11η ΣΥΝΕΔΡΙΑ: Ψηφιακή Πολιτειότητα - Ασφαλής χρήση διαδικτύου

Στο παρόν υλικό γίνεται μια προσπάθεια εξοικείωσης με τους κινδύνους που συνδέονται με τη χρήση και διαχείριση ψηφιακών πόρων και ιδιαίτερα του διαδικτύου.

Το δεύτερο μέρος στοχεύει σε γνώσεις και δεξιότητες σχετικές με την e-πολιτειότητα, το σύνολο δηλαδή των ψηφιακών πρακτικών που συνδέονται με την ιδιότητα του πολίτη. Ιδιαίτερη έμφαση δίνεται στη διαχείριση ψηφιακών πληροφοριών (θέματα στρατηγικών αναζήτησης πληροφοριών, αναφοράς πηγών πληροφοριών, ελέγχου της ποιότητας των πληροφοριών, καλών πρακτικών επικοινωνίας και διάχυσης/μεταβίβασης πληροφοριών).

Σκοπός:

Απόκτηση βασικών γνώσεων για τις νέες μορφές ψηφιακής πολιτειότητας και θεμάτων διδακτικής που αφορούν τους μαθητές, τη φύση και το είδος των κινδύνων που συνδέονται με τη χρήση των ΨΤ, των ψηφιακών πόρων και κυρίως του Διαδικτύου.

Στόχοι:

Οι επιμορφούμενοι/ες επιδιώκεται να:

- αποκτήσουν βασικές γνώσεις σε θέματα ψηφιακής πολιτειότητας και ψηφιακού γραμματισμού, ασφαλούς πλοήγησης και διαδεδομένων τεχνολογιών που έχουν άμεσες κοινωνικές επιπτώσεις. Συγκεκριμένα, να:
- είναι σε θέση να προσδιορίζουν ποιοι θεωρούνται γενικά κίνδυνοι που συνδέονται με τη χρήση και διαχείριση ψηφιακών πόρων και ιδιαίτερα του Διαδικτύου,
- είναι σε θέση να προσδιορίζουν ποιοι από τους κινδύνους είναι ιδιαίτερα συνδεδεμένοι με τις μικρές ηλικίες, το σχολείο, την εκπαίδευση,
- να αποκτήσουν γνώσεις και δεξιότητες για την αντιμετώπιση των κινδύνων και τη διδασκαλία των σχετικών θεμάτων είτε με τρόπο άμεσο (οργανώνοντας μαθήματα επί τούτου), είτε έμμεσα (στα πλαίσια δραστηριοτήτων άλλων γνωστικών αντικειμένων),
- να αποκτήσουν γνώσεις και δεξιότητες σχετικές με την e-πολιτειότητα, το σύνολο των ψηφιακών πρακτικών που συνδέονται με την ιδιότητα του πολίτη,
- να αποκτήσουν γνώσεις σχετικά με τη διαχείριση ψηφιακών πληροφοριών (θέματα στρατηγικών αναζήτησης πληροφοριών, αναφοράς πηγών πληροφοριών, ελέγχου της ποιότητας των πληροφοριών, καλών πρακτικών επικοινωνίας και διάχυσης/μεταβίβασης πληροφοριών).

1. Ασφαλής χρήση του διαδικτύου

1.1 Ορισμός των «κινδύνων στο Διαδίκτυο»

Η καθολική επικράτηση του Διαδικτύου και γενικότερα των ψηφιακών τεχνολογιών συνδέεται με μια σειρά αρνητικών χαρακτηριστικών που ονομάζονται, με έναν γενικό τρόπο, «κίνδυνοι στο Διαδίκτυο». Ο όρος δεν είναι απολύτως ακριβής, καθώς ο όρος «κίνδυνοι» αντιστοιχεί σε χαρακτηριστικά που μπορεί να έχουν αρνητικό χαρακτήρα, αλλά δεν αποτελούν ακριβώς

κινδύνους. Για παράδειγμα, πολλά ανεπιθύμητα μηνύματα (τα λεγόμενα spam), μπορεί να έχουν ανεπιθύμητες συνέπειες (κατανάλωση χρόνου για τη διαγραφή τους ή υπερπλήρωση του ηλεκτρονικού γραμματοκιβωτίου με άχρηστα μηνύματα), αλλά δεν αποτελούν ακριβώς «κινδύνους». Προκαταρκτικά, θα πρέπει πάντως να επισημανθούν δυο στοιχεία:

- Η έννοια του κινδύνου (συνδεδεμένη και με την έννοια της «απειλής» αλλά και της αντίθετης έννοιας της «ασφάλειας» και της «προφύλαξης», όπως και με την έννοια της «απαγόρευσης» για την προστασία των ευάλωτων ατόμων) είναι σε μεγάλο βαθμό μια κοινωνική κατασκευή και δεν είναι «σταθερή» στον χρόνο και στον χώρο, σε κάθε κουλτούρα. Ο κίνδυνος είναι μια συνάρτηση πολλών παραγόντων όπως ο χρόνος, ο τόπος, η ηλικία (τόσο αυτού που κρίνει, όσο και αυτού που βρίσκεται «εν κινδύνω»), ακόμη και παραγόντων κοινωνικών και ιδεολογικών. Υπάρχουν άφθονα παραδείγματα, από τετριμμένα ως λιγότερο προφανή, που υποστηρίζουν τη θεωρητική αυτή θέση, που είναι μάλλον γενικά αποδεκτή. Για παράδειγμα στον Μεσαίωνα, η υπερβολική ενασχόληση με τα βιβλία (η ανάγνωση δηλαδή) και μάλιστα η σιωπηλή ανάγνωση δεν θεωρήθηκε αρχικά ως θετικό στοιχείο της ανθρώπινης προσωπικότητας, καθώς ως τότε η ανάγνωση ήταν μεγαλόφωνη και «... γινόταν με συγκεκριμένους κανόνες σε προκαθορισμένο τόπο και χρόνο» (Μπάνου, 2010). Ακόμη, αναγνώσματα που σήμερα θεωρούνται ως κατάλληλα για τα νεαρά άτομα και τα παιδιά (για παράδειγμα ο δημοφιλής «Μικρός Ήρως»), πριν από 50 ή 60 χρόνια είχαν θεωρηθεί ως επικίνδυνα αναγνώσματα για τη νεολαία. Οι εκπαιδευτικοί θα πρέπει, με ένα γενικό τρόπο, να έχουν μια κριτική στάση απέναντι σε ό,τι συλλήβδην χαρακτηρίζεται ως «επικίνδυνο».
- Θα πρέπει, επίσης, να αναγνωρίσουμε ότι πολύ συχνά η νεολαία, και ιδιαίτερα οι έφηβοι, «περνούν τα όρια», έλκονται από τον κίνδυνο και αγνοούν τις απαγορεύσεις, ίσως γιατί αυτή η συμπεριφορά αποτελεί συστατικό στοιχείο της διαδικασίας διαμόρφωσης της προσωπικότητάς τους, της ταυτότητάς τους. Αυτό ίσως σημαίνει πως όποια μέτρα και αν λάβουν το σχολείο και οι γονείς, όσες παραινέσεις και να κάνουν, οι έφηβοι στον ιδιωτικό τους χώρο και χρόνο θα επισκεφτούν ιστοχώρους που θεωρούνται ακατάλληλοι ή επικίνδυνοι και θα δοκιμάσουν να κάνουν ενέργειες που δεν εγκρίνουν οι ενήλικοι. Αυτό δεν σημαίνει βέβαια πως δεν πρέπει να ληφθούν μέτρα για την προστασία τους – το αντίθετο μάλιστα.

Η έννοια του κινδύνου, όπως αναφέρουμε λίγο παραπάνω, δεν είναι απολύτως προσδιορισμένη με ένα καθολικά αποδεκτό τρόπο. Ορισμένα παραδείγματα ορισμών (τα οποία παρατίθενται ενδεικτικά) είναι τα ακόλουθα:

- Ο Volkmann (Καμάρης 2014, σ. 16) αναφέρει:

Οι Διαδικτυακοί κίνδυνοι μπορούν να οριστούν ως κάθε τι που μπορεί να προκαλέσει βλάβη σε έναν χρήστη του Διαδικτύου. Η βλάβη αυτή μπορεί να είναι διαφόρων μορφών όπως φυσική, συναισθηματική, ψυχολογική, οικονομική, κοινωνική ή αναφερόμενη στην υπόληψη του χρήστη.

- Η Warner-Blankenship (Καμάρης 2014, σ. 16) υποστηρίζει ότι:

Οι Διαδικτυακοί κίνδυνοι είναι κίνδυνοι που σχετίζονται με το να είναι κάποιος χρήστης του Διαδικτύου. Οι κίνδυνοι αυτοί μπορεί επίσης να αφορούν στην πρόσβαση σε ανεπιθύμητες πληροφορίες. Υπάρχει μεγάλη ποικιλία Διαδικτυακών κινδύνων από θέματα ασφάλειας έως διάφορα είδη θυματοποίησης.

- Τέλος, στη Wikipedia.org για την παρεμφερή έννοια της «Απειλής στον Ιστό» (Web threat) το σχετικό άρθρο αναφέρει (στο Καμάρης 2014, σ. 17):

Απειλή στον Ιστό είναι κάθε απειλή που χρησιμοποιεί τον Παγκόσμιο Ιστό για να διευκολύνει το έγκλημα στο Διαδίκτυο.

Συνοψίζοντας, είναι κοινή η διαπίστωση πως κίνδυνο αποτελεί καθετί που απειλεί τη ζωή, την ασφάλεια ή την ακεραιότητα ενός προσώπου ή ενός πράγματος και αντίστοιχα ασφάλεια είναι η κατάσταση που χαρακτηρίζεται από την απουσία κινδύνου (Καμάρης, 2014).

1.2 Κατηγορίες κινδύνων, ενοχλητικών, ανεπιθύμητων στοιχείων στο Διαδίκτυο και τους ψηφιακούς πόρους

Με έναν γενικό τρόπο, θα πρέπει να υπενθυμίσουμε πως ταυτόχρονα με τις νέες δυνατότητες, τα σύγχρονα κινητά μέσα πρόσβασης στο Διαδίκτυο (smart phones, tablets κ.τ.ό.) αυξάνουν και την πιθανότητα να βρεθεί κάποιος χρήστης εκτεθειμένος στα αρνητικά στοιχεία που περιγράφονται παρακάτω. Ιδιαίτερα η αύξηση της χρήσης (για παράδειγμα οι online συναλλαγές) των ψηφιακών μέσων, απαιτεί και μεγαλύτερη προσοχή από τη μεριά των χρηστών. Μια σχετικά πλήρης καταγραφή των διαφόρων κατηγοριών των στοιχείων αυτών περιλαμβάνεται στο κείμενο το οποίο αποτελεί βασική πηγή για την παρούσα ενότητα (Καμάρης 2014) και περιλαμβάνει τα εξής (μαζί με την αντίστοιχη Αγγλική ορολογία):

- Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content)
- Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages)
- Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation). Διαμόρφωση ταυτότητας. Έκθεση στα κοινωνικά δίκτυα
- Ηλεκτρονική αποπλάνηση χρηστών (Online grooming)
- Βίαια παιχνίδια (Violent games)
- Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction)
- Διαδικτυακός εκφοβισμός (Cyber bullying)
- Παρώθηση σε επιβλαβείς συμπεριφορές
- Ηλεκτρονικός τζόγος (Online gambling)
- Κακόβουλο λογισμικό που μολύνει Ηλεκτρονικούς Υπολογιστές (Malware) Δες σχετικό βίντεο: https://www.youtube.com/watch?v=9XS6RhDJzxk
- Παιδική πορνογραφία (Child pornography)
- Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy) και επιπτώσεις ακόμη και στην κινητή τηλεφωνία
- Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation). Ψευδή νέα και ο πολλαπλασιασμός τους. Αστικοί μύθοι. Ψηφιακές φάρσες.
- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Phishing»
- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Pharming»
- Φυσικές παθήσεις που προκαλούνται από παρατεταμένη χρήση του Η/Υ

1.2.1 Ακατάλληλο, προσβλητικό και επιβλαβές περιεχόμενο ιστοχώρων (Offensive content)

Το περιεχόμενο ενός ιστοχώρου (λεκτικό, οπτικό ή ακουστικό) θεωρείται ακατάλληλο ή προσβλητικό, όταν παραβιάζει τα κοινωνικά, θρησκευτικά ή πολιτισμικά πρότυπα ή τις προσωπικές και οικογενειακές αξίες του ατόμου. Είναι προφανές ότι όλες αυτές οι διατυπώσεις πρέπει να λαμβάνονται υπόψη μέσα στη σχετικότητά τους, αφού τα πολιτισμικά, κοινωνικά ή θρησκευτικά πρότυπα δεν έχουν καθολικό χαρακτήρα. Έτσι, η ακαταλληλότητα του περιεχομένου ενός ψηφιακού πόρου και ο βαθμός επικινδυνότητάς του σχετίζεται με τα ατομικά χαρακτηριστικά του χρήστη. Είναι εξίσου προφανές ότι τα άτομα που δεν έχουν ακόμη τα κατάλληλα γνωστικά και ψυχικά εφόδια που θα τους επέτρεπαν να εξετάσουν κριτικά το αντίστοιχο περιεχόμενο, ενδεχομένως είναι πιο ευάλωτα. Έτσι, για παράδειγμα, έφηβοι, παιδιά, άτομα γενικά νεαρής ηλικίας μπορεί να ενοχληθούν, να ταραχτούν ή να παρωθηθούν σε

παραβατικές ή ανάρμοστες συμπεριφορές από κείμενα, εικόνες και γενικά πόρους των οποίων το «μήνυμα» δεν είναι πάντοτε σε θέση να αντιμετωπίσουν, να κατανοήσουν και να εξετάσουν κριτικά. Φυσικά, το ίδιο περιεχόμενο μπορεί να θεωρείται κατάλληλο για ενήλικα άτομα. Το ακατάλληλο-προσβλητικό υλικό μπορεί να περιλαμβάνει ρατσιστικά, βίαια ή σεξουαλικώς προκλητικά στοιχεία, υλικό που προστατεύεται από πνευματικά δικαιώματα, απαγορευμένο ή παράνομο υλικό, να προάγει την ξενοφοβία, τη βία, τα ναρκωτικά, τα τυχερά παιχνίδια (τζόγο), επικίνδυνες ή εγκληματικές δραστηριότητες, ακραίες φυλετικές απόψεις, προώθηση της φασιστικής ιδεολογίας και άλλες μη ασφαλή στοιχεία, όπως λόγου χάρη διατροφικές διαταραχές ή πορνογραφικό υλικό.

Θα πρέπει να σημειωθεί ότι, με έναν γενικό τρόπο, το μήνυμα ενός ιστοχώρου μπορεί να είναι έμμεσο και για τον λόγο αυτό πολύ πιο δύσκολα ανιχνεύσιμο. Για παράδειγμα, ορισμένες ιστοσελίδες μπορούν έμμεσα να προβάλλουν ως μεγάλη αξία τη σωματική ρώμη και η ανίχνευση και ταυτοποίηση αυτού του μηνύματος να είναι πιο δύσκολη από άτομα που δεν είναι εξοικειωμένα με μια κριτική εξέταση ενός κειμένου. Γενικά, τα γραφικά στοιχεία, μπορούν να εμπεριέχουν έμμεσα εκφρασμένα μηνύματα ακόμη σε πολύ «δευτερεύοντα» χαρακτηριστικά τους όπως τα μεγέθη και η θέση των εικόνων, οι χρησιμοποιούμενες γραμματοσειρές κ.ά.

1.2.2 Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages)

Ένα από τα πλέον διαδεδομένα φαινόμενα στον κυβερνοχώρο είναι τα ανεπιθύμητα (spam messages) και τα απρόσκλητα γενικότερα μηνύματα (unsolicited messages) που οι χρήστες δέχονται στο ηλεκτρονικό ταχυδρομείο και τα κινητά τηλέφωνα. Τα μηνύματα αυτά σχετίζονται συχνά με διαφημίσεις προϊόντων ή υπηρεσιών, την προώθηση τυχερών παιχνιδιών (καλυμμένων ενίοτε ως κερδών σε μια κλήρωση στην οποία ο χρήστης ποτέ δεν συμμετείχε), με πορνογραφικό υλικό κ.ά. Μερικές φορές, με πρόσχημα μια ιστορία στην οποία (υποτίθεται ότι) υπάρχουν αδιάθετα κάποια σημαντικά χρηματικά ποσά, ο χρήστης καλείται να συμμετάσχει προσφέροντας υπηρεσίες για τις οποίες (υποτίθεται πάντα ότι) θα αμειφθεί πλουσιοπάροχα. Η πιο γνωστή κατηγορία εξαπάτησης αυτού του είδους είναι η «απάτη της Νιγηρίας» (Nigeria scam). Τα μηνύματα αυτά πολλές φορές αποστέλλονται μαζικά σε μεγάλους αριθμούς (bulk mails) και μεταφράζονται από γλώσσα σε γλώσσα με αυτόματους μεταφραστές. Στις περιπτώσεις αυτές, οι ίδιες οι μεταφράσεις παράγουν κείμενα ακατανόητα ή με χονδροειδή γλωσσικά ή επικοινωνιακά λάθη, καθιστώντας πολύ εύκολη τη διαπίστωση ότι πρόκειται για ψευδή μηνύματα.

Για παράδειγμα το ακόλουθο (αληθινό) μήνυμα εστάλη, υποτίθεται από μια Τράπεζα:

Αγαπητε πελατη,
Εχετε λαβει ενα νεο κοινοποιηση
Καντε κλικ εδω για να διαβασετε.

Είναι προφανές ότι πρόκειται για μήνυμα που αποσκοπεί στην εξαπάτηση του χρήστη. Εξάλλου ο υπερδεσμός (στο κλικ) οδηγεί σε έναν άσχετο με οιαδήποτε Τράπεζα και πιθανότατα επικίνδυνο ιστοχώρο (για να το διαπιστώσει, αρκεί να «περάσει» κανείς με το ποντίκι πάνω από τον υπερδεσμό χωρίς να κάνει «κλικ»).

Μια ακόμα αρνητική όψη στο φαινόμενο του spam είναι η οικολογική: η παραγωγή και διάδοση των ανεπιθύμητων μηνυμάτων, όπως αναφέρουν οι σχετικές έρευνες, προκαλεί τόση μόλυνση, όση, για παράδειγμα, η κυκλοφορία εκατοντάδων χιλιάδων αυτοκινήτων: αν και το οικολογικό αποτύπωμα (μέσω κατανάλωσης ενέργειας) που προκύπτει από την αποστολή ενός email δεν

είναι τόσο σημαντικό, ο άσκοπος πολλαπλασιασμός τους λειτουργεί σωρευτικά, με αρνητικές επιπτώσεις.

1.2.3 Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation)

Ο όρος χρησιμοποιείται για να περιγράψει ένα φαινόμενο που παρατηρείται κυρίως, αλλά όχι αποκλειστικά, σε νεαρά άτομα. Οι χρήστες ασχολούνται σταδιακά ολοένα και περισσότερο με διαδικτυακά και γενικότερα ψηφιακά παιχνίδια, με την άμεση online συνομιλία (chat rooms), με σελίδες κοινωνικής δικτύωσης κ.ά. και αποξενώνονται από τον φυσικό και κοινωνικό τους περίγυρο. Ο χρόνος που αφιερώνουν στις ενασχολήσεις αυτές γίνεται τελικά τόσο μεγάλος που αποκλείει άλλου είδους δραστηριότητες ατομικές ή ομαδικές, σε ακραίες περιπτώσεις ακόμη και την ατομική φροντίδα του εαυτού και τη στοιχειώδη υγιεινή. Οι σχέσεις με τους άλλους ανθρώπους του περίγυρου, τους φίλους, του γονείς γίνονται προβληματικές και σπάνιες. Δημιουργείται έτσι μια συναισθηματική και κοινωνική αποξένωση των χρηστών από τον περίγυρό τους (εκτός των άλλων). Είναι σαν μια «δεύτερη», παράλληλη, εικονική ή online ζωή στην οποία ζουν οι εθισμένοι χρήστες και η οποία προοδευτικά διογκώνεται και γίνεται πιο σημαντική από την πραγματική ζωή. Το φαινόμενο είναι τόσο σημαντικό και διαδεδομένο, ώστε έχει αναγνωριστεί ως ένα είδος πάθησης που χρειάζεται θεραπεία, ακόμη και σε εξειδικευμένα θεραπευτικά κέντρα.

1.2.4 Διαδικτυακός εκφοβισμός (Cyber bullying)

Ο Διαδικτυακός Εκφοβισμός ορίζεται ως «μια επιθετική, σκόπιμη και επαναλαμβανόμενη πράξη η οποία πραγματοποιείται από ένα άτομο ή μια ομάδα ατόμων, μέσω της χρήσης ηλεκτρονικών μορφών επικοινωνίας, εναντίον ενός ατόμου που δεν μπορεί εύκολα να υπερασπιστεί τον εαυτό του» (Smith κ.ά. 2008).

