

ΕΡΩΤΗΣΗ

**ΠΡΟΣ: Υπουργό Ψηφιακής Διακυβέρνησης
Υπουργό Προστασίας του Πολίτη**

ΘΕΜΑ: «Επιχειρησιακή ετοιμότητα της Πολιτείας για την αντιμετώπιση εγκλημάτων με χρήση Τεχνητής Νοημοσύνης και εγγυήσεις κατά τη χρήση συστημάτων ΤΝ από το Δημόσιο»

Αξιότιμε κ.κ. Υπουργοί,

Με τον ν. 5321/2026 (Α' 114) θεσπίστηκαν πρόσφατα, τα εθνικά μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2024/1689 για την Τεχνητή Νοημοσύνη.

Μεταξύ άλλων, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ορίστηκε ως αρμόδια αρχή εποπτείας για συγκεκριμένες κατηγορίες συστημάτων ΤΝ και ως ενιαίο σημείο επαφής, ενώ η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων ορίστηκε ως κοινοποιούσα αρχή.

Παράλληλα, προβλέπονται Κέντρο Συντονισμού και Τεχνογνωσίας για την Τεχνητή Νοημοσύνη στην ΕΕΤΤ, ενιαίο σύστημα υποβολής καταγγελιών, Μητρώο Συστημάτων Τεχνητής Νοημοσύνης που χρησιμοποιούνται από φορείς του δημόσιου τομέα και Παρατηρητήριο Τεχνητής Νοημοσύνης.

Η θέσπιση του νέου νομοθετικού πλαισίου αποτελεί αναγκαίο πρώτο βήμα. Το κρίσιμο ζήτημα, όμως, είναι εάν η Πολιτεία διαθέτει την απαιτούμενη επιχειρησιακή ετοιμότητα, το εξειδικευμένο προσωπικό, τα σύγχρονα τεχνικά μέσα και τους αποτελεσματικούς μηχανισμούς εποπτείας για την εφαρμογή του.

Η Τεχνητή Νοημοσύνη δεν αποτελεί πλέον μόνο ζήτημα τεχνολογικής και οικονομικής ανάπτυξης. Αποτελεί συγχρόνως παράμετρο εθνικής ασφάλειας, δημόσιας τάξης και προστασίας των θεμελιωδών δικαιωμάτων.

Οι ίδιες τεχνολογικές δυνατότητες που μπορούν να αξιοποιηθούν από τις αρμόδιες αρχές για την πρόληψη και τη διερεύνηση του εγκλήματος χρησιμοποιούνται και για την ανάπτυξη νέων μορφών απειλής. Η βαθυπαραποίηση εικόνας και ήχου, η κλωνοποίηση φωνής, η ψηφιακή πλαστοπροσωπία, οι στοχευμένες οικονομικές απάτες και οι εκβιασμοί μπορούν πλέον να πραγματοποιούνται ταχύτερα, μαζικότερα και με μεγαλύτερη πειστικότητα.

Ιδιαίτερα εκτεθειμένοι είναι οι ανήλικοι, οι ηλικιωμένοι, οι πολίτες με περιορισμένη ψηφιακή εξοικείωση και οι μικρές επιχειρήσεις. Οι επιθέσεις αυτές δεν προκαλούν μόνο οικονομική ζημία. Μπορούν να προσβάλουν την προσωπικότητα και την αξιοπρέπεια του πολίτη, να οδηγήσουν στον εκβιασμό θυμάτων και να υπονομεύσουν την εμπιστοσύνη στην ενημέρωση και στους θεσμούς.

Μέχρι σήμερα δεν έχει καταστεί σαφές εάν η Διεύθυνση Δίωξης Κυβερνοεγκλήματος διαθέτει επαρκές εξειδικευμένο προσωπικό και τα αναγκαία τεχνικά εργαλεία για την ανίχνευση και εγκληματολογική εξέταση περιεχομένου που έχει δημιουργηθεί ή αλλοιωθεί με Τεχνητή Νοημοσύνη. Δεν είναι επίσης γνωστό εάν τηρούνται διακριτά στατιστικά στοιχεία για εγκλήματα που τελούνται με τη χρήση της ούτε εάν υπάρχει ενιαίο επιχειρησιακό πρωτόκολλο συνεργασίας μεταξύ των συναρμόδιων αρχών.

Εξίσου κρίσιμο είναι το ζήτημα της χρήσης συστημάτων Τεχνητής Νοημοσύνης από το ίδιο το Δημόσιο. Σύμφωνα με το άρθρο 25 του ν. 5321/2026, οι δημόσιοι φορείς που χρησιμοποιούσαν ήδη τέτοια συστήματα κατά την έναρξη ισχύος του νόμου οφείλουν να τα δηλώσουν στο σχετικό Μητρώο το αργότερο έως την 31η Δεκεμβρίου 2026.

Στο Μητρώο προβλέπεται να καταγράφονται, μεταξύ άλλων, οι δυνατότητες και τα τεχνικά χαρακτηριστικά κάθε συστήματος, οι κατηγορίες αποφάσεων που λαμβάνονται ή υποστηρίζονται από αυτό, οι πιθανοί κίνδυνοι για δικαιώματα και ελευθερίες, τα μέτρα ασφαλούς λειτουργίας και οι απαιτούμενες εκτιμήσεις επιπτώσεων.

