

# Blockchain και Διαφάνεια στα Συστήματα Τεχνητής Νοημοσύνης

**Δέσποινα Δοξάκη**

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΟΥ ΔΙΚΑΙΟΥ  
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ & ΤΡΑΠΕΖΙΚΗΣ ΔΙΟΙΚΗΤΙΚΗΣ

Πανεπιστήμιο Πειραιώς  
17 Σεπτεμβρίου 2026



# Η διαφάνεια ως προϋπόθεση εμπιστοσύνης

## Πώς ελέγχουμε μια απόφαση ΤΝ που επηρεάζει τον άνθρωπο;

Υγεία

Πίστωση

Απασχόληση

Δικαιοσύνη

Η πολυπλοκότητα των μοντέλων δυσχεραίνει την κατανόηση και την αμφισβήτηση των αποτελεσμάτων τους.

# Τι είναι το blockchain

Ειδική μορφή τεχνολογίας κατανεμημένου καθολικού (DLT)

- |           |                                  |                                                                    |
|-----------|----------------------------------|--------------------------------------------------------------------|
| <b>01</b> | <b>Κατανεμημένη<br/>τήρηση</b>   | Πολλοί κόμβοι διατηρούν και συγχρονίζουν το καθολικό.              |
| <b>02</b> | <b>Κρυπτογραφική<br/>σύνδεση</b> | Κάθε συστοιχία συνδέεται με το αποτύπωμα της προηγούμενης.         |
| <b>03</b> | <b>Συναίνεση</b>                 | Το δίκτυο εφαρμόζει κανόνες για την επικύρωση των εγγραφών.        |
| <b>04</b> | <b>Επαληθεύσιμο<br/>ιστορικό</b> | Οι αλλοιώσεις γίνονται ανιχνεύσιμες υπό τις εγγυήσεις του δικτύου. |

# Οι διαστάσεις της διαφάνειας στην ΤΝ

## 01 Εξηγησιμότητα

Γιατί προέκυψε μια συγκεκριμένη απόφαση;

## 02 Ιχνηλασιμότητα

Ποια δεδομένα και ποια έκδοση μοντέλου χρησιμοποιήθηκαν;

## 03 Ελεγχιμότητα

Πώς ελέγχονται η ανάπτυξη και η λειτουργία του συστήματος;

## 04 Ενημέρωση

Γνωρίζει ο άνθρωπος ότι αλληλεπιδρά με ΤΝ ή συνθετικό περιεχόμενο;

# AI Act: οι υποχρεώσεις του άρθρου 50

Διαφορετικές υποχρεώσεις για παρόχους και φορείς εφαρμογής

| Υπόχρεος              | Αντικείμενο διαφάνειας                                                       |
|-----------------------|------------------------------------------------------------------------------|
| Πάροχος συστήματος    | Ενημέρωση για την άμεση αλληλεπίδραση με ΤΝ.                                 |
| Πάροχος γεννητικής ΤΝ | Μηχανικά αναγνώσιμη σήμανση και ανιχνευσιμότητα του συνθετικού περιεχομένου. |
| Φορέας εφαρμογής      | Γνωστοποίηση deepfakes και ορισμένων κειμένων δημόσιου ενδιαφέροντος.        |
| Φορέας εφαρμογής      | Ενημέρωση για αναγνώριση συναισθημάτων ή βιομετρική κατηγοριοποίηση.         |

Οι ειδικές εξαιρέσεις και οι προϋποθέσεις κάθε υποχρέωσης παραμένουν κρίσιμες.

# Χρόνος εφαρμογής και κυρώσεις

| Ημερομηνία               | Πεδίο εφαρμογής                                                                        |
|--------------------------|----------------------------------------------------------------------------------------|
| <b>2 Αυγούστου 2026</b>  | Έναρξη εφαρμογής των υποχρεώσεων του άρθρου 50.                                        |
| <b>2 Δεκεμβρίου 2026</b> | Ειδική μεταβατική περίοδος για τη σήμανση του άρθρου 50 §2 σε προϋφιστάμενα συστήματα. |
| <b>2 Δεκεμβρίου 2027</b> | Υποχρεώσεις για συστήματα υψηλού κινδύνου του Παραρτήματος III.                        |
| <b>2 Αυγούστου 2028</b>  | Υποχρεώσεις για συστήματα υψηλού κινδύνου ενσωματωμένα σε ρυθμιζόμενα προϊόντα.        |

**Άρθρο 99: έως €15 εκατ. ή 3% του παγκόσμιου ετήσιου κύκλου εργασιών.**

Για επιχειρήσεις λαμβάνεται το υψηλότερο όριο. Ειδικός κανόνας για ΜΜΕ: το χαμηλότερο.

