

# Τεχνητή Νοημοσύνη και νομικά θέματα προστασίας Δεδομένων Προσωπικού Χαρακτήρα μετά τη θέση σε εφαρμογή του ΓΚΠΔ και του νόμου 4624/2019

## Κωνσταντίνος Λαμπρινουδάκης

Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς  
Μέλος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[clam@unipi.gr](mailto:clam@unipi.gr)

## Εμμανουήλ Δημογεροντάκης

Δικηγόρος, L.L.M

(Αν.) Μέλος Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

[m.Dimogerontakis@legalshield365.com](mailto:m.Dimogerontakis@legalshield365.com)

*28 Ιανουαρίου 2020*



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Τεχνητή Νοημοσύνη

- Η Τεχνητή Νοημοσύνη (AI) είναι η έννοια που χρησιμοποιείται για να περιγράψει συστήματα υπολογιστών που μπορούν να μάθουν από τις δικές τους εμπειρίες και να λύσουν πολύπλοκα προβλήματα σε διαφορετικές καταστάσεις.....
- .....και είναι δεδομένα, **σε πολλές περιπτώσεις προσωπικά δεδομένα**, που τροφοδοτούν αυτά τα συστήματα, επιτρέποντάς τους να μάθουν και να γίνουν έξυπνα

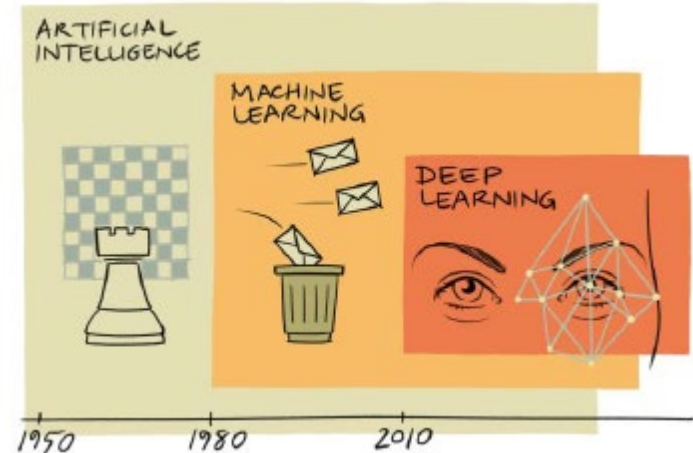


ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Μηχανική Μάθηση

- Η τεχνητή νοημοσύνη είναι ένας όρος ομπρέλα που εμπεριέχει πολλούς διαφορετικούς τύπους μηχανικής μάθησης.
- Η μηχανική μάθηση μπορεί να περιγραφεί ως «ένα σύνολο τεχνικών και εργαλείων που επιτρέπουν στους υπολογιστές να 'σκέφτονται' δημιουργώντας αλγορίθμους βασισμένους σε συσσωρευμένα δεδομένα».

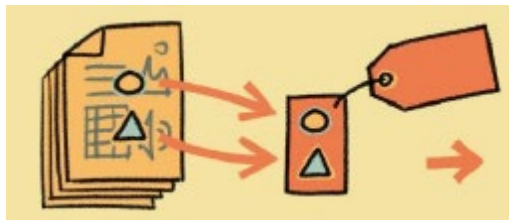


- Το σύστημα μπορεί να φθάσει σε μια κατάσταση που ενεργεί ανεξάρτητα από την ανθρώπινη είσοδο και μπορεί να κατασκευάσει το ίδιο νέους αλγορίθμους

# Μέχρι σήμερα.....

## Εποπτευόμενη Μάθηση

- Η εποπτευόμενη μάθηση περιλαμβάνει τη χρήση ετικετών δεδομένων, μέσω των οποίων γίνεται η επίβλεψη.
- Τα δεδομένα κατάρτισης μπορούν για παράδειγμα να αποτελούνται από εικόνες και ετικέτες με πληροφορίες για το περιεχόμενο κάθε εικόνας.

