



ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»
Ακαδημαϊκό έτος 2025-2026

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
του Ραφαήλ-Νικόλαου Μανωλάκου (Α.Μ.: ΜΔΙ 2433)

[ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΗΝ ΨΗΦΙΟΠΟΙΗΣΗ ΤΗΣ
ΔΙΚΑΙΟΣΥΝΗΣ]

[CYBERSECURITY AND ARTIFICIAL INTELLIGENCE IN THE DIGITALIZATION OF
JUSTICE]

Επιβλέπουσα:

Λίλιαν Μήτρου, Καθηγήτρια Πανεπιστημίου Αιγαίου, Δικηγόρος

Πειραιάς, Απρίλιος 2026

Σε ό,τι με διαμόρφωσε και σε ό,τι βρίσκεται σταθερά δίπλα μου...

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ.....	6
ABSTRACT.....	8
ΚΕΦΑΛΑΙΟ Ι ΤΟ ΟΙΚΟΣΥΣΤΗΜΑ ΤΗΣ ΨΗΦΙΑΚΗΣ ΔΙΚΑΙΟΣΥΝΗΣ (E- JUSTICE)	10
1.1 Η έννοια και η εξέλιξη της ηλεκτρονικής δικαιοσύνης.....	10
1.1.1 Η μετάβαση από το φυσικό αρχείο στο ψηφιακό περιβάλλον	11
1.1.2. Ταχύτητα, διαφάνεια και προσβασιμότητα στα πλαίσια διασυνοριακής διαλειτουργικότητας	12
1.2 Διασυνοριακή λειτουργικότητα	13
1.2.1. EUR-Lex	13
1.2.3 N-Lex.....	14
1.2.3. eu-LISA.....	14
1.2.4. e-CODEX.....	15
1.2.5. ECRIS	16
1.2.6 Το Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων (ΟΣΔΔΥ-ΔΔ)	18
1.2.7 Ηλεκτρονική κατάθεση δικογράφων στην Ελλάδα	18
1.2.8 Εφαρμογή παρακολούθησης Δικών	19
ΚΕΦΑΛΑΙΟ ΙΙ : ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΗ ΔΙΚΑΣΤΙΚΗ ΛΕΙΤΟΥΡΓΙΑ..	20
2.1. Η ιστορία της ΤΝ.....	20
2.1.1. Ο ορισμός της ΤΝ	21
2.1.2. Εκτίμηση αντικτύπου της τεχνητής νοημοσύνης στη δικαιοσύνη	22
2.1.3 Μηχανική Μάθηση (Machine Learning).....	23
2.1.4. Βαθιά Μάθηση (Deep Learning).....	24
2.2. ΕΦΑΡΜΟΓΕΣ ΤΝ	25
2.2.1. Προώθηση Ψηφιακών Δικαστικών Αιθουσών	25
2.2.2. Οι προδικαστικές ενέργειες.....	26

