

Άγγελος Ανδρουλιδάκης

Πόσο έτοιμοι είμαστε για την επανάσταση της τεχνητής νοημοσύνης;

Οι τελευταίοι μήνες σημαδεύτηκαν αναμφίβολα από μια έκρηξη του ενδιαφέροντος για τα συστήματα τεχνητής νοημοσύνης, ορόσημο της οποίας ήταν η διάθεση στο ευρύ κοινό του διάσημου πλέον μοντέλου γλώσσας ChatGPT τον Νοέμβριο του 2022, το οποίο -σύμφωνα και με το ίδιο- «διαθέτει προηγμένες δυνατότητες Επεξεργασίας Φυσικής Γλώσσας, εκπαίδευση μεγάλης κλίμακας σε ποικίλα δεδομένα κειμένου, επίγνωση των συμφραζόμενων και ευελιξία στην εκτέλεση ενός ευρέος φάσματος εργασιών που σχετίζονται με τη γλώσσα».

Στην πραγματικότητα, η επιτυχία του ChatGPT αποτελεί απλά έναν καταλύτη των εξελίξεων σε έναν τομέα που σημειώνει μια αλματώδη πρόοδο εδώ και περισσότερο από μια δεκαετία, με την έλευση των τεχνολογιών Deep Learning και την υπολογιστική ισχύ των συστημάτων αυτών να διπλασιάζεται κάθε έξι μόλις μήνες. Ήδη βρισκόμαστε σε ένα κομβικό σημείο όπου είναι πλέον δυσδιάκριτο εάν ένα κείμενο, μια εικόνα ή ένα βίντεο έχουν παραχθεί από κάποιον αλγόριθμο ή από τον άνθρωπο ή εάν ένας διάλογος είναι πραγματικός.

Πόσο προετοιμασμένοι είμαστε όμως για την επανάσταση που έρχεται; Καθόλου δυστυχώς, αυτή είναι η σκληρή πραγματικότητα. Τη στιγμή που κανείς μας -ούτε οι πλέον «ψηφιακά εγγράμματοι»- δεν είναι προετοιμασμένος για τις κοσμογονικές αλλαγές που θα επιφέρουν οι εξελίξεις στον τομέα της τεχνητής νοημοσύνης, ένα μεγάλο ποσοστό του κόσμου δεν διαθέτει ούτε τα στοιχειώδη εφόδια επιβίωσης στον σύγχρονο ψηφιακό κόσμο. Πρόσφατα αναρτήθηκε στο facebook μια πληθώρα από πανομοιότυπες, καταφανώς ψεύτικες σελίδες με την ονομασία «Μικρό σπίτι», οι οποίες υπόσχονται να χαρίσουν «δύο μίνι σπίτια» σε όσους γράψουν... «Συγχαρητήρια» σε σχόλιο. Οι πληροφορίες κάθε μίας από αυτές τις σελίδες είναι απολύτως κενές, καμία εταιρεία που να κατασκευάζει ή έστω να εμπορεύεται «προκάτ» σπίτια, καμία διεύθυνση, κανένα τηλέφωνο, καμία ιστοσελίδα, ενώ είχαν αναρτηθεί ελάχιστες -και αλιευμένες προφανώς από το διαδίκτυο- φωτογραφίες από ξύλινα «προκάτ» σπίτια. Θα έλεγες ότι οι δημιουργοί των σελίδων αυτών, οι οποίοι αποσκοπούν σε προσέλκυση ακολούθων με στόχο την υπεξαίρεση των προσωπικών δεδομένων εύπιστων χρηστών, δεν κατέβαλαν ιδιαίτερη προσπάθεια προκειμένου να τις καταστήσουν αληθοφανείς. Και όμως, είναι χιλιάδες οι χρήστες που έσπευσαν να σχολιάσουν «Συγχαρητήρια» και ίσως να καταχωρήσουν τον τηλεφωνικό τους αριθμό ή άλλα προσωπικά δεδομένα στη συνέχεια.

