή μνήμη και συναισθηματικά προσανατολισμένες τεχνολογίες. Τα deathbots, griefbots και ghostbots δεν αποτελούν μεμονωμένα τεχνολογικά πειράματα, αλλά μέρος μιας αναδυόμενης αγοράς που σχετίζεται με την ψηφιακή αθανασία, την προσωποποιημένη τεχνητή νοημοσύνη και την υποστήριξη της ψυχικής υγείας μέσω ψηφιακών μέσων.

Η αγορά αυτή βρίσκεται ακόμη σε πρώιμο στάδιο, όμως παρουσιάζει αυξανόμενο ενδιαφέρον τόσο επιχειρηματικά όσο και ερευνητικά.

5.1.1 Τάσεις που ευνοούν την ανάπτυξη grief-tech

a. Τεχνολογική ωρίμανση της γενετικής ΤΝ και της ψηφιακής αθανασίας (digital immortality)

Η πρόοδος των LLMs, των τεχνικών προσωποποίησης και των πολυτροπικών συστημάτων (συνδυασμός φωνής, κειμένου και εικόνας) έχει καταστήσει τεχνικά εφικτή τη δημιουργία «virtual humans» και συστημάτων «digital immortality», τα οποία μπορούν να παράγουν αμφίδρομη αλληλεπίδραση με βάση ψηφιακά ίχνη **[20]**. Η δυνατότητα αυτή μετατρέπει την παραδοσιακή ψηφιακή μνήμη (στατικές αναρτήσεις, memorial pages) σε διαδραστική προσομοίωση ταυτότητας, στοιχείο που διαφοροποιεί σημαντικά τα griefbots από παλιότερες μορφές online memorialization **[11]**.

b. Εξοικείωση χρηστών με conversational agents και «emotional AI»

Η διάδοση των chatbots/virtual assistants σε εφαρμογές έχει συμβάλει στη γενικότερη κοινωνική αποδοχή της αλληλεπίδρασης με συστήματα ΤΝ, ακόμη και σε ευαίσθητα πεδία. Αυτό λειτουργεί ως «γέφυρα υιοθέτησης» και για grief-tech εφαρμογές, καθώς οι χρήστες έχουν ήδη εμπειρία από συστήματα που προσομοιώνουν ενσυναίσθηση ή/και υποστήριξη.

c. **Αύξηση των ψηφιακών κατάλοιπων (digital remains)**

   Η καθημερινή ψηφιακή δραστηριότητα δημιουργεί τεράστιους όγκους δεδομένων (μηνύματα, φωτογραφίες, φωνητικές σημειώσεις), τα οποία μετά τον θάνατο παραμένουν ως ψηφιακά κατάλοιπα. Η ύπαρξη αυτών των δεδομένων αποτελεί τον «πρώτο πόρο» πάνω στον οποίο χτίζονται τα griefbots, αλλά ταυτόχρονα ενισχύει και τα ηθικά/νομικά διλήμματα της χρήσης τους μετά των θάνατο των φυσικών προσώπων.

5.1.2 Στάδιο ωριμότητας και χαρακτηριστικά ζήτησης

Η grief-tech αγορά μπορεί να περιγραφεί ως early-stage/ανερχόμενη αγορά: δεν διαθέτει ακόμη πλήρως σταθεροποιημένους ορισμούς, καθολικά πρότυπα, ούτε ενιαίο ρυθμιστικό καθεστώς. Σε αυτό το στάδιο, η καινοτομία προηγείται της κανονιστικής ωρίμανσης, οδηγώντας σε έντονο πειραματισμό σε προϊόντα και εμπειρίες χρήστη. Η ζήτηση είναι εκ φύσεως εξειδικευμένη αλλά δυνητικά διεθνής, αφού το πένθος αποτελεί καθολική εμπειρία, ενώ οι ψηφιακές πλατφόρμες προσφέρουν παγκόσμια κλιμάκωση.

Η υιοθέτηση τεχνολογιών «συνομιλίας με τους νεκρούς» δεν είναι μόνο θέμα λειτουργικότητας, αλλά και ηθικής αποδοχής, ψυχολογικής επίδρασης και κοινωνικών προσδοκιών, άρα η ζήτηση είναι ευαίσθητη σε δημόσιο διάλογο και αντιδράσεις.

5.1.3 Καινοτομία προϊόντος και διαφοροποίηση

Η καινοτομία στο grief-tech δεν περιορίζεται σε τεχνικά χαρακτηριστικά, αλλά επεκτείνεται σε διαφοροποίηση εμπειρίας. Το προϊόν συνήθως προωθεί μία μορφή συνέχειας δεσμού διατήρησης μνήμης ή/και αίσθησης παρουσίας. Αυτό αλλάζει το ανταγωνιστικό επίπεδο, αφού πλέον βασικός παράγοντας διαφοροποίησης γίνεται ο συνδυασμός:

a. Ποιότητας προσωποποίησης
b. Πολυτροπικών δυνατοτήτων
c. Αφηγηματικών λειτουργιών
d. Σχεδιασμού εμπιστοσύνης και ασφάλειας.

Επιπλέον, τα griefbots αποτελούν τμήμα μιας αναδυόμενης «digital afterilife industry», η οποία δημιουργεί νέα ερωτήματα για το ποια οντότητα έχει δικαίωμα να ορίζει την ψηφιακή ταυτότητα μετά τον θάνατο ενός φυσικού προσώπου και ύπο ποιες προυποθέσεις. Η διαφοροποίηση, λοιπόν, δεν είναι μόνο τεχνολογική, αλλά και θεσμική/δεοντολογική.