2.2.3. Τα Smart Courts της Κίνας.....	26
2.2.4. Περίπτωση Εσθονίας	28
2.2.5 e-Curia: Ηλεκτρονική κατάθεση και επίδοση διαδικαστικών εγγράφων	29
2.3. ΤΟ ΔΙΚΑΙΩΜΑ ΣΤΗ ΔΙΚΑΙΗ ΔΙΚΗ ΜΕΣΩ ΤΝ	30
2.3.1 Η επίδραση της Τεχνητής Νοημοσύνης στην αρχή του νόμιμου δικαστή	30
2.3.2 Η αρχή του «ανθρώπινου ελέγχου» και η διαφύλαξη της δικαστικής ανεξαρτησίας	31
2.3.3. Το πλαίσιο της Αλγοριθμικής Δικαιοσύνης: Διανεμητική και Διαδικαστική προσέγγιση	34
2.3.4. Τήρηση των θεμελιωδών δικαιωμάτων και αρχών	34
2.3.5 Τηλεδιασκέψεις (ΕΔΔΑ. Sakniouski κατά Ρωσίας, Αριθμ. 21272/03, 2 Νοεμβρίου 2010; Marcello Viola κατά Ιταλίας, Αριθμ. 45106/04, 5 Οκτωβρίου 2006).....	36
2.4 ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ.....	37
2.4.1 Τεχνητή Νοημοσύνη στο Αστικό και Ποινικό Δίκαιο	37
2.4.2 Έκδοση αποφάσεων	39
2.4.5. Προγνωστική Αστυνόμευση	41
2.4.6 Προγνωστική Ταυτοποίηση	42
2.4.7 Ανωνυμοποίηση αποφάσεων μέσω ΤΝ.....	43
ΚΕΦΑΛΑΙΟ ΙΙΙ Κυβερνοασφάλεια στο Ψηφιακό Δικαστικό Σύστημα.....	44
3.1 Ορισμός πληροφοριακού συστήματος	44
3.2. Περί Κυβερνοασφάλειας.....	45
3.2.1. Η Κυβερνοασφάλεια ως εγγύηση της Ψηφιακής Δικαιοσύνης	46
3.2.2 Το Ευρωπαϊκό Κανονιστικό Πλαίσιο: Υπο την Οδηγία NIS στην NIS 2	47
3.2.3. Το νομοθετικό πλαίσιο στην Ελλάδα και την Ευρωπαϊκή ένωση.....	48
3.2.4. Η συμβολή της Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια στη δικαστική χρήση κατά τον Κανονισμό AI ACT	50
ΚΕΦΑΛΑΙΟ ΙV Κυβερνοέγκλημα και Ποινική Δικαιοσύνη	52
4.1.1 Ορισμός κυβερνοεγκλήματος	52

4.1.2 Είδη ηλεκτρονικού εγκλήματος.....	53
4.1.3 Deepfakes ως μέσο παραπλάνησης της δικαιοσύνης.....	54
4.1.4 Η ποινική προστασία των δεδομένων προσωπικού χαρακτήρα και η αντιμετώπιση τους από τη Δικαιοσύνη	56
ΚΕΦΑΛΑΙΟ V ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΤΝ ΣΤΗ ΔΙΚΑΙΟΣΥΝΗ.....	57
5.1 Κίνδυνοι Προγνωστικής Δικαιοσύνης	57
5.1.1. Τήρηση των θεμελιωδών δικαιωμάτων και αρχών	58
5.1.2. Η προκατάληψη ως κίνδυνος έκδοσης μεροληπτικών αποφάσεων και διαιώνισης υφιστάμενων διακρίσεων	59
5.1.3. Έλλειψη διαφάνειας των αλγοριθμικών συστημάτων	61
5.1.4. Πλεονεκτήματα της χρήσης ΤΝ στη Δικαιοσύνη.....	62
5.2 Προτεινόμενες λύσεις.....	63
5.2.1 Ο ανθρώπινος έλεγχος ως θεμελιώδης εγγύηση της δικαστικής ανεξαρτησίας	65
5.2.2 Αρχές δεοντολογίας (Χάρτης CEPEJ).....	66
ΚΕΦΑΛΑΙΟ VI ΣΥΜΠΕΡΑΣΜΑ	68
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	72
ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ	77

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εξετάζει δύο από τις πιο κομβικές παραμέτρους που διαμορφώνουν σήμερα το τοπίο της ψηφιακής δικαιοσύνης: την Τεχνητή Νοημοσύνη και την Κυβερνοασφάλεια. Αφετηρία της ανάλυσης αποτελεί η διαπίστωση ότι τα δικαστικά συστήματα δεν μπορούν πλέον να παραμένουν αναλλοίωτα μπροστά στη ραγδαία τεχνολογική εξέλιξη· η ψηφιοποίηση της δικαιοσύνης δεν είναι επιλογή, αλλά αναγκαιότητα.

