ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

«Προστασία προσωπικών δεδομένων στα συστήματα ΤΝ

Οι προκλήσεις κατά τον έλεγχο συμμόρφωσης από τις ΑΠΔ»

Γεωργία Παναγοπούλου

Μηχανικός Η/Υ και Πληροφορικής, DESS, ITIL

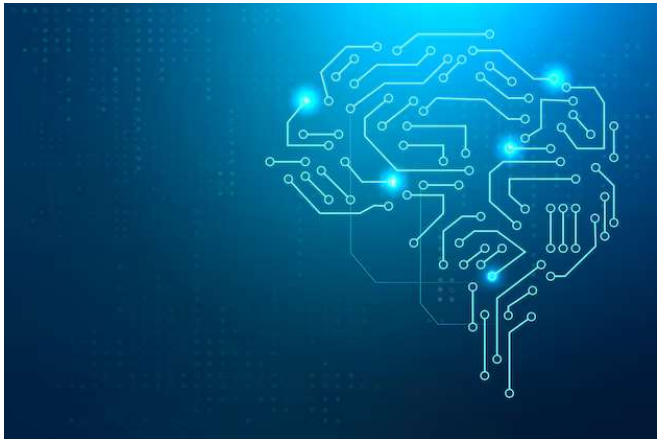
ΕΕΠ Ελέγκτρια Πληροφορικής

Προϊσταμένη Τμήματος Ελέγχων και Ασφάλειας

Μοντέλο ΤΝ

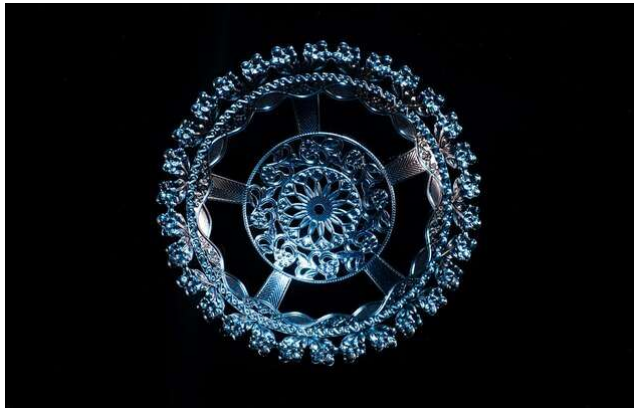
Ένα μοντέλο ΤΝ προκύπτει από μηχανισμούς εκπαίδευσης που εφαρμόζονται σε ένα σύνολο δεδομένων εκπαίδευσης, στο πλαίσιο της Τεχνητής Νοημοσύνης, συμπεριλαμβανομένων της Μηχανικής Μάθησης, της Βαθιάς Μάθησης ή άλλων συναφών τεχνολογιών.

Τα μοντέλα τεχνητής νοημοσύνης μπορεί να υποβληθούν και σε περαιτέρω εκπαίδευση, βελτιστοποίηση ή/και ανάπτυξη.



Κύκλος ζωής συστήματος ΤΝ

Φάσεις κύκλου ζωής ενός συστήματος που βασίζεται σε ΤΝ :



- Σχεδιασμός και ανάλυση
- Ανάπτυξη (έρευνα, επιλογή, ανάλυση και καθαρισμός δεδομένων, πρωτοτυποποίηση, σχεδιασμός, εκπαίδευση, δοκιμή, εφαρμογή σε λογισμικό και/ή υλικό, ενοποίηση ως μέρος μιας συνολικής επεξεργασίας και επικύρωση)
- Λειτουργία
- Συντήρηση
- Απόσυρση

Τα στάδια επιδέχονται επανάληψης, ανάλογα με το επιλεγμένο μοντέλο ανάπτυξης.

ΓΚΠΔ και ΤΝ

- Πτυχές προστασίας δεδομένων σχετίζονται με τόσο με την εκπαίδευση όσο και με την ανάπτυξη και τη χρήση μοντέλων τεχνητής νοημοσύνης.