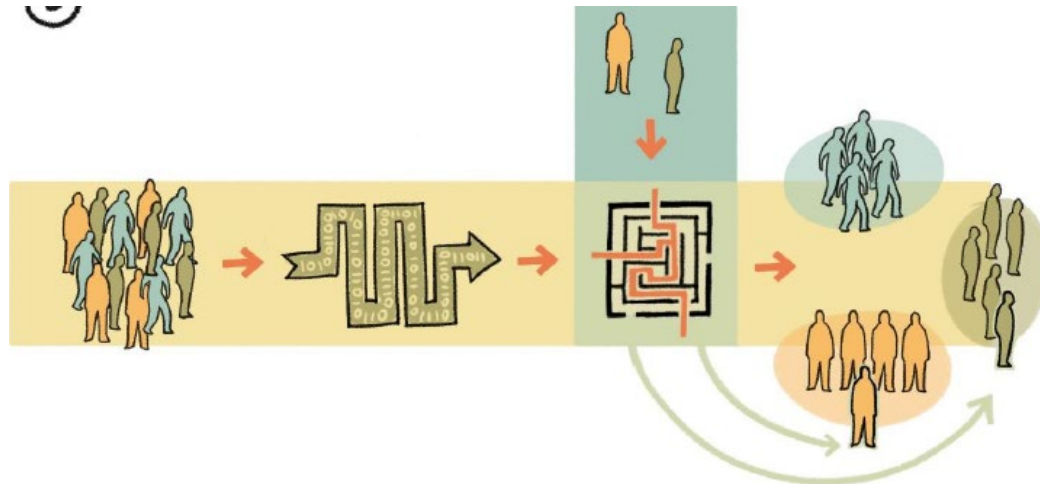


→ Cat

# Μέχρι σήμερα.....

## Μη Εποπτευόμενη Μάθηση

- Σε μη εποπτευόμενη μάθηση, χρησιμοποιούνται δεδομένα που δεν έχουν επισημανθεί εκ των προτέρων, καθώς στόχος είναι το σύστημα να ομαδοποιεί παρόμοια δεδομένα.



# Σήμερα.....

## Ενισχυτική Μάθηση

- Αυτή η μορφή μάθησης βασίζεται σε δοκιμές και σφάλματα, καθώς και στη βελτιστοποίηση, καθώς το μοντέλο μαθαίνει ποιες ενέργειες βοηθούν στην επίτευξη του στόχου. Αυτό σημαίνει ότι απαιτούνται λιγότερα δεδομένα, ή καθόλου δεδομένα, για να μάθει το σύστημα.



# Σήμερα.....

## Ενισχυτική Μάθηση

Βασικές έννοιες που αφορούν την ΕΜ είναι οι εξής:

- η πολιτική (policy)
- η συνάρτηση ανταμοιβής (reward function)
- η συνάρτηση αξίας (value function) και
- (προαιρετικά) το μοντέλο του περιβάλλοντος (environment model)



# Ενισχυτική Μάθηση - Πολιτική

- Η πολιτική ορίζει τον τρόπο συμπεριφοράς του πράκτορα ανά δεδομένη χρονική στιγμή καθώς είναι μια αντιστοίχιση των καταστάσεων (states) ή παρατηρήσεων (observations) που αντιλαμβάνεται ο πράκτορας, με τις ενέργειες (actions) που επιλέγει όταν βρίσκεται σε αυτές.
- Η πολιτική ουσιαστικά αποτελεί τον πυρήνα ενός πράκτορα ΕΜ, καθώς υπό μία έννοια, από μόνη της αρκεί για να καθορίσει την συμπεριφορά του.



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)



# Ενισχυτική Μάθηση - Ανταμοιβή

- Η συνάρτηση ανταμοιβής αντιστοιχίζει κάθε κατάσταση (ή και ζεύγος κατάστασης-ενέργειας) του περιβάλλοντος, σε έναν αριθμό, την ανταμοιβή (reward), που δηλώνει πόσο επιθυμητό είναι να βρισκόμαστε στην κατάσταση αυτή (ή να επιλέγουμε την συγκεκριμένη ενέργεια, βρισκόμενοι στην συγκεκριμένη κατάσταση, αντίστοιχα)
- Η μοναδική αποστολή ενός πράκτορα EM είναι η μεγιστοποίηση της συνολικής ανταμοιβής που λαμβάνει μακροπρόθεσμα
- Ο πράκτορας μπορεί να βασιστεί στην συνάρτηση ανταμοιβής για να αλλάξει την πολιτική του.



