Τεχνητή Νοημοσύνη
και
Γενικός Κανονισμός Προστασίας Δεδομένων

Λίλιαν Μήτρου

Καθηγήτρια Πανεπιστημίου Αιγαίου – Δικηγόρος
Πρόεδρος του Ινστιτούτου για το Δίκαιο Προστασίας της Ιδιωτικότητας, των Προσωπικών Δεδομένων και την Τεχνολογία.

L.mitrou@aegean.gr

Τεχνητή νοημοσύνη ως «ρουτίνα»;

- Βασικός πυλώνας και μοχλός της 4ης Βιομηχανικής Επανάστασης σε διάδραση με τα Big Data και το Διαδίκτυο των Πραγμάτων.
- Η σχετική έρευνα δεν οδηγείται πλέον πρωτίστως από την επιστημονική περιέργεια αλλά από οικονομικές και κοινωνικές απαιτήσεις.
- Η διαθεσιμότητα και επεξεργασία ασύλληπτης ποσότητας δεδομένων διανοίγει νέες τεχνολογικές δυνατότητες και προοπτικές
- Αγγίζει και αφορά πλέον τον «μέσο χρήστη»: μέσω της προσβασιμότητας σε φθηνή, τεράστια υπολογιστική ισχύ και σύνδεση οι άνθρωποι χρησιμοποιούν πλέον εφαρμογές τεχνητής νοημοσύνης στην καθημερινότητά τους (personal assistants, facial and pattern recognition).

Τεχνητή νοημοσύνη και προσωπικά δεδομένα

- Οι σχετικές εφαρμογές είναι σχεδιασμένες ώστε, μεταξύ άλλων, να αξιολογούν και να προδιαγιγνώσκουν συμπεριφορές, προτιμήσεις, επιδόσεις των προσώπων.
- Κατάρτιση προφίλ υποψήφιου δανειολήπτη, υπό εξέταση ασφαλισμένου, καταναλωτή στους τομείς των τραπεζικών ή ασφαλιστικών υπηρεσιών ή του μάρκετιγκ
- Ανάλυση/ Κατηγοριοποίηση ως υποστήριξη ή αντικατάσταση μίας διαδικασίας λήψης αποφάσεων

“Νέα μυθολογία” ή “νέα δυστοπία”;

- Η προσφορά και η χρήση υπηρεσιών κι εφαρμογών προϋποθέτει ή και δημιουργεί διαρκώς νέες προσωπικές πληροφορίες
- Τα προσωπικά δεδομένα και η Τεχνητή Νοημοσύνη είναι διπλής κατεύθυνσης: τα προσωπικά δεδομένα τροφοδοτούν την Τεχνητή Νοημοσύνη και αυτή παράγει περισσότερα δεδομένα
- *Επιταχύνει η Τεχνητή Νοημοσύνη την αμφισβήτηση της προστασίας δεδομένων και της ρυθμιστικής επάρκειας των κανονιστικών εργαλείων της;*

Ο ΓΚΠΔ και η Τεχνητή Νοημοσύνη

- Οι απαιτήσεις του ΓΚΠΔ αφορούν τόσο τη φάση της ανάπτυξης της ΤΝ όσο και τη χρήση της για την ανάλυση και τη λήψη αποφάσεων σε σχέση με πρόσωπα.
- Διεύρυνση (ή και μη προδιαγνωσιμότητα) των (δυνατοτήτων και) σκοπών επεξεργασίας ως εγγενές χαρακτηριστικό της ανάλυσης μέσω ΤΝ που ανευρίσκει νέες συσχετίσεις ή δημιουργεί νέους τύπους/ κατηγορίες δεδομένων
- Αρχή της ελαχιστοποίησης (as few data as possible) ως όριο ή εμπόδιο στο τι μπορεί να παράξει ή να μάθει ο αλγόριθμος;