5.1.4 Ανταγωνιστικό τοπίο και εμπόδια εισόδου

Το ανταγωνιστικό τοπίο χαρακτηρίζεται από μικρό αριθμό εξειδικευμένων startups, αλλά και πιθανή «σκιά» μεγάλων παικτών (platforms/ AI providers) που διαθέτουν πρόσβαση σε δεδομένα, υποδομές και μοντέλα. Τα σημαντικότερα εμπόδια εισόδου είναι:

Δεδομένα και συναίνεση: η πρόσβαση σε δεδομένα υψηλής ποιότητας (και η νόμιμη/ηθική χρήση τους) αποτελεί κρίσιμο περιορισμό

Ασφάλεια και εμπιστοσύνη: η φύση των δεδομένων και η ευαλωτότητα των χρηστών απαιτούν αυξημένα μέτρα ασφάλειας, περιορίζοντας την «εύκολη» είσοδο.

Κανονιστικός και νομικός κίνδυνος: το πεδίο της ψηφιακής «ανάστασης» και των μεταθανάτιων αναπαραστάσεων αναλύεται ήδη ως αναδυόμενο πεδίο νομικών προκλήσεων, με έμφαση σε δικαιώματα προσωπικότητας, ταυτότητας και παραπλάνησης.

Συνολικά, το grief-tech βρίσκεται σε δυναμική αλλά και εύθραυστη φάση ανάπτυξης. Η τεχνολογική δυνατότητα επιτυγχάνει την καινοτομία, όμως η αποδοχή της αγοράς εξαρτάται σε μεγάλο βαθμό από την εμπιστοσύνη, τη διαφάνεια και τη διαχείριση κινδύνων. Αυτές οι συνθήκες καθιστούν κρίσιμη την κατανόηση των επιχειρηματικών μοντέλων που υιοθετούν οι πλατφόρμες ψηφιακής αθανασίας, τα οποία αναλύονται στην επόμενη ενότητα.

5.2 Business Models σε πλατφόρμες ψηφιακής αθανασίας

Οι πλατφόρμες grief-tech και ψηφιακής αθανασίας υιοθετούν επιχειρηματικά μοντέλα που διαφοροποιούνται σημαντικά από τα παραδοσιακά SaaS ή consumer AI μοντέλα, λόγω της έντονης συναισθηματικής διάστασης, της ευαλωτότητας των χρηστών και των αυξημένων απαιτήσεων εμπιστοσύνης. Η βιβλιογραφία επισημαίνει ότι η εμπορευματοποίηση υπηρεσιών που σχετίζονται με το πένθος και την ψηφιακή ταυτότητα απαιτεί ιδιαίτερη προσοχή στον τρόπο τιμολόγησης, παροχής αξίας και επικοινωνίας με το κοινό **[7]**.

Σε γενικές γραμμές, τα επιχειρηματικά μοντέλα των grief-tech πλατφορμών ομαδοποιούνται σε τέσσερις βασικές κατηγορίες.

5.2.1 Συνδρομητικά μοντέλα

Το συχνότερο εμφανιζόμενο μοντέλο στον χώρο των griefbots είναι το συνδρομητικό, όπου ο χρήστης πληρώνει περιοδικό αντίτιμο για πρόσβαση σε εξατομικευμένες λειτουργίες, όπως συνεχή συνομιλία, αποθήκευση μνήμης ή προηγμένες μορφές προσωποποίησης. Το μοντέλο αυτό αντλεί στοιχεία μνήμης από τις πλατφόρμες conversational AI και mental health applications, όπου η συνεχής χρήση και η προσωποποιημένη εμπειρία δικαιολογούν επαναλαμβανόμενη χρέωση.

5.2.2 Μοντέλα εφάπαξ αγοράς και «digital legacy packages»

Μια εναλλακτική προσέγγιση είναι τα μοντέλα εφάπαξ χρέωσης, όπου ο χρήστης πληρώνει για τη δημιουργία ενός ψηφιακού avatar ή griefbot χωρίς συνεχή συνδρομή. Το μοντέλο αυτό συχνά συνδέεται με την έννοια της ψηφιακής κληρονομιάς και προσεγγίζει το griefbot ως αναμνηστικό ή αρχειακό προϊόν, αντί για διαρκή υπηρεσία.

Η συγκεκριμένη προσέγγιση θεωρείται από ορισμένους ερευνητές ως ηθικά ηπιότερη, καθώς μειώνει τον κίνδυνο εμπορικής εκμετάλλευσης της συναισθηματικής κατάστασης του χρήστη, αν και περιορίζει τις δυνατότητες συνεχούς αναβάθμισης του συστήματος.

5.2.3 Freemium και staged personalization

Ορισμένες grief-tech πλατφόρμες υιοθετούν freemium μοντέλα, προσφέροντας βασικές λειτουργίες δωρεάν και χρεώνοντας για προηγμένες δυνατότητες, όπως πολυτροπική αλληλεπίδραση (φωνή, βίντεο), αυξημένη μνήμη ή προσαρμοσμένες αφηγηματικές ροές. Το μοντέλο αυτό είναι ευρέως διαδεδομένο σε consumer AI εφαρμογές και επιτρέπει χαμηλό φράγμα εισόδου για νέους χρήστες.

Στο πλαίσιο του grief-tech, το freemium μοντέλο ενέχει αυξημένο κίνδυνο δημιουργίας «dark patterns», καθώς η μετάβαση από τη δωρεάν στην premium (με χρέωση) εμπειρία μπορεί να βασίζεται σε συναισθηματικούς μηχανισμούς προσκόλλησης.

5.2.4 B2B και θεσμικά μοντέλα

Πέρα από τις απευθείας καταναλωτικές υπηρεσίες, αναδύονται και B2B μοντέλα, όπου οι grief-tech πλατφόρμες συνεργάζονται με γραφεία τελετών, παρόχους memorial services, μουσεία ή πολιτιστικά ιδρύματα και παρόχους ψυχολογικής υποστήριξης.