# Ενισχυτική Μάθηση - Αξία

- Σε αντίθεση με την συνάρτηση ανταμοιβής που καθορίζει τι είναι καλό άμεσα, μια συνάρτηση αξίας καθορίζει τι είναι καλό μακροπρόθεσμα. Η αξία μιας κατάστασης ορίζεται ως το συνολικό ποσό ανταμοιβής που μπορεί να συγκεντρώσει μελλοντικά ο πράκτορας, ξεκινώντας από αυτή την κατάσταση.
- Η αξία μιας κατάστασης καταδεικνύει πόσο επιθυμητή είναι μια κατάσταση μακροπρόθεσμα, λαμβάνοντας υπ' όψιν τις καταστάσεις που θα ακολουθήσουν και τις διαθέσιμες ανταμοιβές που μπορούν να ληφθούν κατά τη μετάβαση, από και προς αυτές.
  - Για παράδειγμα, μπορεί μια κατάσταση να επιφέρει πάντα μικρή ανταμοιβή, ωστόσο η αξία της μπορεί να είναι μεγάλη, επειδή συνήθως ακολουθείται από καταστάσεις που επιφέρουν μεγάλες ανταμοιβές (ή και το αντίστροφο).



# Ενισχυτική Μάθηση - Περιβάλλον

- Το μοντέλο του περιβάλλοντος, είναι μια τεχνητή (νοητή) οντότητα, που προσπαθεί να μιμηθεί την συμπεριφορά του περιβάλλοντος.
- Για παράδειγμα, δεδομένης μιας κατάστασης και μιας ενέργειας, το μοντέλο θα μπορούσε να χρησιμοποιηθεί για την πρόβλεψη της επόμενης ανταμοιβής.
- Τα μοντέλα χρησιμοποιούνται για την επιλογή συγκεκριμένων τρόπων δράσης (σχεδιασμός ενεργειών – planning), λαμβάνοντας υπόψη μελλοντικές καταστάσεις, πριν αυτές αντιμετωπιστούν από τον πράκτορα



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

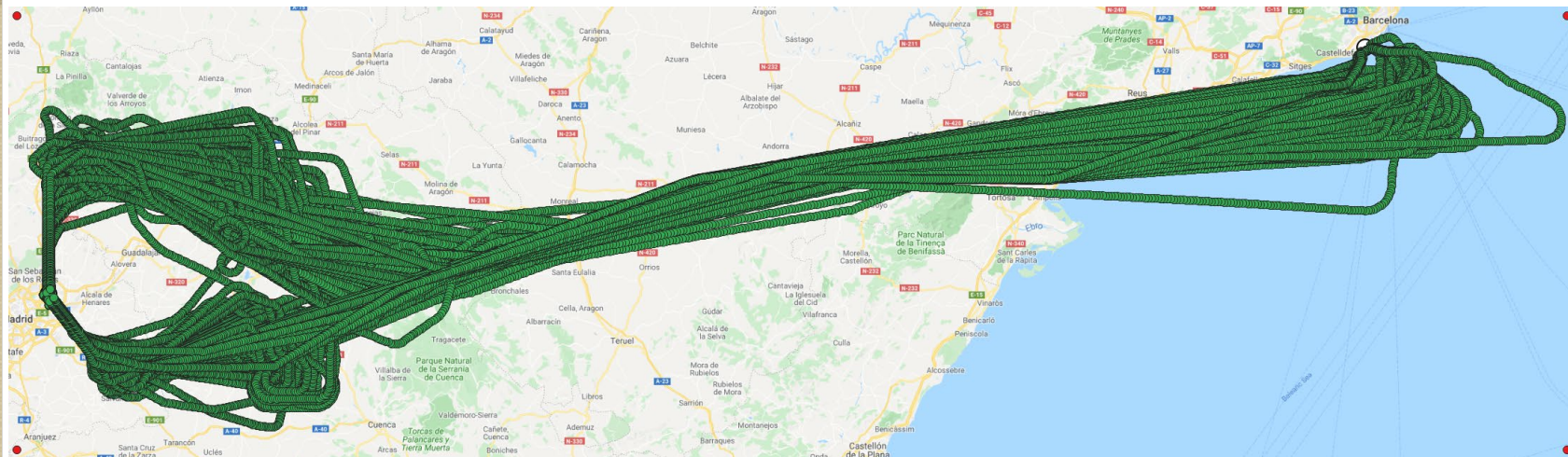
[www.dpa.gr](http://www.dpa.gr)

# Αποτελέσματα της Εκμάθησης

- Ανεξάρτητα από τους αλγορίθμους ή τις μεθόδους που χρησιμοποιούνται για την εκμάθηση μηχανών, το αποτέλεσμα θα είναι ένα "μοντέλο", το οποίο μπορεί στη συνέχεια να τροφοδοτηθεί με νέα δεδομένα για να παράγει τον επιθυμητό τύπο αποτελέσματος.
- Ένα μοντέλο μπορεί να χρησιμοποιηθεί με δύο τρόπους:
  - Τον **στατικό** που το μοντέλο θα λειτουργεί πάντοτε με τον ίδιο τρόπο και θα παράγει τα ίδια αποτελέσματα καθ' όλη τη διάρκεια του κύκλου ζωής του.
  - Η άλλη δυνατότητα παρέχεται από ένα **δυναμικό μοντέλο** το οποίο είναι σε θέση να χρησιμοποιήσει τα δεδομένα εισόδου για να βελτιώσει και να προσαρμοστεί στις αλλαγές.