- Προσωπικά δεδομένα μπορεί να αποτελούν μέρος του σχετικού συνόλου δεδομένων στα οποία το μοντέλο εκπαιδεύεται, βελτιστοποιείται ή ενημερώνεται.

- Ο ΓΚΠΔ είναι τεχνολογικά ουδέτερος, η επεξεργασία που σχετίζεται με την τεχνητή νοημοσύνη, ιδιαίτερη/πρωτότυπη/καινοτόμα/σύνθετη, καλύπτεται από τον ΓΚΠΔ κάθε φορά που υποβάλλονται σε επεξεργασία προσωπικά δεδομένα.

Έλεγχος συμμόρφωσης ΓΚΠΔ σε ΤΝ

- Προϋπόθεση: το σύστημα ΤΝ να εκτελεί επεξεργασία προσωπικών δεδομένων σε κάποιο στάδιο του κύκλου ζωής του ή η σχετική επεξεργασία να οδηγεί σε δημιουργία προφίλ ή να αυτοματοποιεί αποφάσεις σχετικά με φυσικά πρόσωπα που ενδέχεται να συνεπάγονται νομικές συνέπειες ή να επηρεάσουν σημαντικά τα πρόσωπα αυτά.

- Όταν τα δεδομένα εκπαίδευσης περιέχουν προσωπικά δεδομένα, υφίστανται μετασχηματισμό κατά τη διαδικασία μηχανικής μάθησης, μετατρέποντάς τα σε αφηρημένες μαθηματικές αναπαραστάσεις. Αυτή η διαδικασία αφαίρεσης έχει ως αποτέλεσμα την απώλεια συγκεκριμένων χαρακτηριστικών και αναφορών σε συγκεκριμένα άτομα. Το εάν και πότε μπορεί να θεωρηθεί ότι δεν πραγματοποιείται επεξεργασία ΠΔ σε ένα μοντέλο θα γίνει σύμφωνα με τον ορισμό του ανώνυμου δεδομένου.

- Σε κάθε περίπτωση θα πρέπει η διαδικασία ανωνυμοποίησης να είναι πλήρως τεκμηριωμένη. Ο έλεγχος περιλαμβάνει ανάλυση του βαθμού ανωνυμοποίησης που πραγματοποιήθηκε στα δεδομένα που χρησιμοποιούνται στην επεξεργασία, τον υπολογισμό ή την εκτίμηση του πιθανού κινδύνου επαναπροσδιορισμού του υπάρχει.

PETs σε ΤΝ

- Η εφαρμογή τεχνολογιών βελτίωσης της ιδιωτικότητας (PETs) σε προσωπικά δεδομένα στα συστήματα ΤΝ ενέχει επίσης προκλήσεις.
- Μια προσέγγιση είναι τα συνθετικά δεδομένα: συνθετικά δεδομένα μπορούν να δημιουργηθούν χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης που μαθαίνουν μοτίβα από πραγματικά δεδομένα και στη συνέχεια χρησιμοποιούν αυτά τα μοτίβα για να δημιουργήσουν νέα δεδομένα που είναι στατιστικά παρόμοια, αλλά δεν περιέχουν αναγνωρίσιμες προσωπικές πληροφορίες.
- Καμία τεχνική ενίσχυσης της ιδιωτικής ζωής δεν πρέπει να θεωρείται ως πανάκεια όσον αφορά τον μετριασμό των σχετικών κινδύνων που απορρέουν από τη διαδικασία του μοντέλου εκπαίδευσης
- Η εφαρμογή μιας τεχνικής ενίσχυσης της ιδιωτικής ζωής μπορεί επίσης να επηρεάσει την συνολική ακρίβεια του μοντέλου.

Ειδικές ευπάθειες ΤΝ

- Οι επιθέσεις αντιστροφής μοντέλου συμβαίνουν όταν ένας εισβολέας αναστρέψει το μοντέλο για να εξάγει πληροφορίες από αυτό.