Σε αυτές τις περιπτώσεις, το griefbot λειτουργεί ως υπηρεσία υποδομής, ενσωματώνεται σε ευρύτερα οικοσυστήματα φροντίδας ή μνήμης. Το μοντέλο αυτό θεωρείται δυνητικά πιο βιώσιμο και κοινωνικά αποδεκτό, καθώς μεταφέρει μέρος της ευθύνης και της εποπτείας σε θεσμικούς φορείς.

5.2.5 Δεδομένα, αξία και μακροπρόθεσμη βιωσιμότητα

Κεντρικό στοιχείο όλων των παραπάνω επιχειρηματικών μοντέλων είναι η διαχείριση των δεδομένων. Σε αντίθεση με άλλα AI προϊόντα, τα grief-tech δεδομένα έχουν περιορισμένη δυνατότητα επαναχρησιμοποίησης λόγω νομικών, ηθικών και κοινωνικών περιορισμών. Αυτό περιορίζει τις δυνατότητες data monetization και καθιστά τη βιωσιμότητα των επιχειρηματικών μοντέλων πιο εξαρτημένη από άμεση αξία προς τον χρήστη, παρά από έμμεση εκμετάλλευση δεδομένων.

Η μακροπρόθεσμη επιβίωση των grief-tech επιχειρήσεων εξαρτάται από την ικανότητα τους να εξισορροπήσουν την τεχνολογική καινοτομία με την ηθική υπευθυνότητα και τη ρυθμιστική συμμόρφωση.

Η ανάλυση των επιχειρηματικών μοντέλων δείχνει ότι οι grief-tech πλατφόρμες λειτουργούν σε ένα πεδίο όπου η οικονομική βιωσιμότητα συνδέεται άμεσα με την κοινωνική αποδοχή και την εμπιστοσύνη. Η κατανόηση αυτών των μοντέλων αποτελεί προϋπόθεση για την ανάλυση του οικοσυστήματος των νεοφυών επιχειρήσεων, το οποίο εξετάζεται στην επόμενη ενότητα.

5.3 Παρουσίαση startup οικοσυστήματος

Το οικοσύστημα των grief-tech νεοφυών επιχειρήσεων χαρακτηρίζεται από έντονο πειραματισμό, περιορισμένη κανονιστική καθοδήγηση και υψηλό δημόσιο ενδιαφέρον. Οι περισσότερες επιχειρήσεις κινούνται στο μεταίχμιο μεταξύ πειραματικής καινοτομίας και εμπορικής αξιοποίησης, αξιοποιώντας τεχνολογίες conversational AI και ψηφιακής προσωποποίησης για τη δημιουργία εμπειριών που προσομοιώνουν την παρουσία αποθανόντων.

5.3.1 Project December

Το Project December αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα grief-tech εφαρμογών, καθώς έγινε ευρέως γνωστό μέσα από τη χρήση μεγάλων γλωσσικών μοντέλων για τη δημιουργία chatbots που μιμούνται την προσωπικότητα αποθανόντων προσώπων.

Η πλατφόρμα βασίστηκε στην εισαγωγή ιστορικών συνομιλιών και χαρακτηριστικών προσωπικότητας, επιτρέποντας στους χρήστες να «συνομιλούν» με μια ψηφιακή αναπαράσταση αγαπημένου προσώπου.

Από επιχειρηματική σκοπιά, το Project December λειτούργησε περισσότερο ως πείραμα proof-of-concept, παρά ως ώριμο προϊόν, αναδεικνύοντας τόσο τη ζήτηση όσο και τους κινδύνους του συγκεκριμένου μοντέλου. Η έντονη συναισθηματική εμπλοκή των χρηστών ανέδειξε ζητήματα ψυχολογικής επιβάρυνσης και ορίων χρήσης, τα οποία έχουν επισημανθεί και στη βιβλιογραφία περί parasocial interactions με τεχνητές οντότητες **[7]**.

5.3.2 Replika

Η Replika αποτελεί μία από τις πιο επιτυχημένες εμπορικά πλατφόρμες συνομιλιακής AI, αν και δεν σχεδιάστηκε αρχικά αποκλειστικά ως grief-tech εφαρμογή. Παρόλα αυτά, έχει χρησιμοποιηθεί από χρήστες ως μέσο συναισθηματικής υποστήριξης, διατήρησης δεσμών και, σε ορισμένες περιπτώσεις, προσομοίωσης αποθανόντων προσώπων. Αυτή βασίζεται σε μακροχρόνια αλληλεπίδραση και προσωποποίηση, ενισχύοντας την ανάπτυξη παρακοινωνικών σχέσεων μεταξύ χρήστη και AI.

Επιχειρηματικά, ακολουθεί συνδρομητικό μοντέλο που προσφέρει κλιμακούμενη προσωποποίηση και λειτουργίες, γεγονός που την καθιστά παράδειγμα βιώσιμης εμπορικής εφαρμογής conversational AI με έμμεσες grief-tech χρήσεις.

5.3.3 HereAfter AI

Η HereAfter AI επικεντρώνεται στη δημιουργία διαδραστικών ψηφιακών αρχείων ζωής, επιτρέποντας σε άτομα να καταγράφουν φωνή, ιστορίες, μέχρι και απαντήσεις σε ερωτήσεις πριν τον θάνατο τους. Το προϊόν παρουσιάζεται ως εργαλείο ψηφιακής κληρονομιάς, με έμφαση στη διατήρηση μνήμης και όχι στην πλήρη προσομοίωση συνομιλίας.

Σε αντίθεση με πιο «ζωντανά» griefbots, η προσέγγιση αυτή μειώνει τον βαθμό ψυχολογικής προσομοίωσης, κάτι που ορισμένοι ερευνητές θεωρούν ηθικά ηπιότερο **[20]**.

Επιχειρηματικά, το εν λόγω μοντέλο προσεγγίζει την grief-tech ως αναμνηστικό προϊόν, με σαφέστερα όρια χρήσης και χαμηλότερο κίνδυνο συναισθηματικής εξάρτησης.