Στο πρώτο κεφάλαιο αναλύεται το οικοσύστημα της ηλεκτρονικής δικαιοσύνης (e-Justice), με αναφορά στα κύρια ευρωπαϊκά εργαλεία διασυνοριακής διαλειτουργικότητας, EUR-Lex, N-Lex, e-CODEX, ECRIS, καθώς και στα ελληνικά συστήματα ψηφιοποίησης, όπως το ΟΣΔΔΥ-ΔΔ και η ηλεκτρονική κατάθεση δικογράφων. Στο δεύτερο κεφάλαιο ερευνάται ο ρόλος της Τεχνητής Νοημοσύνης στη δικαστική λειτουργία, από τις βασικές έννοιες της μηχανικής μάθησης και της βαθιάς μάθησης έως τις εφαρμογές της σε πραγματικές συνθήκες: ψηφιακές δικαστικές αίθουσες, έξυπνα δικαστήρια στην Κίνα, το εγχείρημα της Εσθονίας για αυτοματοποιημένη επίλυση μικροδιαφορών και την πλατφόρμα e-Curia. Παράλληλα, εξετάζεται η επίδραση της ΤΝ στο δικαίωμα στη δίκαιη δίκη, στην αρχή του νόμιμου δικαστή και στη διαδικαστική δικαιοσύνη υπό το πρίσμα του Ευρωπαϊκού Χάρτη Θεμελιωδών Δικαιωμάτων και της ΕΣΔΑ.

Το τρίτο κεφάλαιο αφιερώνεται στην κυβερνοασφάλεια ως θεμελιώδη εγγύηση λειτουργίας του ψηφιακού δικαστικού συστήματος. Αναλύονται το ευρωπαϊκό κανονιστικό πλαίσιο, από την Οδηγία NIS 1 στη NIS 2, καθώς και το ελληνικό νομοθετικό οπλοστάσιο, ενώ ιδιαίτερη έμφαση δίνεται στη σχέση μεταξύ Τεχνητής Νοημοσύνης και κυβερνοασφάλειας στο πλαίσιο του Κανονισμού AI Act. Στο τέταρτο κεφάλαιο εξετάζεται το κυβερνοέγκλημα και η αντιμετώπισή του από την ποινική δικαιοσύνη: phishing, pharming, hacking, deepfakes ως αποδεικτικά μέσα, καθώς και η ποινική προστασία των προσωπικών δεδομένων βάσει του ν. 4624/2019 και του GDPR.

Στο πέμπτο και τελευταίο κεφάλαιο καταγράφονται οι βασικές προκλήσεις που θέτει η χρήση της ΤΝ στη δικαιοσύνη, αλγοριθμική προκατάληψη, έλλειψη διαφάνειας, κίνδυνος υποκατάστασης του δικαστή, και αναζητούνται προτεινόμενες λύσεις που εξισορροπούν την τεχνολογική αποδοτικότητα με την προστασία των θεμελιωδών δικαιωμάτων.

Κεντρικό συμπέρασμα της εργασίας είναι ότι η ΤΝ μπορεί να συμβάλει ουσιαστικά στον εκσυγχρονισμό της δικαιοσύνης, υπό την αδιαπραγμάτευτη προϋπόθεση ότι παραμένει εργαλείο υποστήριξης, και όχι υποκατάστασης, της ανθρώπινης δικαστικής κρίσης. Η αρχή του ανθρώπινου ελέγχου, η διαφάνεια των αλγοριθμικών συστημάτων και μια ισχυρή κυβερνοασφάλεια δεν αποτελούν τεχνικές λεπτομέρειες, αλλά συνταγματικές και δικονομικές εγγυήσεις που δεν επιδέχονται συμβιβασμό.