Π.χ εισβολείς μπορούν να ανασυνθέσουν εικόνες προσώπων τις οποίες ένα σύστημα τεχνολογίας αναγνώρισης προσώπου έχει εκπαιδευτεί να αναγνωρίζει. Όταν δίνεται στο μοντέλο η εικόνα ενός ατόμου του οποίου το πρόσωπο αναγνωρίζει, το μοντέλο επιστρέφει την καλύτερη εικασία για το όνομα του ατόμου και το σχετικό ποσοστό εμπιστοσύνης. Οι επιτιθέμενοι θα μπορούσαν να διερευνήσουν το μοντέλο υποβάλλοντας πολλές διαφορετικές, τυχαία δημιουργημένες εικόνες προσώπου. Παρατηρώντας τα ονόματα και τις βαθμολογίες εμπιστοσύνης που έδωσε το μοντέλο, θα μπορούσαν να ανασυνθέσουν τις εικόνες προσώπων που σχετίζονται με τα άτομα που περιλαμβάνονται στα δεδομένα εκπαίδευσης.

Ειδικές ευπάθειες ΤΝ

- Οι επιθέσεις συμπερασμάτων μέλους (Membership inference attacks) επιτρέπουν σε κακόβουλους να συμπεράνουν εάν ένα συγκεκριμένο άτομο ήταν παρόν στα δεδομένα εκπαίδευσης ενός μοντέλου ΤΝ. Ωστόσο, σε αντίθεση με την αντιστροφή μοντέλου, δεν μαθαίνουν απαραίτητα πρόσθετα προσωπικά δεδομένα για το άτομο.

Π.χ εάν τα νοσοκομειακά αρχεία χρησιμοποιούνται για την εκπαίδευση ενός μοντέλου που προβλέπει πότε ένας ασθενής θα πάρει εξιτήριο, οι εισβολείς θα μπορούσαν να χρησιμοποιήσουν αυτό το μοντέλο σε συνδυασμό με άλλα δεδομένα για ένα συγκεκριμένο άτομο (που έχουν ήδη) για να διαπιστώσουν εάν ήταν μέρος των δεδομένων εκπαίδευσης. Αυτό δεν θα αποκάλυπτε τα δεδομένα οποιουδήποτε ατόμου από το ίδιο το σύνολο δεδομένων εκπαίδευσης, αλλά στην πράξη θα αποκάλυπτε ότι είχαν επισκεφτεί ένα από τα νοσοκομεία που παρήγαγαν τα δεδομένα εκπαίδευσης κατά την περίοδο συλλογής των δεδομένων.

Ειδικές ευπάθειες ΤΝ

Επιθέσεις «μαύρου κουτιού» και «λευκού κουτιού»

- Λευκού κουτιού: ο εισβολέας έχει πλήρη πρόσβαση στο ίδιο το μοντέλο και μπορεί να επιθεωρήσει τον υποκείμενο κώδικα και τις ιδιότητές του (αν και όχι τα δεδομένα εκπαίδευσης).

π.χ ορισμένοι πάροχοι τεχνητής νοημοσύνης δίνουν σε τρίτους ένα ολόκληρο προεκπαιδευμένο μοντέλο και τους επιτρέπουν να το εκτελούν τοπικά. Οι επιθέσεις λευκού κουτιού επιτρέπουν τη συλλογή πρόσθετων πληροφοριών, όπως τον τύπο του μοντέλου και τις παραμέτρους που χρησιμοποιούνται, οι οποίες θα μπορούσαν να βοηθήσουν έναν εισβολέα να συναγάγει προσωπικά δεδομένα από το μοντέλο.

- Μαύρου κουτιού: ο εισβολέας έχει μόνο τη δυνατότητα να ρωτήσει το μοντέλο και να παρατηρήσει τις σχέσεις μεταξύ εισόδων και εξόδων.

π.χ, πάροχοι τεχνητής νοημοσύνης επιτρέπουν σε τρίτους να έχουν πρόσβαση στη λειτουργικότητα ενός μοντέλου ΤΝ στο διαδίκτυο για να στείλουν ερωτήματα που περιέχουν δεδομένα εισόδου και να λάβουν την απάντηση του μοντέλου.