Η ανάλυση των βασικών «παικτών» του grief-tech οικοσυστήματος δείχνει ότι η επιχειρηματική επιτυχία δεν εξαρτάται αποκλειστικά από την τεχνολογία, αλλά από την ικανότητα να διαχειριστεί συναισθήματα, ηθικά και κοινωνικά ζητήματα. Τα χαρακτηριστικά αυτά επηρεάζουν άμεσα τις δυνατότητες κλιμάκωσης και το επενδυτικό ενδιαφέρον, τα οποία εξετάζονται στη συνέχεια.

5.4 Δυνατότητες κλιμάκωσης και επενδυτικό ενδιαφέρον

Η κλιμάκωση (scalability) των grief-tech υπηρεσιών δεν εξαρτάται μόνο από την τεχνολογική ικανότητα ενός griefbot να παράγει πειστικές απαντήσεις, αλλά από ένα σύνολο παραγόντων που συνδυάζουν οικονομικά κόστη AI, διακυβέρνηση/συμμόρφωση, κοινωνική νομιμοποίηση και διαχείριση κινδύνου.

Η βιβλιογραφία που σχετίζεται με τη «digital afterlife industry» δείχνει ότι ο κλάδος έχει έντονα χαρακτηριστικά εμπορευματοποίησης ψηφιακών καταλοίπων, κάτι που δημιουργεί ευκαιρίες ανάπτυξης αλλά και υψηλές απαιτήσεις εμπιστοσύνης **[21]**.

5.4.1 Παράγοντες που ευνοούν την κλιμάκωση

a. Υποδομές cloud και modular AI αρχιτεκτονικές

Η σύγχρονη AI ανάπτυξη (ιδίως σε νεοφυείς επιχειρήσεις) διευκολύνει την κλιμάκωση μέσω cloud υποδομών, API-based μοντέλων και modular αρχιτεκτονικών, όπου το προϊόν μπορεί να επεκτείνεται λειτουργικά χωρίς αντίστοιχη αύξηση ανθρώπινων πόρων. Η αξιοποίηση AI δυνατοτήτων, επιταχύνει την κλιμάκωση όταν συνδυάζεται με ικανότητες «AI governance» και προσαρμογή σε ρυθμιστικές απαιτήσεις.

b. Διεθνοποίηση αγοράς

Οι grief-tech υπηρεσίες έχουν δυνητικά παγκόσμια αγορά, καθώς προσφέρονται ψηφιακά, με χαμηλό κόστος διανομής. Όμως, η κλιμάκωση «cross-border» αυξάνει την πολυπλοκότητα συμμόρφωσης, ειδικά όταν οι υπηρεσίες εμπλέκουν προσωπικά δεδομένα και συνθετικό περιεχόμενο.

c. Επαγγελματοποίηση και τυποποίηση υπηρεσιών

Πρόσφατες εργασίες για τον χώρο της ψηφιακής μετά θάνατον διαχείρισης αναγνωρίζουν μια τάση professionalization, δηλαδή μετάβαση από «πειραματικές εφαρμογές» σε πιο δομημένες υπηρεσίες, διαδικασίες και επαγγελματικά standards. Αυτή η εξέλιξη μπορεί να λειτουργήσει ως μηχανισμός κλιμάκωσης, επειδή ενισχύει τη θεσμική αξιοπιστία και μειώνει τη μεταβλητότητα του προϊόντος/υπηρεσίας.

5.4.2 Παράγοντες που περιορίζουν την κλιμάκωση

a. Compliance costs και ρυθμιστική αβεβαιότητα (ιδίως στην ΕΕ)

Η κλιμάκωση grieftech στην Ευρώπη επηρεάζεται από την αυξανόμενη ρυθμιστική επιβάρυνση για συστήματα AI και από τα κόστη συμμόρφωσης (τεκμηρίωση, risk management, transparency, human oversight). Μελέτες που εξετάζουν τον AI Act επισημαίνουν ότι οι startup/SME αντιμετωπίζουν δυσανάλογη πίεση από κόστη πιστοποίησης/συμμόρφωσης και αυξημένη οργανωτική πολυπλοκότητα. Αυτό σημαίνει

πως μία grief-tech επιχείρηση μπορεί να χρειάζεται κεφάλαιο όχι μόνο για R&D, αλλά και για compliance engineering.

b. Trust and Safety ως «gating factor» ανάπτυξης

Σε αντίθεση με πολλά consumer AI προϊόντα, τα griefbots λειτουργούν σε πλαίσιο συναισθηματικής ευαλωτότητας. Η κακή δημοσιότητα, ένα περιστατικό παραπλάνησης ή μία αστοχία ασφάλειας μπορεί να λειτουργήσει ως «growth stopper». Η λογική αυτή τονίζει τον ρόλο της λογοδοσίας/εμπιστοσύνης ως κρίσιμοι παράγοντες σε εφαρμογές AI.

Η κλιμάκωση προϋποθέτει κλιμάκωση δεδομένων, όμως, στα griefbots, τα δεδομένα αυτά είναι πιο ευαίσθητα, λιγότερο ανακυκλώσιμα και περιορίζονται από συναίνεση ή ηθικά όρια. Έτσι διαφοροποιούνται από άλλα AI-first προϊόντα και αυξάνει το κόστος απόκτησης/διαχείρισης δεδομένων.