# Παράδειγμα: Τροχιές Αεροπλάνων (Training set)



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Παράδειγμα: Τροχιές Αεροπλάνων (Clusters identified in the Training set)



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

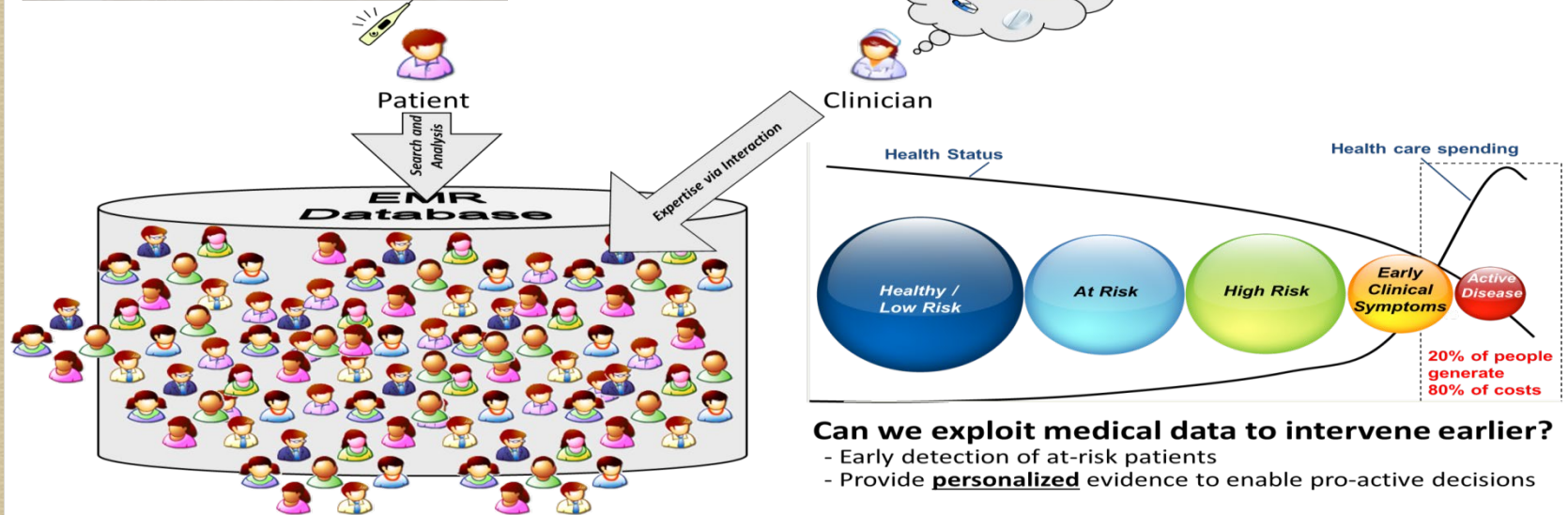
# Παράδειγμα: Τροχιές Αεροπλάνων (Πρόβλεψη Τροχιάς με αλγόριθμο Ενισχυτικής Μάθησης)



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Το Μοντέλο Παροχής Υπηρεσιών Υγείας .....



**Can we exploit medical data to intervene earlier?**

- Early detection of at-risk patients
- Provide **personalized** evidence to enable pro-active decisions