Έλεγχος συμμόρφωσης από ΑΠΔ σε ΤΝ

- Κριτήρια: νομιμότητα, δικαιοσύνη και διαφάνεια, περιορισμός σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης, ακεραιότητα και εμπιστευτικότητα, λογοδοσία.

- Το εύρος του ελέγχου προσαρμόζεται στο προς έλεγχο σύστημα

π.χ, στην περίπτωση ενός συστήματος το οποίο, βάσει ανάλυσης δεδομένων εισόδου, λαμβάνει αποφάσεις που μπορεί να επηρεάσουν σημαντικά ένα άτομο, στερώντας του την πρόσβαση σε βασικές υπηρεσίες ή περιορίζοντας τις ελευθερίες του, προφανώς το πεδίο εφαρμογής του αντίστοιχου ελέγχου και ο βαθμός εξαντλητικότητας κατά την ανάλυση των στοιχείων ελέγχου θα είναι υψηλότερος από ό,τι θα ήταν για ένα σύστημα του οποίου η λειτουργία περιορίζεται, για παράδειγμα, στην ταξινόμηση ορισμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου στο φάκελο Ανεπιθύμητα.

Αντικείμενα Ελέγχου

- Η ύπαρξη ή η απουσία προσωπικών δεδομένων.
- Η ανάλυση της αποτελεσματικότητας της ανωνυμοποίησης και των μεθόδων ψευδωνυμοποίησης
- Οι νομικές βάσεις επεξεργασίας και ο προσδιορισμός των ρόλων (υπεύθυνος επεξεργασίας - εκτελών την επεξεργασία)
- Η δημιουργία προφίλ ή αυτοματοποιημένων αποφάσεων σχετικά με τα υποκείμενα των δεδομένων. Η εκπλήρωση των περιορισμών στις αυτοματοποιημένες αποφάσεις, η εκτίμηση, κατά περίπτωση, της ποιότητας της ανθρώπινης παρέμβασης και των εποπτικών μηχανισμών που υιοθετήθηκαν.
- Η επαλήθευση και η εκτέλεση των δοκιμών σχετικά με την καταλληλότητα των αλγορίθμων που χρησιμοποιούνται για τη δημιουργία προφίλ και την εξαγωγή συμπερασμάτων

Αντικείμενα Ελέγχου

- Η ενημέρωση και η αποτελεσματικότητα των μηχανισμών διαφάνειας που έχουν εφαρμοστεί και η επάρκεια των μηχανισμών για άσκηση δικαιωμάτων
- Η εφαρμογή της αρχής της λογοδοσίας και διαχείρισης κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (ΕΑΠΔ)
- Η εκ των προτέρων ανάλυση της ανάγκης επεξεργασίας προσωπικών δεδομένων, από πλευράς ποσότητας και έκτασης, σε διάφορες φάσεις σύμφωνα με κριτήρια ελαχιστοποίησης.
- Η ανάλυση της ακρίβειας, της αξιοπιστίας, της ποιότητας και μεροληψίας των δεδομένων που χρησιμοποιήθηκαν ή συγκεντρώθηκαν για την ανάπτυξη ή τη λειτουργία του συστήματος ΤΝ
- Η καταλληλότητα των μέτρων ασφαλείας για την αποφυγή κινδύνων προστασίας της ιδιωτικής ζωής