# Τέσσερα πεδία συμπληρωματικότητας

| Πεδίο                | Τι μπορεί να τεκμηριώσει το blockchain               |
|----------------------|------------------------------------------------------|
| Δεδομένα εκπαίδευσης | Προέλευση, εκδόσεις και μετασχηματισμούς δεδομένων.  |
| Κύκλος ζωής μοντέλου | Αλλαγές, εγκρίσεις και αποτελέσματα αξιολόγησης.     |
| Διακυβέρνηση         | Κανόνες πρόσβασης και καταγραφή ενεργειών.           |
| Περιεχόμενο          | Δηλωμένη προέλευση και ακεραιότητα ψηφιακών αρχείων. |

Η αξία του έγκειται στη δυνατότητα επαλήθευσης από περισσότερους συμμετέχοντες.

# Ένα «διαβατήριο» δεδομένων εκπαίδευσης

Ενδεικτική εφαρμογή καταγραφής προέλευσης

- |           |                               |                                                       |
|-----------|-------------------------------|-------------------------------------------------------|
| <b>01</b> | <b>Ταυτοποίηση συνόλου</b>    | Πηγή, χρόνος συλλογής και όροι νόμιμης χρήσης.        |
| <b>02</b> | <b>Ψηφιακό αποτύπωμα</b>      | Υπολογισμός hash για συγκεκριμένη έκδοση δεδομένων.   |
| <b>03</b> | <b>Καταγραφή</b>              | Αποτύπωμα και αναγκαία μεταδεδομένα στο καθολικό.     |
| <b>04</b> | <b>Μεταγενέστερος έλεγχος</b> | Σύγκριση με το αρχείο που διατηρείται εκτός αλυσίδας. |

# Το αρχείο ελέγχου του μοντέλου

| Στάδιο                 | Ενδεικτικά στοιχεία καταγραφής                    |
|------------------------|---------------------------------------------------|
| Ανάπτυξη               | Έκδοση μοντέλου και αναφορά στο σύνολο δεδομένων. |
| Αξιολόγηση             | Δοκιμές, αποτελέσματα και γνωστοί περιορισμοί.    |
| Έγκριση και λειτουργία | Υπεύθυνος έγκρισης, χρόνος διάθεσης και συμβάντα. |
| Επικαιροποίηση         | Μεταβολές, νέα έκδοση και αιτιολογία αλλαγών.     |

Το ιστορικό βοηθά τον ελεγκτή να ανασυνθέσει την εξέλιξη του συστήματος.

# Έξυπνα συμβόλαια και διακυβέρνηση

## Αυτοματοποιημένοι κανόνες

Έλεγχος εξουσιοδοτήσεων

Καταγραφή παροχής ή ανάκλησης  
συναίνεσης

Καταγραφή χρήσης και εγκρίσεων

## Οργανωτική ευθύνη

Καθορισμός αρμοδιοτήτων

Έλεγχος εγκυρότητας των όρων

Διαδικασίες διόρθωσης και  
παρέμβασης

Ο κώδικας εκτελεί τον κανόνα που έχει οριστεί. Η νομιμότητά του απαιτεί χωριστό έλεγχο.

# Προέλευση και ακεραιότητα περιεχομένου

**Ποιος το εξέδωσε;  
Πώς μεταβλήθηκε;**

**Ψηφιακές υπογραφές  
Μεταδεδομένα προέλευσης  
Υδατογραφήματα και  
αποτυπώματα**

Το C2PA επιτρέπει επαληθεύσιμα στοιχεία προέλευσης.  
Η λειτουργία του δεν προϋποθέτει blockchain.

Η επαλήθευση προέλευσης δεν αποτελεί πιστοποίηση της αλήθειας του περιεχομένου.

# Τα όρια της τεχνικής καταγραφής

- 01 Ερμηνεία απόφασης** Το ιστορικό γεγονότων αφήνει ανοικτό το «γιατί» του αποτελέσματος.
- 02 Ποιότητα δεδομένων** Σφάλματα και μεροληψίες μπορούν επίσης να καταγραφούν.
- 03 Αξιοπιστία εισόδου** Η επαλήθευση εξαρτάται και από τον φορέα που εισάγει τα στοιχεία.
- 04 Κόστος και κλίμακα** Αποθήκευση, υπολογιστική ισχύς και διακυβέρνηση έχουν κόστος.