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

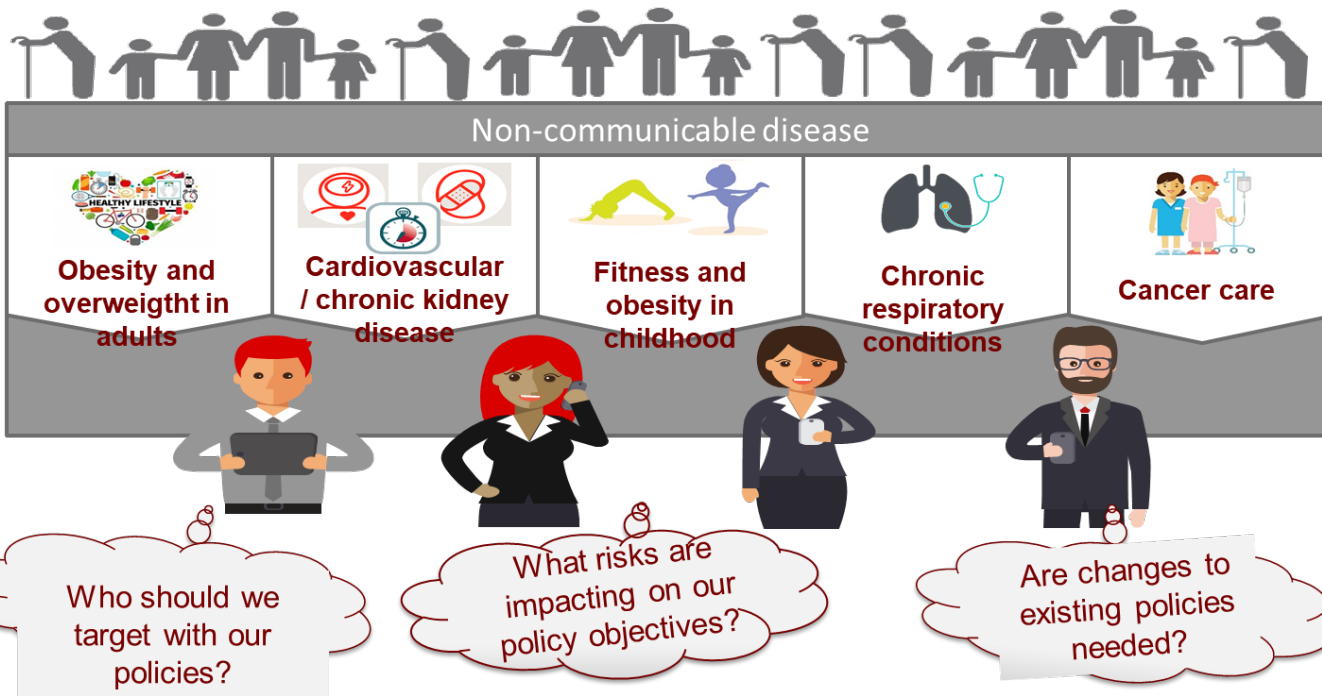
[www.dpa.gr](http://www.dpa.gr)





CrowdHEALTH

# Big Data Analytics to support Public Health Policies



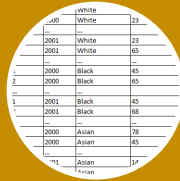
Kyriazis, et al, CrowdHEALTH: Holistic health records and big data analytics for health policy making and personalized health (2017) Studies in Health Technology and Informatics, 238, pp. 19-23.



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

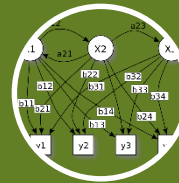
[www.dpa.gr](http://www.dpa.gr)

# Ανάπτυξη μοντέλου MM

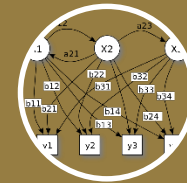


	white	
2000	White	23
2001	White	23
2001	White	65
2000	Black	45
2000	Black	65
2001	Black	45
2001	Black	68
2000	Asian	78
2000	Asian	85
2001	Asian	71
2001	Asian	71