5.4.3 Επενδυτικό ενδιαφέρον και το «governance lens» των επενδυτών

Το επενδυτικό ενδιαφέρον για grief-tech επηρεάζεται από το ευρύτερο περιβάλλον χρηματοδότησης digital innovation, όπου οι επενδυτές αξιολογούν όχι μόνο το προϊόν, αλλά και το «governance» (νομικοί κίνδυνοι, κανονιστική προοπτική). Έρευνα πάνω στις αντιλήψεις των venture capital επενδυτών για τη διακυβέρνηση ψηφιακής καινοτομίας δείχνει ότι η ικανότητα διαχείρισης κινδύνων και η «ρυθμιστική ετοιμότητα» λειτουργούν ως παράγοντες αξιολόγησης **[22]**. Αυτό μεταφράζεται πρακτικά σε προϋποθέσεις επένδυσης, όπως σαφές privacy & security posture, governance μηχανισμοί όπως policy, logs, audits, όρια χρήσης και προστασία ευάλωτων χρηστών και συμμόρφωση και προσαρμοστικότητα σε κανονιστικές εξελίξεις.

Συνολικά, η κλιμάκωση των grief-tech υπηρεσιών είναι εφικτή τεχνικά, αλλά επιχειρηματικά εξαρτάται από την ισορροπία μεταξύ growth και trust/compliance. Η δυναμική αυτή εξηγεί γιατί ορισμένες πλατφόρμες αναζητούν θεσμικές συνεργασία ή προσπαθούν να διαφοροποιηθούν μέσω αυξημένων πρακτικών ασφάλειας και ηθικής, πριν επιχειρήσουν επιθετική επέκταση.

5.5 Επιχειρηματικοί κίνδυνοι

Οι grief-tech startups δραστηριοποιούνται σε ένα περιβάλλον υψηλής αβεβαιότητας, όπου οι επιχειρηματικοί κίνδυνοι δεν περιορίζονται σε οικονομικούς ή τεχνολογικούς παράγοντες, αλλά επεκτείνονται σε νομικές, ηθικές και κοινωνικές διαστάσεις. Οι κίνδυνοι αυτοί είναι στενά αλληλένδετοι και μπορούν να επηρεάσουν άμεσα τη βιωσιμότητα και την κοινωνική αποδοχή των grief-tech υπηρεσιών.

5.5.1 Νομικοί κίνδυνοι

Το νομικό ρίσκο αποτελεί έναν από τους σημαντικότερους παράγοντες επιχειρηματικής αβεβαιότητας για τις grief-tech επιχειρήσεις. Η χρήση δεδομένων αποθανόντων, η προσομοίωση ταυτότητας και η δημιουργία συνθετικού περιεχομένου εγείρουν ζητήματα που δεν καλύπτονται πλήρως από την υφιστάμενη νομοθεσία.

Στην ΕΕ, οι grief-tech επιχειρήσεις επηρεάζονται έμμεσα από τον ΓΚΠΔ, καθώς παρότι τα δεδομένα αποθανόντων δεν καλύπτονται άμεσα, εμπλέκονται δεδομένα τρίτων προσώπων.

Επιπλέον, η εισαγωγή του AI Act αυξάνει τις υποχρεώσεις διαφάνειας, τεκμηρίωσης και διαχείρισης του κινδύνου για AI συστήματα που αλληλοεπιδρούν με ανθρώπους. Σε άλλες δικαιοδοσίες, όπως των ΗΠΑ, το νομικό ρίσκο εντείνεται από τον κατακερματισμό του ρυθμιστικού πλαισίου και από την έμφαση σε ζητήματα παραπλάνησης και impersonation. Η απουσία σαφούς πλαισίου για την «ψηφιακή ανάσταση» δημιουργεί τον κίνδυνο εκ των υστέρων ρύθμισης, η οποία μπορεί να επηρεάσει αρνητικά ήδη λειτουργούσες επιχειρήσεις.

5.5.2 Ηθικοί κίνδυνοι και δημόσια εικόνα

Πέρα από το νομικό πλαίσιο, οι grief-tech επιχειρήσεις αντιμετωπίζουν έντονο ηθικό και reputational risk. Η εμπορική αξιοποίηση της ανθρώπινης απώλειας μπορεί να προκαλέσει κοινωνικές αντιδράσεις, ιδιαίτερα όταν οι υπηρεσίες παρουσιάζονται ως υποκατάστατο ανθρώπινων σχέσεων ή ψυχολογικής υποστήριξης.

Η βιβλιογραφία αναφέρει ότι τα griefbots ενδέχεται να ενισχύσουν συναισθηματική εξάρτηση ή να παρατείνουν το πένθος, ειδικά όταν δεν υπάρχουν σαφή όρια χρήσης και διαφάνειας σχετικά με τη φύση του συστήματος **[23]**. Ένα μεμονωμένο περιστατικό κακής χρήσης, παραπλάνησης ή συναισθηματικής βλάβης μπορεί να οδηγήσει σε αρνητική δημοσιότητα, επηρεάζοντας δυσανάλογα την αξιοπιστία μιας νεοφυής επιχείρησης.

Από επιχειρηματική σκοπιά, το reputational risk λειτουργεί ως πολλαπλασιαστής κινδύνου, καθώς μπορεί να επηρεάσει ταυτόχρονα την εμπιστοσύνη των χρηστών, το επενδυτικό ενδιαφέρον και τη ρυθμιστική στάση των αρχών **[7]**.

5.5.3 Τεχνικοί περιορισμοί και κίνδυνοι της τεχνητής νοημοσύνης

Οι grief-tech επιχειρήσεις βασίζονται σε προηγμένα συστήματα τεχνητής νοημοσύνης, τα οποία παρουσιάζουν εγγενείς τεχνικούς περιορισμούς. Η αδυναμία πλήρους ελέγχου της συμπεριφοράς μεγάλων γλωσσικών μοντέλων, η πιθανότητα παραγωγής ακατάλληλου ή παραπλανητικού περιεχομένου και η ευπάθεια σε επιθέσεις (πχ. prompt injection) αποτελούν σοβαρούς τεχνικούς κινδύνους.

Επιπλέον η εξάρτηση από τρίτους παρόχους AI υποδομών δημιουργεί τεχνολογικό και επιχειρησιακό ρίσκο (vendor lock-in, αλλαγές όρων χρήσης, διακοπές υπηρεσιών). Τέτοιοι τεχνικοί περιορισμοί μπορούν να μετατραπούν σε επιχειρηματικούς κινδύνους όταν δεν υπάρχουν εναλλακτικές αρχιτεκτονικές ή μηχανισμοί ελέγχου.