Ενδεικτικά σημεία ελέγχου - διαφάνεια

- ✓ Είναι τεκμηριωμένες οι πηγές των δεδομένων;
- ✓ Τα χαρακτηριστικά των δεδομένων που χρησιμοποιούνται για την εκπαίδευση του συστήματος ΤΝ προσδιορίζονται, τεκμηριώνονται και αιτιολογούνται δεόντως;
- ✓ Είναι τεκμηριωμένη η επεξήγηση του κώδικα του αλγορίθμου προκειμένου να διευκολυνθεί η αναγνωσιμότητα, η λογική κατανόηση και η εσωτερική του συνέπεια;
- ✓ Περιλαμβάνει η τεκμηρίωση του κώδικα αλγορίθμου πληροφορίες σχετικά με τα μεταδεδομένα του συστήματος που βασίζεται σε ΤΝ;Η λογική του και οι συνέπειες που μπορεί να προκύψουν από τη χρήση του είναι προσβάσιμα στα υποκείμενα των δεδομένων μαζί με τα μέσα ή τους διαθέσιμους μηχανισμούς για την άσκηση των δικαιωμάτων τους σε περίπτωση αντιρρήσεων αποτελέσματα;
- ✓ Οι αποφάσεις που λαμβάνονται από ένα σύστημα ΤΝ μπορούν να επεξηγηθούν, βάσει της γενικότερης τεκμηρίωσης που παρέχεται; (επεξηγησιμότητα)
- ✓ Σε περίπτωση λανθασμένης συμπεριφοράς του συστήματος που βασίζεται σε ΤΝ που θα μπορούσε να προκαλέσει βλάβη στα υποκείμενα των δεδομένων, έχουν δημιουργηθεί μηχανισμοί για την ελαχιστοποίηση αυτής της ζημίας; παρέχονται κανάλια επικοινωνίας για τη διευκόλυνση της επικοινωνίας μεταξύ όλων των ενδιαφερομένων που εμπλέκονται στη διαδικασία;

Ενδεικτικά σημεία ελέγχου - σκοπός

- ✓ Είναι τεκμηριωμένος ο επιδιωκόμενος σκοπός του συστήματος που βασίζεται σε ΤΝ;
- ✓ Υπάρχει σχέση μεταξύ της χρήσης του συστήματος τεχνητής νοημοσύνης με τον απώτερο σκοπό της επεξεργασίας και των όρων που εγγυώνται τη νομιμότητα αυτής της επεξεργασίας;
- ✓ Εντοπίζονται οι διαφορετικές δυναμικές, δραστηριότητες ή/και διαδικασίες εντός του οργανισμού στον οποίο ενσωματώνεται το στάδιο του κύκλου ζωής του ελεγχόμενου συστήματος ΤΝ, οριοθετώντας όσο το δυνατόν περισσότερο το πλαίσιο χρήσης;
- ✓ Οι πιθανοί χρήστες του συστήματος που βασίζεται σε τεχνητή νοημοσύνη κατηγοριοποιούνται;
- ✓ Υπάρχουν άλλες πιθανές χρήσεις και δευτερεύοντες χρήστες για το σύστημα ΤΝ; Έχουν τεκμηριωθεί επαρκώς;

Ενδεικτικά σημεία ελέγχου – αναλογικότητα, αναγκαιότητα, ακρίβεια

- ✓ Έχει αξιολογηθεί η χρήση του συστήματος ΤΝ έναντι άλλων πιθανών επιλογών από μια προσέγγιση που εστιάζει στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων;
- ✓ Έχει αναλυθεί και αντιμετωπιστεί ο κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που εισάγεται με τη χρήση ενός συστήματος που βασίζεται σε τεχνητή νοημοσύνη στην επεξεργασία δεδομένων;
- ✓ Εντοπίζονται οι κατηγορίες των υποκειμένων των δεδομένων που επηρεάζονται από την ανάπτυξη του συστήματος ΤΝ και τη χρήση του στο πλαίσιο της προβλεπόμενης επεξεργασίας;
- ✓ Εντοπίζονται οι βραχυπρόθεσμες και μακροπρόθεσμες συνέπειες που μπορεί να έχει η εφαρμογή του συστήματος τεχνητής νοημοσύνης στις κατηγορίες των υποκειμένων των δεδομένων;
- ✓ Υπάρχει τεκμηριωμένη διαδικασία για τη διαχείριση και τη διασφάλιση της σωστής διακυβέρνησης δεδομένων, η οποία επιτρέπει την επαλήθευση και την παροχή εγγυήσεων για την ακρίβεια, την ακεραιότητα, την ακρίβεια, την ενημέρωση και την επάρκεια των συνόλων δεδομένων που χρησιμοποιούνται για εκπαίδευση, δοκιμή και λειτουργία;
- ✓ Υπάρχουν εποπτικοί μηχανισμοί για τις διαδικασίες συλλογής, επεξεργασίας, αποθήκευσης και χρήσης δεδομένων;