Dataset



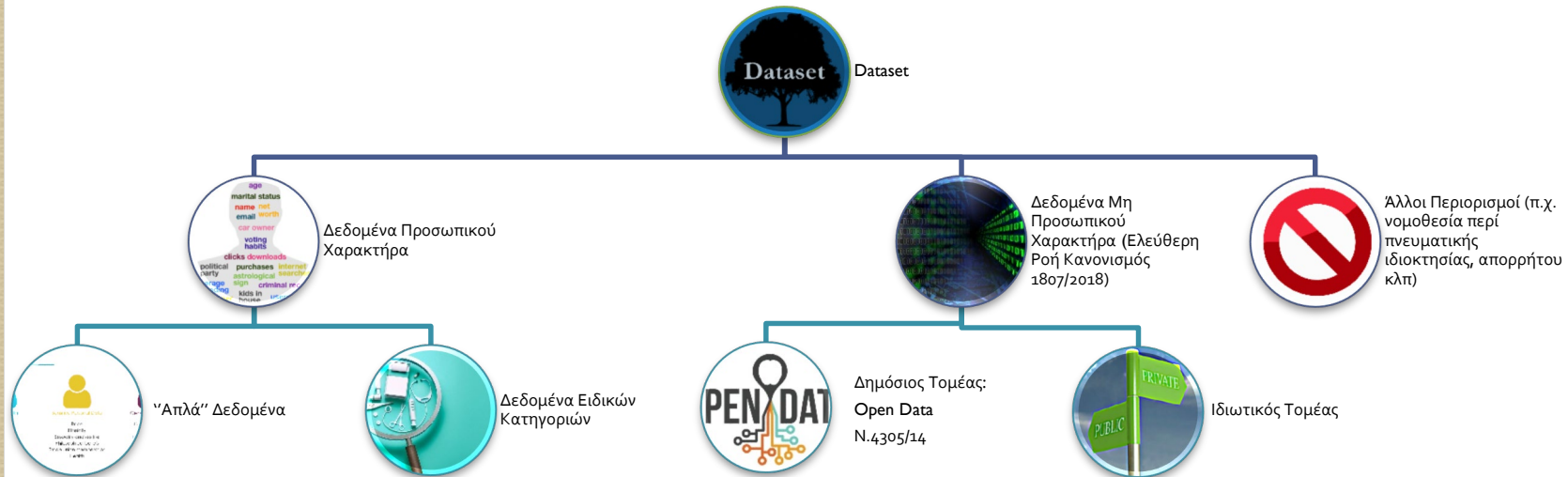
Σχεδιασμός  
Μοντέλου  
Μηχανικής Μάθησης



Λειτουργία –  
Αποτέλεσμα



# Αρχικό Dataset



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Πότε είναι νόμιμη η Συλλογή των δεδομένων του Dataset;

## ΓΕΝΙΚΕΣ ΑΡΧΕΣ

Περιορισμού του σκοπού

Ελαχιστοποίησης Δεδομένων

Περιορισμού χρόνου αποθήκευσης

Συγκατάθεση

Σύμβαση

Ένομη Υποχρέωση ΥΕ

Δημόσιο Συμφέρον/ Δημόσια Εξουσία

Ζωτικό Συμφέρον Υποκειμένου

Όταν έχουν συλλεγεί για άλλον σκοπό από αυτόν για τον οποίο θέλουμε να τα επεξεργαστούμε;

# Επεξεργασία για άλλον σκοπό από αυτόν που έχουν αρχικώς συλλεγεί



Συγκατάθεση Υποκειμένου

- Διακριτή θετική δήλωση ή πράξη
- Καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας
- Συγκατάθεση για όλους τους σκοπούς
- Ανακλητή όσο εύκολα δόθηκε



Προβλέπεται στο Εθνικό Δίκαιο ή Δίκαιο Ε.Ε.



Συμβατότητα σκοπών

- -Σχέση σκοπών συλλογής και περαιτέρω επεξεργασίας.
- - Πλαίσιο Συλλογής
- – Σχέση Υποκ. και ΥΕ
- - Φύση Δεδομένων
- - Κατάλληλες εγγυήσεις
- (ψευδωνυμοποίηση, κρυπτογράφηση)

Υπάρχει εξαίρεση στην συλλογή και επεξεργασία δεδομένων για σκοπούς έρευνας Α. 89 ΓΚΠΔ και Α. 30 Νόμου

4624/2019

1/30/2020

# Επεξεργασία για σκοπούς

# Επιστημονικής Έρευνας (Α. 89 ΓΚΠΔ και Α. 30

Νόμου 4624/2019)

- Κατά παρέκκλιση δυνατότητα επεξεργασίας δεδομένων ειδικών κατηγοριών χωρίς συγκατάθεση υποκειμένου.