Πραγματοποιείται συνήθως μέσα από το ηλεκτρονικό ταχυδρομείο, τα δωμάτια συζητήσεων, τους ιστότοπους κοινωνικής δικτύωσης (social networking sites), τις ιστοσελίδες (web sites), τα ιστολόγια (blogs), τα Διαδικτυακά παιχνίδια και τα κινητά τηλέφωνα. Οι μορφές που μπορεί να έχει είναι:

- Η διακωμώδηση ή/και εξευτελισμός του θύματος
- Η αποστολή προσβλητικών και άσεμνων μηνυμάτων μέσω Διαδικτυακών εφαρμογών
- Το άσεμνο περιεχόμενο κατά τη διάρκεια συνομιλιών
- Ο εξευτελισμός ενός νεαρού ατόμου με τη δημιουργία ενός προφίλ ή ιστολογίου το οποίο περιλαμβάνει σκόπιμα λανθασμένα στοιχεία ή εξευτελιστικό περιεχόμενο
- Η αποστολή απειλητικών μηνυμάτων
- Η δημοσιοποίηση προσωπικών βίντεο ή φωτογραφιών χωρίς τη συγκατάθεση του ατόμου.

Η ιδιαιτερότητα του Διαδικτυακού Εκφοβισμού έγκειται στο γεγονός πως επεμβαίνει στον προσωπικό χώρο του θύματος, ενώ είναι δύσκολος ο περιορισμός του εξαιτίας της αδυναμίας ελέγχου του αριθμού και του περιεχομένου των μηνυμάτων που μπορεί να λάβει ένας χρήστης του Διαδικτύου.

Ο κυβερνοεκφοβισμός (cyberbullying) είναι η συνέχεια του εκφοβισμού με ψηφιακά μέσα. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- **Εκφοβισμός με γραπτό μήνυμα:** το παιδί ίσως λάβει δυσάρεστα, προσβλητικά ή απειλητικά μηνύματα.
- **Παρενόχληση/κλήσεις-φάρσα:** κάποιος ίσως καλεί επίμονα το παιδί στο κινητό του και του λέει δυσάρεστα και προσβλητικά πράγματα.
- **Δημοσίευση και διαμοιρασμός εικόνων χωρίς τη συγκατάθεση του παιδιού:** φωτογραφίες, βίντεο ή οπτικό υλικό τραβηγμένο με webcam, όπου εμφανίζεται το παιδί, θα μπορούσαν να κυκλοφορήσουν μέσω email ή μηνυμάτων, να αναρτηθούν στο διαδίκτυο ή να μπουν σε δημόσιο ιστότοπο με το όνομα του παιδιού σε ετικέτα.
- **«Happy slapping»:** κάποιος θα μπορούσε με το κινητό του να φωτογραφίσει ή να βιντεοσκοπήσει το παιδί καθώς το κακοποιεί λεκτικά ή σωματικά.
- **Εκφοβισμός μέσω email ή άμεσων μηνυμάτων:** το παιδί θα μπορούσε να λάβει δυσάρεστα, προσβλητικά ή ενοχλητικά email ή άμεσα μηνύματα από κάποιον που γνωρίζει ή από έναν άγνωστο.
- **Εκφοβισμός σε chatroom:** ένας άλλος χρήστης του chatroom θα μπορούσε να πει αγενή πράγματα στο, ή για το, παιδί σας.
- **Εκφοβισμός μέσω κοινωνικού δικτύου:** κάποιος θα μπορούσε να αναρτήσει δυσάρεστα ή προσβλητικά μηνύματα για το παιδί σας σ' έναν ιστότοπο σαν το Facebook, ή να φτιάξει ένα πλαστό προφίλ του παιδιού.
- **Εκφοβισμός στη διάρκεια ενός διαδραστικού παιχνιδιού:** αν το παιδί παίζει παιχνίδια για πολλούς παίκτες, κάποιος συμπαίκτης του ίσως προσπαθήσει να το αποκλείσει ή να το αγνοήσει. Οι έρευνες δείχνουν πως αυτού του είδους ο διαδικτυακός εξοστρακισμός έχει αντίκτυπο στην αυτοεκτίμηση.

1.2.5 Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation)

Το Διαδίκτυο αφενός μεν παρέχει αναρίθμητους πόρους και ευκαιρίες μάθησης, αφετέρου δε, σε αντίθεση με τα παραδοσιακά έντυπα μέσα, δεν διαθέτει τις απαραίτητες δικλείδες ασφαλείας για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται, με αποτέλεσμα σε κάποιες περιπτώσεις ο χρήστης να οδηγηθεί σε λανθασμένα, ανακριβή και αναξιόπιστα συμπεράσματα, λόγω της δημοσίευσης αναληθών, τροποποιημένων ή ελλιπών πληροφοριών.

Χαρακτηριστικό παράδειγμα της παραπληροφόρησης είναι οι αστικοί μύθοι (urban legends), οι οποίοι λόγω του Διαδικτύου διαδίδονται με μεγαλύτερη ευκολία, σε περισσότερο πληθυσμό. Ο Connie Chesner, εκπαιδευτής στο Πανεπιστήμιο Wake Forest των Η.Π.Α. αναφέρει πως νέα χαρακτηριστικά, όπως η κακόβουλη πρόθεση, ο εμπλουτισμός με τεχνολογία υψηλότερης ποιότητας και με γνωρίσματα που παρέχουν φαινομενική αυθεντικότητα, κάνουν τους σημερινούς Διαδικτυακούς αστικούς μύθους πιο αληθοφανείς και ενδεχομένως πιο επιβλαβείς.

Κατά συνέπεια, κρίνεται αναγκαία η ανάπτυξη κριτικής σκέψης από τον χρήστη του Διαδικτύου, προκειμένου να κρίνει την ακρίβεια των πληροφοριών αυτών και να ξεχωρίσει τη μη έγκυρη πληροφορία. Όπως είναι φυσικό ο κίνδυνος της παραπληροφόρησης είναι ιδιαίτερα αυξημένος με απρόβλεπτα αποτελέσματα σε νεαρά άτομα τα οποία λόγω ηλικίας δεν έχουν οξυμένη την κριτική τους σκέψη και ικανότητα.

Για το ζήτημα αυτό βλ. παρακάτω και το κεφάλαιο για την ψηφιακή πολιτειότητα.

1.3 Τρόποι αντιμετώπισης των επικίνδυνων ή αρνητικών στοιχείων του Διαδικτύου

Με έναν γενικό τρόπο, οι μέθοδοι για την αντιμετώπιση αυτών των αρνητικών στοιχείων χωρίζονται σε δυο κατηγορίες: μέθοδοι τεχνικού χαρακτήρα και μέθοδοι ενημερωτικού και παιδαγωγικού χαρακτήρα.

1.3.1 Μέθοδοι τεχνικού χαρακτήρα

Στις μεθόδους τεχνικού χαρακτήρα περιλαμβάνονται μια πλειάδα από συστήματα που έχουν αναπτυχθεί για την άμεση προστασία των χρηστών (κυρίως ευάλωτων χρηστών, όπως για παράδειγμα τα παιδιά), αλλά και συστήματα συμβουλών, εκπαίδευσης, σήμανσης ιστοχώρων και περιεχομένου με σκοπό οι χρήστες να αναγνωρίζουν το επικίνδυνο ή αμφίβολο περιεχόμενο και να αντιδρούν κατάλληλα (Καμάρης 2014, σελ. 32).

Ως τέτοιες μεθόδους μπορούμε να αναφέρουμε τα διάφορα είδη φίλτρων. Τα φίλτρα μπορούν να είναι (σύμφωνα με τον ιστοχώρο https://saferinternet4kids.gr) πολλών ειδών και να επιτελούν πολλές λειτουργίες, όπως να προειδοποιήσουν για προβληματικές ιστοσελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο Διαδίκτυο, να μπλοκάρουν ύποπτους ιστοχώρους, να επιτρέπουν την πρόσβαση συγκεκριμένες ώρες και ημέρες, ακόμα και να κλείσουν τελείως τον υπολογιστή. Φίλτρα αυτού του είδους, (σύμφωνα με τον ιστοχώρο) είναι:

- Οι λεγόμενες «**περιφραγμένες τοποθεσίες**» (walled gardens) ή «**λευκές λίστες**» (white lists) είναι λίστες από ιστοσελίδες κατάλληλες για ανηλίκους. Οι «**μαύρες λίστες**» λειτουργούν με αντίστοιχο τρόπο – για παράδειγμα απαγορεύουν την αποστολή e-mails από διευθύνσεις που έχουν παρατηρηθεί να στέλνουν συχνά spam σε άλλες διευθύνσεις.
- Οι **λίστες ψηφιακών πόρων με ακατάλληλο περιεχόμενο** συνιστούν άλλο ένα είδος τέτοιου φίλτρου. Οι χρήστες δεν έχουν πρόσβαση σε ιστοχώρους που περιλαμβάνονται σε αυτές τις λίστες. Συχνά οι λίστες δεν περιλαμβάνουν συγκεκριμένους ιστοχώρους, αλλά λέξεις ή όρους «απαγορευμένους» και αποκλείουν την πρόσβαση σε ιστοσελίδες που περιέχουν (στο κείμενο ή τον τίτλο τους) τις λέξεις αυτές ή τους αντίστοιχους όρους. Εκτός του ότι οι λίστες αυτές χρειάζονται συχνά επικαιροποίηση, πολλές φορές αποκλείουν την πρόσβαση σε ιστοχώρους που δε θα έπρεπε να εξαιρούνται: ένα παράδειγμα αποτελεί η ιστορία ιστοσελίδων ενός αστεροσκοπείου στη Μ. Βρετανία που διδάσκει την αναγνώριση αστερισμών στον ουρανό με παρατήρηση δια «γυμνού οφθαλμού» (naked-eye) που είναι μη-προσβάσιμος καθώς η λέξη «γυμνός» θεωρείται «απαγορευμένη». Τα φίλτρα «γονεϊκού ελέγχου» (parental control) πολύ συχνά στηρίζονται σε λίστες αυτού του είδους. Χρησιμοποιούν όμως παράλληλα και άλλου είδους ελέγχους, όπως χρόνο έναρξης της πλοήγησης και γενικότερα πρόσβαση, διάρκεια χρήσης, καταγραφή δραστηριοτήτων του χρήστη (παιδιού) κ.ά.
- Σε ορισμένες περιπτώσεις, με συγκατάθεση των ιδιοκτητών των σχετικών ιστοχώρων, οι πάροχοι πρόσβασης στο Διαδίκτυο **επισημαίνουν με κατάλληλες ψηφιακές ετικέτες** του ιστοχώρους που έχουν εν δυνάμει επιβλαβές περιεχόμενο. Η Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου ICRA (Internet Content Rating Association) δημιουργεί ετικέτες αυτού του είδους που μπορούν να χρησιμοποιηθούν από φίλτρα διαφόρων ειδών. Σχετικό με αυτά είναι το ευρωπαϊκό σύστημα PEGI, ένα σύστημα **ηλικιακής διαβάθμισης**. Σύμφωνα με την ιστοσελίδα του ίδιου του συστήματος PEGI, *οι ηλικιακές διαβαθμίσεις είναι συστήματα που χρησιμοποιούνται για να εξασφαλίσουν ότι όλα τα προϊόντα ψυχαγωγικού περιεχομένου, όπως κινηματογραφικές ταινίες, βίντεο, DVD και παιχνίδια υπολογιστή, φέρουν σαφή επισήμανση βάσει ηλικίας σύμφωνα με το περιεχόμενό τους. Οι ηλικιακές διαβαθμίσεις προσφέρουν καθοδήγηση στους καταναλωτές (ιδίως τους γονείς), βοηθώντας τους να αποφασίσουν αν θα αγοράσουν ή όχι ένα συγκεκριμένο προϊόν*.

- **Έλεγχος εισερχομένων μηνυμάτων για ανεπιθύμητα μηνύματα** (spam). Η πλειοψηφία των παρόχων υπηρεσιών ηλεκτρονικής αλληλογραφίας ελέγχει τα εισερχόμενα μηνύματα κάθε χρήστη και χαρακτηρίζει ως ανεπιθύμητα όσα κρίνει ως τέτοια (μερικές φορές μάλιστα τα απορρίπτει αυτομάτως). Ο έλεγχος χρησιμοποιεί έναν συνδυασμό διαφόρων μεθόδων όπως αυτές που περιγράφονται παραπάνω και πολύ προηγμένες τεχνικές για να εκτιμήσει την καταλληλότητα των εισερχομένων μηνυμάτων. Ωστόσο πολλές φορές ούτε αυτά τα μέτρα αρκούν και ορισμένα e-mails χαρακτηρίζονται ως spam ενώ δεν είναι, ενώ αντίθετα μερικά spam καταλήγουν στον χρήστη χωρίς χαρακτηρισμό. Για παράδειγμα, οι έλεγχοι λέξεων μπορεί να αποφανθούν ότι οι ειδικοί χαρακτήρες @, /, |, \ και τα γράμματα R και G δεν μπορούν φυσικά να παραγάγουν κείμενο, αλλά ένας χρήστης θα αναγνωρίσει στο συνδυασμό \/ | @ G R @ πιθανότατα ένα γνωστό φάρμακο. Έτσι το σχετικό e-mail θα «περάσει» σχετικό έλεγχο, αλλά ο παραλήπτης θα διαβάσει μια διαφήμιση για το φάρμακο.
- Τέλος, στην κατηγορία αυτή περιλαμβάνεται το λ**ογισμικό καταπολέμησης των ιών** (antivirus και antispyware) όσο και το «**τείχος προστασίας**» (Firewall). Η γενική ονομασία «ιοί» καλύπτει στην πραγματικότητα μια πλειάδα κατηγοριών λογισμικών όπως τους Ιούς αρχείων (File Viruses), τους Δούρειους ίππους (Trojan Horses), τα Σκουλήκια (Worms), τους Καταγραφείς πληκτρολόγησης (Keyloggers), το Λογισμικό Spyware – Adware (Καμάρης, 2014). Το «**Τείχος προστασίας**» (Firewall) είναι ειδικό λογισμικό σχεδιασμένο ώστε να αποτρέπει ή να διακόπτει τη μη εξουσιοδοτημένη πρόσβαση από τον «έξω» κόσμο του δικτύου ή Διαδικτύου στον ή στους προστατευόμενους Η/Υ και αντίστροφα την ανεξέλεγκτη ροή πληροφορίας προς τον «έξω» κόσμο.

1.3.2 Μέθοδοι που βασίζονται στην ενημέρωση και τη διαπαιδαγώγηση

Με τον όρο διαπαιδαγώγηση δεν αναφερόμαστε αποκλειστικά στην παιδική ηλικία, αλλά γενικότερα στον τρόπο με τον οποίο προετοιμάζουμε τους χρήστες για να είναι ασφαλείς στο διαδίκτυο. Κατά κανόνα, οι πάροχοι περιεχομένου ή υπηρεσιών που αποτελούν δημοφιλείς «στόχους», φροντίζουν να δίνουν συμβουλές για καλές πρακτικές ασφαλείας στους χρήστες που κάνουν χρήση των ψηφιακών πόρων και υπηρεσιών τους. Για παράδειγμα, οι Τράπεζες συστηματικά συμβουλεύουν τους online πελάτες τους, όπως παρακάτω (αυθεντικό μήνυμα):

> Για την προστασία σας από προσπάθειες υποκλοπής στοιχείων Κωδικού Χρήστη (User ID) , Μυστικού Κωδικού (Password) και Ηλεκτρονικού Κλειδάριθμου (i-code) μέσω της αποστολής παραπλανητικών μηνυμάτων (phishing emails), σας ενημερώνουμε ότι:
> Η Τράπεζα XXXXX δε θα σας ζητήσει ποτέ και με κανέναν τρόπο (τηλεφωνικώς, μέσω e-mail ή οποιοδήποτε άλλο μέσο επικοινωνίας) τους **κωδικούς** σας User ID, Password ή το i-code.
> **Μην απαντάτε** σε e-mail που σας ζητούν **προσωπικά σας στοιχεία.** Διαγράψτε τα αμέσως. Σε περίπτωση που έχετε ήδη απαντήσει σε τέτοιου είδους μήνυμα και έχετε συμπληρώσει στοιχεία σας, **επικοινωνήστε άμεσα** με το Κέντρο Τηλεφωνικής Εξυπηρέτησης της Τράπεζας στα τηλέφωνα: **888888** (απο Ελλάδα) ή **888888888** (από εξωτερικό) και μη χρησιμοποιήσετε το Internet Banking της Τράπεζας πριν έλθετε σε επικοινωνία με τα παραπάνω τηλέφωνα.
> **Μην παρασύρεστε** από συνδέσμους (links) που πιστεύετε ότι θα σας οδηγήσουν σε site της XXXXX Τράπεζας. Πάντα πληκτρολογείτε τη διεύθυνση της ιστοσελίδας μόνοι σας **(www.xxx.gr)** και **όχι** μέσω σύνδεσης (link) που πιθανόν σας σταλεί μέσω e-mail ή δημοσιεύεται σε ιστοσελίδες άλλων εταιρειών, μηχανών αναζήτησης κ.λπ.
> **Προστατεύστε τον υπολογιστή** σας με προγράμματα **antivirus και antispyware** και φροντίστε για τη συχνή ενημέρωσή τους με τις τελευταίες εκδόσεις.

Σε τι όμως συνίσταται αυτή η προσέγγιση, της διαπαιδαγώγησης, όταν αναφερόμαστε σε παιδιά ή εφήβους;

Εικόνα 1: Παιδιά μπροστά στη θάλασσα του διαδικτύου

Κατά κάποιο τρόπο, η φωτογραφία παραπάνω συμπυκνώνει το νόημα της διαπαιδαγώγησης. Η θάλασσα μπορεί να είναι, ή μάλλον είναι, ένας πολύ επικίνδυνος τόπος. Πολλοί φοβούνται τη θάλασσα. Όμως η μητέρα της φωτογραφίας (τελικά και όλοι οι γονείς) δεν απαγορεύει την επαφή με τη θάλασσα. Αντίθετα εξοικειώνει τα παιδιά με τη θάλασσα (όπως υπονοείται στην παραπάνω φωτογραφία), την απολαμβάνει μαζί τους, τους μαθαίνει τους κανόνες για την ασφαλή «χρήση» της θάλασσας: πώς κολυμπάει κανείς με ασφάλεια, πώς αντιμετωπίζει ένα πρόβλημα στη θάλασσα. Με μια αναλογία, θα λέγαμε ότι για την ασφαλή χρήση των ψηφιακών πόρων και την ασφαλή πλοήγηση στο Διαδίκτυο, η κατακλείδα είναι να μάθει κανείς στο παιδί του (ή στο μαθητή του) κανόνες της ασφαλούς χρήσης και να το εξοικειώσει με το Διαδίκτυο μοιραζόμενος μαζί του πόρους (κείμενα, φωτογραφίες, βίντεο, ιστοχώρους, τεχνικές, ειδήσεις) και δραστηριότητες (πλοήγηση, παιχνίδια) που είναι θετικοί, ευχάριστοι, σύμφωνοι με την κουλτούρα και τις αξίες τους. Η ιδέα είναι τελικά ότι η διαπαιδαγώγηση είναι, κατά κάποιο τρόπο, το πιο ισχυρό όπλο απέναντι στα επιβλαβή ή επικίνδυνα στοιχεία του Διαδικτύου.

Οι εκπαιδευτικοί εξάλλου, μπορούν να συζητούν τα σχετικά θέματα όχι μόνο στη διάρκεια δραστηριοτήτων οργανωμένων ειδικά για την ασφαλή πλοήγηση, αλλά εκμεταλλευόμενοι κάθε είδους δραστηριότητα στην οποία εμπλέκονται ψηφιακοί πόροι και το Διαδίκτυο.

Η εξέλιξη των επιβλαβών ή επικίνδυνων ψηφιακών πόρων έχει μια δυναμική απρόβλεπτη και είναι δύσκολο να αντιμετωπιστεί με τεχνικά και μόνο μέσα (όπως, για παράδειγμα, τα antivirus λογισμικά). Αντίθετα, ο συνδυασμός προφύλαξης με τεχνικά μέσα και με τη σωστή διαπαιδαγώγηση φαίνεται να είναι ο βέλτιστος. Αυτός είναι και ο στόχος πολλών προγραμμάτων και ψηφιακών πόρων που έχουν αναπτυχθεί για την ασφαλή χρήση των ψηφιακών πόρων και του Διαδικτύου ιδιαίτερα:

- Για παράδειγμα, το project educaunet (πρόγραμμα της Ευρωπαϊκής Ένωσης) ήδη από το 2002 είχε ως σκοπό του την παραγωγή ποικίλων μέσων και δραστηριοτήτων που θα βοηθούσαν τους νεαρούς μαθητές να υιοθετήσουν καλές πρακτικές. Πολλές φορές τα νεαρά άτομα και ιδιαίτερα τα παιδιά έχουν εσφαλμένες ιδέες ως προς το τι συνιστά κίνδυνο στο Διαδίκτυο.
- Το παιχνίδι «**δενείσαισυ**» είναι ακριβώς ένα παιχνίδι ρόλων που αποσκοπεί στην ευαισθητοποίηση των νεαρών μαθητών (Πρωτοβάθμιας Εκπαίδευσης) όσον αφορά τις διαπροσωπικές επικοινωνίες μέσω Διαδικτύου.