Συνολικά, οι επιχειρηματικοί κίνδυνοι αυτών των επιχειρήσεων μπορούν να θεωρηθούν συστημικοί, καθώς η αποτυχία σε ένα τομέα όπως της ηθικής ή της ασφάλειας, μπορεί να επηρεάσει άμεσα και τους υπόλοιπους. Η βιωσιμότητα των grief-tech επιχειρήσεων εξαρτάται από την ικανότητα τους να ενσωματώνουν πρακτικές υπεύθυνης και διαφανούς AI, πριν αυτές επιβληθούν αυστηρά από τις ρυθμιστικές αρχές.

5.6 Προοπτικές για το μέλλον των grief-tech υπηρεσιών

Οι grief-tech υπηρεσίες βρίσκονται σε ένα μεταβατικό στάδιο, όπου η τεχνολογική δυνατότητα προηγείται της κοινωνικής, ηθικής και κανονιστικής ωρίμανσης. Το μέλλον του κλάδου δεν θα καθοριστεί αποκλειστικά από τις εξελίξεις στην τεχνητή νοημοσύνη, αλλά από τον τρόπο με τον

οποίο θα διαπραγματευτούν τα όρια της ψηφιακής αναπαράστασης της ανθρώπινης ταυτότητας μετά τον θάνατο οι επιχειρήσεις, οι ρυθμιστικές αρχές και η κοινωνία.

5.6.1 Τεχνολογικές εξελίξεις και μετασχηματισμός προϊόντων

Σε τεχνολογικό επίπεδο, αναμένεται περαιτέρω βελτίωση της ποιότητας και της πολυτρο-πικότητας των griefbots, μέσω της ενσωμάτωσης πιο εξελιγμένων μεγάλων γλωσσικών μοντέλων, συνθετικής φωνής και οπτικών avatar. Η μετάβαση από απλά text-based συστήματα σε immersive virtual humans θα ενισχύσει την αίσθηση παρουσίας, αλλά ταυτόχρονα θα αυξήσει την πολυπλοκότητα των κινδύνων παραπλάνησης και συναισθηματικής χειραγώγησης.

Παράλληλα, προβλέπεται ενίσχυση αρχιτεκτονικών που δίνουν έμφαση σε έλεγχο και επεξήγηση, καθώς η ανεξέλεγκτη συμπεριφορά μοντέλων θεωρείται κρίσιμο εμπόδιο για την ευρεία υιοθέτηση σε ευαίσθητα κοινωνικά πλαίσια **[16]**.

5.6.2 Κανονιστική ωρίμανση και θεσμική ενσωμάτωση

Η κανονιστική εξέλιξη, ιδιαίτερα στην Ευρωπαϊκή Ένωση, αναμένεται να διαμορφώσει καθοριστικά το μέλλον του grief-tech. Η εισαγωγή του AI Act και η αυξανόμενη έμφαση στη διαφάνεια, την ανθρώπινη εποπτεία και τη διαχείριση κινδύνου ενδέχεται να περιορίσουν ορισμένες πρακτικές, αλλά ταυτόχρονα να ενισχύσουν τη θεσμική νομιμοποίηση των υπηρεσιών που συμμορφώνονται.

Σε αυτό το πλαίσιο, οι grief-tech υπηρεσίες είναι πιθανό να μετακινηθούν από «πειραματικές εφαρμογές» σε θεσμικά ενσωματωμένες λύσεις, π.χ. σε συνεργασία με επαγγελματίες ψυχικής υγείας, πολιτιστικά ιδρύματα ή υπηρεσίες μνήμης.

5.6.3 Μετατόπιση από «digital resurrection» σε «digital remembrance»

Ένα από τα πιο σημαντικά πιθανά σενάρια εξέλιξης είναι η εννοιολογική μετατόπιση του grieftech από τη λογική της «ψηφιακής ανάστασης» προς τη λογική της «ψηφιακής μνήμης και αφήγησης». Αντί για πλήρη προσομοίωση συνομιλίας με τον αποθανόντα, οι μελλοντικές υπηρεσίες ενδέχεται να δίνουν έμφαση σε αφηγηματικά, αρχειακά ή εκπαιδευτικά εργαλεία μνήμης. Η προσέγγιση αυτή θεωρείται από αρκετούς ερευνητές ηθικά ηπιότερη, καθώς μειώνει τον κίνδυνο σύγχυσης μεταξύ πραγματικού και συνθετικού υποκειμένου και περιορίζει την πιθανότητα παθολογικής προσκόλλησης **[23]**,**[7]**.

5.6.4 Επιχειρηματικές προοπτικές και στρατηγική βιωσιμότητας

Από επιχειρηματική σκοπιά, το μέλλον των grieftech υπηρεσιών θα εξαρτηθεί από την ικανότητά τους να υιοθετήσουν στρατηγικές υπεύθυνης και διαφοροποιημένης καινοτομίας. Οι επιχειρήσεις που θα επενδύσουν έγκαιρα σε ασφάλεια, διαφάνεια και ηθικό σχεδιασμό είναι πιθανότερο να αποκτήσουν ανταγωνιστικό πλεονέκτημα σε ένα αυστηρότερο κανονιστικό περιβάλλον. Επιπλέον, οι επενδυτές τείνουν να ευνοούν επιχειρήσεις που επιδεικνύουν μακροπρόθεσμο όραμα, παρά επιθετική αλλά επισφαλή ανάπτυξη.

