



# Η “ρύθμιση” της Τεχνητής Νοημοσύνης ή το δίλημμα του Collingridge

Λίλιαν Μήτρου  
Καθηγήτρια Πανεπιστημίου Αιγαίου  
Πρόεδρος του Ινστιτούτου για την  
Ιδιωτικότητα, την Προστασία Δεδομένων  
και την Τεχνολογία

# Η Τεχνητή Νοημοσύνη ως καθημερινότητα;

- ▶ Βασικός πυλώνας και μοχλός της 4<sup>ης</sup> Βιομηχανικής Επανάστασης σε διάδραση με τα Δεδομένα Μεγάλης Κλίμακας (Big Data) και το Διαδίκτυο των Πραγμάτων (IoT).
- ▶ Η διαθεσιμότητα και επεξεργασία ασύλληπτης ποσότητας δεδομένων διανοίγει νέες τεχνολογικές δυνατότητες και προοπτικές
- ▶ Αγγίζει και αφορά πλέον όλο και περισσότερο 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).





# Νομικά/ Ερμηνευτικά κενά και ανασφάλεια (δικαίου);

- ▶ Η Τεχνητή Νοημοσύνη και η Ρομποτική εξελίσσονται με πολύ μεγαλύτερη ταχύτητα από τη διαδικασία διατύπωσης των ζητημάτων και της αναζήτησης απαντήσεων στα ηθικά, νομικά και κοινωνικά ερωτήματα που τίθενται.
- ▶ Το κανονιστικό πλαίσιο εξ ορισμού υπολείπεται σε ταχύτητα εξέλιξης σε σχέση με την τεχνολογία που καλείται να οριοθετήσει/ρυθμίσει
- ▶ Νομικά/ ερμηνευτικά κενά
- ▶ Ανασφάλεια (δικαίου;) και έλλειψη εμπιστοσύνης ως προς την προστασία δικαιωμάτων / συμφερόντων και την ασφάλεια.



# Ηθικές και κανονιστικές απαιτήσεις

- ▶ Εμπλοκή του ανθρώπινου παράγοντα/ Ανθρώπινη παρέμβαση και εποπτεία
- ▶ Τεχνική στιβαρότητα και ασφάλεια
- ▶ Προστασία δεδομένων και διαχείριση της πληροφορίας
- ▶ Διαφάνεια
- ▶ Πολυμορφία, απαγόρευση διακρίσεων και θεμιτός χαρακτήρας (fairness)
- ▶ Κοινωνική και περιβαλλοντική ευημερία
- ▶ Λογοδοσία



## ΤΝ και προσωπικά δεδομένα: “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 τεχνολογική ουδετερότητα του Γενικού Κανονισμού Προστασίας Δεδομένων

- ▶ Ο ΓΚΠΔ δεν ρυθμίζει ειδικά την επεξεργασία με τη χρήση Τεχνητής Νοημοσύνης
- ▶ Τεχνολογικά ουδέτερο κείμενο
- ▶ Μία συνειδητή απόφαση προκειμένου να αντιμετωπιστεί η έλλειψη προδιαγνωσιμότητας των τεχνολογικών εξελίξεων (και αναταραχών) και να διασφαλιστεί η βιωσιμότητα της νομοθεσίας.
- ▶ Η έμφαση δεν τίθεται στην τεχνολογική υποδομή αλλά στα αποτελέσματά της, τους κινδύνους και τις επιπτώσεις στα δικαιώματα



# Χρειάζεται αναθεώρηση ο ΓΚΠΔ;

- ▶ Ο ΓΚΠΔ διατυπώνει γενικές αρχές και απαιτήσεις (σκοπός, αναλογικότητα, διαφάνεια, λογοδοσία) ανοιχτές στην ερμηνεία και την εξέλιξη
- ▶ Καινοτόμα κανονιστικά εργαλεία/ μοντέλα όπως η προστασία δεδομένων by design ή η εκτίμηση επιπτώσεων μπορεί να χρησιμεύσουν ώστε να αντιμετωπιστεί προληπτικά σε μη προβλεφθείσες ή μη προβλέψιμες τεχνολογικές προκλήσεις ή/και να περιοριστούν/ μετριαστούν οι σχετικοί κίνδυνοι
- ▶ EDPB: εστίαση στην ανάπτυξη των υφιστάμενων κανόνων για τη διαφάνεια, τη λογοδοσία και την εκτίμηση επιπτώσεων της επεξεργασίας στην προστασία δεδομένων





# Το δίλημμα του Collingridge

- ▶ Χρειάζεται η “ρύθμιση” της ΤΝ την επεξεργασία νέων λύσεων ή νέων κανόνων;
- ▶ Η μεταρρύθμιση ως παγίδα: ένας φαύλος κύκλος τεχνολογικών εξελίξεων που σημειώνονται ήδη κατά τη φάση της εκπόνησης των κανόνων - Αμφίπλευρος κίνδυνος ανασφάλειας δικαίου
- ▶ “Collingridge dilemma”:
  - ▶ κατά τα αρχικά στάδια μίας νέας τεχνολογίας, η νομοθέτηση είναι δυσχερής καθώς δεν υπάρχει επαρκής γνώση/ πληροφόρηση/ συνείδηση των ζητημάτων
  - ▶ Όταν αναδεικνύονται οι ανεπιθύμητες επιπτώσεις της τεχνολογίας, έχει διεισδύσει τόσο στη ζωή και την οικονομία που κάθε απόπειρα ρυθμιστικού ελέγχου συναντά την αντίδραση των προσώπων που την αναπτύσσουν, τους επενδυτές αλλά και τους ίδιους τους χρήστες
- ▶ EDPB : Η πρόσθετη νομοθέτηση στον τομέα των προσωπικών δεδομένων προκειμένου να «αντιμετωπιστεί» μία ειδική τεχνολογία θα ήταν «πρώιμη»
  - ▶ Απαιτείται κυρίως η εφαρμογή του νόμου και η δημόσια συζήτηση