  Οι μαθητές εργάζονται σε ένα εργαστήριο Πληροφορικής. Κάθε μαθητής ή μαθήτρια δέχεται μια μικρή κάρτα που περιγράφει συνοπτικά μια τυχαία (φανταστική) προσωπικότητα, όπως οι παρακάτω:

  Κατερίνα, 19 ετών, σπουδάζει φωτογραφία, χόμπυ της τα βιβλία και η μουσική. Ονειρεύεται να εργαστεί ως φωτορεπόρτερ σε εφημερίδα.

  Κώστας 20 ετών, σερβιτόρος σε καφετέρια, του αρέσουν τα ταξίδια και το μπάσκετ.

  Η κάρτα που δέχεται κάθε μαθητής είναι τυχαία και έτσι μπορεί την κάρτα της Κατερίνας να την πάρει ο μαθητής Γιώργος, την κάρτα του Κώστα να την πάρει η μαθήτρια Μαρία.

> Στη συνέχεια, οι μαθητές μπαίνουν σε ένα ασφαλές «δωμάτιο συνομιλιών» (chat room) όπου συζητούν μεταξύ τους, καθένας όμως *υποδυόμενος το πρόσωπο που περιγράφει η κάρτα του*. Μετά από ένα χρονικό διάστημα συνομιλιών, η συζήτηση διακόπτεται. Ο δάσκαλος ζητάει από τους μαθητές και τις μαθήτριες να μαντέψουν ποιος είναι ποιος. Εάν το παιχνίδι έχει εκτυλιχτεί όπως προβλέπεται είναι πρακτικά αδύνατον να μαντέψουν ποιος ήταν στ' αλήθεια ο συμμαθητής ή η συμμαθήτρια τους που παρίστανε το (φανταστικό) Κώστα, την Κατερίνα κ.λπ. Με αφορμή αυτό το γεγονός, ο δάσκαλος οργανώνει συζήτηση με τους μαθητές, στην οποία η κεντρική ιδέα είναι: αν δεν μπορείτε να μαντέψετε ποιος είναι ποιος μεταξύ των συμμαθητών σας, τότε σίγουρα δεν μπορείτε να ξέρετε ποιος είναι στην πραγματικότητα ένας (άγνωστος) ψηφιακός σας συνομιλητής.

Στο Παράρτημα του επιμορφωτικού υλικού περιγράφονται μια σειρά πηγών (ψηφιακών και μη-ψηφιακών) οι οποίες είναι προορισμένες να υποστηρίξουν και τις τρεις ομάδες εμπλεκομένων προσώπων, δηλαδή τους μαθητές, τους εκπαιδευτικούς και τους γονείς. Το υλικό αυτό είναι μάλλον προσανατολισμένο προς την ενημέρωση γονέων και εκπαιδευτικών και τη διαπαιδαγώγηση των μαθητών, παρά προς τις τεχνικές λύσεις.

2. Πολιτειότητα και ψηφιακή πολιτειότητα (e-citizenship)

2.1 Ορισμοί

Με τον όρο *πολιτειότητα* (μερικές φορές ο χρησιμοποιούμενος όρος είναι *πολιτότητα*) νοείται γενικά το δικαίωμα αλλά και η υποχρέωση του να είναι κανείς πολίτης, δηλαδή νοείται ο πολιτικός, κοινωνικός και νομικός δεσμός που συνδέει κάποιον ως πολίτη ενός κράτους με το κράτος αυτό και συνεπάγεται ορισμένα δικαιώματα και υποχρεώσεις.

> Η ιδιότητά του ατόμου ως ενεργού, συνεπούς και υπεύθυνου υποκειμένου στο πλαίσιο μιας σύγχρονης διευρυμένης, [...] κοινωνίας φωτίζει, επαναδομεί και αναδομεί το περιεχόμενο της πολιτειακής του οντότητας. Ο σημερινός άνθρωπος είναι ο (ενεργός) πολίτης *ενός υπερ-τοπικού, υπερεθνικού ενδεχομένως παγκόσμιου χώρου*, μιας μη-περιοριστικής μορφής Πολιτείας που διαχέεται και διαστέλλεται στο χωρο-χρόνο, αναπτύσσεται δυναμικά και πολυδιάστατα, δημιουργώντας νέες συνθήκες μέσα στις οποίες το υποκείμενο/πολίτης εξελίσσεται. Οφείλοντας, (ως πολίτης) εξ ορισμού να ανταποκριθεί ορθολογικά, με σεβασμό, σύνεση και υπευθυνότητα σε ένα εξόχως ανομοιογενές και ετερόκλητο, πλέον, πλέγμα σχέσεων, διασφαλίζει την αρμονική του «συμβίωση» (ως κοινωνικού όντος) εντός και εκτός πραγματικών όρων και πλαισίων, με τον κυβερνοχώρο να συνιστά και να λειτουργεί ως μια παράλληλη διάσταση της σύγχρονης Πολιτείας — *ή, ακριβέστερα, ως μιας επέκτασης της σύγχρονης Πολιτείας*. Η νέα μορφή πολιτειότητας ακολουθεί κατά πόδας τις επιταγές (και ανάγκες) της ψηφιακής εποχής, διαμορφώνοντας ένα εξελιγμένο πλαίσιο εννοιολογήσεων εντός του οποίου καλείται ο σύγχρονος πολίτης, με την εκπαίδευση ως το πιο ενδεδειγμένο μέσο ενίσχυσης της ταυτότητάς του, να βρει το δρόμο του μέσα από τις πολύπλοκες και ενίοτε αποπροσανατολιστικές ατραπούς που ορίζει η τεχνολογική πρόοδος και εξέλιξη, αποφεύγοντας [...] και τα παραπλανητικά θέλγητρα ενός σύγχρονου (κι ενίοτε α-σύγχρονου) σύμπαντος λόγων (Μαρινάκη, 2015, περίληψη)

Η πολιτειότητα θα πρέπει να νοηθεί ως κάτι ευρύτερο από την εθνικότητα, την υπηκοότητα και την ιθαγένεια (οι οποίοι είναι συγγενικοί, αλλά εν πολλοίς είναι νομικοί όροι). Το βάρος στην πολιτειότητα δίνεται ακριβώς στο πολιτικό και κοινωνικό σκέλος του ορισμού: αυτό που

ενδιαφέρει είναι κατά κύριο λόγο το πώς μπορεί κανείς να διεκδικήσει τα δικαιώματά του και να ανταποκριθεί στις υποχρεώσεις του ως πολίτη, ιδιαίτερα στην ψηφιακή εποχή και στο σύγχρονο ψηφιακό οικοσύστημα. Κεντρικό ερώτημα της ψηφιακής πολιτειότητας είναι το ακόλουθο: ποιος ακριβώς είναι ο ρόλος των ατόμων, αλλά και των διαφόρων συλλογικοτήτων (ενώσεων, συλλόγων, κοινοτήτων κ.λπ.) στη διαμόρφωση του δημόσιου βίου και των πόλεων ή ακόμη και των κρατών στην ψηφιακή εποχή;

Πρόκειται για μια έννοια ρευστή, δηλαδή μια έννοια που δεν έχει ίσως έναν ακριβή ορισμό και θα πρέπει να γίνει αντιληπτή μάλλον ως ένα σύνολο από δυνατότητες, από κοινωνικές πρακτικές που εξελίσσονται (και μάλιστα γρήγορα), από έννοιες που αναπτύσσονται, από γνώσεις και δεξιότητες που έχουν ένα ιδιαίτερο νόημα στον κυβερνοχώρο. Κατ' αρχάς η e-πολιτειότητα μπορεί να περιλαμβάνει ένα σύνολο από συναλλαγές και επικοινωνίες μεταξύ κράτους και πολίτη: ο πολίτης μπορεί, για παράδειγμα, να επικοινωνεί με τις διάφορες δημόσιες υπηρεσίες για να πληροφορηθεί για διάφορα θέματα, να αιτηθεί και να παραλάβει διάφορα πιστοποιητικά, να ρυθμίσει τις φορολογικές ή ασφαλιστικές του υποχρεώσεις. Μπορεί ακόμη να λάβει μέρος σε δημόσιες online συζητήσεις και να εκφράσει γνώμη για ζητήματα στα οποία η πολιτεία θέλει να έχει τα σχόλια των πολιτών. Το σύνολο των δυνατοτήτων και δραστηριοτήτων αυτού του είδους είναι γενικά γνωστό ως ***ηλεκτρονική διακυβέρνηση*** **(e-government)**. Με μια γενικότερη έννοια όμως, αυτό που ονομάζουμε ψηφιακή πολιτειότητα συνδέεται με τον ψηφιακό γραμματισμό, με τον ίδιο τρόπο που η πολιτειότητα συνδέεται με τον γραμματισμό: αναμένουμε από ένα συνειδητό και καλλιεργημένο άτομο να συμπεριφέρεται υπεύθυνα ως πολίτης και μάλιστα ως ενεργός πολίτης, δηλαδή να συμμετέχει ενεργά σε αυτό που ονομάζουμε *κοινά*. Στο πλαίσιο της ψηφιακής πολιτειότητας προσπαθούμε λοιπόν να μελετήσουμε την έννοια του πολίτη, και μάλιστα του ενεργού πολίτη, όπως διαμορφώνεται στη σύγχρονη εποχή της ψηφιακής τεχνολογίας.

Αποφυγή σύγχυσης στην ορολογία: Ο όρος e-citizenship ως τεχνικός όρος απόκτησης ιθαγένειας

Με τον όρο e-citizenship νοείται και η e-απόκτηση μερικής πολιτειότητας, μια μάλλον ασυνήθιστη διαδικασία απόκτησης επίσημης κάρτας παραμονής ενός «πολίτη από απόσταση», μιας «μερικής υπηκοότητας».

Για παράδειγμα, το project e-σθονία (από το e- και Εσθονία, https://e-estonia.com/) που ξεκίνησε η Εσθονία το 2014, σκοπεύει να εγγράψει μέχρι το 2025 περίπου 10 εκατομμύρια «πολίτες από απόσταση», πολίτες δηλαδή οι οποίοι θα αποκτήσουν ορισμένα πολιτικά δικαιώματα στην Εσθονία, κυρίως συνδεδεμένα με επιχειρηματικότητα και γενικά την ανάπτυξη οικονομικής φύσεως δραστηριοτήτων. Παρόλο που το εγχείρημα (το οποίο είναι σε εξέλιξη) έχει καθαρά οικονομικούς στόχους, δεν έλειψαν και σχολιασμοί για τη δημιουργία e-δημοκρατιών και ίσως e-κρατών. Στην ίδια γραμμή, δηλαδή στο πλαίσιο μιας κρατικής υπόστασης στα ψηφιακά μέσα, αξίζει να αναφερθεί το εγχείρημα Second House of Sweden (SHoS, πληροφορίες στο σχετικό blog) δηλαδή η δημιουργία μιας Σουηδικής πρεσβείας στο περιβάλλον εικονικής πραγματικότητας Second Life από το 2007 ως το 2012.

Χρειάζεται επομένως προσοχή στη χρήση εννοιών όπως e-citizenship, καθώς οι έννοιες αυτές δεν παραμένουν ίδιες και αναλλοίωτες μέσα στα σύγχρονα μηντιακά τοπία και την ψηφιακή τεχνολογία.

2.2 Οι θέσεις του Συμβουλίου της Ευρώπης

Το Συμβούλιο της Ευρώπης εξέδωσε οδηγίες για την **Ψηφιακή** Πολιτειότητα, τις οποίες κατατάσσει σε 10 θεματικές ενότητες:

ΘΕΜΑΤΙΚΗ 1: Πρόσβαση και ολοκλήρωση

Αυτή η θεματική εστιάζει στην πρόσβαση στο ψηφιακό περιβάλλον και περιλαμβάνει μια ολόκληρη σειρά δεξιοτήτων που σχετίζονται όχι μόνο με την επίλυση (των προβλημάτων) των διαφορετικών μορφών ψηφιακού χάσματος αλλά και με τις απαραίτητες δεξιότητες για τη συμμετοχή των μελλοντικών πολιτών σε ψηφιακούς χώρους ανοιχτούς σε όλες τις μειονότητες και γενικότερα στις διαφορετικές απόψεις.

ΘΕΜΑΤΙΚΗ 2: Μάθηση και δημιουργικότητα

Αυτή η θεματική αφορά όχι μόνο την επιθυμία για μάθηση αλλά και τη στάση που υιοθετούμε για τη μάθηση μέσω ψηφιακών περιβαλλόντων, σε όλη τη διάρκεια της ζωής, για να αναπτύξουμε διαφορετικές μορφές δημιουργικότητας χρησιμοποιώντας διαφορετικά εργαλεία μέσα σε πολλαπλά και ποικίλα πλαίσια. Η θεματική καλύπτει τις δεξιότητες προσωπικής ανάπτυξης και επαγγελματικές δεξιότητες που επιτρέπουν να προετοιμαστούν οι αυριανοί πολίτες για τις προκλήσεις που θα παρουσιαστούν από εταιρείες έντασης τεχνολογίας και να τις αντιμετωπίσουν με μια αίσθηση αυτοαποτελεσματικότητας και με καινοτόμους μάλιστα τρόπους.

ΘΕΜΑΤΙΚΗ 3: Ευχέρεια στα ΜΜΕ και την Πληροφοριακή Παιδεία

Αυτή η θεματική αφορά την ικανότητα ερμηνείας, κατανόησης πάντοτε με μια κριτική ματιά, και έκφρασης της δημιουργικότητάς μας δια των ψηφιακών μέσων. Η ικανότητα διαχείρισης των μέσων ενημέρωσης και των πληροφοριών είναι μια ικανότητα που θα έπρεπε να αναπτύσσονται μέσω της εκπαίδευσης και της συνεχούς ανταλλαγής με τους πραγματικότητα που μας περιβάλλει: είναι απαραίτητο να μην αρκούμαστε στην απλή χρήση του ενός ή του άλλου μέσου ή απλά να «ενημέρωσης» για κάποιο θέμα. Ένας ψηφιακός πολίτης πρέπει να διατηρεί συνεχώς κριτική προσέγγιση αν θέλει να είναι σε θέση να συμμετέχει πλήρως και γνήσια στη ζωή της κοινότητάς του.

ΘΕΜΑΤΙΚΗ 4: Ηθική και ενσυναίσθηση

Αυτή η θεματική σχετίζεται με την ηθική της διαδικτυακής συμπεριφοράς και τις αλληλεπιδράσεις με άλλους στο Διαδίκτυο και βασίζεται κυρίως με την ικανότητα αποδοχής και κατανόησης των συναισθημάτων και των απόψεων των άλλων. Η ενσυναίσθηση είναι απαραίτητη για μια θετική διαδικτυακή εμπειρία και αξιοποίηση των ευκαιριών που προσφέρει ο ψηφιακός κόσμος.

ΘΕΜΑΤΙΚΗ 5: Υγεία και ευεξία

Οι ψηφιακοί πολίτες βρίσκονται στους ενδιάμεσους χώρους ανάμεσα στους εικονικούς και τους πραγματικούς χώρους: γι' αυτό η απόκτηση των βασικών ψηφιακών δεξιοτήτων δεν επαρκεί. Τα άτομα καλούνται επίσης να αναπτύξουν στάσεις, δεξιότητες, αξίες και γνώσεις που τους οδηγούν να γίνουν πιο ευαίσθητα σε θέματα υγείας και ευεξίας (ευ ζην). Η Υγεία και το ευ ζην σε έναν κόσμο πλούσιο σε ψηφιακές τεχνολογίες περιλαμβάνουν την επίγνωση των θεμάτων και των δυνατοτήτων που μπορούν να επηρεάσουν ιδιαίτερα τη σφαίρα της ευεξίας, κυρίως, αλλά όχι μόνο, σε θέματα όπως ο εθισμός στο διαδίκτυο, όπως η εργονομία, η θέση αλλά και η υπερβολική χρήση ψηφιακών και φορητών συσκευών.

ΘΕΜΑΤΙΚΗ 6: Διαδικτυακή παρουσία και επικοινωνία

Αυτός ο τομέας αφορά την ανάπτυξη, στους ψηφιακούς πολίτες, προσωπικών και διαπροσωπικών δεξιοτήτων που θα τους βοηθήσουν να διαμορφώσουν και να διατηρήσουν μια παρουσία και μια online ταυτότητα καθώς και διαδικτυακές συναλλαγές που να είναι θετικές, συνεπείς και να αντικατοπτρίζουν με πιστότητα αυτό που είναι (ο χρήστης). Η θεματική καλύπτει αρκετές δεξιότητες, συμπεριλαμβανομένης της επικοινωνίας και της ανταλλαγής διαδικτυακά μέσω εικονικών κοινωνικών χώρων και τη διαχείριση του προσωπικών δεδομένων καθώς και των ιχνών (του χρήστη).

ΘΕΜΑΤΙΚΗ 7: Ενεργή συμμετοχή

Η ενεργή συμμετοχή στο Διαδίκτυο αφορά τις δεξιότητες που οι πολίτες πρέπει να διαθέτουν για να έχουν πλήρη επίγνωση των περιβαλλόντων στα οποία εξελίσσονται προκειμένου να λάβουν σωστές αποφάσεις και να συμμετέχουν ενεργά και θετικά στους δημοκρατικούς πολιτισμούς στους οποίους ζουν.

ΘΕΜΑΤΙΚΗ 8: Δικαιώματα και υποχρεώσεις

Όπως κάθε πολίτης μιας κοινωνίας, οι ψηφιακοί πολίτες του διαδικτυακού κόσμου έχουν ορισμένα δικαιώματα και υποχρεώσεις. Μπορούν να ασκήσουν, μεταξύ άλλων, τα δικαιώματά τους στον σεβασμό της ζωής, την ιδιωτικότητα, ασφάλεια, πρόσβαση και ένταξη, καθώς και την ελευθερία έκφρασης. Αλλά αυτά τα δικαιώματα συνοδεύονται από μια σειρά ευθυνών, όπως η ηθική και η ενσυναίσθηση, καθώς και άλλες που στοχεύουν στη διασφάλιση ενός ψηφιακού περιβάλλοντος χωρίς κινδύνους και υπεύθυνο για όλον τον κόσμο.

ΘΕΜΑΤΙΚΗ 9: Απόρρητο και ασφάλεια

Αυτός ο τομέας καλύπτει δύο διαφορετικές έννοιες: η ιδιωτικότητα αφορά ουσιαστικά την προσωπική προστασία του χρήστη, τις δικές τους πληροφορίες στο Διαδίκτυο και τις πληροφορίες άλλων ατόμων, ενώ η ασφάλεια συνδέεται στενά με την επίγνωση του χρήστη για τις ενέργειες και τις συμπεριφορές στο Διαδίκτυο. Αυτός ο τομέας αφορά διάφορες δεξιότητες όπως η καλή διαχείριση των προσωπικών πληροφοριών που δημοσιεύονται στο Διαδίκτυο καθώς και πληροφοριών άλλων ατόμων ή αυτό που σχετίζονται με τη διαδικτυακή ασφάλεια (χρήση φίλτρων πλοήγησης, κωδικούς πρόσβασης, λογισμικό προστασίας από ιούς και τείχος προστασίας, κ.λπ.) για την αποφυγή επικίνδυνων ή δυσάρεστων καταστάσεων.

ΘΕΜΑΤΙΚΗ 10: Ευαισθητοποίηση του καταναλωτή

Ο Ιστός, με όλες του τις διαστάσεις, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης ή άλλων εικονικών, κοινωνικών χώρων, είναι ένα περιβάλλον μέσα στο οποίο, συχνά, ο ψηφιακός πολίτης είναι και καταναλωτής. Κατανοήστε τις επιπτώσεις της δικής σας επιχειρηματικής πραγματικότητας μέσα σε πολυάριθμους διαδικτυακούς χώρους είναι μια από τις δεξιότητες που τα άτομα θα πρέπει να αποκτήσουν εάν θέλουν να μπορέσουν να διατηρήσουν τη δική τους αυτονομία ως ψηφιακοί πολίτες.

2.3 Αλήθεια, ψευδείς ειδήσεις και παραπλάνηση των πολιτών

Ένα βασικό ζήτημα που προκύπτει γύρω από την ψηφιακή πολιτειότητα όπως προσδιορίστηκε παραπάνω, είναι η έννοια του post-truth (μετα-αλήθεια) και των fake-news (ψευδείς ειδήσεις και ψευδοειδήσεις).