Ενδεικτικά σημεία ελέγχου – νομική βάση, ελαχιστοποίηση

- ✓ Εντοπίζονται νομικές βάσεις για την επεξεργασία προσωπικών δεδομένων στα διάφορα στάδια του κύκλου ζωής του συστήματος που βασίζεται σε τεχνητή νοημοσύνη;
- ✓ Είναι επαρκώς προσδιορισμένα και τεκμηριωμένα τα κριτήρια για τη διενέργεια προηγούμενης εκκαθάρισης των αρχικών συνόλων δεδομένων και τυχόν άλλων εργασιών που απαιτούνται κατά τη διάρκεια των διαφορετικών επαναλήψεων της εκπαιδευτικής διαδικασίας που βασίζεται σε τεχνητή νοημοσύνη;
- ✓ Οι τεχνικές «εκκαθάρισης» δεδομένων και οι βέλτιστες πρακτικές που χρησιμοποιούνται στη διαδικασία καθαρισμού δεδομένων έχουν επιλεγεί και τεκμηριωθεί σωστά;
- ✓ Τα δεδομένα έχουν προηγουμένως ταξινομηθεί σε κατηγορίες, ταξινομώντας τα σε μη προσωπικά και προσωπικά δεδομένα και, για τα τελευταία, προσδιορίζοντας ποια πεδία αποτελούν αναγνωριστικά, οιονεί αναγνωριστικά και ειδικές κατηγορίες δεδομένων;
- ✓ Έχουν καθοριστεί και εφαρμοστεί κριτήρια ελαχιστοποίησης δεδομένων στα διαφορετικά στάδια του συστήματος ΤΝ, χρησιμοποιώντας στρατηγικές όπως η απόκρυψη δεδομένων, διαχωρισμός, αφαίρεση, ανωνυμοποίηση και ψευδωνυμοποίηση που ενδέχεται να ισχύουν για τους σκοπούς βελτίωσης της ιδιωτικότητας των δεδομένων;
- ✓ Έχει πραγματοποιηθεί ανάλυση ανωνυμοποίησης δεδομένων, συμπεριλαμβανομένου του πιθανού κινδύνου επαναπροσδιορισμού;

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Ενδεικτικά σημεία ελέγχου – μεροληψία

- ✓ Έχουν καθοριστεί κατάλληλες διαδικασίες για τον εντοπισμό και την άρση, ή τουλάχιστον τον περιορισμό, τυχόν μεροληψίας στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του σχετικού μοντέλου;
- ✓ Έχει επαληθευτεί ότι στην εκπαίδευση τα δεδομένα δεν είχαν προηγούμενες προκαταλήψεις;
- ✓ Υπάρχουν μηχανισμοί ανθρώπινης εποπτείας που εφαρμόζονται προκειμένου να ελέγχεται και να διασφαλίζεται ότι τα αποτελέσματα είναι απαλλαγμένα από μεροληψία;
- ✓ Εφαρμόζονται μηχανισμοί που επιτρέπουν στα υποκείμενα των δεδομένων να ζητούν ανθρώπινη παρέμβαση, να παρέχουν ανατροφοδότηση ή να αντικρούουν τα αποτελέσματα που λαμβάνονται μέσω αυτοματοποιημένων αλγορίθμων λήψης αποφάσεων;