ABSTRACT

This thesis examines two of the most pivotal parameters shaping the contemporary landscape of digital justice: Artificial Intelligence and Cybersecurity. The starting point of the analysis is the observation that judicial systems can no longer remain stagnant in the face of rapid technological evolution, making it clear that the digitalization of justice is not an option, but a necessity.

The first chapter analyzes the electronic justice (e-Justice) ecosystem, with reference to the main European cross-border interoperability tools, such as EUR-Lex, N-Lex, e-CODEX, and ECRIS, as well as the Greek digitalization systems, such as OSDDY-DD and the electronic filing of legal documents. In the second chapter, the role of Artificial Intelligence in judicial function is explored, from the basic concepts of machine learning and deep learning to its real-world applications: digital courtrooms, smart courts in China, Estonia's project for automated small claims resolution, and the e-Curia platform. At the same time, the impact of AI on the right to a fair trial, the principle of the "lawful judge," and procedural justice is examined under the light of the European Charter of Fundamental Rights and the ECHR.

The third chapter is dedicated to cybersecurity as a fundamental guarantee for the operation of the digital judicial system. The European regulatory framework is analyzed, from the NIS 1 to the NIS 2 Directive, as well as the Greek legislative arsenal, while particular emphasis is placed on the relationship between Artificial Intelligence and Cybersecurity within the framework of the AI Act. This is followed by a brief reference regarding cybercrime and its treatment by criminal justice: phishing, pharming, hacking, deepfakes as evidence, as well as the criminal protection of personal data based on Law 4624/2019 and the GDPR. In the fifth and final chapter, the key challenges posed by the use of AI in justice are recorded, algorithmic bias, lack of transparency, the risk of replacing the judge and proposed solutions are sought that balance technological efficiency with the protection of fundamental rights.

The central conclusion of the paper is that AI can contribute substantially to the modernization of justice, under the non-negotiable condition that it remains a tool for supporting, and not replacing, human judicial judgment. The principle of human control, the transparency of algorithmic systems, and robust cybersecurity are not technical details, but constitutional and procedural guarantees that do not permit compromise.

ΚΕΦΑΛΑΙΟ Ι ΤΟ ΟΙΚΟΣΥΣΤΗΜΑ ΤΗΣ ΨΗΦΙΑΚΗΣ ΔΙΚΑΙΟΣΥΝΗΣ (E-JUSTICE)

1.1 Η έννοια και η εξέλιξη της ηλεκτρονικής δικαιοσύνης

Τα τελευταία έτη, η ραγδαία τεχνολογική πρόοδος έχει επιφέρει βαθιές μεταβολές σε όλους σχεδόν τους τομείς της κοινωνικής και θεσμικής ζωής, φέρνοντας τον σύγχρονο άνθρωπο σε διαρκή αλληλεπίδραση με καινοτόμες τεχνολογίες, μεταξύ των οποίων δεσπόζουσα θέση κατέχει η Τεχνητή Νοημοσύνη (εφεξής T.N), η έννοια της οποίας θα αναλυθεί στα επόμενα κεφάλαια. Η αυξανόμενη διείσδυση της TN δεν θα μπορούσε να αφήσει ανεπηρέαστο τον χώρο της δικαιοσύνης, γεγονός που αποτυπώνεται στην αυξανόμενη σημασία της για τα δικαστικά συστήματα των κρατών μελών.

Το 2024 σηματοδότησε ένα καθοριστικό ορόσημο για τη ρύθμιση της TN σε ευρωπαϊκό και διεθνές επίπεδο, καθώς υιοθετήθηκε για πρώτη φορά ένα ολοκληρωμένο και δεσμευτικό κανονιστικό πλαίσιο που επιχειρεί να ρυθμίσει οριζόντια την ανάπτυξη και τη χρήση συστημάτων TN.¹ Καθοριστικό επίσης ρόλο για την ψηφιοποίηση της δικαιοσύνης έφερε και η πανδημία COVID-19 όπου στάθηκε καταλύτης των σχετικών εξελίξεων, χωρίς, ωστόσο, να αποτελεί παράλληλα το αφετηριακό σημείο τούτων.²