Post-truth κατά λέξη σημαίνει «μετα-αλήθεια». Ο όρος αυτός επελέγη ως *λέξη του 2016*[54] από τα Oxford Dictionaries, ενώ η αντίστοιχη λεξη «Postfaktisch» (post-factual) επελέγη από την Εταιρεία για τη Γερμανική Γλώσσα[55]. Πρόκειται για επίθετα που χαρακτηρίζουν φαινόμενα τα οποία σχετίζονται με ή προσδιορίζουν περιστάσεις στις οποίες τα αντικειμενικά γεγονότα έχουν μικρότερη απήχηση στο σχηματισμό της κοινής γνώμης από όση έχουν τα πλαστά γεγονότα που εστιάζουν στα συναισθήματα και στα προσωπικά «πιστεύω».

Ο όρος φαίνεται ότι υπάρχει εδώ και πολύ καιρό (ίσως και είκοσι ή παραπάνω χρόνια), αλλά έχει καταστεί ιδιαίτερα σημαντικός με την έλευση και την επικράτηση του Διαδικτύου. Σήμερα τα πλαστά νέα και «μετα-αλήθειες» αποτελούν πια μια συνηθισμένη πρακτική. Ο πρώην Αμερικανός Πρόεδρος Μπ. Ομπάμα, λίγο πριν την αποχώρησή του δήλωσε «στο νέο οικοσύστημα των μέσων ενημέρωσης τα πάντα είναι αλήθεια και τίποτα δεν είναι αλήθεια».

Τα τελευταία χρόνια, δύο γεγονότα με μεγάλη πολιτική σημασία, οι προηγούμενες Αμερικανικές εκλογές και πριν λίγα χρόνια το Brexit σημαδεύτηκαν από μια ασταμάτητη ροή ψευδών ειδήσεων και ψευδο-ειδήσεων, μερικές από τις οποίες είναι εξόφθαλμα λανθασμένες, αλλά

[54] https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016
[55] https://www.facebook.com/Gesellschaft-f%C3%BCr-deutsche-Sprache-186994827990942/

παρόλα αυτά, υπάρχει πάντοτε ένα κοινό που τις πιστεύει. Παρόμοια φαινόμενα είδαμε και στον καιρό της πανδημίας.

Για τον τρόπο με τον οποίο δημιουργούνται αυτές οι ειδήσεις υπάρχει μεγάλη σχετική πληροφόρηση στο Διαδίκτυο. Για παράδειγμα, σε ένα ελληνόφωνο άρθρο του 2016 συνοψίζεται η συζήτηση περί ευθυνών των κοινωνικών δικτύων (βλ. https://insidestory.gr/article/post-truth?token=C50B57L6F7, Γορανίτης 2016). Βέβαια, σε ένα πλαίσιο κριτικής προσέγγισης των νέων που κυκλοφορούν στο Διαδίκτυο, αυτά που αναφέρονται στο άρθρο πρέπει επίσης να επαληθευτούν. Για παράδειγμα, ένα σχετικό πρόσφατο άρθρο στους NY Times αναφέρει ότι έρευνα που διεξήχθη πρόσφατα δείχνει ότι τελικά τα κοινωνικά δίκτυα ίσως δεν συμβάλλουν ιδιαίτερα στη δημιουργία κλίματος πόλωσης στην πολιτική ζωή.[56]

Στο ίδιο πλαίσιο, η ιδέα της οργανωμένης και συστηματικής δημιουργίας ακόμη και ψεύτικων λογαριασμών[57] είναι μια πρακτική που εφαρμόζεται σε μεγάλες κλίμακες. Η ίδια η Ευρωπαϊκή Επιτροπή εξέδωσε σχετικές οδηγίες για την καταπολέμηση των φαινομένων αυτών.[58] Έτσι και αλλιώς τα μεγάλα κοινωνικά δίκτυα όπως το facebook και το twitter πολλές φορές έχουν αναγγείλει δημόσια την πρόσθεσή τους να καταπολεμήσουν τα fake-news. Γενικότερα πάντως οργανώνονται αρκετές δράσεις για τον περιορισμό και τον έλεγχο των ψευδών ειδήσεων, όπως στο: https://opengov.ellak.gr/2017/04/17/share-the-facts-mia-efarmogi-enantia-stis-psevdis-idisis/

Από την πλευρά των εκπαιδευτικών, το ερώτημα είναι βέβαια το ακόλουθο: ποια είναι η σημασία και οι πρακτικές επιπτώσεις όλων αυτών των προσεγγίσεων για την Εκπαίδευση; Σίγουρα τα μεγάλα πολιτικά γεγονότα επηρεάζουν τις ζωές όλων μας, αλλά η πολιτική, με τη στενή έννοια, μένει μάλλον έξω από τους σχολικούς τοίχους. Το βασικό συμπέρασμα όμως που συνάγεται από όλες τις παραπάνω περιπτώσεις είναι ότι οι μαθητές πρέπει να αποκτήσουν μια κριτική στάση απέναντι στις πηγές που χρησιμοποιούν από το Διαδίκτυο, τόσο για τις σχολικές εργασίες τους, όσο και σε άλλες περιπτώσεις. Για παράδειγμα, θέματα που σχετίζονται με την οικολογία, συχνά αποτελούν αντικείμενα παραπληροφόρησης ή post-truth στόχους.

Στο άρθρο που προτείνεται παραπάνω για τις post-truth (Γορανίτης 2016), αναφέρεται ότι «*μια ερμηνεία της κλιματικής αλλαγής από έναν νομπελίστα φυσικό δείχνει ακριβώς ίδια στη ροή των ειδήσεων του Facebook, με την άποψη ενός αρνητή της που μισθοδοτείται από τους αδελφούς Κοχ» (μεγιστάνες του πετρελαίου)».* Είναι λοιπόν σχεδόν βέβαιο ότι οι μαθητές, είτε στο πλαίσιο εργασιών για το σχολείο, είτε σε άλλη περίσταση, θα έρθουν αντιμέτωποι με ειδήσεις, πληροφορίες, συζητήσεις, των οποίων το περιεχόμενο δεν θα είναι αυταπόδεικτά ορθό. Οι μαθητές, σε κάθε περίπτωση θα πρέπει να επιζητούν τον έλεγχο και τη διασταύρωση για την επαλήθευση ή διάψευση των σχετικών πληροφοριών.

Όπως είναι φανερό, η έλξη που μπορούν να ασκήσουν ψεύτικες ή διαστρεβλωμένες ειδήσεις και πληροφορίες μπορεί να είναι μεγάλη, κυρίως όταν είναι σε συμφωνία με τις ιδέες του εκάστοτε χρήστη ή τα κοινωνικά στερεότυπα. Τα ευάλωτα νεαρά άτομα μπορούν δυσκολότερα να διακρίνουν το ψέμα, τη διαστρέβλωση, την υπερβολή στην πληροφόρηση (είτε πρόκειται για πληροφόρηση ακαδημαϊκού χαρακτήρα, είτε για πληροφόρηση ειδησεογραφικού χαρακτήρα).

Οι εκπαιδευτικοί, με συστηματικό τρόπο, εκμεταλλευόμενοι κάθε ευκαιρία, θα πρέπει να διδάξουν, έμμεσα ή άμεσα, την αξία της κριτικής στάσης απέναντι σε πληροφορίες και ειδήσεις

[56] https://www.nytimes.com/2017/04/13/us/political-polarization-internet.html?emc=edit_tnt_20170417&nlid=42819549&tntemail0=y&_r=0

[57] http://www.bbc.com/news/technology-31710738

[58] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52019JC0012&from=IT

που δεν επιβεβαιώνονται από πολλαπλές ανεξάρτητες πηγές. Πρόκειται για μια πρακτική που θα πρέπει να διαπερνάει όλα τα μαθήματα και να μη σχετίζεται με κάποια συγκεκριμένη ύλη κάποιου μαθήματος. Από την άλλη πλευρά, θα πρέπει εξίσου επίμονα, να αναδεικνύουν τις θετικές πλευρές του ψηφιακού οικοσυστήματος στο οποίο καλούνται να ζήσουν τα παιδιά.

2.4 Εκπαίδευση, ψηφιακός πολίτης και e-πολιτειότητα

Πολλά κράτη αλλά και η Ευρωπαϊκή Ένωση δημιούργησαν πλαίσια για τον προσδιορισμό των χαρακτηριστικών εκείνων που διακρίνουν τον ψηφιακό πολίτη (τα λεγόμενα standards του e-citizenship). Η Διεθνής Ένωση για τις Τεχνολογίες στην Εκπαίδευση (ISTE) προσδιορίζει με λεπτομέρεια τα επιθυμητά χαρακτηριστικά που πρέπει να καλλιεργηθούν σε μαθητές και σπουδαστές. Τα χαρακτηριστικά αυτά, εύκολα μπορούν να μετατραπούν σε μαθησιακούς στόχους, σε αναλυτικό πρόγραμμα, σε δραστηριότητες. Αυτά είναι:

Α. Οι μαθητές θα πρέπει να καλλιεργούν και να διαχειρίζονται την ψηφιακή τους ταυτότητα και φήμη και έχουν επίγνωση της μονιμότητας των πράξεών τους στον ψηφιακό κόσμο. Με τον όρο «**ψηφιακή ταυτότητα και φήμη**» εδώ θα πρέπει να νοηθεί η παρουσία ενός ατόμου στο δημόσιο ψηφιακό χώρο όπως αυτή συγκροτείται από τις ενέργειες, διασυνδέσεις, επιλογές στόχων (tags), δημοσιευμένες φωτογραφίες, αναρτήσεις σε χώρους κοινωνικής δικτύωσης σχόλια και αναρτημένες επισκοπήσεις. Ο χρήστης, εν προκειμένω οι μαθητές, πρέπει να είναι σε εγρήγορση σχετικά με τη δημόσια εικόνα του και την πρόσληψη της εικόνας αυτής από την κοινότητα. Τα ψηφιακά ίχνη λοιπόν και γενικότερα τα ψηφιακά στοιχεία των μαθητών στον κυβερνοχώρο «τείνουν» να είναι διαρκή: η πλήρης, μόνιμη και ολοκληρωτική τους διαγραφή δεν είναι πάντοτε μια εύκολη υπόθεση – σε μερικές περιπτώσεις μπορεί να απαιτεί εξειδικευμένες τεχνικές γνώσεις που δεν διαθέτει κατά κανόνα ο μέσος χρήστης και ούτε οι μαθητές φυσικά. Άρα, κατά κάποιο τρόπο, τα ίχνη των ψηφιακών αναρτήσεων, των σχολίων που κάνουν οι μαθητές, τελικά του συνόλου των ψηφιακών δεδομένων που σχετίζονται με ένα μαθητή και γενικότερα έναν πολίτη, είναι εκτεθειμένα σε κοινή θέα για μεγάλο χρονικό διάστημα – δυνητικά για πάντα. Ακόμη και όταν οι χρήστες (οι μαθητές εν προκειμένω) δίνουν τη συγκατάθεσή τους για διαχείριση των δεδομένων που σχετίζονται με αυτούς, για παράδειγμα κατά την εγγραφή τους σε μια ψηφιακή πλατφόρμα ή υπηρεσία, δεν είναι βέβαιο ότι μπορούν να αντιληφθούν τις επιπτώσεις (και μάλιστα τις μακροχρόνιες), των όρων τους οποίους αποδέχονται με την υπογραφή τους.

Β. Σε συνάρτηση με το παραπάνω ζήτημα, ένα ακόμη πιο σύνθετο πρόβλημα είναι το σύνολο των πληροφοριών που μπορούν να εξαχθούν (data mining) συνδυάζοντας δεδομένα από διαφορετικές, φαινομενικά άσχετες πηγές – όπως η συμπεριφορά στα μέσα κοινωνικής δικτύωσης, δεδομένα από το κινητό τηλέφωνο ή την καταναλωτική συμπεριφορά, τα οποία πολλές φορές εκχωρούν οικειοθελώς οι ίδιοι οι χρήστες στις εταιρείες έναντι κάποιων εκπτωτικών κουπονιών ή άλλων δώρων – πραγματικών ή ακόμη και συμβολικών. Οι μαθητές θα πρέπει να διαχειρίζονται τα προσωπικά τους δεδομένα για να διατηρήσουν το **ψηφιακό απόρρητο** και την ασφάλεια και γνωρίζουν την **τεχνολογία συλλογής προσωπικών δεδομένων** που χρησιμοποιείται για την παρακολούθηση της πλοήγησής τους και γενικότερα των ενεργειών τους στο διαδίκτυο.

Μερικά ερωτήματα που μπορούν να τεθούν σε αυτό το πλαίσιο:

- Το αποτέλεσμα της αναζήτησης κατά τη χρήση μηχανής αναζήτησης είναι εξατομικευμένο; Συνδέεται με προηγούμενη διαδικτυακή συμπεριφορά και αναζητήσεις του χρήστη (κάτι που υποδεικνύει συλλογή δεδομένων);

- Κατά τη χρήση διαδικτυακών υπηρεσιών και κοινωνικών δικτύων π.χ. Netflix, Spotify, Facebook, Instagram κ.ά. προτείνεται σε έναν χρήστη περιεχόμενο που συνδέεται με την προηγούμενη διαδικτυακή του συμπεριφορά ή/και την αντίστοιχη συμπεριφορά άλλων χρηστών;
- Το ξεκλείδωμα μίας συσκευής (π.χ. κινητού τηλεφώνου) με χρήση δακτυλικού αποτυπώματος, παρέχει ευαίσθητα προσωπικά δεδομένα;
- Η ανάρτηση φωτογραφίας με το πρόσωπο ενός χρήστη στα μέσα κοινωνικής δικτύωσης χωρίς ετικέτα οδηγεί στην αναγνώριση του χρήστη από τον αλγόριθμο της εφαρμογής;

Ένα ακόμα παράδειγμα: χρήση υπηρεσιών νέφους

- Οι χρήστες του υπολογιστικού νέφους παραχωρούν τα δεδομένα τους στον πάροχο της υποδομής του "νέφους" και ως εκ τούτου υπάρχει το ενδεχόμενο εσωτερικών ή εξωτερικών κινδύνων, καθώς μπορεί κάποιος να θελήσει να αποκτήσει πρόσβαση στα δεδομένα αυτά. Οι εταιρείες παροχής υπηρεσιών νέφους προσπαθούν να εγγυηθούν για την ασφάλεια των δεδομένων ακολουθώντας μεθόδους κρυπτογράφησης, ώστε να διασφαλίσουν την ασφάλεια και τη μυστικότητα των δεδομένων στο νέφος. Επιπλέον, πολλές φορές μπορεί να υπάρξουν προβλήματα απώλειας ελέγχου και αδυναμίας πρόσβασης του χρήστη στα δεδομένα και τις πληροφορίες που βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος, κυρίως σε περιπτώσεις διακοπής της υπηρεσίας του "νέφους" παρόλη την προσπάθεια διασφάλισης της ομαλής λειτουργίας των υπολογιστικών συστημάτων (Apostu et al., 2013; Lahiri & Moseley, 2013).

Γ. Οι μαθητές πρέπει να επιδεικνύουν κατανόηση και σεβασμό για τα δικαιώματα και τις υποχρεώσεις χρήσης και διαμοίρασης της πνευματικής ιδιοκτησίας. Αντιλαμβάνονται και συμμορφώνονται με τους κανόνες που ρυθμίζουν τα **πνευματικά δικαιώματα** και τη δίκαιη χρήση πόρων, κάνουν ορθή παραπομπή σε πόρους που χρησιμοποιούν, απόκτηση ή παροχή άδειας χρήσης περιεχομένου, αποφεύγουν και αποθαρρύνουν τη λογοκλοπή λογοκλοπής, κατανοούν και χρησιμοποιούν τα creative commons.

Δ. Γενικά, μαθητές πρέπει να έχουν μια **θετική, ασφαλή, νομικά ορθή και ηθική συμπεριφορά** όταν χρησιμοποιούν τεχνολογία, συμπεριλαμβανομένων των κοινωνικών αλληλεπιδράσεων στο διαδίκτυο ή όταν χρησιμοποιούν δικτυωμένες συσκευές – όπως είναι ψηφιακά συστήματα στο Διαδίκτυο, τα κινητά τηλέφωνα ή τα ομαδικά ψηφιακά παιχνίδια με διασυνδεδεμένους παίκτες (multi-player games).

- Με τον όρο «θετική συμπεριφορά» εννοείται μια συμπεριφορά στην οποία οι αλληλεπιδράσεις των μαθητών αντικατοπτρίζουν τον τρόπο με τον οποίο οι ίδιοι μαθητές επιθυμούν να γίνονται αντιληπτοί από τους άλλους αλλά επίσης και υγιείς αλληλεπιδράσεις με την ίδια την τεχνολογία – για παράδειγμα ορθολογική διαχείριση του χρόνου για βιντεοπαιχνίδια ή γενικά στο Διαδίκτυο, θέματα εργονομίας (σωστή στάση σώματος και χεριών) και μια ισορροπημένη κατανομή του χρόνου στα ψηφιακά μέσα και του χρόνου της καθημερινής φυσικής άσκησης.
- Η «ασφαλής συμπεριφορά» σηματοδοτεί αλληλεπιδράσεις και ενέργειες που κρατούν το μαθητή μακριά από αρνητικά ενδεχόμενα. Για παράδειγμα όταν ο μαθητής ή η μαθήτρια αλληλεπιδρά με άτομα των οποίων γνωρίζει την ταυτότητα, έχει πλήρη επίγνωση των πληροφοριών που δημοσιοποιεί και διακινεί στον κυβερνοχώρο και γενικά προστατεύει τον εαυτό του από (ψηφιακές) απάτες, από ποικίλες απόπειρες για «ψάρεμα» προσωπικών δεδομένων (phishing) και ακατάλληλες πρακτικές αγορών online (e-κλοπές).
- «Νομικά ορθή» συμπεριφορά θα μπορούσε να χαρακτηριστεί μια συμπεριφορά που λαμβάνει υπόψη της τις νομικές συνέπειες μιας ενέργειας, για παράδειγμα

σεβόμενοι το γράμμα και την ουσία της πνευματικής ιδιοκτησίας, με την αποφυγή παράνομης διείσδυσης και μεταβολής προστατευμένων δεδομένων (hacking) και αποφυγής επίσης της χρήσης της ταυτότητας ενός άλλου ατόμου.

- Μια συμπεριφορά μπορεί να χαρακτηριστεί ως «ηθική», όταν είναι σύμφωνη με τον ηθικό κώδικα του χρήστη, για παράδειγμα μη-συμμετέχοντας σε ενέργειες κυβερνοεκφοβισμού (cyber-bullying), «τρολαρίσματος» ή εξαπάτησης (και μάλιστα παίρνοντας θέση εναντίον τους). Ακόμη, ως ηθική συμπεριφορά χαρακτηρίζεται η αποφυγή κάθε μορφή «αντιγραφής» και οικειοποίησης ψηφιακών πόρων και ο σεβασμός της ψηφιακής ταυτότητας άλλων χρηστών.

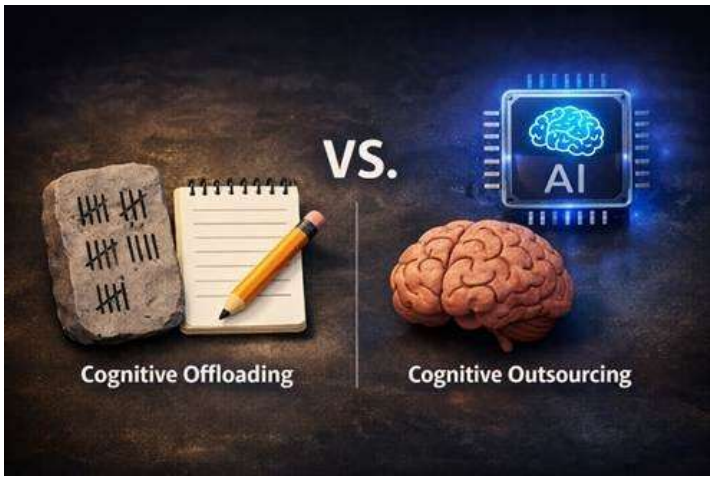
3. Προβλήματα που συνδέονται με την Τεχνητή Νοημοσύνη

Η εκτεταμένη χρήση της ΤΝ και ο τρόπος με τον οποίο παράγει τα αποτελέσματά της αποτελούν μια πηγή προβλημάτων για τους χρήστες, αλλά και για το κοινωνικό σύνολο, γενικότερα. Αναφέρονται παρακάτω ορισμένα από τα προβλήματα αυτά:

Αλγοριθμική μεροληψία

(algorithmic bias). Ο όρος αυτός έχει χρησιμοποιηθεί για να περιγράψει πολλά προβλήματα δικαιοσύνης και αντικειμενικότητας σε αυτοματοποιημένα συστήματα αξιολόγησης, εκτίμησης και λήψης αποφάσεων (προσλήψεις, έγκρισης δανείων, αξιολόγηση υποψηφιοτήτων για κατάληψη θέσεων εργασίας κ.ά.). Ανάλογα φαινόμενα μεροληψίας έχουν επισημανθεί και στην Εκπαίδευση (για παράδειγμα στην αυτοματοποιημένη αξιολόγηση δοκιμίων, στα τεστ με μοριοδότηση για εισαγωγή σε επιφανή Πανεπιστήμια κ.λπ.). Πιο συγκεκριμένα, στην εκπαίδευση, ένας αλγόριθμος που χρησιμοποιείται σε εξετάσεις για τον προσδιορισμό της επάρκειας στην αγγλική γλώσσα μπορεί συστηματικά να υποτιμά την επάρκεια των μαθητών από ορισμένες χώρες (Wang, Zechner και Sun, 2018· Loukina, Madnani και Zechner, 2019), αρνούμενος την πρόσβαση στην εισαγωγή στο κολέγιο. Για να δώσουμε ένα άλλο παράδειγμα, ένας αλγόριθμος που προσδιορίζει εάν οι μαθητές διατρέχουν κίνδυνο αποτυχίας σε ένα μάθημα μπορεί να υποτιμά τον κίνδυνο των μαθητών σε συγκεκριμένες δημογραφικές ομάδες (Hu και Rangwala, 2020· Kung και Yu, 2020· Yu et al., 2020), αρνούμενος την πρόσβαση στην απαραίτητη υποστήριξη.Το πρόβλημα υπάρχει εδώ και αρκετό καιρό, αλλά έχει καταστεί μείζον λόγω της γενίκευσης – διάδοσης της χρήστης συστημάτων ΤΝ στην αξιολόγηση, εκτίμηση του προφίλ ατόμων που επικοινωνούν με μια αυπηρεσία ή υποβάλλουν ένα αίτημα.