Ενδεικτικά σημεία ελέγχου – ασφάλεια

- ✓ Έχει διενεργηθεί ανάλυση επικινδυνότητας σχετικά με τους κινδύνους για τα δικαιώματα και τις ελευθερίες των προσώπων; Έχουν χρησιμοποιηθεί τα αποτελέσματα αυτής της ανάλυσης κινδύνου για τον προσδιορισμό των απαιτήσεων ασφάλειας και απορρήτου του συστήματος που βασίζεται σε ΤΝ στο πλαίσιο της επεξεργασίας;
- ✓ Έχουν ληφθεί υπόψη τα πρότυπα και οι βέλτιστες πρακτικές για την ασφαλή διαμόρφωση και ανάπτυξη του σχετικού συστήματος ΤΝ;
- ✓ Εφαρμόζονται μέτρα που προσανατολίζονται στην εγγύηση της εμπιστευτικότητας μέσω της ανωνυμοποίησης ή ψευδωνυμοποίησης δεδομένων και της ακεραιότητας για την προστασία από τυχαία ή εκούσια χειραγώγηση;
- ✓ Έχουν εφαρμοστεί διαδικασίες για την ορθή παρακολούθηση της λειτουργίας του μοντέλου και τον έγκαιρο εντοπισμό τυχόν πιθανής διαρροής δεδομένων, μη εξουσιοδοτημένης πρόσβασης ή άλλες παραβιάσεις ασφαλείας;
- ✓ Έχει εξεταστεί εάν το μοντέλο είναι ευάλωτο σε επιθέσεις αντιστροφής μοντέλου ή επιθέσεις συμπερασμάτων μέλους και έχουν εφαρμοστεί τεχνικές αποφυγής (πχ αποφυγή «υπερπροσαρμογής»)
- ✓ Έχουν εφαρμοστεί μέτρα για την αποφυγή επιθέσεων μαύρου κουτιού, παρακολούθηση ερωτημάτων από τους χρήστες του API, προκειμένου να εντοπιστούν ύποπτες ενέργειες; (πχ ως μέρος κοινών τεχνικών παρακολούθησης σε πραγματικό χρόνο που χρησιμοποιούνται για την προστασία από άλλες απειλές ασφαλείας, όπως ο «περιορισμός ρυθμού» (μείωση του αριθμού των ερωτημάτων που μπορεί να εκτελεστεί από έναν συγκεκριμένο χρήστη σε ένα δεδομένο χρονικό όριο).

ΑΠΔ, ΕΣΠΔ και ΤΝ

- Η Ιρλανδική Αρχή στις 4/9/2024 υπέβαλε αίτημα στο ΕΣΠΔ για γνωμοδότηση σύμφωνα με το άρθρο 64 παράγραφος 2 του ΓΚΠΔ.

- Η γνωμοδότηση καλεί το EDPB να εξετάσει, μεταξύ άλλων, τον βαθμό στον οποίο δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σε διάφορα στάδια της εκπαίδευσης και λειτουργίας ενός μοντέλου τεχνητής νοημοσύνης, καθώς και το θέμα της αξιολόγησης της νομικής βάσης που επικαλείται ο υπεύθυνος επεξεργασίας δεδομένων για να θεμελιώσει την εν λόγω επεξεργασία.

- Με σκοπό συμφωνία, σε επίπεδο ΕΣΠΔ, σχετικά με ορισμένα από τα βασικά ζητήματα που προκύπτουν στο πλαίσιο της επεξεργασίας με σκοπό την ανάπτυξη και εκπαίδευση ενός μοντέλου τεχνητής νοημοσύνης, φέρνοντας έτσι κάποια αναγκαία σαφήνεια στη σύνθετη αυτή περιοχή.

ΑΠΔ, ΕΣΠΔ, ΕΕΠΔ και ΤΝ

- https://www.aepd.es/sites/default/files/2020-07/adecuacion-rgpd-ia-en.pdf
- https://autoriteitpersoonsgegevens.nl/uploads/2024-01/AI%20%26%20Algorithmic%20Risks%20Report%20Netherlands%20-%20winter%202023%202024.pdf
- https://ico.org.uk/media/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf
- https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/ai-auditing_en
- https://www.cnil.fr/en/self-assessment-guide-artificial-intelligence-ai-systems
- https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf
- https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/2024-06-03-first-edps-orientations-euis-using-generative-ai_en
- https://www.edps.europa.eu/system/files/2024-06/EDPS-2024-09-Generative-AI-guidelines_EN.pdf
- https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checklist_LLM_Chatbots_EN.pdf
- https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf
- https://www.cnil.fr/fr/webform/questionnaire-sur-lapplication-du-rgpd-aux-modeles-dia-questionnaire-application-gdpr-ai-models
- https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en

Ευχαριστώ πολύ για την προσοχή σας !