Η μετάβαση της δικαστικής λειτουργίας στην ψηφιακή εποχή δεν αποτελεί μια απλή τεχνική αναβάθμιση, αλλά μια θεμελιώδη αλλαγή του τρόπου απονομής του δικαίου. Η έννοια της ηλεκτρονικής δικαιοσύνης (e-Justice) περιλαμβάνει το σύνολο των εργαλείων πληροφορικής και επικοινωνιών που αποσκοπούν στη βελτίωση της πρόσβασης των πολιτών στη δικαιοσύνη, καθώς και στην ενίσχυση της ταχύτητας και της διαφάνειας των δικαστικών διαδικασιών. Όπως επισημαίνεται, η ψηφιοποίηση λειτουργεί ως καταλύτης για τον εκσυγχρονισμό του κράτους δικαίου, επιτρέποντας την

¹ Βλ. ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1689 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Ιουνίου 2024 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη).

² Βλ. Loveday B., (2000) 'Address to EGPA Conference, Cape Sounion, Greece', σε M. Fabri et al. (eds.), "The Challenge of Change for Judicial Systems", σελ. 23.

αποϋλοποίηση των εγγράφων και τη μείωση της γραφειοκρατίας που παραδοσιακά χαρακτήριζε τα δικαστικά συστήματα, ιδίως την Ελλάδα.³

Η εξέλιξη αυτή καθοδηγείται σε μεγάλο βαθμό από τις ευρωπαϊκές στρατηγικές, οι οποίες θέτουν ως προτεραιότητα τη διαλειτουργικότητα των συστημάτων μεταξύ των κρατών μελών. Η ανάγκη για ένα ασφαλές ψηφιακό περιβάλλον είναι επιτακτική, καθώς η διαχείριση δικαστικών υποθέσεων συνεπάγεται την επεξεργασία μεγάλου όγκου δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, η ασφάλεια των συστημάτων δικτύου και πληροφοριών αποτελεί τον ακρογωνιαίο λίθο για την εμπιστοσύνη των χρηστών στο ψηφιακό οικοσύστημα ⁴

Τέλος, προκειμένου να κατανοήσει πλήρως κανείς την έννοια της ψηφιακής δικαιοσύνης, αρκεί μόνο να ερευνήσει τη φιλοσοφική και γλωσσολογική καταγωγή της, όπως τις διαμόρφωσαν τα εννοιακά εκείνα πρόσωπα που επιχείρησαν να τη δαμάσουν και να την εντάξουν στο δικό τους οντολογικό πλαίσιο.⁵

1.1.1 Η μετάβαση από το φυσικό αρχείο στο ψηφιακό περιβάλλον

Η ιστορική εξάρτηση της δικαιοσύνης από το έγχαρτο αρχείο δημιούργησε διαχρονικά προβλήματα λειτουργίας, όπως η δυσκολία στην ανάκτηση πληροφοριών και ο κίνδυνος απώλειας κρίσιμων εγγράφων. Η υιοθέτηση ψηφιακών μέσων επιτρέπει τη δημιουργία ολοκληρωμένων πληροφοριακών συστημάτων όπου η ροή της υπόθεσης παρακολουθείται σε πραγματικό χρόνο. Αυτή η μετάβαση δε, όπου στην Ελλάδα εκτιμάται σύμφωνα με επίσημες ανακοινώσεις ότι θα έχει ολοκληρωθεί μέχρι το καλοκαίρι του 2026⁶, αφορά μόνο την αποθήκευση αλλά και την εγκυρότητα των

³ Βλ. Διπλωματική εργασία της Σουλδάτου Μ. (2024) «Τεχνητή Νοημοσύνη και Δικαιοσύνη» του Παν. Μακεδονίας, σελ 15.