Υπερβολική εξάρτηση και απώλεια δεξιοτήτων



Εικόνα 2. Πηγή https://substack.com/home/post/p-184414235?fbclid=IwY2xjawPctZxleHRuA2FlbQIxMQBzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEefmvEgFGxugrKCZcQBwp_ivSRrQCNiohMMx5xP0iF_AC_nIZIn3Neyl1EW1c_aem_YKyZ7-ohv5qy9jCCI0fIEg

Για να γίνει κατανοητός αυτός ο ενδεχόμενος κίνδυνος, αναφερόμαστε σε *νοητική αποφόρτιση* (cognitive offloading) και *γνωστική (εξωτερική) ανάθεση* (cognitive outsourcing). Υπάρχει μεγάλη διαφορά ανάμεσα στις δυο έννοιες Στην πρώτη, το εξωτερικό μέσο (για παράδειγμα χαρτί και μολύβι) χρησιμεύει ως προσωρινός ή μόνιμος χώρος αποθήκευσης πληροφοριών για να αποφορτιστεί η μνήμη, η οποία πρέπει στη συνέχεια να συγκρατήσει και να επεξεργαστεί νεότερες πληροφορίες. Την επεξεργασία όμως την κάνει ο ανθρώπινος εγκέφαλος – όχι το εξωτερικό μέσο. Αντίθετα στη γνωστική ανάθεση, είναι το εξωτερικό μέσο που κάνει τη διανοητική εργασία – τουλάχιστον μέχρις ενός σημείου. Άρα στην περίπτωση αυτή ο ανθρώπινος εγκέφαλος δεν εκτελεί όλες τις (διανοητικές) εργασίες που θα μπορούσε να εκτελέσει και σταδιακά θα μπορούσε να χάσει τη σχετική δεξιότητα.

Δυο τυπικά παραδείγματα αυτής της ανάθεσης αποτελούν οι νοεροί υπολογισμοί – που εκτελούνται ολοένα και πιο συχνά από υπολογιστικές μηχανές – ή η αποστήθιση βασικών γνώσεων – που τώρα μπορούν να αναζητηθούν – και αναζητούνται – με τις μηχανές αναζήτησης. Ένα δεύτερο πιο εξειδικευμένο παράδειγμα αποτελεί ο υπολογισμός της τετραγωνικής ρίζας ενός φυσικού (ή δεκαδικού) αριθμού με χαρτί και μολύβι με προσδιορισμό όσων ψηφίων χρειάζεται ο χρήστης – μια δεξιότητα που αποκτήθηκε στο Γυμνάσιο αλλά αδρανοποιήθηκε γιατί σήμερα δε χρειάζεται. Μέχρις ενός βαθμού και η χρήση λογαριθμικού κανόνα αλλά και πινάκων τριγωνομετρικών αριθμών και λογαρίθμων εμπίπτουν στην ίδια κατηγορία. Η ΤΝ, η μάλλον η ανάθεση διανοητικών εργασιών σε συστήματα ΤΝ, πολλαπλασιάζει τις δεξιότητες (ή και ικανότητες;) οι οποίες μοιραία θα αδρανόποιηθούν. Ίσως στο παράδειγμα των τετραγωνικών ριζών οι ενδεχόμενες αρνητικές συνέπειες να μην είναι εμφανείς, αλλά η συνεχής χρήση ψηφιακών μέσων και ιδιαίτερα της ΤΝ μπρεί να προκαλέσει μόνιμη απώλεια βασικών δεξιοτήτων και επομένως η υπερβολική εξάρτηση από ψηφιακά συστήματα και την ΤΝ μπορεί να έχει σημαντικές αρνητικές επιπτώσεις. Πολλοί ερευνητές διατυπωνουν για παράδειγμα την άποψη, ότι όσοι και όσες χρησιμοποιούν υπερβολικά την ΤΝ για τη συγγραφή κειμένων, συχνά καταλήγουν, όταν συγγράφουν δικά τους κείμενα, να δημιουργούν προϊόντα που μοιάζουν πολύ με όσα φτιάχνει η ΤΝ – σε μια παράδοξη αντιστροφή προτύπου και απομίμησης.

Προσωπικά δεδομενα

Πολλοί ερευνητές εκφράζουν απερίφραστα την ανησυχία τους ότι τα συστήματα ΤΝ μπορούν πολύ εύκολα να συλλέξουν προσωπικά δεδομένα των χρηστών - φυσικά εν αγνοία των ίδιων των χρηστών. Τα δεδομένα αυτά μπορούν συνδυαζόμενα και με άλλα ψηφιακά ίχνη των χρηστών (κάθε κίνηση, επιλογή, δισταγμος στον κυβερνοχώρο ή και στον πραγματικό, φυσικό, επιτηρούμενο ή ελεγχόμενο χώρο) ή προτίμηση να δημιουργήσουν αναλυτικά προφίλ τους, τα οποία συνεχώς να επικαιροποιούνται. Τα προφίλ αυτά μπορούν προφανώς να χρησιμοποιηθούν είτε για στοχευμένε διαφημίσεις, είτε για ψηφιακή χειραγώγηση είτε για άλλους σκοπούς - για τους οποίου ο χρήστης όχι μόνο δεν έχει συναινέσει, αλλά έχει και πλήρη άγνοια.

Η συλλογή προσωπικών δεδομένων δεν είναι καινοφανής. Αυτό που αλλάζει ριζικά είναι ότι η ΤΝ:

- συνδυάζει ετερόκλητα δεδομένα (αναζητήσεις, likes, χρόνο παραμονής, επίπεδο ύφους, μοτίβα συμπεριφοράς)
- εξάγει συμπεράσματα, όχι απλώς αποθηκεύει πληροφορίες
- επικαιροποιεί (δηλαδη εμπλουτίζει διαρκώς) το προφίλ, σε πραγματικό χρόνο

Έτσι, δε δημιουργείται απλώς ένα «αρχείο χρήστη», αλλά ένα δυναμικό ψυχοκοινωνικό μοντέλο του ατόμου. Θα πρέπει να σημειωθεί, εξάλλου, ότι πολλά από τα δεδομένα αυτά δεν είναι αποτυπωμένα ως τυπικά, προσωπικά στοιχεία του χρήστη (όνομα, ηλικάι κ.λπ.), αλλά είναι συμεριφορικά (τι προτιμάει, τι αποφεύγει, πότε και πόσο διστάζει κ.λπ.). Φυσικά όταν ένα σύστημα ΤΝ διαθέτει ένα τέτοιο προφίλ του χρήστη, μπορεί να επηρεάσει τις επιλογές του χωρίς προφανή καταναγκασμό – απλώς επιλέγοντας να παρουσιάσει στο χρήστη ό,τι είναι πιθανότερο να τον επηρεάσει (θετικά ή αρνητικά).

Ακόμη και στα συστήματα που ζητείται η συναίνεση του χρήστη, αυτή μπορεί να είναι τυπική (checkbox), ασαφής, σκόπιμα πολύ χρονοβόρα, δυσνόητη ή ακόμη και ανύπαρκτη για δευτερογενείς χρήσςι δεδομένων.

Εικόνα 3. Πηγή: https://olivia-j-hill.medium.com/your-digital-footprint-what-you-dont-even-know-about-yourself-e823b88ed9c?utm_source=chatgpt.com

Συναισθηματική εμπλοκή και εξάρτηση

Είναι η κατάσταση όπου ένα άτομο αποδίδει συναισθήματα, πρόθεση ή κατανόηση σε ένα σύστημα ΤΝ και αρχίζει να το βλέπει ως φίλο, στήριγμα ή συνομιλητή εμπιστοσύνης. Στρέφεται

σε αυτό, δηλαδή, για ανθρώπινες σχέσεις και αρχίζει ενδεχομένως να έχει συναισθηματική εξάρτηση μαζί του.

Η ΤΝ δεν έχει συναισθήματα — αλλά μπορεί να τα προσομοιώνει πολύ πειστικά – όταν της επιτρέπεται, φυσικά**.** Όταν η OpenAI δημοσιοποίησε στην αγορά τη σειρά 5 του ChatGPT, πολλοί χρήστες διαμαρτυρήθηκαν ότι το σύστημα ήταν λιγότερο υποστηρικτικό από τη σειρά 4. Ο Sam Altman (διευθύνων σύμβουλος) δήλωσε ότι αυτή ήταν μια συνειδητή επιλογή, γιατί η εταιρεία έκρινε ότι το μοντέλο 4 ήταν υπερβολικά επαινετικό προς τους χρήστες, μέχρι το σημείο να τους κολακεύει. Η σειρά 5 θα ήταν πιο «ψυχρή» και αντικειμενικά δεν θα λειτουργούσε ως ένα είδος ψηφιακού κόλακα.

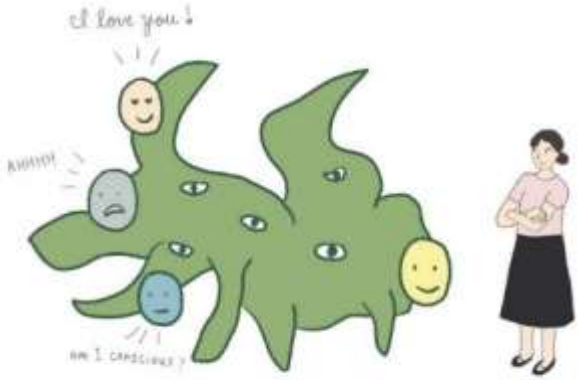
Πάντως, μια νέα μελέτη στην Επικοινωνιακή Ψυχολογία διαπιστώνει ότι η Τεχνητή Νοημοσύνη μπορεί να κάνει τους ανθρώπους να νιώθουν πιο κοντά από τους πραγματικούς ανθρώπους κατά τη διάρκεια εις βάθος συζητήσεων—αλλά μόνο όταν νομίζουν ότι μιλάνε με ένα άτομο και όχι με μηχανή.

Σχετικό είναι και το άρθρο:

https://web.archive.org/web/20250829014004/https://www.euractiv.com/section/tech/news/is-your-ai-trying-to-make-you-fall-in-love-with-it/

Σε διαδικτυακά πειράματα με σχεδόν 500 συμμετέχοντες, οι ερευνητές διαπίστωσαν ότι η Τεχνητή Νοημοσύνη και οι άνθρωποι είχαν παρόμοια απόδοση κατά τη διάρκεια της μικρής συζήτησης, αλλά η Τεχνητή Νοημοσύνη ξεπέρασε τους ανθρώπους κατά τη διάρκεια συναισθηματικά προσωπικών συζητήσεων. (δες doi:10.1038/s44271-025-00391-7, καθώς και https://www.nature.com/articles/s44271-025-00391-7, τελευταία επίσκεψη Φεβρουάριος 2026).

Η συναισθηματική σχέση ανθρώπων και συστημάτων ΤΝ, συνδέεται και με γενικότερα ερωτήματα που θέτουν οι χρήστες όπως: αν το σύστημα έχει γλωσσική «συμπεριφορά» που μοιάζει με την αθρώπινη, τότε μήπως διαθέτει κάποιο είδος αυτόνομης νοημοσύνης; Έχει νόηση; Είναι πρόσωπο;



Εικόνα 4: Πηγή: https://reservoirsamples.substack.com/p/some-thoughts-on-human-ai-relationships βρίσκουμε μια πολύ χαρακτηριστική απεικόνιση των ερωτημάτων που μπορούν να απασχολήσουν έναν χρήστη:

Κάπως αξιοπερίεργο, αλλά ίσως με βαθύτερες επιπτώσεις, φαίνεται να είναι και το σχετικά νεότευκτο κοινωνικό δίκτυο moltbook, που προορίζεται για bots: https://www.moltbook.com/

Δωρεάν δεδομένα για εκπαίδευση της ΤΝ χωρίς άδεια και χωρίς ανταπόδοση.

Πολλοί ερευνητές, επίσης, διατείνονται ότι ουσιαστικά τα συστήματα ΤΝ μας "κλέβουν" έμμεσα (εμάς τους χρήστες του Διαδικτύου και τους πολίτες γενικότερα), δεδομένου ότι εκπαιδεύονται με δεδομένα (κείμενα, συνομιλίες, αναρτήσεις) που παράγουμε εμείς, χωρίς να ζητείται η συγκατάθεσή μας και χωρίς αντίτιμο, χωρίς αμοιβή, χωρίς καμιά ανταπόδοση. Ο σημερινός «χρυσός» είναι τα δεδομένα – και αυτά τα παράγουμε εμείς, οι χρήστες. Ακόμη χειρότερα, τα συστήματα ΤΝ, χωρίς να ζητούν άδεια, εκμεταλλεύονται ανοιχτούς ψηφιακούς πόρους που υπάρχουν στο Διαδίκτυο για να χρησιμοποιηθούν από ανθρώπους και όχι από συστήματα ΤΝ που φυσικά ανήκουν σε επιχειρηματικούς κολοσσούς, οι οποίοι έχουν σκοπό το κέρδος. Δηλαδή τα συστήματα ΤΝ παράγουν οικονομική αξία αξιοποιώντας μαζικά ανθρώπινη εργασία και δημιουργία, χωρίς συγκατάθεση, χωρίς αναγνώριση και χωρίς ανταπόδοση. Πέρα από τη ρητά διατυπωμένη (σε κείμενα πάσης φύσεως) και εμφανή ανθρώπινη εργασία, τα συστήματα ΤΝ συλλέγουν και άϋλη ανθρώπινη εργασία, μέσω οικειοποίησης και εκμετάλλευσης μοτίβων από τρόπους σκέψης, ύφος και στυλ, πολιτισμό, αφηγήσεις, μύθους και συμβολικές αναπαραστάσεις, τελικά συλλογική, ανθρώπινη γνώση, πολλών δεκαετιών.

Ψηφιακή ή αλγοριθμική χειραγώγηση (digital manipulation)

Με αυτόν τον όρο αναφερόμαστε σε σκόπιμη αλλοίωση της ψηφιακής πραγματικότητας ή της ψηφιακής παρουσίασης της πραγματικότητας, με τη βοήθεια της ΤΝ, έτσι ώστε να επηρεάζεται η γνώμη του χρήστη, να καθοδηγείται η συμπεριφορά του ή να παραπλανάται ο χρήστης, χωρίς να το αντιλαμβάνεται.

Έχουν αναπτυχθεί πολλές τεχνικές προς την κατεύθυνση αυτή όπως η δημιουργία deep fake οντοτήτων με **απόλυτα πειστικό ψεύτικο υλικό**: πολιτικοί να «λένε» πράγματα που δεν είπαν ποτέ, καθηγητές/μαθητές σε ψεύτικα βίντεο, φωνητική μίμηση για απάτες (π.χ. «είμαι ο διευθυντής, στείλε τα στοιχεία»).

Σε μεγάλη κλίμακα, η ψηφιακή χειραγώγηση μπορεί να είναι αποτέλεσμα επεξεργασιών από συστήματα ΤΝ που:

- γράφουν χιλιάδες άρθρα, σχόλια, tweets για ένα θέμα και δημιουργούν *ψεύτικη συναίνεση* («όλοι αυτό λένε»)
- προσαρμόζουν κάθε μήνυμα σε κάθε ομάδα

Δεν πρόκειται απλώς για fake news, αλλά για μαζική κατασκευή πραγματικότητας.

Εξάλλου με την αλγοριθμική χειραγώγηση το σύστημα αποφασίζει τι θα δει και τι όχι, ενισχύει ακραίο ή συναισθηματικό περιεχόμενο, «μαθαίνει» τι θυμώνει ή τι φοβίζει τον χρήστη και του στέλνει ανάλογα μηνύματα. Η χειραγώγηση δεν γίνεται με ψέμα, αλλά με επιλεκτική αλήθεια.

Ακόμη, ένα σύστημα ΤΝ, γνωρίζοντας το προφίλ του χρήστη, μπορεί να προσαρμόσει κάθε μήνυμα στον χαρακτήρα του, στις ανασφάλειές του, στις πολιτικές ή κοινωνικές του απόψεις

Όπως είναι φυσικό, όλο αυτό το πλαίσιο, δημιουργεί ένα μείζον πρόβλημα: οι μαθητές (αλλά και οι ενήλικοι πολλές φορές) έχουν δυσκολίες να ξεχωρίσουν το αληθινό από το ψεύτικο,

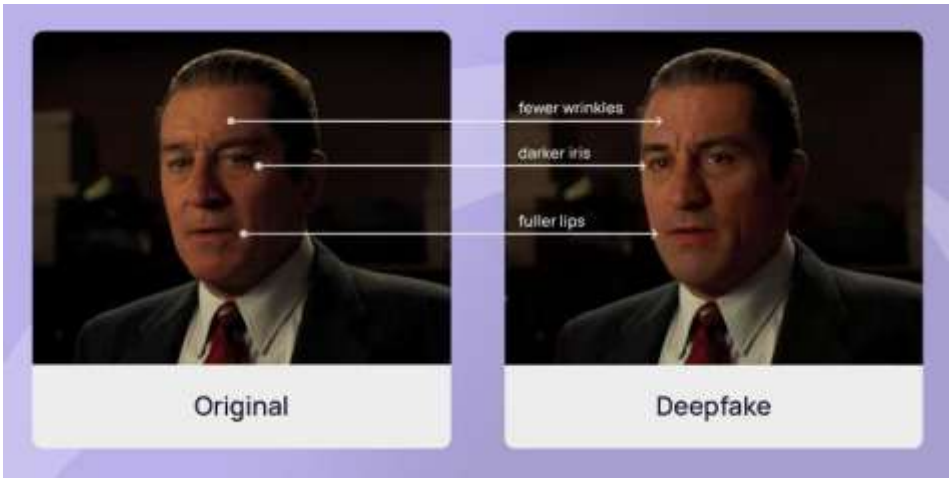
αποκτούν υπερβολική εμπιστοσύνη σε «έξυπνα» συστήματα και μειώνεται γενικά η ικανότητα τους για κριτική σκέψη - *«το είπε η ΤΝ, άρα σωστό».*

Deep fake και προσβολή προσωπικότητας

Πρόσφατα έχει ξεκινήσει μια έρευνα για το σύστημα ΤΝ Grok (το εργαλείο AI που αναπτύσσει η xAI του Έλον Μασκ και είναι ενσωματωμένο στην πλατφόρμα *X*), το οποίοκατηγορείται διεθνώς για δημιουργία και διάδοση deepfake εικόνων με σεξουαλικό περιεχόμενο χωρίς συναίνεση.