Η τεχνητή νοημοσύνη ως black box και η θεμιτή επεξεργασία

- Ένα από τα μείζονα ζητήματα είναι η «αδιαφάνεια» που χαρακτηρίζει τις εφαρμογές της ΤΝ.
- Δύσκολο να εξηγήσει και να κατανοήσει κανείς αυτά τα «μαύρα κουτιά», τον εσωτερικό τρόπο λειτουργίας και τη λογική λήψης αποφάσεων, που βασίζεται σε αλγόριθμους και στατιστικούς συσχετισμούς δεδομένων.
- Η έλλειψη διαφάνειας εγείρει ζητήματα θεμιτής επεξεργασίας και λογοδοσίας
- Ενσωμάτωση προκαταλήψεων στις μεθόδους και το αντικείμενο της ανάλυσης αλλά και τις πηγές των δεδομένων

Είναι η τεχνητή νοημοσύνη (επ)εξηγήσιμη);

- Το δικαίωμα (και υποχρέωση) της ενημέρωσης (φαίνεται να) είναι δυσχερώς εφαρμόσιμο στο πλαίσιο της τεχνητής νοημοσύνης
- Ανάγκη κατανόησης της λογικής, των σκοπών και των αποτελεσμάτων της επεξεργασίας.
- Σε συνδυασμό με το αίτημα της «ανθρώπινης παρέμβασης» όταν οι αποφάσεις «παράγουν έννομα αποτελέσματα» ή «επηρεάζουν σημαντικά» ένα πρόσωπο
- Πόσο είναι εφικτή αλλά και χρήσιμη η εκτενής και αναλυτική τεχνική πληροφορία;
- Αναπόδραστη η ασυμμετρία γνώσης και κατανόησης;

Η τεχνολογική ουδετερότητα του ΓΚΠΔ

- Ο ΓΚΠΔ δεν ρυθμίζει ειδικά την επεξεργασία μέσω ΤΝ
- Τεχνολογικά ουδέτερο κείμενο
- Η έμφαση δεν τίθεται στην τεχνολογική υποδομή αλλά στα αποτελέσματά της, τους κινδύνους και τις επιπτώσεις στα δικαιώματα
- Ο ΓΚΠΔ διαθέτει την απαραίτητη ευελιξία αλλά κι εκείνα τα εργαλεία που επιτρέπουν να επιτυγχάνεται η απαιτούμενη ισορροπία μεταξύ της προστασίας των δικαιωμάτων και της τεχνολογικής και οικονομικής εξέλιξης

Τα εργαλεία του ΓΚΠΔ

- Το πλέον σημαντικό είναι η εκτίμηση αντικτύπου της επεξεργασίας δεδομένων που πρέπει να διενεργείται, όταν πρόκειται να σχεδιαστούν ή να υιοθετηθούν τεχνολογικές εφαρμογές «υψηλού κινδύνου».
- Προστασία δεδομένων by design: εντοπισμός κανονιστικών απαιτήσεων, σχεδιασμός και ανάπτυξη συστημάτων και εφαρμογών τεχνητής νοημοσύνης διασφαλίζοντας σύννομη και θεμιτή χρήση και σεβασμό δικαιωμάτων.

Νόμος και ethics

- Η λογοδοσία και η διαφάνεια θέτουν αναμφίβολα απαιτήσεις τεχνικού χαρακτήρα για τον μετριασμό των κινδύνων
- Ωστόσο η προστασία δεδομένων, η προστασία δικαιωμάτων, έστω by design, δεν είναι τεχνικό ζήτημα
- Αφορά την προστασία αξιών, αρχών δικαιωμάτων που πρέπει να συμπροσδιορίζουν την ανάπτυξη και χρήση ΤΝ.
- Η έμφαση στην ηθική δέσμευση, στα ethics που παρατηρείται τελευταία μπορεί να ενισχύει αλλά δεν (πρέπει να) υποκαθιστά τη συμμόρφωση προς τον νόμο.

Για μία πληρέστερη ανάλυση

- Lilian Mitrou, Data protection, Artificial Intelligence and cognitive services - Is the general data protection regulation (GDPR) “artificial intelligence-proof” ? March 2019 (**https://lnkd.in/d8nKeA8**)
- Απ. Βορράς και Λ. Μήτρου, Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, ΔΙΜΕΕ 4/2018, 460-466
- Ap. Vorras and L. Mitrou, Regulation and Policy in the Algorithmic Society, ICIL 2019 (to be published)

Σας ευχαριστώ

για την προσοχή σας