# Οι εγγενείς δυσχέρειες της ρύθμισης της TN

- ▶ Μη αποτελεσματική εφαρμογή της ισχύουσας νομοθεσίας
- ▶ Μεταβαλλόμενη λειτουργικότητα των συστημάτων TN
- ▶ Αβεβαιότητα και αλλαγές αναφορικά με την αντίληψη της «ασφάλειας» ως προς τη χρήση συστημάτων TN
  - ▶ θα συμπεριλάμβανε μία τέτοια ρύθμιση : αλλαγές αναφορικά με τα ζητήματα ασφάλειας και ευθύνης για τα προϊόντα της Τεχνητής Νοημοσύνης (General Product Safety Directive, Machinery Directive κλπ.) ή θα έπρεπε να στραφεί κανείς σε νέες κατηγορίες ρυθμίσεων
- ▶ One size does not fit for all: η επιλογή του κανονιστικού εργαλείου και η επιλογή της έντασης της επέμβασης εξαρτάται από τον τύπο του συστήματος, το πεδίο εφαρμογής και τον βαθμό/ αξιολόγηση του κινδύνου και των δικαιωμάτων και εννόμων συμφερόντων που διακυβεύονται
- ▶ Αβεβαιότητα ως προς τον προσδιορισμό της ευθύνης και των υπευθύνων στην αλυσίδα της παροχής υπηρεσιών/ εφαρμογών/ συστημάτων TN



# Ποιο το πεδίο μίας μελλοντικής ρύθμισης;

- ▶ Προαπαιτούμενο: η διευκρίνιση των βασικών στοιχείων που συναποτελούν την ΤΝ, δηλ. δεδομένα και αλγοριθμοί
- ▶ Τα πεδία που ήδη υπόκεινται σε - οριζόντιου ή κάθετου χαρακτήρα - ρυθμίσεις, θα πρέπει να εξακολουθήσουν να διέπονται από αυτές
- ▶ [Στον βαθμό/ στην έκταση που απαιτείται ] το νέο κανονιστικό πλαίσιο της ΤΝ θα πρέπει να είναι σε θέση να επιτύχει τους ρυθμιστικούς στόχους χωρίς να είναι υπέρμετρα (και λεπτομερώς) «ρυθμιστικά» προκαλώντας δυσανάλογο βάρος συμμόρφωσης
- ▶ Η αναλογικότητα στην έκταση της ρύθμισης απαιτεί μια αξιολόγηση του είδους και του ύψους των κινδύνων που συνεπάγονται οι εκάστοτε εφαρμογές ΤΝ
  - ▶ Εκτίμηση επιπτώσεων της ΤΝ αλλά και της ρύθμισης



# Ανοιχτά ερωτήματα/1

- ▶ Εμείς (μπορούμε) να σχεδιάσουμε κανονιστικά το μέλλον για την Τεχνητή Νοημοσύνη; Ή μήπως η Τεχνητή Νοημοσύνη έχει ήδη σχεδιάσει ή σχεδιάζει, προδιαγράφει το μέλλον;
- ▶ [Αναγκαίο] Ταντάλειο έργο ή [μάταια] Σισύφεια προσπάθεια;
- ▶ Είναι εφικτή η ρύθμιση της τεχνολογικής εξέλιξης ;
- ▶ Είναι ζήτημα ευρωπαϊκής ρύθμισης τη στιγμή που η Τεχνητή Νοημοσύνη, όπως κάθε τεχνολογία εξελίσσεται και αναπτύσσεται σε παγκόσμιο επίπεδο;



## Ανοιχτά ερωτήματα/2

- ▶ Η ερώτηση της Γκρέτε :Είναι επιθυμητή μίας τέτοια ρύθμιση; Πως θα επιδρούσε η ρύθμιση στην εξέλιξη;
  - ▶ Μήπως θα ήταν ένα «θεσμικό εμπόδιο» που θα άφηνε την Ευρώπη πίσω από τους άλλους παγκόσμιους παίκτες;
  - ▶ Ή μήπως αυτή είναι η προστιθέμενη αξία, η αξιακή διαφορά της Ευρώπης



# Οι δημοκρατικές δεσμεύσεις και η ηθική της τεχνητής νοημοσύνης

- ▶ Ποιες πολιτικές απαιτούνται ώστε αφενός να προσδιοριστούν και να αξιοποιηθούν οι ευκαιρίες της Τεχνητής Νοημοσύνης και αφετέρου να εξασφαλιστεί ότι η ανάπτυξη αυτή θα ενισχύσει την ευημερία της κοινωνίας και όχι ανισότητες ; Ότι θα σεβαστεί τα δικαιώματα των πολιτών και τα έννομα συμφέροντα των καταναλωτών και δεν θα οδηγήσει σε περιορισμούς αυτών;
- ▶ Ποιος είναι ο ρόλος και η ευθύνη των παραγωγών τεχνολογίας και εφαρμογών τεχνητής νοημοσύνης; Μπορεί να διαμορφωθεί μία ηθική της τεχνητής νοημοσύνης (artificial intelligence ethics) κατ' αναλογία και κατ' εξέλιξη της ψηφιακής ηθικής (digital ethics);



Ευχαριστώ για  
▶ την προσοχή σας

Λίλιαν Μήτρου  
Πανεπιστήμιο Αιγαίου