⁴ Βλ. Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ΕΕ L 194/1.

⁵ Βλ. Διπλωματική Εργασία της Α. Ν. Βιδάκη, (2022) “Ψηφιοποίηση της δικαιοσύνης: Κανονιστικό πλαίσιο, ζητήματα δεοντολογίας και μελλοντικές προκλήσεις”, σελ. 17, Διώνη

⁶ Βλ. Υπουργείο Δικαιοσύνης (2025) « Ψηφιοποίηση αρχείων δεδομένων του Υπουργείου Δικαιοσύνης» Διαθέσιμο στο: https://ministryofjustice.gr/?page_id=14882 (ημ πρόσβασης 27/12/2025).

εγγράφων, η οποία πλέον διασφαλίζεται μέσω της χρήσης εγκεκριμένων ηλεκτρονικών υπογραφών προσδίδοντας στα ηλεκτρονικά έγγραφα την ίδια ισχύ με τα φυσικά.⁷

Η ψηφιοποίηση των δικαστηρίων στην Ελλάδα, με την εισαγωγή συστημάτων όπως το ΟΣΔΔΥ-ΔΔ, όπως αυτό θα αναλυθεί περαιτέρω, αποτελεί το πλέον χαρακτηριστικό παράδειγμα αυτής της μεταβολής. Το σύστημα αυτό ενσωματώνει όλες τις φάσεις της δικαστικής διαδικασίας, από την ηλεκτρονική κατάθεση του δικογράφου έως την έκδοση και δημοσίευση της απόφασης. Η επιτυχία τέτοιων συστημάτων εξαρτάται άμεσα από τη σταθερότητα των υποδομών και την ικανότητα αντιμετώπισης κυβερνοαπειλών που θα μπορούσαν να θέσουν σε κίνδυνο την ακεραιότητα της δικαιοσύνης.⁸

1.1.2. Ταχύτητα, διαφάνεια και προσβασιμότητα στα πλαίσια διασυννοριακής διαλειτουργικότητας

Τα τελευταία έτη, η Ευρωπαϊκή Ένωση, μετά από τις δειλές προσπάθειες των προηγούμενων περιόδων, έχει προβεί σε σημαντικά βήματα προς την ψηφιοποίηση της δικαιοσύνης, με αποκορύφωμα την περίοδο 2020, η οποία χαρακτηρίζεται από έντονη νομοθετική δράση⁹. Αυτή η τάση φαίνεται να αποτελεί στόχο και για τα επόμενα έτη, σύμφωνα με τη στρατηγική του Συμβουλίου της ΕΕ για την ηλεκτρονική δικαιοσύνη που αφορά τη περίοδο 2024-2028. Παρακάτω, παρουσιάζονται κάποιες πρωτοβουλίες στον τομέα της διασυννοριακής διαλειτουργικότητας, της ηλεκτρονικής πρόσβασης σε ευρωπαϊκή νομοθεσία και νομολογία και της τεχνητής νοημοσύνης, οι οποίες αποτελούν απτά παραδείγματα της προσπάθειας για επιτάχυνση της διαδικασίας ψηφιοποίησης και της προώθησης της χρήσης ψηφιακών υπηρεσιών στην ηλεκτρονική δικαιοσύνη.

Αξίζει να προστεθεί πως στο EUR-Lex είναι αναρτημένες όλες οι εκδόσεις της Επίσημης Εφημερίδας της Ευρωπαϊκής Ένωσης και από τον Ιούλιο του 2013 δημοσιεύεται στην πύλη η ηλεκτρονική έκδοση της Εφημερίδας, παράγοντας συνάμα έννομα

⁷ Βλ. Ιγγλεζάκης Ι. (2021), *Δίκαιο Πληροφορικής*, Δ' Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 449.