Η τυπική καταχώριση, όμως, δεν αρκεί. Οι πολίτες δικαιούνται να γνωρίζουν ποιος δημόσιος φορέας χρησιμοποιεί σύστημα Τεχνητής Νοημοσύνης, για ποιον σκοπό, με ποια δεδομένα, υπό ποιον έλεγχο και σε ποιο βαθμό συμμετέχει στη λήψη αποφάσεων που τους αφορούν.

Καμία διοικητική ή άλλη απόφαση που επηρεάζει δικαιώματα, παροχές ή έννομα συμφέροντα των πολιτών δεν πρέπει να λαμβάνεται αποκλειστικά από έναν αλγόριθμο. Πρέπει να διασφαλίζονται ουσιαστική ανθρώπινη εποπτεία, ενημέρωση του ενδιαφερομένου, ειδική αιτιολόγηση και δυνατότητα αποτελεσματικής αμφισβήτησης της απόφασης.

Η Πολιτεία οφείλει να αξιοποιήσει τις δυνατότητες της Τεχνητής Νοημοσύνης για την προστασία του πολίτη και την καταπολέμηση του εγκλήματος. Οφείλει, όμως, ταυτόχρονα να αποτρέψει τη δημιουργία μηχανισμών μαζικής επιτήρησης, αυτοματοποιημένης στοχοποίησης ή περιορισμού των ατομικών ελευθεριών.

Η ασφάλεια του πολίτη και η ελευθερία του δεν αποτελούν αντικρουόμενες επιδιώξεις. Αποτελούν δύο εξίσου δεσμευτικές υποχρεώσεις μιας δημοκρατικής Πολιτείας.

Κατόπιν των ανωτέρω, ερωτώνται οι κ.κ. Υπουργοί :

1. Υπάρχει ενιαία εθνική στρατηγική για την πρόληψη, ανίχνευση και αντιμετώπιση εγκλημάτων που αξιοποιούν Τεχνητή Νοημοσύνη, όπως η βαθυπαραποίηση εικόνας και ήχου, η κλωνοποίηση φωνής, η ψηφιακή πλαστοπροσωπία, οι οικονομικές απάτες και οι εκβιασμοί; Ποιος φορέας έχει την ευθύνη του κεντρικού συντονισμού;
2. Διαθέτει η Διεύθυνση Δίωξης Κυβερνοεγκλήματος επαρκές εξειδικευμένο προσωπικό και κατάλληλα τεχνικά εργαλεία για την ανίχνευση και εγκληματολογική εξέταση υλικού που έχει δημιουργηθεί ή αλλοιωθεί με Τεχνητή Νοημοσύνη; Πόσα στελέχη της έχουν λάβει σχετική ειδική εκπαίδευση και πόσες αντίστοιχες καταγγελίες έχουν καταγραφεί κατά τα έτη 2024, 2025 και το πρώτο εξάμηνο του 2026;

3. Υπάρχει ενιαίο επιχειρησιακό πρωτόκολλο συνεργασίας μεταξύ της Ελληνικής Αστυνομίας, της Εθνικής Αρχής Κυβερνοασφάλειας, της ΑΠΔΠΧ, της ΕΕΤΤ και των λοιπών αρμόδιων φορέων; Με ποια διαδικασία μπορεί ο πολίτης να καταγγέλλει περιστατικά κακόβουλης χρήσης ΤΝ, να υποβάλλει με ασφάλεια το σχετικό ψηφιακό υλικό και να ενημερώνεται για την πορεία της υπόθεσής του;
4. Σε ποιο στάδιο βρίσκεται η επιχειρησιακή ενεργοποίηση της ΑΠΔΠΧ ως αρχής εποπτείας και ενιαίου σημείου επαφής, του Κέντρου Συντονισμού και Τεχνογνωσίας στην ΕΕΤΤ και του ενιαίου συστήματος υποβολής καταγγελιών; Με πόσο εξειδικευμένο προσωπικό, ποιους οικονομικούς πόρους και ποιες τεχνικές υποδομές θα λειτουργήσουν;
5. Έχει τεθεί σε λειτουργία το Μητρώο Συστημάτων Τεχνητής Νοημοσύνης του άρθρου 21 του ν. 5321/2026; Πόσα συστήματα και πόσοι δημόσιοι φορείς έχουν ήδη καταχωριστεί και ποιο είναι το σχέδιο για την τήρηση της προθεσμίας της 31ης Δεκεμβρίου 2026; Θα είναι δημόσια προσβάσιμα τα βασικά στοιχεία του Μητρώου και ποιος θα ελέγχει την πληρότητα και την ακρίβεια των δηλώσεων;
6. Ποιοι μηχανισμοί διασφαλίζουν ότι η χρήση συστημάτων ΤΝ από δημόσιες και διωκτικές αρχές υπόκειται σε έλεγχο νομιμότητας, ανθρώπινη εποπτεία και επαρκείς εγγυήσεις κυβερνοασφάλειας και προστασίας προσωπικών δεδομένων; Ενημερώνεται ο πολίτης όταν απόφαση που τον αφορά έχει ληφθεί ή υποστηριχθεί από σύστημα ΤΝ και διαθέτει δικαίωμα ανθρώπινης επανεξέτασης και αποτελεσματικής αμφισβήτησής της;

Ο Ερωτών Βουλευτής

Α' Ανατολικής Αττικής

Τάσος Οικονομόπουλος