Συνολικά, οι grieftech υπηρεσίες αναμένεται να συνεχίσουν να αναπτύσσονται, αλλά όχι ως μαζικά καταναλωτικά προϊόντα χωρίς περιορισμούς. Το μέλλον του κλάδου θα διαμορφωθεί από μια ισορροπία μεταξύ τεχνολογικής καινοτομίας, κανονιστικής συμμόρφωσης και κοινωνικής

αποδοχής. Όπως υπογραμμίζει η βιβλιογραφία για την ψηφιακή μεταθανάτια ταυτότητα, η επιτυχία των grieftech υπηρεσιών δεν θα κριθεί από το πόσο «ρεαλιστικά» μιμούνται τον νεκρό, αλλά από το αν μπορούν να λειτουργήσουν με τρόπο ασφαλή, υπεύθυνο και ανθρώπινα αποδεκτό.

6

Συμπεράσματα και Προτάσεις για Μελλοντική Έρευνα

6.1 Συνοπτικά Συμπεράσματα

Η παρούσα διατριβή εξέτασε το αναδυόμενο φαινόμενο των deathbots, griefbots και ghostbots από την οπτική γωνία της ασφάλειας, της επιχειρηματικότητας και της κοινωνικό-ηθικής τους διάστασης. Μέσω μιας συστηματικής ανασκόπησης της βιβλιογραφίας και ανάλυσης περιπτώσεων, αποκαλύφθηκε ότι οι υπηρεσίες grief-tech δεν είναι απλώς τεχνολογικά προϊόντα, αλλά κοινωνικό-τεχνικά συστήματα που αλληλοεπιδρούν με ευάλωτες ανθρώπινες εμπειρίες, όπως ο θρήνος και η απώλεια.

Ένα βασικό συμπέρασμα είναι ότι οι τεχνολογικές εξελίξεις στην τεχνητή νοημοσύνη έχουν καταστήσει τεχνικά εφικτή τη δημιουργία πειστικών ψηφιακών αναπαραστάσεων της ταυτότητας, αλλά η κοινωνική και κανονιστική ωριμότητα του τομέα υστερεί. Αυτή η ασυμμετρία δημιουργεί ένα περιβάλλον αυξημένου κινδύνου τόσο για τους χρήστες όσο και για τις εταιρείες που δραστηριοποιούνται στον τομέα [7].

Ταυτόχρονα, η ανάλυση ασφάλειας και η μοντελοποίηση απειλών έχουν δείξει ότι τα griefbots ενέχουν σημαντικούς κινδύνους, όπως παραβιάσεις δεδομένων, απάτη ταυτότητας και κατάχρηση συνθετικού περιεχομένου. Αυτοί οι κίνδυνοι δεν είναι μόνο τεχνικοί, αλλά συνδέονται άμεσα με την εμπιστοσύνη, τη λογοδοσία και τη συμμόρφωση με ρυθμιστικά πλαίσια όπως ο ΓΚΠΔ και ο Ευρωπαϊκός Νόμος για την Τεχνητή Νοημοσύνη (AI Act – Κανονισμός ΕΕ 2024/1689).

Σε επιχειρηματικό επίπεδο, οι υπηρεσίες grief-tech έχουν αποδειχθεί ότι έχουν πραγματικό δυναμικό ανάπτυξης, αλλά η βιωσιμότητά τους εξαρτάται από την ικανότητα εξισορρόπησης της καινοτομίας με την υπεύθυνη εφαρμογή. Οι εταιρείες που αγνοούν τις διαστάσεις της ασφάλειας, της ηθικής και της δημόσιας εικόνας είναι πιθανό να αντιμετωπίσουν δυσανάλογα τον υψηλό κίνδυνο αποτυχίας.

6.2 Προτάσεις για υπεύθυνη υλοποίηση griefbots

Με βάση τα ευρήματα της μελέτης, προκύπτουν ορισμένες κρίσιμες κατευθυντήριες γραμμές για την υπεύθυνη ανάπτυξη και διανομή υπηρεσιών grief-tech:

i. Πρώτον, η ενσωμάτωση των αρχών «Privacy by Design» και «Secure AI Lifecycle» θα πρέπει να αποτελεί βασικό στοιχείο του σχεδιασμού από τα αρχικά στάδια της ανάπτυξης. Η ελαχιστοποίηση των δεδομένων, η σαφής διαχείριση της συγκατάθεσης και η ξεχωριστή καταγραφή συμβάντων (αρχεία καταγραφής ελέγχου χωρίς περιεχόμενο) μπορούν να μειώσουν σημαντικά τόσο τους τεχνικούς όσο και τους νομικούς κινδύνους.

ii. Δεύτερον, απαιτείται διαφάνεια προς τους χρήστες, ειδικά όσον αφορά το τι είναι και τι δεν είναι τα griefbots. Η σαφής δήλωση ότι πρόκειται για μια συνθετική αναπαράσταση και όχι για «συνέχιση της ύπαρξης» του αποθανόντος αποτελεί κρίσιμο στοιχείο προστασίας από την εξαπάτηση και τη συναισθηματική εκμετάλλευση.

iii. Τρίτον, οι πλατφόρμες grief-tech πρέπει να υιοθετήσουν όρια χρήσης και μηχανισμούς αποκλιμάκωσης (περιόδους παύσης, περιορισμούς έντασης αλληλεπίδρασης), εφόσον στοχεύουν σε χρήστες που έχουν χάσει κάποιο αγαπημένο τους πρόσωπο. Τέτοιες πρακτικές έχουν προταθεί στη βιβλιογραφία ως μέσο μείωσης των κινδύνων παθολογικής προσκόλλησης **[20]**.

Τέλος, σε επιχειρηματικό επίπεδο, οι επενδύσεις στη διακυβέρνηση, την ηθική και τη διαχείριση κινδύνων δεν πρέπει να θεωρούνται εμπόδιο, αλλά ανταγωνιστικό πλεονέκτημα σε ένα περιβάλλον αυξανόμενης αυστηρότητας των κανονιστικών ρυθμίσεων.