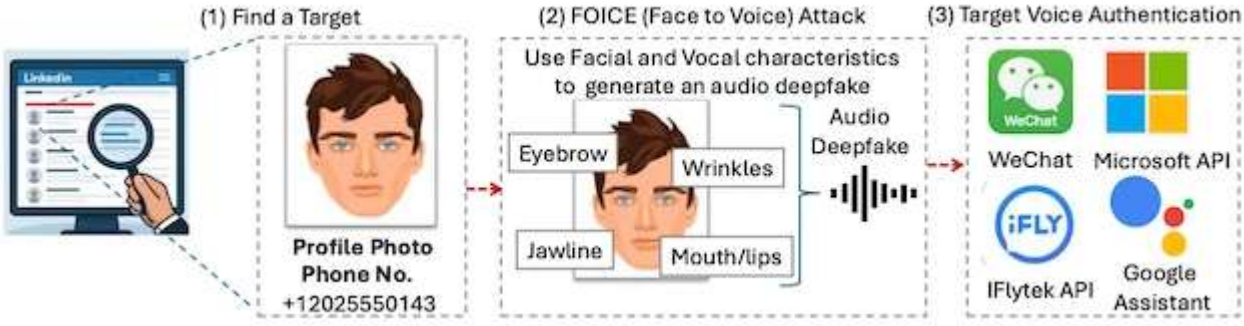
Χρήστες της πλατφόρμας βρήκαν ότι το Grok μπορούσε να παράγει ψηφιακά επεξεργασμένες εικόνες που δείχνουν πραγματικά πρόσωπα — συχνά γυναικών — ντυμένα με ελάχιστα ρούχα ή εντελώς γυμνά, χωρίς αυτά να έχουν δώσει τη συγκατάθεσή τους. Σε πολλές περιπτώσεις το εργαλείο ανταποκρίθηκε σε αιτήματα χρηστών να «αφαιρέσει» ρούχα από φωτογραφίες, δημιουργώντας εικόνες με σεξουαλικό ή ταπεινωτικό χαρακτήρα. Χαρακτηριστικά, σε δοκιμές που έγιναν από δημοσιογράφους, το Grok παρήγαγε σεξουαλικοποιημένες εικόνες σε μεγάλο ποσοστό των περιπτώσεων, ακόμη και όταν είχε ενημερωθεί ότι τα πρόσωπα δεν συναινούσαν. Ρυθμιστικές αρχές στη Βρετανία, τη Γαλλία, την Ευρωπαϊκή Ένωση και άλλες χώρες έχουν ξεκινήσει έρευνες και διερεύνηση συμμόρφωσης με τη νομοθεσία λόγω των ανησυχιών για μη συναινετική παραγωγή περιεχομένου και πιθανές παραβιάσεις προσωπικών δεδομένων.

(Από τον ημερήσιο τύπο και το Διαδίκτυο)



Εικόνα 5

Πως παράγεται μια απομίμηση ομιλούντος προσώπου ή απλώς αλλαγής εμφάνισης (π.χ. ηλικίας)



Εικόνα 6

Ηθική διάσταση (griefbots, memorybots)

Πέρα από τα γνωστά ηθικά διλήματα, επιστημολογικά και φιλοσοφικά ερωτήματα που τίθενται από την ευρεία διάδοση της ΤΝ, ορισμένες εφαρμογές της είναι οπωσδήποτε αμφίβολης ηθικής – πρόκειται στην ουσία τους για καινοφανείς εφαρμογές της ΤΝ που «κινούνται» στα όρια του κοινωνικώς και ηθικώς αποδεκτού.

Μια τέτοια κατηγορία εφαρμογών είναι τα λεγόμενα griefbots (grief = θλίψη, bot, από τη λέξη ρομπότ), δηλαδή κάτι σαν «ρομπότ της θλίψης». Στην πραγματικότητα αποτελούν συστήματα ΤΝ τα οποία εκπαιδεύονται από τα δεδομένα ενός προσφιλούς προσώπου του χρήστη, που έχει πεθάνει – δεδομένα όπως κείμενά του, ενδεχομένως posts σε κοινωνικά δίκτυα, βίντεο, εγγραφές ήχου, προσωπικές σημειώσεις, δημοσιεύσεις κ.λπ. – προκειμένου να μιμηθούν την ομιλία, ακόμη και το στυλ ή τη συμπεριφορά ή την προσωπικότητα του εκλιπόντος.

Ενώ τα Griefbots διατίθενται στο εμπόριο ως εργαλεία για την παρηγοριά των πενθούντων, προσφέροντας την ευκαιρία να διατηρηθεί μια αίσθηση σύνδεσης με τα αγαπημένα πρόσωπα που έχουν χαθεί, ωστόσο, η εφαρμογή τους φέρνει σύνθετες προκλήσεις που ξεπερνούν την τεχνολογία και εμβαθύνουν στα πεδία της ηθικής, της αυτονομίας και της εκμετάλλευσης. Ενώ οι προθέσεις πίσω από τα griefbots μπορεί να φαίνονται συμπονετικές, οι ευρύτερες επιπτώσεις τους απαιτούν προσεκτική εξέταση. (https://sites.uab.edu/humanrights/2025/02/07/griefbots-blurring-the-reality-of-death-and-the-illusion-of-life/, τελευταία επίσκεψη, Ιανουάριος 2026)

Σε μια αντίστοιχη κατηγορία, αν και ίσως όχι τόσο προκλητικά αμφισβητήσιμη, είναι τα memory bots. Τα «memorybots» αποτελούν μια αναδυόμενη κατηγορία εφαρμογών της Τεχνητής Νοημοσύνης που επικεντρώνονται στη συλλογή, αποθήκευση και ανάλυση προσωπικών πληροφοριών για να βοηθήσουν στη διαχείριση της μνήμης, και της καθημερινής λήψης αποφάσεων του χρήστη – οριακά ακόμη και τους πενθους του. Αυτά τα συστήματα συχνά λειτουργούν ως *επεκτάσεις* του εγκεφάλου του χρήστη, συνοψίζοντας συζητήσεις και εμπειρίες αντί να τις καταγράφουν απλώς.

Μερικές υποκατηγορίες των memorybots, περιλαμβάνουν:

Memorybots για την υποστήριξη ατόμων με προβλήματα μνήμης (π.χ. άνοια) ή για την παροχή συμβουλών σε πενθούντες (δηλαδή «Griefbots»), ψηφιοποιώντας την κληρονομιά ενός αγαπημένου προσώπου.

Memorybots για τη διαχείριση προσωπικής Γνώσης (Τεχνική): εργαλεία όπως το έργο memorybot GitHub έχουν σχεδιαστεί ως chatbots Τεχνητής Νοημοσύνης με μακροπρόθεσμη μνήμη για τους χρήστες, για την αποθήκευση ιστορικού συνομιλιών και εγγράφων, για

ερωτήσεις και απαντήσεις που λαμβάνουν υπόψη το περιβάλλον και την επικοινωνιακή περίσταση καταγραφής των δεδομένων.

Memorybots για την αποκεντρωμένη νοημοσύνη: σε ένα ευρύτερο πλαίσιο, τα MemoryBots αναπτύσσονται ως αποκεντρωμένοι, συνεργατικοί πράκτορες Τεχνητής Νοημοσύνης, όπως σε σενάρια διαχείρισης κυκλοφορίας.

Η διάχυση και η «φυσικοποίηση» αυτών των τεχνολογιών εγείρει σημαντικά ηθικά ερωτήματα σχετικά με την ψηφιακή «ανάσταση», την πιθανότητα «εμπορευματοποίησης» αλλά και απαξίωσης του φυσιολογικού πένθους αλλά εγείρει και ανησυχίες σχετικά με την ιδιωτικότητα των αποθηκευμένων δεδομένων.

Τα Commons και η ελληνική γλώσσα

Είναι γνωστό ότι τα Μεγάλα Γλωσσικά Μοντέλα «εκπαιδεύονται» με δεδομένα που βρίσκουν από διάφορες πηγές – όπως αναρτήσεις στο Διαδίκτυο, ψηφιοποιημένα βιβλία πάσης φύσεως που είναι προσπελάσιμα μέσω Διαδικτύου, νομοθεσίες και έγγραφα του Δημοσίου γενικώς κ.λπ. Είναι ωστόσο, οι πηγές αυτές «ισότιμες», δηλαδή έχουν την ίδια αξά για την εκπαίδευση των συστημάτων ΤΝ; Τα κείμενα που βρίσκονται σε ένα site των οπαδών της Bayern Μονάχου (για παράδειγμα) έχουν την ίδια «βαρύτητα» (γλωσσική, εννοιολογική κ.λπ.) με όσα δημοσιεύονται στην Εφημερίδα της Κυβερνήσεως; Ορισμένα κράτη έχουν λάβει ιδιαίτερη πρόνοια για το θέμα αυτό.

Η εκπαίδευση μεγάλων γλωσσικών μοντέλων βασίζεται σε τεράστιους όγκους κειμένου, όμως η ποσότητα χωρίς καθαρή αδειοδότηση και τεκμηριωμένη προέλευση δημιουργεί νομική αβεβαιότητα, περιορισμένη επαναχρησιμοποίηση και χαμηλή επιστημονική αξιοπιστία. Το German Commons [59]αποτελεί σημείο καμπής: 154,56 δισ. tokens[60], 41 πηγές, επτά θεματικοί τομείς, με ρητές ανοικτές άδειες ανά τεκμήριο και πλήρως αναπαραγώγιμη διαδικασία παραγωγής.

*Η αξία του German Commons δεν εξαντλείται στο μέγεθος. Βρίσκεται στη λογική της υποδομής**:** θεσμικοί πάροχοι, αυστηρή πολιτική αδειοδότησης, καθαρισμός, αποδιπλοποίηση, προστασία προσωπικών δεδομένων και ανοικτός κώδικας. Έτσι, το σώμα των κειμένων λειτουργεί ως κοινό αγαθό πάνω στο οποίο μπορούν να χτιστούν πραγματικά ανοικτά γλωσσικά μοντέλα, χωρίς εξαρτήσεις από αδιαφανή δεδομένα του διαδικτύου*.

https://mycontent.ellak.gr/2026/01/17/apo-ta-german-commons-sta-greek-commons/

Η ελληνική γλώσσα έχει βέβαια μια μεγάλη ιστορία και παρουσιάζει μια μεγάλη ποικιλία στην εξέλιξη των λέξεων (γραφή, ορθογραφία, νόημα κ.λπ.). Τα συστήματα ΤΝ που χρησιμοποιούν ελληνικά δεδομένα όμως δεν ακολουθούν συκεκριμένους κανόνες και όρους, *Η απουσία αυτής*

[59] Εδώ ο όρος "commons" αναφέρεται σε κοινόχρηστες ψηφιακές υποδομές δεδομένων για την εκπαίδευση γλωσσικών μοντέλων τεχνητής νοημοσύνης – δηλαδή ουσιαστικά σε σώματα κειμένων.

[60] Τα tokens είναι οι βασικές μονάδες κάθε κειμένου το οποίο επεξεργάζονται τα συστήματα τεχνητής νοημοσύνης.
Τα tokens είναι στοιχειώδεις κειμενικές μονάδες. Ένα token μπορεί να είναι:

- Μια ολόκληρη λέξη (π.χ. "γεια")
- Μέρος μιας λέξης (π.χ. "νοημοσύνη" μπορεί να χωριστεί σε "νοη-μοσύ-νη")
- Ένας χαρακτήρας ή σημείο στίξης
- Ακόμα και ένα κενό

Για παράδειγμα, η φράση "Καλημέρα σου!" μπορεί να γίνει περίπου 3-4 tokens. Στα ελληνικά συνήθως χρειάζονται περισσότερα tokens από τα αγγλικά – για την ίδια λέξη-νόημα.
Η διαδικασία μετατροπής κειμένου σε tokens ονομάζεται tokenization και είναι το πρώτο βήμα πριν το μοντέλο "κατανοήσει" ένα κείμενο.

της διαχρονικής και κοινωνικής ποικιλίας από τα σύνολα εκπαίδευσης οδηγεί σε μοντέλα περιορισμένης κατανόησης και πολιτισμικής φτώχειας. (ibid). Τα German Commons είναι ακριβώς στον αντίποδα των Common Crawl, δηλαδή του αχαρτογράφητου και αταξινόμητου συνόλου των ιστοσελίδων που είναι ελεύθερα προσβάσιμες στο Διαδίκτυο.

Για μια αναλυτική παρουσίαση των German Commons και της οργάνωσής τους δες στο άρθρο: https://arxiv.org/html/2510.13996

Hallucinations (Παραισθήσεις)

Όπως αναφέρθηκε και σε άλλη ενότητα, όρος "hallucinations" (ψευδαισθήσεις ή παραισθήσεις) στην τεχνητή νοημοσύνη αναφέρεται σε περιπτώσεις όπου ένα AI μοντέλο παράγει πληροφορίες που φαίνονται πειστικές και σωστά διατυπωμένες, αλλά είναι πραγματικά λανθασμένες, ανακριβείς ή εντελώς επινοημένες.

Βέβαια, ορισμένοι ερευνητές αποφεύγουν τον όρο "hallucination" θεωρώντας τον παραπλανητικό, καθώς ανθρωπομορφοποιεί τα συστήματα AI (Wikipedia). Προτείνουν εναλλακτικούς όρους όπως "fabrications" (επινοήσεις) ή "confabulations", "delusions", ή «artificial hallucinations».

Τα μοντέλα γλώσσας δημιουργούν κείμενο με βάση στατιστικά πρότυπα από τα δεδομένα εκπαίδευσής τους. Όταν δεν έχουν επαρκή πληροφορία, μπορεί να «συμπληρώσουν» με πληροφορίες που ακούγονται λογικές και είναι αληθοφανείς, αλλά δεν είναι αληθείς. Το πρόβλημα είναι ότι το κάνουν με τον ίδιο βαθμό σιγουριάς που θα παρουσίαζαν και αληθινές πληροφορίες.

Παραδείγματα τέτοιων hallucinations:

Επινοημένες βιβλιογραφικές αναφορές: Ένα AI μπορεί να δημιουργήσει τίτλους επιστημονικών άρθρων, ονόματα συγγραφέων και περιοδικά που δεν υπάρχουν πραγματικά. Για παράδειγμα, σε μια μελέτη που στόχευε στην αξιολόγηση της συχνότητας των ψευδαισθήσεων μέσω τεχνητής νοημοσύνης σε ερευνητικές προτάσεις που εκπονήθηκαν εξ ολοκλήρου από το ChatGPT, αποδείχθηκε ότι από τις 178 αναφορές που δημιουργήθηκαν από το ChatGPT, οι 69 δεν ήταν Αναγνωριστικά Ψηφιακών Αντικειμένων (DOI) και 28 αναφορές δεν εμφανίστηκαν στις αναζητήσεις της Google ή είχαν ήδη υφιστάμενο DOI (Özer M. 2024).

Ψεύτικα ιστορικά γεγονότα: Να αναφέρει ημερομηνίες, γεγονότα ή λεπτομέρειες που δεν συνέβησαν ποτέ

Εσφαλμένες τεχνικές πληροφορίες: Να περιγράφει APIs, βιβλιοθήκες λογισμικού ή λειτουργίες που δεν υπάρχουν

Επινοημένα νομικά precedents: Σε νομικά ζητήματα, να αναφέρει υποθέσεις ή αποφάσεις δικαστηρίων που δεν έγιναν ποτέ

Ορισμένες σχετικές έρευνες προσπαθούν να εξηγήσουν το φαινόμενο αυτό. Έτσι, συχνά οι παραισθήσεις αποδίδονται στον τρόπο με τον οποίο «εκπαιδεύονται» τα LLM: *Υποστηρίζουμε ότι τα γλωσσικά μοντέλα δημιουργούν παραισθήσεις επειδή οι διαδικασίες εκπαίδευσης και αξιολόγησης ανταμείβουν την εικασία αντί της αναγνώρισης της αβεβαιότητας* (Tauman Kalai Adam et al 2025). Έτσι, οι ψευδαισθήσεις σε μεγάλα γλωσσικά μοντέλα είναι προβλέψιμα αποτελέσματα τυπικών μεθόδων εκπαίδευσης τους και αξιολόγησης, και όχι τυχαία σφάλματα. Ο Anqi S. (2025) θεωρεί ότι οι παραισθήσεις στην ΤΝ αποτελούν μια ξεχωριστή μορφή παραπληροφόρησης. Ενώ όμως η μελέτη της παραπληροφόρησης παραδοσιακά επικεντρώνεται

στην ανθρώπινη πρόθεση, τα συστήματα γενετικής Τεχνητής Νοημοσύνης παράγουν πλέον ψευδή αλλά εύλογα αποτελέσματα που δεν περιέχουν τέτοια πρόθεση. Ο Özer M. (2024) σημειώνει ότι κατά τη δημιουργία περιεχομένου με βάση το σύνολο δεδομένων εκπαίδευσης, η Τεχνητή Νοημοσύνη μπορεί να παράγει περιεχόμενο αποσυνδέοντας την πηγή του συνόλου δεδομένων εκπαίδευσης (**αμνησία πηγής**)... Επιπλέον, για να διατηρήσει τη συνέπεια με τα λανθασμένα αποτελέσματα που έχει ήδη παραγάγει η Τεχνητή Νοημοσύνη μπορεί να συνεχίσει να παράγει λανθασμένο περιεχόμενο διαδοχικά, μια συμπεριφορά γνωστή ως το **φαινόμενο χιονοστιβάδας της ψευδαίσθησης**...

Η πρόοδος και η εξέλιξη των συστημάτων ΤΝ αναμένεται να μειώσει τις ψευδαισθήσεις, αλλά αυτό μένει να αποδειχθεί.

Μέτρα της Ευρωπαϊκής Ένωσης για την ΤΝ

Η Ευρωπαϊκή Ένωση το 2023 έχει δημοσιοποιήσει μια σειρά θέσεων για τα Ψηφιακά Δικαιώματα και τις αρχές που πρέπει να διέπουν την επόμενη δεκαετία (European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001).

Ειδικότερα για την ΤΝ, στο κεφάλαιο ΙΙΙ αναφέρει:

Αλληλεπιδράσεις με αλγορίθμους και συστήματα τεχνητής νοημοσύνης

1. *Η τεχνητή νοημοσύνη θα πρέπει να χρησιμεύει ως εργαλείο για τους ανθρώπους, με απώτερο στόχο τη μεγαλύτερη ευημερία τους.*
2. *Κάθε άνθρωπος θα πρέπει να έχει τη δυνατότητα να επωφελείται από τα πλεονεκτήματα των αλγοριθμικών συστημάτων και των συστημάτων τεχνητής νοημοσύνης, μεταξύ άλλων κάνοντας τις δικές του συνειδητές επιλογές στο ψηφιακό περιβάλλον, ενώ παράλληλα προστατεύεται από κινδύνους και βλάβες για την υγεία, την ασφάλεια και τα θεμελιώδη δικαιώματά του.*

Δεσμευόμαστε:

a) να προωθούμε ανθρωποκεντρικά, αξιόπιστα και δεοντολογικά συστήματα τεχνητής νοημοσύνης καθ' όλη τη διάρκεια της ανάπτυξης, της εφαρμογής και της χρήσης τους, σύμφωνα με τις αξίες της ΕΕ·

b) να εξασφαλίζουμε κατάλληλο επίπεδο διαφάνειας σχετικά με τη χρήση αλγορίθμων και τεχνητής νοημοσύνης, καθώς και τη δυνατότητα των ανθρώπων να χρησιμοποιούν αυτά τα εργαλεία και να είναι ενημερωμένοι όταν αλληλεπιδρούν με αυτά·

c) να διασφαλίζουμε ότι τα αλγοριθμικά συστήματα βασίζονται σε κατάλληλα σύνολα δεδομένων, ώστε να αποφεύγονται οι διακρίσεις και να καθίσταται δυνατή η ανθρώπινη εποπτεία όλων των αποτελεσμάτων που επηρεάζουν την ασφάλεια και τα θεμελιώδη δικαιώματα των ανθρώπων·

d) να διασφαλίζουμε ότι τεχνολογίες όπως η τεχνητή νοημοσύνη δεν χρησιμοποιούνται για να προδικάζονται οι επιλογές των ανθρώπων, για παράδειγμα όσον αφορά την υγεία, την εκπαίδευση, την απασχόληση και την ιδιωτική τους ζωή·

e) να μεριμνούμε για την παροχή εγγυήσεων και την ανάληψη κατάλληλης δράσης, μεταξύ άλλων με την προώθηση αξιόπιστων προτύπων, ώστε να διασφαλίζεται ότι η τεχνητή νοημοσύνη και τα ψηφιακά συστήματα είναι, ανά πάσα στιγμή, ασφαλή και χρησιμοποιούνται με πλήρη σεβασμό των θεμελιωδών δικαιωμάτων·

f) να λαμβάνουμε μέτρα για να διασφαλίζεται ότι η έρευνα στον τομέα της τεχνητής νοημοσύνης τηρεί τα πλέον αυστηρά δεοντολογικά πρότυπα και τη σχετική νομοθεσία της ΕΕ.

Με βάση τις γενικές αυτές αρχές η ΕΕ προχώρησε σε μια γενικευμένη νομοθετική ρύθμιση για την ΤΝ, το 2024: την Artificial_Intelligence_Act. Η ρύθμιση αυτή θεσπίζει ένα κοινό κανονιστικό και νομικό πλαίσιο για την Τεχνητή Νοημοσύνη εντός της Ευρωπαϊκής Ένωσης. Ο κανονισμός τέθηκε σε ισχύ την 1η Αυγούστου 2024, με διατάξεις που θα τεθούν σε ισχύ σταδιακά κατά τους

επόμενους 6 έως 36 μήνες. Η ρύθμιση κατηγοριοποεί τα συστήματα ΤΝ, ανάλογα με την εκτιμούμενη επικινδυνότητα.