- Μέτρα ασφαλείας (ιδίως ψευδωνυμοποίηση, Κρυπτογράφηση, ορισμός ΥΠΔ).
- Περιορισμός Δικαιωμάτων Υποκειμένων.
- Ρητή Υποχρέωση για ανωνυμοποίηση



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Νομιμότητα Επεξεργασίας – Σχεδιασμός μοντέλου

## Γενικές Αρχές Επεξεργασίας

Νόμιμη

Θεμιτή

Διαφανής

Ακεραιότητα και Εμπιστευτικότητα

Privacy by Design, Privacy by Default

ΛΟΓΟΔΟΣΙΑ

## Δικαιώματα Υποκειμένου

Διαφανούς ενημέρωσης

Πρόσβασης

Διόρθωσης και Διαγραφής

Περιορισμού και Φορητότητας

Εναντίωση σε κατάρτιση προφίλ



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Περιεχόμενο Διαφάνειας – Δικαιώματος ενημέρωσης και πρόσβασης – Αρχή Λογοδοσίας



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)



# Νομιμότητα Επεξεργασίας – Σχεδιασμός μοντέλου

- Risk based approachment (Υποχρεώσεις ανάλογες του ρίσκου που συνεπάγεται η επεξεργασία)
- Εκτίμηση Αντικτύπου
- Ιδιωτικότητα εκ σχεδιασμού (Privacy by Design)
- Ιδιωτικότητα εξ ορισμού (Privacy by Default)



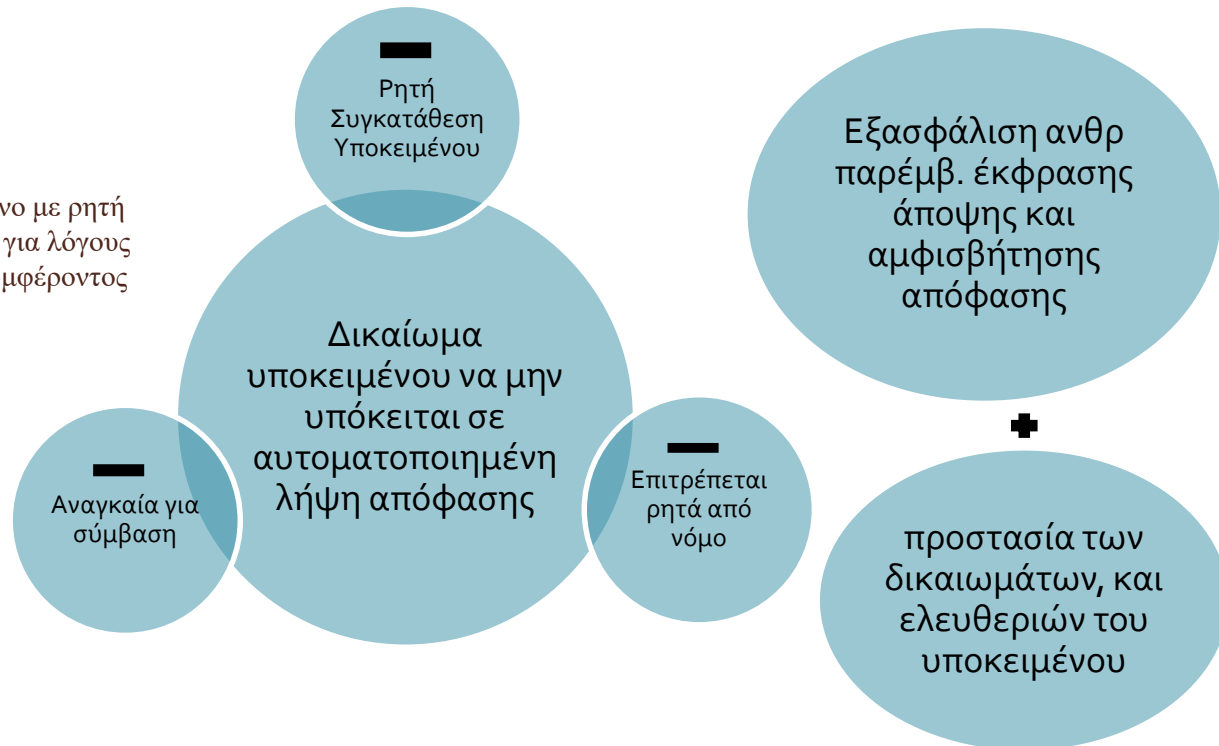
ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Λειτουργία Μοντέλου – Output

Λήψη Απόφασης χωρίς ανθρώπινη παρέμβαση;

Δεδομένα Ειδικών Κατηγοριών: Μόνο με ρητή συγκατάθεση, ή αν είναι απαραίτητη για λόγους επιδίωξης ουσιαστικού Δημοσίου Συμφέροντος



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Λειτουργία Μοντέλου – Output