Ποιος θα προστατέψει αυτούς τους χρήστες από την κατάχρηση των εξελιγμένων συστημάτων τεχνητής νοημοσύνης όταν είναι τόσο ευάλωτοι σε εύκολα αναγνωρίσιμες απάτες; Πράττοντας αυτό που θεωρούσαμε καθήκον μας, υποβάλαμε αναφορά στο facebook για απάτη και ψεύτικη σελίδα, το οποίο μας ενημέρωσε ότι η εν λόγω σελίδα «δεν παραβιάζει κανέναν από τους συγκεκριμένους Όρους της κοινότητάς μας», κι αυτό παρότι στους Όρους αναφέρεται ρητά ότι δεν επιτρέπονται «πρακτικές εξαπάτησης όσον αφορά την ταυτότητα, τον σκοπό ή την προέλευση της εκπροσωπούμενης οντότητας», όπως και η «εξαπάτηση άλλων για τη δημιουργία οικονομικού ή προσωπικού οφέλους μέσω της ίδρυσης ψεύτικων επιχειρήσεων ή οντοτήτων».

Στη συνέχεια, υποβάλλαμε καταγγελία στη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, η οποία -παρότι παραδέχθηκε ότι «παρόμοια περιστατικά που μας έχουν καταγγελλθεί στο παρελθόν αποδείχτηκαν ότι ήταν απάτες», μας συνέστησε να μην αποστέλλουμε τραπεζικά ή προσωπικά στοιχεία και - εφόσον το επιθυμούμε- να μεταβούμε σε οποιαδήποτε

Δικαστική ή Αστυνομική Αρχή για την υποβολή μηνυτήριας αναφοράς. Είναι εύλογο λοιπόν ότι το υφιστάμενο πλαίσιο λειτουργίας των ελάχιστων μεγάλων εταιρειών που ελέγχουν σχεδόν απόλυτα τον ψηφιακό μας κόσμο, όσο και το υπάρχον θεσμικό πλαίσιο, αδυνατούν σε μεγάλο βαθμό να μας προστατέψουν επαρκώς -και σίγουρα εγκαίρως- από την κατάχρηση των ψηφιακών μέσων, ενώ -μπροστά την επέλαση της τεχνητής νοημοσύνης- αποδεικνύεται ότι είμαστε ανεπίτρεπτα αθωράκιστοι.

Τι πρέπει να γίνει, λοιπόν; Μπορούν ο κυοφορούμενος -και άτολμος σε κρίσιμα σημεία- Ευρωπαϊκός Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act) ή άλλες νομοθετικές πρωτοβουλίες να αναχαιτίσουν τους κινδύνους για τους πολίτες; Σίγουρα ένα ρυθμιστικό πλαίσιο είναι καλύτερο από την ανεξέλεγκτη ανάπτυξη και διάθεση ολοένα και ισχυρότερων εργαλείων τεχνητής νοημοσύνης, όμως κανένα νομοθετικό πλαίσιο δεν θα είναι αποτελεσματικό χωρίς πολίτες ικανούς να αντιμετωπίζουν κριτικά το ψηφιακό περιβάλλον τους, να αμφισβητούν την αυθεντία των αλγορίθμων και να διεκδικούν το σεβασμό των ψηφιακών τους δικαιωμάτων. Απαιτείται μεγαλύτερη κινητοποίηση της κοινωνίας στην κατεύθυνση μιας μεγάλης κλίμακας εκστρατείας «ψηφιακού αλφαριθμητισμού». Το αν η εκάστοτε πολιτική εξουσία θα σταθεί αρωγός αυτής της προσπάθειας είναι υπό συζήτηση: η ανάπτυξη της κριτικής σκέψης των πολιτών προκειμένου να μην είναι ευάλωτοι στη χειραγωγή δεν ήταν διαχρονικά μέσα στις προτεραιότητές της.

[ΠΗΓΗ: Εφημερίδα των Συντακτώ ν, 10.02.2023](#)