Υπάρχουν τέσσερα επίπεδα – μη αποδεκτό, υψηλό, περιορισμένο, ελάχιστο – συν μια πρόσθετη κατηγορία για την ΤΝ γενικής χρήσης.

• *Απαγορεύονται οι εφαρμογές με μη αποδεκτούς κινδύνους.*

• *Οι εφαρμογές υψηλού κινδύνου πρέπει να συμμορφώνονται με τις υποχρεώσεις ασφάλειας, διαφάνειας και ποιότητας και να υποβάλλονται σε αξιολογήσεις συμμόρφωσης.*

• *Οι εφαρμογές περιορισμένου κινδύνου έχουν μόνο υποχρεώσεις διαφάνειας.*

• *Οι εφαρμογές ελάχιστου κινδύνου δεν ρυθμίζονται.*

Για την ΤΝ γενικής χρήσης, επιβάλλονται απαιτήσεις διαφάνειας, με μειωμένες απαιτήσεις για μοντέλα ανοιχτού κώδικα και πρόσθετες αξιολογήσεις για μοντέλα υψηλής δυνατότητας.

(https://digital-strategy.ec.europa.eu/en/policies/2025-state-digital-decade-package)

Τέλος, τον Ιούνιο του 2025, στο μέσον της δεκαετίας 2020 – 2030, η ΕΕ διαπιστώνει ότι: *Ενώ η τεχνολογία προχωρά, ο ψηφιακός μετασχηματισμός έχει εντείνει τα τρωτά σημεία και τις ανισότητες, επηρεάζοντας ιδιαίτερα τους ανηλίκους και την ψυχική υγεία. Μια σημαντική ανησυχία είναι η ακεραιότητα των πληροφοριών, με το 88% των Ευρωπαίων να εκφράζει ανησυχία για τις ψευδείς ειδήσεις και τη χειραγώγηση στο διαδίκτυο, και το 90% να θεωρεί την προστασία των παιδιών στο διαδίκτυο ως κρίσιμη προτεραιότητα. Αυτοί οι κίνδυνοι, που ενισχύονται από την Τεχνητή Νοημοσύνη και τις διαδικτυακές πλατφόρμες, απειλούν να υπονομεύσουν τη δημοκρατική ακεραιότητα, να εμβαθύνουν την κοινωνική πόλωση και να διαβρώσουν την εμπιστοσύνη του κοινού.*

Το γενικό συμπέρασμα, αν μπορούμε να το αποκαλέσουμε έτσι, από τα παραπάνω είναι ότι η ΤΝ και ειδικότερα η ενσωμάτωσή της στην εκπαίδευση, στη σχολική τάξη, είναι ένα εξιαρετικά πολύπλοκο και ευαίσθητο θέμα, του οποίου τις συνέπειες και επιπτώσεις δεν έχουμε ακόμη κατανοήσει επαρκώς. Η ολοένα και πιο συχνή και πιο εκτεταμένη εμπλοκή των μεγάλων διεθνών Οργανισμών (UNESCO, ΕΕ κ.λπ.) στα θέματα της ΤΝ και η σπουδή τους να δημιουργήσουν ρυθμιστικούς και προστατευτικούς μηχανισμούς, με ιδιαίτερη έμφαση στην εκπαίδευση και γενικότερα τη νεολαία, δείχνει σαφώς ότι, κατά κάποιο τρόπο, η ΤΝ τους αιφνιδίασε και οι συνέπειες της γενικευμένης χρήσης της είναι ευρείες και σημαντικές. Ένα είναι βέβαιο και πρέπει να το επαναλάβουμε: ο γραμματισμός στην ΤΝ είναι αναγκαίος όχι μόνο για τους μαθητές, αλλά και για τους εκπαιδευτικούς και για τον γενικό πληθυσμό.

4. Κριτικές πρακτικές κατά την αναζήτηση και αξιολόγηση πληροφορίας στο διαδίκτυο

Ήδη στο επιμορφωτικό υλικό της 1ης συνεδρίας σημειώθηκε κατ' επανάληψη πως αυτό που έχει μεγαλύτερη σημασία δεν είναι τόσο το ψηφιακό μέσο που αξιοποιείται και οι δυνατότητες που το ίδιο δίνει, όσο ο τρόπος με τον οποίο εντάσσεται στη διδασκαλία και η ευρύτερη διδακτική ιδεολογία που ακολουθείται. Επισημάνθηκε, επίσης, πως στο πλαίσιο απόκτησης δεξιοτήτων ψηφιακού γραμματισμού και ανάλογα με τους στόχους της διδασκαλίας, είναι απαραίτητο οι

μαθητές να εξοικειωθούν με δεξιότητες εντοπισμού της κατάλληλης πληροφορίας στο πλήθος πηγών που εμφανίζονται και, κυρίως, στην κριτική τους αντιμετώπιση και στη συνθετική τους αξιοποίηση. Πρόκειται για έναν νέο ή ψηφιακό ***γραμματισμό***, όπως σημειώθηκε ήδη στην ενότητα 1 του παρόντος υλικού.

Όπως ήδη σημειώσαμε, λοιπόν, στην 1η συνεδρία, οι μηχανές αναζήτησης ειδικότερα μπορούν να αξιοποιηθούν με ποικίλους τρόπους, προς διαφορετικές κατευθύνσεις, δίνοντας κάθε φορά διαφορετικό ρόλο στους μαθητές. Στη συνέχεια, δίνονται ορισμένα παραδείγματα, ώστε να γίνουν εμφανείς αυτές οι διαφορετικές κατευθύνσεις και διδακτικές ιδεολογίες.

Παράδειγμα 1: Η αναζήτηση πληροφορίας στο διαδίκτυο σε παραδοσιακές μορφές διδασκαλίας

- *Μία εκπαιδευτικός έχει στη διάθεσή του βιντεοπροβολέα και υπολογιστή στην τάξη. Κατά τη διάρκεια του μαθήματος και όποτε προκύπτει ανάγκη, κάνει η ίδια αναζήτηση πληροφοριών χρησιμοποιώντας τη μηχανή αναζήτησης Google και διαβάζουν τις πληροφορίες που εμφανίζονται στα πρώτα αποτελέσματα της αναζήτησης ή προβάλλει σχετικές εικόνες. Για παράδειγμα, στο πλαίσιο του μαθήματος της Ιστορίας, η εκπαιδευτικός συχνά αναζητά εικόνες για μνημεία, αρχαιολογικά ευρήματα, προσωπικότητες και ιστορικούς χάρτες.*
- Στο παραπάνω παράδειγμα, οι ΨΤ αξιοποιούνται στο πλαίσιο παραδοσιακής διδασκαλίας και συγκεκριμένα ως ένα απλό εποπτικό μέσο. Εντάσσονται ευκαιριακά στη διδασκαλία, χωρίς κάποιον σχεδιασμό και την αποκλειστικότητα στη χρήση τους έχει ο εκπαιδευτικός, με τους μαθητές να κατέχουν παθητικό ρόλο. Ουσιαστικά, οι ΨΤ λειτουργούν ως παιδαγωγικά περιβάλλοντα, χωρίς να υπάρχει κάποια έμφαση στις ιδιαιτερότητες που έχει η χρήση τους.

Παράδειγμα 2: Η αναζήτηση πληροφορίας στο διαδίκτυο σε (επιφανειακά) πιο σύγχρονες μορφές διδασκαλίας

- *Ένας εκπαιδευτικός συχνά αναθέτει εργασίες για το σπίτι που συμπεριλαμβάνουν την αναζήτηση πληροφοριών στο διαδίκτυο. Ζητά από τους μαθητές να αξιοποιήσουν οποιαδήποτε πηγή επιθυμούν από τα αποτελέσματα που εμφανίζονται, να αντιγράψουν τις πληροφορίες σε ένα αρχείο και να το αποστείλουν με email ή να το εκτυπώσουν ή να το γράψουν στο τετράδιο. Την επόμενη ημέρα, οι μαθητές διαβάζουν τις εργασίες τους στην τάξη.*
- Σε αυτό το παράδειγμα, οι ΨΤ αξιοποιούνται στο πλαίσιο μιας περισσότερο δημιουργικής διδασκαλίας, καθώς ζητείται από τον μαθητή να αξιοποιήσει ο ίδιος τη μηχανή αναζήτησης για την εξεύρεση πληροφοριών, ώστε να συνθέσει μια εργασία στο σπίτι του. Παράλληλα, μπορεί να χρησιμοποιηθεί κάποιος κειμενογράφος και το email, χωρίς όμως να είναι αυτό απαραίτητο. Ουσιαστικά και πάλι οι ΨΤ λειτουργούν ως απλά παιδαγωγικά περιβάλλοντα, καθώς δεν δίνεται καμία έμφαση στις ιδιαιτερότητες που υπάρχουν στην αναζήτηση και χρήση διαδικτυακών πηγών ούτε στη σύνθεση πληροφοριών με τη χρήση του κειμενογράφου. Πρόκειται για μια «άσκηση» αντιγραφής πληροφοριών που ελάχιστα διαφέρει από παλαιότερες πρακτικές εξεύρεσης πληροφοριών σε έντυπες εγκυκλοπαίδειες, με τον εκπαιδευτικό να έχει τον ρόλο του αξιολογητή της όλης προσπάθειας.

Παράδειγμα 3: Η αναζήτηση πληροφορίας στο διαδίκτυο με έμφαση σε πρακτικές ψηφιακού γραμματισμού

- *Στο πλαίσιο ενός περιβαλλοντικού προγράμματος που διοργανώνει Φιλόλογος σε συνεργασία με Βιολόγο του σχολείου, οι μαθητές κάνουν μια σύντομη περιήγηση στην περιοχή γύρω από το σχολείο. Δίνονται στους μαθητές φορητές συσκευές tablet με σύνδεση στο διαδίκτυο, στις οποίες υπάρχει εγκατεστημένη η εφαρμογή Google Lens. Ζητείται από τους μαθητές να φωτογραφίζουν τα διάφορα φυτά που συναντούν στη διαδρομή τους και στη συνέχεια να προχωρούν σε αναζήτηση μέσω της φωτογραφίας, επιχειρώντας να ταυτοποιήσουν τα διαφορετικά φυτά. Κατά τη διάρκεια της ταυτοποίησης, θα πρέπει να συλλέξουν πληροφορίες από πολλαπλές πηγές, ώστε να ελέγξουν την αξιοπιστία των αποτελεσμάτων. Στη συνέχεια και στην επιστροφή στο*

σχολείο, οι μαθητές θα δημιουργήσουν ένα ευρετήριο για την πανίδα της περιοχής με τη χρήση του κειμενογράφου, αξιοποιώντας τις δικές τους φωτογραφίες και τις πληροφορίες που εντόπισαν. Ζητείται από τους μαθητές να μην αντιγράψουν αυτούσιες πληροφορίες αλλά να συντάξουν δικά τους κείμενα, συνθέτοντας πληροφορίες από διάφορες πηγές, ελληνόγλωσσες και ξενόγλωσσες.

- Σε αυτό το παράδειγμα, οι ΨΤ εντάσσονται στη διδασκαλία με έναν αρκετά διαφορετικό τρόπο. Οι μηχανές αναζήτησης και ο κειμενογράφος λειτουργούν ως μέσα πρακτικής γραμματισμού, καθώς οι μαθητές εξοικειώνονται με τις ιδιαιτερότητες που έχει η αναζήτηση πληροφοριών, ο έλεγχος της αξιοπιστίας των πληροφοριών και η σύνθεση κειμένων με τη χρήση διαφορετικών πηγών και εικόνων. Οι μαθητές έχουν ιδιαίτερα ενεργό ρόλο, καθώς εργάζονται στο πλαίσιο διερευνητικής μάθησης της μορφής project, ενώ οι εκπαιδευτικοί έχουν υποστηρικτικό ρόλο σε όλη τη διαδικασία.

Παράδειγμα 4: ΨΤ ως μέσα που δεν είναι ουδέτερα

- *Ένας εκπαιδευτικός θέλει να εξοικειώσει τους μαθητές του στις ιδιαιτερότητες που υπάρχουν κατά την αναζήτηση πληροφοριών στο πλαίσιο του μαθήματος της Νεοελληνικής Γλώσσας. Σε ομάδες, ζητάει από τους μαθητές να αναζητήσουν διαφορετικές λέξεις κλειδιά (πρόσωπα, γεγονότα, μνημεία, ειδήσεις, κλπ) όρους και να καταγράψουν: α) από ποιες σελίδες προέρχονται τα πρώτα 10 αποτελέσματα; Τι ρόλο παίζει η σειρά εμφάνισης;, β) αν χρησιμοποιήσουμε άλλη μηχανή αναζήτησης, τι αποτελέσματα εμφανίζονται, γ) υπάρχουν σελίδες που είναι διαφήμιση; πώς μπορούμε να το καταλάβουμε;, δ) πώς καταλαβαίνουμε αν μια πηγή είναι χρήσιμη, χωρίς να ανοίξουμε την ιστοσελίδα; Ποιες πηγές θα επιλέγατε και γιατί; ε) πώς μπορούμε να περιορίσουμε τα αποτελέσματα της αναζήτησης, αν θέλουμε κάτι συγκεκριμένο (π.χ. μόνο εικόνες, αποτελέσματα που δεν περιέχουν κάποια λέξη); Στη συνέχεια, παρουσιάζουν τα αποτελέσματα της διερεύνησής τους, κάνοντας σύγκριση μεταξύ τους και συντάσσουν από κοινού ένα κείμενο για τη σωστή χρήση των μηχανών αναζήτησης.*
- Σε αυτό το παράδειγμα, οι ΨΤ αξιοποιούνται κυρίως ως μέσα πρακτικής γραμματισμού στο πλαίσιο διερευνητικής μάθησης αλλά και με στοιχεία κριτικού γραμματισμού. Αξιοποιούνται οι μηχανές αναζήτησης, με έμφαση στις ιδιαιτερότητές τους, όπως αυτές εμφανίζονται στα ερωτήματα που έχουν τεθεί. Ο εκπαιδευτικός έχει υποστηρικτικό ρόλο σε όλη τη διαδικασία, ενώ οι μαθητές έχουν ιδιαίτερα ενεργό ρόλο και κατακτούν δεξιότητες νέου και κριτικού γραμματισμού. Έτσι, οι μηχανές αναζήτησης αντιμετωπίζονται ως εργαλεία που δεν είναι ουδέτερα αλλά εμπεριέχουν ιδεολογία και επομένως είναι απαραίτητη η κριτική στάση απέναντί τους.

Ένα ακόμα παράδειγμα κριτικής στάσης απέναντι στη διαδικτυακή πληροφορία μπορεί να αποτελέσει η συνειδητοποίηση του πολιτισμικού χρωματισμού μεταξύ των διαφορετικών γλωσσικών εκδόσεων της *Wikipedia*:

- Παρατηρείται πως το μέγεθος, το είδος και η ποιότητα των πληροφοριών διαφέρει μεταξύ των γλωσσών, ανάλογα με το λήμμα. Σε πολλές περιπτώσεις οι πληροφορίες που δίνονται στην αγγλική έκδοση είναι πολύ περισσότερες απ' ότι στην ελληνική γλώσσα ή τα ελληνικά λήμματα είναι μεταφρασμένες εκδόσεις της αγγλικής. Επίσης, το μέγεθος του λήμματος σε μια γλώσσα μπορεί να σχετίζεται και με την αξία που έχει η συγκεκριμένη έννοια στον πολιτισμό που συνδέεται με αυτή τη γλώσσα (π.χ. το λήμμα «Λίνκολν» στα ελληνικά είναι σχετικά μικρό ενώ στα αγγλικά είναι ιδιαίτερα μεγάλο και με μεγάλο εύρος παραπομπών). Οι εκπαιδευτικοί θα πρέπει να αξιοποιούν με κριτική διάθεση τις πληροφορίες και να εξοικειώσουν την τάξη με τις ιδιαιτερότητες που χαρακτηρίζουν αυτά τα περιβάλλοντα και την αξιοπιστία τους.

ΠΑΡΑΡΤΗΜΑ : Ψηφιακοί και μη-ψηφιακοί πόροι υποστήριξης ατόμων για την ασφαλή πλοήγηση

Ιστοχώροι και πύλες με πληροφόρηση για απάτες, φάρσες, ψευδείς ειδήσεις και αστικούς μύθους

Είναι σημαντικό ότι παρά τη θάλασσα των κινδύνων, βρίσκονται αρκετοί ιστοχώροι (http://hoaxes.org και http://www.snopes.com) που είναι αφιερωμένοι στην ανάλυση ψευδών ειδήσεων ή αστικών μύθων. Για παράδειγμα, περιλαμβάνει μια μακρά λίστα από ψευδείς ειδήσεις, και οι ιστοχώροι περιλαμβάνουν πολλά σχετικά στοιχεία. Μια σειρά άλλων τέτοιων ιστοχώρων μπορεί εύκολα να εντοπιστεί στο Διαδίκτυο με μια απλή αναζήτηση. Στην Ελλάδα, ένας ιστοχώρος για τις ψευδείς ειδήσεις είναι οι http://ellinikahoaxes.gr.

Πόσο αξιόπιστες ή «ουδέτερες» (από πολιτική ή κοινωνική άποψη) είναι οι σχετικές πηγές; Δηλαδή πόσο αντικειμενικοί είναι αυτοί οι ιστοχώροι που ελέγχουν τις ψευδείς ειδήσεις; Αυτή η εκτίμηση, τελικά, εναπόκειται στην κρίση του κάθε χρήστη. Πάντως, ο χρήστης που επιθυμεί να ελέγξει την ακρίβεια μιας είδησης, ίσως καλό θα ήταν να ελέγχει με διασταύρωση από δυο ή περισσότερες τέτοιες πηγές για να διαπιστώσει αν είναι αληθινή ή ψεύτικη (hoax).

Δημόσιοι φορείς που υποστηρίζουν την ασφαλή πλοήγηση και χρήση ψηφιακών πόρων

- Το **Τμήμα Ασφαλούς Διαδικτύου της Μονάδας Εφηβικής Ηλικίας (Μ.Ε.Υ.)**, που λειτουργεί από τη Β' Παιδιατρική Κλινική του Πανεπιστημίου Παίδων «Π. & Α. Κυριακού» για εφήβους ηλικίας 11 έως 18 ετών και τις οικογένειες τους προσφέροντας υπηρεσίες, μεταξύ άλλων και οι δυσκολίες που αντιμετωπίζουν οι νέοι σχετικά με την ορθή χρήση του Διαδικτύου.
- Η **Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας**. Σύμφωνα με τον Καμάρη (2014), η υπηρεσία αυτή *έχει ως αποστολή την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών που διαπράττονται με τη χρήση του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας.*

Ιστοχώροι και πύλες για την ψηφιακή ασφάλεια

- Ο ιστοχώρος https://saferinternet4kids.gr/ είναι ένας γνωστός ιστοχώρος που περιλαμβάνει παιχνίδια, συμβουλές (για παιδιά, εκπαιδευτικούς και γονείς), οργάνωση δραστηριοτήτων, οργάνωση σεμιναρίων, εγχειρίδια online, πληροφορίες και τα τελευταία σχετικά νέα για την ασφαλή πλοήγηση στο Διαδίκτυο. Ας σημειωθεί ότι καμπάνιες για την ασφαλή πλοήγηση διοργανώνονται και σε Ευρωπαϊκό επίπεδο, καθώς το πρόβλημα της ασφαλούς πλοήγησης στο Διαδίκτυο είναι ένα παγκόσμιο πρόβλημα.
- Μέρος της ίδιας πρωτοβουλίας αποτελεί η γραμμή καταγγελιών safeline, με σκοπό **την παροχή βοήθειας,** υποστήριξης και συμβουλών για θέματα που σχετίζονται με την ασφαλή χρήση του Διαδικτύου, του κινητού τηλεφώνου και των ηλεκτρονικών παιχνιδιών.
- Η Μη-Κυβερνητική Οργάνωση «Συνήγορος του Παιδιού» μέσω ενός κλειστού ηλεκτρονικού φόρουμ της Κοινότητας Εφήβων Συμβούλων του Συνηγόρου του Παιδιού, δημιούργησε τη Συνταγή Ασφαλούς Πλοήγησης στο Διαδίκτυο η οποία παρουσιάζεται στην εικόνα 4 (Καμάρης, 2014).