6.3 Προτάσεις για περαιτέρω ερευνητική μελέτη

Ως μελέτη βασισμένη σε δεδομένα (desktop research), η έρευνα αυτή έχει ορισμένους περιορισμούς και ανοίγει τον δρόμο για περαιτέρω έρευνα σε πολλαπλά επίπεδα.

Σε εμπειρικό επίπεδο, μελλοντικές μελέτες θα μπορούσαν να εξετάσουν τις πραγματικές εμπειρίες των χρηστών των griefbots, εστιάζοντας στις ψυχολογικές επιπτώσεις της μακροχρόνιας χρήσης, καθώς και στους παράγοντες που επηρεάζουν το θετικό ή αρνητικό αποτέλεσμα της εμπειρίας του πένθους. Τέτοιες μελέτες θα μπορούσαν να συνδυάζουν ποιοτικές και ποσοτικές μεθόδους.

Σε τεχνικό επίπεδο, συνιστάται περαιτέρω έρευνα σχετικά με τους μηχανισμούς ελέγχου, ανίχνευσης και πρόληψης της κατάχρησης της τεχνητής νοημοσύνης, ιδίως σε σχέση με τα deepfake griefbots, την πλαστογράφηση ταυτότητας και την άμεση εισαγωγή δεδομένων. Η σύνδεση της μοντελοποίησης απειλών με πλαίσια κινδύνου ειδικά για την τεχνητή νοημοσύνη είναι ένας ιδιαίτερα καρποφόρος τομέας για μελλοντική έρευνα.

Τέλος, σε νομικό και κανονιστικό επίπεδο, απαιτείται μια συστηματική μελέτη της μεταθανάτιας ψηφιακής ταυτότητας και της θέσης της στο δίκαιο της προστασίας των δεδομένων και των δικαιωμάτων της προσωπικότητας. Η ανάπτυξη του δικαίου της τεχνητής νοημοσύνης και η πιθανή αναθεώρηση των υφιστάμενων πλαισίων ενδέχεται να δημιουργήσουν νέες υποχρεώσεις και δικαιώματα, τα οποία αξίζουν ειδική ακαδημαϊκή έρευνα.

Βιβλιογραφία

[1] M. Figueroa-Torres, «Affection as a service: Ghostbots and the changing nature of mourning,» *Computer Law & Security Review,* p. 105943, 2024.

[2] H. AI, «HereAfter AI,» HereAfter AI, [Ηλεκτρονικό]. Available: https://www.hereafter.ai/.

[3] P. December, «Project December,» Project December, [Ηλεκτρονικό]. Available: https://projectdecember.net/.

[4] T. Hollanek και K. Nowaczyk-Basińska, «Griefbots, deadbots, postmortem avatars,» *Philosophy & Technology,* p. 63, 2024.

[5] N. F. Lindemann, «The ethics of 'deathbots',» *Science and Engineering Ethics,* p. 60, 2022.

[6] H. o. Information, «History of Information,» History of Information, [Ηλεκτρονικό]. Available: https://historyofinformation.com/detail.php?id=1035.

[7] C. Öhman και L. Floridi, «An ethical framework for the digital afterlife industry,» *Nature Human Behaviour,* pp. 318-320, 2018.

[8] E. Kasket, All the ghosts in the machine, Robinson, 2019.

[9] T. Brown, B. Mann, N. Ryder και e. al., «Language models are few-shot learners,» *Advances in Neural Information Processing Systems,* pp. 1877-1901, 2020.

[10] E. Kübler-Ross και D. Kessler, On grief and grieving, Scribner, 2005.

[11] J. R. Brubaker, G. R. Hayes και P. Dourish, «Beyond the grave,» *The Information Society,* pp. 152-163, 2013.

[12] T. Walter, «New mourners, old mourners,» *New Review of Hypermedia and Multimedia,* pp. 10-24, 2015.

[13] C. Nass και Y. Moon, «Machines and mindlessness,» *Journal of Social Issues,* pp. 81-103, 2000.

[14] L. Floridi, «Establishing the rules for building trustworthy AI,» *Ethics, Governance, and Policies in Artificial Intelligence,* p. 41–45, 2021.

[15] I. a. P. C. o. Ontario, «Privacy by Design: The 7 Foundational Principles,» 2009.

[16] L. Floridi, J. Cowls, M. Beltrametti και e. al., «AI4People—An ethical framework for a good AI society,» *Minds and Machines,* pp. 689-707, 2018.

[17] E. Union, «General Data Protection Regulation (GDPR),» 2016.

[18] M. K. Ohlhausen, «Privacy challenges and opportunities,» *Journal of Public Policy & Marketing,* pp. 4-9, 2014.

[19] K. Yeung, «Recommendation of the council on artificial intelligence,» *International Legal Materials,* pp. 27-34, 2020.

[20] M. Savin-Baden και D. Burden, «Digital immortality and virtual humans,» *Postdigital Science and Education,* pp. 87-103, 2019.

[21] C. Öhman και L. Floridi, «The political economy of death in the age of information,» *Minds and Machines,* pp. 639-662, 2017.

[22] J. Salgado-Criado, C. Mataix-Aldeanueva και e. al., «How should we govern digital innovation?,» *Technological Forecasting and Social Change,* p. 123198, 2024.

[23] N. F. Lindemann, «The ethical permissibility of chatting with the dead,» 2022.

[24] L. Edwards και E. Harbinja, «Protecting post-mortem privacy,» *Cardozo Arts & Entertainment Law Journal,* p. 83, 2013.

[25] LINDDUN, «LINDDUN Threat Trees,» [Ηλεκτρονικό]. Available: https://linddun.org/threat-trees/.

[26] Hollanek, T. and Nowaczyk-Basińska, K., 2024. Griefbots, deadbots, postmortem avatars: On responsible applications of generative AI in the digital afterlife industry. Philosophy & Technology, 37(2), p.63.