## Υπό ρύθμιση ζητήματα.

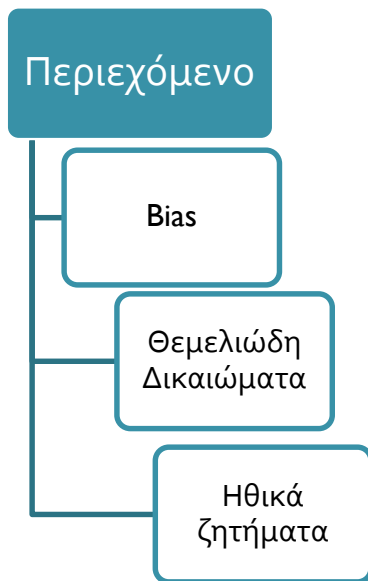
- BIAS - Διακρίσεις
- Θεμελιώδη Δικαιώματα
- Ηθικά ζητήματα



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

# Προτεινόμενη Ενίσχυση του ρόλου της εκτίμησης Κινδύνου και Αντικτύπου



# Βασικά σημεία προβληματισμού

## dataset

- Περιορισμός του σκοπού.
- Αρχή Ελαχιστοποίησης.
- Χρόνος αποθήκευσης.
- Περαιτέρω επεξεργασία για διαφορετικό σκοπό.

## Σχεδιασμός του μοντέλου

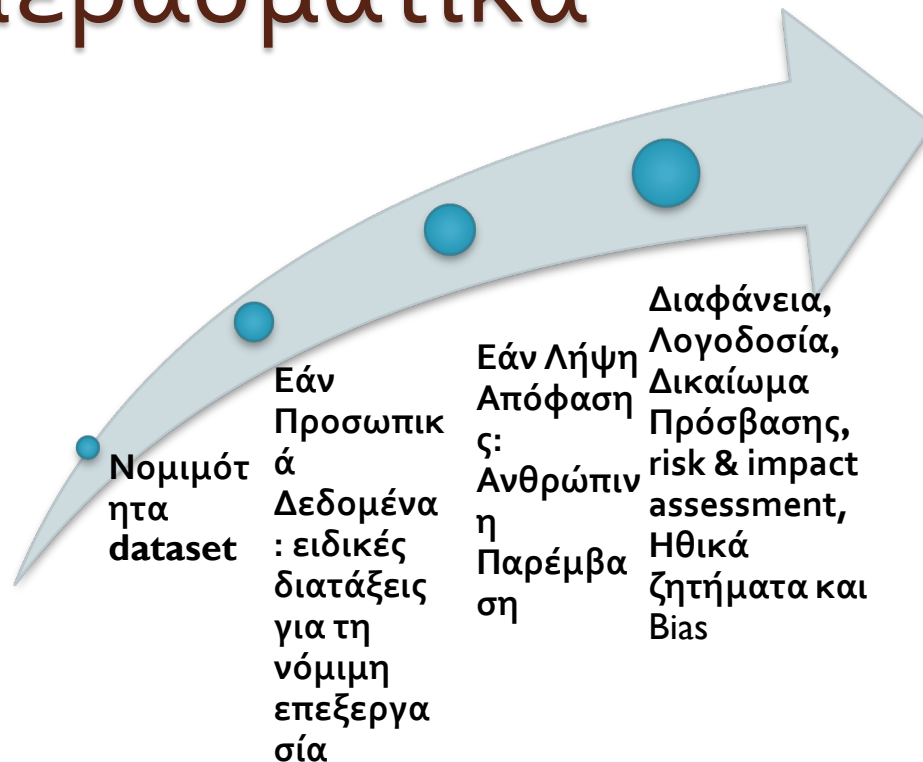
- Διαφάνεια
- Λογοδοσία
- Θεμιτή Επεξεργασία
- Privacy by design-by default
- Δικαίωμα Ενημέρωσης και Πρόσβασης
- Risk and Impact Assessment

## operation- output

- Το υποκείμενο να μην υπόκειται σε απόφαση κατόπιν αυτοματοποιημένης επεξεργασίας χωρίς προηγούμενη ανθρώπινη παρέμβαση.
- Algorithmic decision-making and fairness:
- Bias
- Ηθικά ζητήματα



# Συμπερασματικά



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

Ευχαριστούμε πολύ για την προσοχή σας!



ΑΡΧΗ  
ΠΡΟΣΤΑΣΙΑΣ  
ΔΕΔΟΜΕΝΩΝ  
ΠΡΟΣΩΠΙΚΟΥ  
ΧΑΡΑΚΤΗΡΑ

[www.dpa.gr](http://www.dpa.gr)

Ημερίδα ΑΠΔΠΧ

28/01/2020