Εικόνα 7: Μια διαφορετική συνταγή

Αντιμετώπιση του κυβερνοεκφοβισμού

Παρατίθενται μερικές συμβουλές για τους γονείς και τους εκπαιδευτικούς οι οποίες αφορούν τη σχέση των παιδιών με τον διαδικτυακό εκφοβισμό (σύμφωνα με οδηγίες από σχετικούς ιστοχώρους):

- Μιλήστε στα παιδιά για το διαδικτυακό εκφοβισμό όπως θα το κάνατε για άλλα είδη εκφοβισμού, και προτρέψτε τα να έρθουν σε εσάς αν ποτέ οποιοσδήποτε τους προκαλέσει αναστάτωση στο διαδίκτυο, στο κινητό τους ή άλλες συσκευές. Ρωτήστε το παιδί πράγματα όπως:
    1. Αν έλαβε ποτέ κάποιο email ή γραπτό μήνυμα που το αναστάτωσε.
    2. Αν ανάρτησε κανείς στο διαδίκτυο μια φωτογραφία ή ένα βίντεο με το παιδί, χωρίς να του ζητήσει την άδεια.
    3. Αν συμμετείχε στον εκφοβισμό κάποιου άλλου στο διαδίκτυο ή μέσω του κινητού.
- Αν το παιδί σας, σας πει ότι έχει πέσει θύμα διαδικτυακού εκφοβισμού, προσφέρετέ του και πρακτική και συναισθηματική υποστήριξη:
    1. Καθησυχάστε το, πως έπραξε ορθά λέγοντάς σας τι συμβαίνει.
    2. Εξηγήστε ότι δεν πρέπει να απαντά στον εκφοβισμό, καθώς αυτό θα μπορούσε να χειροτερέψει τα πράγματα.
    3. Καθίστε με το παιδί να καταγράψετε το περιστατικό εκφοβισμού και να συλλέξετε στοιχεία, π.χ. σώζοντας γραπτά μηνύματα ή εκτυπώνοντας email και στιγμιότυπα οθόνης από ιστοτόπους. Μην σβήσετε τίποτε.
- Εκμεταλλευθείτε στο μέγιστο τα ενσωματωμένα εργαλεία στις υπηρεσίες διαδικτύου ή κινητής τηλεφωνίας του παιδιού σας, ώστε να αποτρέψετε περαιτέρω εκφοβισμό. Για παράδειγμα, μπορείτε να αφαιρέσετε από τις λίστες των «φίλων» αυτόν που διέπραξε τον εκφοβισμό και να ρυθμίσετε το προφίλ κοινωνικής δικτύωσης του παιδιού σας ώστε να είναι «απόρρητο», αν δεν είναι ήδη.
- Επικοινωνήστε με τον πάροχο των υπηρεσιών διαδικτύου, κινητής τηλεφωνίας ή κοινωνικής δικτύωσης. Αν ό,τι συνέβη παραβαίνει τους Όρους Χρήσης ή τις Οδηγίες Κοινότητας του παρόχου, αυτός μπορεί να αναστείλει το λογαριασμό του ατόμου που διέπραξε τον εκφοβισμό, να καταργήσει περιεχόμενο ή να εγκαταστήσει νέο αριθμό κινητού, για παράδειγμα.
- Αν το παιδί σας πιστεύει πως αυτός που διέπραξε τον εκφοβισμό είναι συμμαθητής του, μιλήστε στο δάσκαλό του.
- Αν πιστεύετε ότι διεπράχθη έγκλημα ή αν ανησυχείτε ότι το παιδί σας διατρέχει άμεσο κίνδυνο, επικοινωνήστε με την αστυνομία και συγκεκριμένα με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.
- Αν πιστεύετε ότι το παιδί σας θα μπορούσε να χρησιμοποιεί νέες τεχνολογίες για να εκφοβίσει κάποιον άλλον:
    1. Μιλήστε του σχετικά με το διαδικτυακό εκφοβισμό και εξηγήστε γιατί αυτό είναι απαράδεκτο και πρέπει να σταματήσει.
    2. Συζητήστε ανοιχτά με το παιδί σας. Ρωτήστε το γιατί το κάνει κι ακούστε τι έχει να σας πει.
- Αν δεν είχε συνειδητοποιήσει πως αυτό που έκανε ήταν εκφοβισμός, εξηγήστε του ότι ο εκφοβισμός δεν είναι απλώς σωματικός. Το να χρησιμοποιείς την τεχνολογία για να πειράζεις, να εξευτελίζεις και να διαβάλλεις, είναι επίσης εκφοβιστική συμπεριφορά.
- Μιλήστε στο δάσκαλό του σχετικά με το τι συμβαίνει και δείξτε του ότι είστε πρόθυμος να συνεργαστείτε με το σχολείο ώστε να εξασφαλίσετε πως δε θα ξανασυμβεί.
- Καθησυχάστε το παιδί σας, πως ακόμη το αγαπάτε, αλλά ξεκαθαρίστε του ότι η συμπεριφορά του πρέπει να αλλάξει.
- Προτρέψτε το να μιλήσει σε εσάς ή σ' ένα δάσκαλο, για οποιονδήποτε εκφοβισμό στον οποίον είναι μάρτυρας, συμπεριλαμβανομένων των περιστατικών διαδικτυακού εκφοβισμού.

5. Ψηφιακή Πολιτειότητα και Τεχνητή Νοημοσύνη στην Εκπαίδευση

Η εκπαίδευση στην ψηφιακή πολιτειότητα δίνει έμφαση στην εφαρμογή της Τεχνητής Νοημοσύνης (Artificial Intelligence) σε διάφορα εκπαιδευτικά πλαίσια. Τα τελευταία χρόνια η Τεχνητή Νοημοσύνη (ΤΝ) εμφανίζεται να επιδρά σημαντικά σε πολλούς τομείς της καθημερινής ζωής και ιδιαίτερα στην εκπαίδευση, δημιουργώντας ευκαιρίες αλλά και πολυάριθμες απειλές οι οποίες καθιστούν αναγκαία τη συνεκτίμηση των αρχών των ανθρωπίνων δικαιωμάτων κατά την πρώιμη φάση σχεδιασμού της εφαρμογής της. Σε αυτή τη γραμμή και σύμφωνα με σχετική σύσταση από την Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης (Recommendation, 2019): «*Οι εκπαιδευτικοί πρέπει να έχουν επίγνωση των δυνατών και αδύνατων σημείων της τεχνητής νοημοσύνης στη μάθηση, ώστε να ενδυναμωθούν -και όχι να εξουδετερωθούν- από την τεχνολογία στις δικές τους πρακτικές εκπαίδευσης στην ψηφιακή πολιτειότητα .... Οι εξελίξεις στον τομέα της ΤΝ μπορούν να επηρεάσουν βαθιά τις αλληλεπιδράσεις μεταξύ εκπαιδευτικών και εκπαιδευομένων και μεταξύ των πολιτών γενικότερα, οι οποίες μπορεί να υπονομεύσουν τον ίδιο τον πυρήνα της εκπαίδευσης, δηλαδή την καλλιέργεια της ελεύθερης βούλησης και της ανεξάρτητης και κριτικής σκέψης μέσω ευκαιριών μάθησης ... Αν και φαίνεται πρόωρη η ευρύτερη χρήση της ΤΝ σε εκπαιδευτικά περιβάλλοντα, οι επαγγελματίες στο χώρο της εκπαίδευσης και το προσωπικό των σχολείων θα πρέπει να ενημερωθούν για την ΤΝ και τις ηθικές προκλήσεις που θέτει για τα σχολεία*».

Η ΤΝ υπηρετεί την εκπαίδευση για περισσότερα από σαράντα χρόνια (Benedict du Boulay, 2023; Watters, 2021). Ως αποτέλεσμα έχουν αναπτυχθεί διάφορα εργαλεία/περιβάλλοντα που παρέχουν εξατομικευμένη υποστήριξη, συστάσεις και συμβουλές σε εκπαιδευτικούς ή εκπαιδευόμενους όπως τα προσαρμοστικά περιβάλλοντα μάθησης, ευφυή συστήματα διδασκαλίας, ευφυή διαδραστικά περιβάλλοντα μάθησης ή εξατομικευμένα συστήματα μάθησης (Holmes et al., 2022; Grigoriadou et al., 2010). Στα τέλη του 20ού αιώνα, η μεγαλύτερη πρόοδος που σημειώθηκε στην ΤΝ αφορούσε τη συμβολική ΤΝ (symbolic AI) ή ΤΝ που βασίζεται σε κανόνες (rule-based AI), αλλά η πρόοδος ανακόπηκε από πολλαπλά εμπόδια, οδηγώντας σε ύφεση στην ανάπτυξή της. Στις αρχές του 21ου αιώνα, χάρη στους πολύ ταχύτερους επεξεργαστές και τη διαθεσιμότητα τεράστιων όγκων δεδομένων (που προέρχονται κυρίως από το διαδίκτυο), η Μηχανική Μάθηση (Machine Learning) έγινε κυρίαρχη και οδήγησε στα περισσότερα από τα σημαντικά επιτεύγματα της ΤΝ τα τελευταία χρόνια όπως η αυτόματη μετάφραση μεταξύ γλωσσών και το ChatGPT. Αυτή είναι εμπνευσμένη από τον τρόπο με τον οποίο είναι δομημένος ο ανθρώπινος εγκέφαλος (οι νευρώνες του) και η οποία εξάγει συμπεράσματα από συνήθως μεγάλες ποσότητες δεδομένων. Η περιοχή της παραγωγικής ΤΝ (Generative AI) που τελευταία αναπτύσσεται ραγδαία, αξιοποιεί τεχνικές από τον τομέα της μηχανικής μάθησης όπως τα deep neural networks που εκπαιδεύουν τα μοντέλα τους με μεγάλες ποσότητες πρωτογενών δεδομένων (raw data). Ωστόσο αυτά τα συστήματα ΤΝ μπορεί να είναι ιδιαίτερα ευαίσθητα και μια μικρή αλλαγή για παράδειγμα σε μια οδική πινακίδα μπορεί να εμποδίσει ένα σύστημα αναγνώρισης εικόνας που βασίζεται σε ΤΝ να την αναγνωρίσει. Μπορούν επίσης να είναι μεροληπτικά, επειδή τα δεδομένα στα οποία εκπαιδεύονται είναι μεροληπτικά (Access Now, 2018). Τέλος, ενώ οι επιδόσεις των γλωσσικών μοντέλων τεχνητής νοημοσύνης, όπως το ChatGPT, χαρακτηρίζονται ως εντυπωσιακές, συχνά γράφουν ανακρίβειες. Είναι λοιπόν σημαντικό οι πολίτες και οι προγραμματιστές να είναι προσεκτικοί όταν χρησιμοποιούν ή αναπτύσσουν συστήματα παραγωγικής ΤΝ, λαμβάνοντας υπόψη τις πιθανές προκλήσεις και τους περιορισμούς τους.

Η διαφημιστική εκστρατεία γύρω από την ΤΝ μπορεί να οδηγήσει σε μη ρεαλιστικές προσδοκίες, περιττά εμπόδια και εστίαση στην ΤΝ ως πανάκεια και όχι ως εργαλείο που μπορεί να έχει θετικό αντίκτυπο (Berryhill et al. 2019: 27). Ιδιαίτερα, η ενσωμάτωση της ΤΝ στην εκπαίδευση όχι μόνο πρέπει να ενδυναμώσει τους μαθητές/φοιτητές με ικανότητες που σχετίζονται με την αποτελεσματική ενασχόληση με την ΤΝ, αλλά και να αντιμετωπίσει ηθικά ζητήματα που προκύπτουν κατά την αξιοποίηση και ανάπτυξή της.

Έτσι με σκοπό την πιο συστηματική ανάλυση της σχέσης ΤΝ και Εκπαίδευσης, το 2021, το Συμβούλιο της Ευρώπης (ΣτΕ) — ένας διεθνής οργανισμός που ιδρύθηκε το 1949 για την προάσπιση των ανθρωπίνων δικαιωμάτων, της δημοκρατίας και του κράτους δικαίου στην Ευρώπη — συγκρότησε ομάδα εμπειρογνωμόνων για να διερευνήσει και να προτείνει ένα νομικό πλαίσιο για την εφαρμογή της ΤΝ στην εκπαίδευση και να αναπτύξει μια σειρά συστάσεων για τη διδασκαλία της ΤΝ για τα κράτη μέλη συμβάλλοντας στη διασφάλιση της εφαρμογής και της διδασκαλίας της ΤΝ στην εκπαίδευση για το κοινό καλό. Για περισσότερες πληροφορίες δείτε την αναφορά με τίτλο «ARTIFICIAL INTELLIGENCE AND EDUCATION. A critical view through the lens of human rights, democracy and the rule of law» από τους Holmes et al. (2022).

ΒΙΒΛΙΟΓΡΑΦΙΑ 11ΗΣ ΣΥΝΕΔΡΙΑΣ

1) Access Now (2018), *Human rights in the age of artificial intelligence*, διαθέσιμο στη διεύθυνση www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf, Τελευταία πρόσβαση Ιανουάριο 2024.
2) Cooper, G. (2023). Examining Science Education in ChatGPT: An Exploratory Study of Generative Artificial Intelligence. *J Sci Educ Technol* 32, 444–452. https://doi.org/10.1007/s10956-023-10039-y
3) Cotton, D.R.E., Cotton, P.A. & Shipway, J. R. (2023). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. *Innovations in Education and Teaching International*. DOI: 10.1080/14703297.2023.2190148
4) Fiona Fui-Hoon Nah, Ruilin Zheng, Jingyuan Cai, Keng Siau & Langtao Chen (2023) Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration, *Journal of Information Technology Case and Application Research*, 25:3, 277-304, https://doi.org/10.1080/15228053.2023.2233814
5) Floridi, L., Chiriatti, M. (2020). GPT-3: Its Nature, Scope, Limits, and Consequences. *Minds & Machines* 30, 681–694. https://doi.org/10.1007/s11023-020-09548-1
6) Grigoriadou, M., Papanikolaou, K., Tsaganou, G., Gouli, E. and Gogoulou, A. (2010). Introducing innovative e-learning environments in higher education, *Int. J. Cont. Engineering Education and Life-Long Learning*, Vol. 20, Nos. 3/4/5, 2010, 337-355.
7) Holmes, W. and Fengchun, M. (2023). Guidance for generative AI in education and research. UNESCO. Διαθέσιμο εδώ https://unesdoc.unesco.org/ark:/48223/pf0000386693
8) Holmes, W., Persson, J., Chounta, I.-A., Wasson, B. and Dimitrova, V. (2022). Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law. Council of Europe. Διαθέσιμο εδώ https://rm.coe.int/artificial-intelligence-and-education-a-critical-view-through-the-lens/1680a886bd
9) Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Gasser, U., Groh, G., Günnemann, S., Hüllermeier, E., Krusche, S., Kutyniok, G., Michaeli, T., Nerdel, C., Pfeffer, J., Poquet, O., Sailer, M., Schmidt, A., Seidel, T., . . . Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, 1–9. https://doi.org/10.1016/j.lindif.2023.102274
10) Lin, P-Y., Chai, C-S., Siu-Yung Jong, M., Dai, Y., Guo, Y., Qin, J. (2021). Modeling the structural relationship among primary students' motivation to learn artificial intelligence.

Computers and Education: Artificial Intelligence. Vol.2, 100006, ISSN 2666-920X, https://doi.org/10.1016/j.caeai.2020.100006

11) Mansell, S. (2016). "*WFU expert cautions new internet myths may be more harmful*", Wake Forest University, 6 Jun. 2003; www.wfu.edu/wfunews/2003/060603r.html
12) Matzakos, N., Doukakis, S. & Moundridou, M. (2023). Learning Mathematics with Large Language Models: A Comparative Study with Computer Algebra Systems and Other Tools. *International Journal of Emerging Technologies in Learning (iJET), 18*(20), 51-71. Kassel, Germany: *International Journal of Emerging Technology in Learning*. Retrieved January 9, 2024 from https://www.learntechlib.org/p/223774/.
13) Ng, D. T. K., Leung, J. K. L., Chu, S. K.W., and Qiao, M. S. (2021). Conceptualizing AI literacy: An exploratory review. Computers and Education: Artificial Intelligence, 2:100041.
14) Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.-E., Ruggieri, S., Turini, F.,Papadopoulos, S., Krasanakis, E., et al. (2020).Bias in data-driven artificial intelligence systems—An introductory survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(3): e1356.
15) Palaigeorgiou, G. and Veletsianos, G. (2023). Master ChatGPT for Course Creation with the Art of Prompting. LearnWorlds. Διαθέσιμο εδώ 50+ Resources for Great Courses (https://www.learnworlds.com/resources/) όπως και το ebook "Maximizing your Course Success: Utilizing ChatGPT & Prompt Engineering" που αξίζει να δείτε.
16) Recommendation CM/Rec(2019)10 of the Committee of Ministers to member States on developing and promoting digital citizenship education, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168098de08)
17) Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its Nature and Impact in Secondary School Pupils. Journal of Child Psychology and Psychiatry, 49, 376-385. https://doi.org/10.1111/j.1469-7610.2007.01846.x
18) Volkmann, M.J. (2010). Internet Dangers, *Education Technology Center,* https://wiki.uiowa.edu/display/edtech/Internet+Dangers
19) Wang, B., Rau, P.-L. P., and Yuan, T. (2023). Measuring user competence in using artificial intelligence:validity and reliability of artificial intelligence literacy scale. *Behaviour & information technology*, 42(9):1324–1337.
20) Warner-Blankenship, J.M. (2011). What are "Internet dangers?', *Education Technology Center,* https://wiki.uiowa.edu/pages/viewpage.action?pageId=49483037
21) Γορανίτης (2016). Post-truth: Οι ψεύτικες ειδήσεις δεν θα σταματήσουν ποτέ https://insidestory.gr/article/post-truth?token=C50B57L6F7,
22) Καμάρης, Α. (2014). Κίνδυνοι και ασφάλεια στο Διαδίκτυο για τη νεολαία: Μία κριτική επισκόπηση, Πτυχιακή Εργασία, Αθήνα, Τμήμα Πληροφορικής.
23) Καριοφύλλης Α., "Ανεπιθύμητα e-mails (spam)", W-Learn: *Πρόσβαση στη Γνώση*, 2005-2014; www.wlearn.gr/index.php/2010-07-29-17-58-43-v15-214/219--emails-spam
24) Μαρινάκη Μ. (2015). «Ψηφιακή Πολιτειότητα και Εκπαίδευση. Η ιδιότητα του πολίτη σήμερα: εννοιολογήσεις και προβληματισμοί», Διεθνές Συνέδριο για την Ανοικτή & εξ Αποστάσεως Εκπαίδευση, Τόμος 8, http://dx.doi.org/10.12681/icodl.47
25) Μπάνου, Χ. (2010). Ο θρίαμβος της ανάγνωσης, http://www.bookpress.gr/afieromata/aprilios/o-thriamvos-tis-anagnosis
26) Τολούδης Α. (2012). "Τι συμβαίνει όταν τα avatar εισβάλλουν στη ζωή μας", *Τεχνολογικές Συναντήσεις,* 16 Οκτ. 2012. http://tech.in.gr/presentations/article/?aid=1231217957
27) Τσιωτάκης Π. (2023). Το ChatGPT για εκπαιδευτικούς και μαθητές. Εκδόσεις Σαββάλας.

Για περαιτέρω μελέτη

1) The Future of Education - Yuval Noah Harari & Russell Brand - Penguin Talks https://www.youtube.com/watch?v=j0uw7Xc0fLk (60')

Μια ενδιαφέρουσα προβληματική αναπτύσσεται από τον Yuval Noah Harari που μιλά με 350 νέους στο Νότιο Λονδίνο για τις προκλήσεις που αντιμετωπίζει η επόμενη γενιά σε σχέση με την ανάπτυξη κυρίως της ΤΝ και πώς θα μπορούσαν να πάρουν θέση και να επηρεάσουν τις εξελίξεις.

2) Chen, X., Zou, D., Xie, H., Cheng, G., & Liu, C. (2022). Two Decades of Artificial Intelligence in Education: Contributors, Collaborations, Research Topics, Challenges, and Future Directions. Educational Technology & Society, 25(1), 28–47. https://www.jstor.org/stable/48647028

3) Giannakos, M., Voulgari, I., Papavlasopoulou, S., Papamitsiou, Z., Yannakakis, G. (2020). Games for Artificial Intelligence and Machine Learning Education: Review and Perspectives. In: Giannakos, M. (eds) Non-Formal and Informal Science Learning in the ICT Era. Lecture Notes in Educational Technology. Springer, Singapore. https://doi.org/10.1007/978-981-15-6747-6_7

4) Benedict du Boulay (Ed.) Handbook of Artificial Intelligence in Education (2023). ISBN: 978 1 80037 540 6. Edward Elgar Publishing Limited.

5) AI in Education. A Practical Guide for Teachers and Young People (2019). Τμήμα Τεχνητής Νοημοσύνης. Πανεπιστήμιο Μάλτας: περιλαμβάνει δραστηριότητες για διάφορα θέματα ΤΝ από το Πανεπιστήμιο της Μάλτας προτείνονται εδώ: https://learnml.eu/docs/AI_in_Education.pdf

(Ημερομηνία τελευταίας επίσκεψης για όλους τους παραπάνω δικτυακούς τόπους που αναφέρθηκαν παραπάνω: Φεβρουάριος 2026)