# Αμεταβλητότητα και προστασία δεδομένων

| Στην αλυσίδα (on-chain)                                            | Εκτός αλυσίδας (off-chain)                                     |
|--------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Μόνο όσα στοιχεία είναι αναγκαία για την επαλήθευση.</b>        | Αρχεία δεδομένων και αναλυτική τεκμηρίωση.                     |
| <b>Αποτυπώματα και περιορισμένα μεταδεδομένα, κατόπιν ελέγχου.</b> | Έλεγχος πρόσβασης, χρόνοι διατήρησης και μηχανισμοί διαγραφής. |
| <b>Αξιολόγηση κινδύνου ταυτοποίησης ή σύνδεσης με πρόσωπο.</b>     | Πρακτική δυνατότητα διόρθωσης και άσκησης δικαιωμάτων.         |

**Ένα hash μπορεί να παραμένει προσωπικό δεδομένο.**

ΓΚΠΔ: ελαχιστοποίηση, προστασία ήδη από τον σχεδιασμό, δικαιώματα διόρθωσης και διαγραφής.

# Πότε προσθέτει αξία το blockchain;

## 01 Κοινό αρχείο

Περισσότεροι φορείς χρειάζονται κοινό, επαληθεύσιμο ιστορικό.

## 02 Αποδεικτική ανάγκη

Η σειρά των γεγονότων και η ακεραιότητα έχουν ουσιαστική σημασία.

## 03 Αναλογικότητα

Το όφελος δικαιολογεί το κόστος και την πολυπλοκότητα.

## 04 Συνδυασμός μέσων

Τεχνικές εξηγησιμότητας, ανεξάρτητος έλεγχος και σαφείς ευθύνες.

AI Act και ΓΚΠΔ δεν επιβάλλουν γενική υποχρέωση χρήσης blockchain.

# Η ΤΝ ως ζήτημα χρηματοπιστωτικής σταθερότητας

## Συγκέντρωση παρόχων

Κοινά βασικά μοντέλα  
και υποδομές cloud

Μία αστοχία μπορεί να επηρεάσει  
πολλά ιδρύματα ταυτόχρονα.

## Συσχετισμένες αποφάσεις

Παρόμοια δεδομένα  
και αρχιτεκτονικές

Ταυτόχρονες αντιδράσεις μπορούν  
να εντείνουν τις διακυμάνσεις.

Τα προηγμένα μοντέλα ΤΝ αυξάνουν επίσης την ταχύτητα και την κλίμακα κυβερνοαπειλών.

# Η εποπτική και κανονιστική ανταπόκριση

| Πλαίσιο                        | Κύριο αντικείμενο                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------|
| <b>AI Act, άρθρα 51 και 55</b> | Ταξινόμηση και πρόσθετες υποχρεώσεις για μοντέλα γενικού σκοπού με συστημικό κίνδυνο.   |
| <b>DORA</b>                    | Διαχείριση κινδύνου ΤΠΕ και εποπτεία κρίσιμων τρίτων παρόχων.                           |
| <b>ESRB/2026/3</b>             | Προειδοποίηση της 25.06.2026 για συστημικούς κυβερνοκινδύνους από προηγμένα μοντέλα ΤΝ. |
| <b>EKT / SSM</b>               | Σχέδια δράσης σημαντικών ιδρυμάτων έως 31.10.2026 για τις εξελισσόμενες κυβερνοαπειλές. |

Η καταγραφή εξαρτήσεων βοηθά τον έλεγχο. Η συγκέντρωση και το herding απαιτούν ευρύτερη εποπτεία.

# Η διαφάνεια απαιτεί συνδυασμό εργαλείων

## Το blockchain μπορεί να προσφέρει επαληθεύσιμη τεκμηρίωση της λειτουργίας της ΤΝ.

Η ουσιαστική λογοδοσία προϋποθέτει επιπλέον:

**Εξηγησιμότητα**  
**Ποιότητα δεδομένων**

**Ανεξάρτητο έλεγχο**  
**Σαφή κατανομή ευθύνης**

# Επιλεγμένες πηγές

## Νομοθεσία

AI Act, Κανονισμός (ΕΕ) 2024/1689  
και Κανονισμός (ΕΕ) 2026/1744

ΓΚΠΔ, Κανονισμός (ΕΕ) 2016/679

DORA, Κανονισμός (ΕΕ) 2022/2554

N. 4961/2022, άρθρο 31

DLT Pilot Regime και MiCA  
Κανονισμοί (ΕΕ) 2022/858 και 2023/1114

## Ερμηνεία και ανάλυση

Ευρωπαϊκή Επιτροπή  
Κατευθυντήριες γραμμές για το άρθρο 50

EKT, Financial Stability Review  
The rise of artificial intelligence, 2024

ESRB/2026/3, 25 Ιουνίου 2026  
Συστημικοί κυβερνοκίνδυνοι από ΤΝ

Content Authenticity Initiative  
Τεκμηρίωση C2PA / Content Credentials

Αναλυτικές παραπομπές στις σημειώσεις των αντίστοιχων διαφανειών.