⁸ Βλ. Διπλωματική εργασία της Ανδρεάδου Χ. (2025) *Αξιοποίηση του κειμένου της δικαστικής απόφασης στο Ολοκληρωμένο Σύστημα Διαχείρισης Διοικητικής Δικαιοσύνης (ΟΣΔΔΥ-ΔΔ) με σύγχρονες εφαρμογές ανάλυσης και επεξεργασίας κειμένου* του Παν. Μακεδονίας, σελ 24.

⁹ Βλ. Συμβούλιο της Ε.Ε., *Ευρωπαϊκή στρατηγική για την ηλεκτρονική δικαιοσύνη για την περίοδο 2024 - 2028 - Εγκριση (15509/2023)*, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 17.11.2023, σελ. 2, σκέψη 2.

αποτελέσματα. Από την άλλη πλευρά, το συγκεκριμένο νομικό εργαλείο έρευνας, διευκολύνει τους επισκέπτες να αποκτήσουν μια πιο ουσιαστική αντίληψη για το δίκαιο της ΕΕ, αφού παρουσιάζονται αναλυτικά όλα τα στάδια που απαιτούνται για την έκδοση των νομικών πράξεων και οι περιλήψεις της νομοθεσίας, οι οποίες περιγράφουν με κατανοητό τρόπο τις νομοθετικές πράξεις.¹⁰

1.2 Διασυνοριακή λειτουργικότητα

1.2.1. EUR-Lex

Το EUR-Lex (υποσημ 10) είναι μια διαδικτυακή πύλη, η οποία προσφέρει πρόσβαση στο δίκαιο της Ευρωπαϊκής Ένωσης, μέσα από ένα ευρύ φάσμα νομικών εγγράφων, τα οποία είναι διαθέσιμα στις 24 επίσημες γλώσσες της Ένωσης και τελεί υπό την διαχείριση της Υπηρεσίας Εκδόσεων της ΕΕ. Κάθε ενδιαφερόμενος έχει τη δυνατότητα, μέσω της πύλης, να αναζητήσει νομικά έγγραφα της ΕΕ, όπως συνθήκες, νομικές πράξεις των θεσμικών οργάνων της, νομολογία, διεθνείς συμφωνίες, προπαρασκευαστικά έγγραφα που αφορούν την νομοθεσία, έγγραφα ΕΖΕΖ (Ευρωπαϊκή Ζώνη Ελευθέρων Συναλλαγών), καθώς και στοιχεία αναφοράς και κείμενα των εθνικών εκτελεστικών μέτρων, με την προϋπόθεση βέβαια, της προηγούμενης συγκατάθεσης των κρατών μελών. Άξιο αναφοράς κρίνεται το γεγονός ότι όλα τα έγγραφα απεικονίζονται με αναλυτικά μεταδεδομένα, δηλαδή δίνονται παράλληλα λεπτομερείς πληροφορίες, που αφορούν τις σχέσεις του εκάστοτε εγγράφου με άλλα νομικά έγγραφα, παραθέτονται οι ερμηνείες της νομολογίας, οι ημερομηνίες έγκρισης, έναρξης ισχύος και εφαρμογής των εγγράφων, και οι τροποποιητικές πράξεις.

Αξίζει να προστεθεί πως στο EUR-Lex είναι αναρτημένες όλες οι εκδόσεις της Επίσημης Εφημερίδας της Ευρωπαϊκής Ένωσης και από τον Ιούλιο του 2013 δημοσιεύεται στην πύλη η ηλεκτρονική έκδοση της Εφημερίδας, παράγοντας συνάμα έννομα αποτελέσματα. Από την άλλη πλευρά, το συγκεκριμένο εργαλείο, διευκολύνει τους επισκέπτες να αποκτήσουν μια πιο ουσιαστική αντίληψη για το δίκαιο της ΕΕ, αφού παρουσιάζονται αναλυτικά όλα τα στάδια που απαιτούνται για την έκδοση των νομικών

¹⁰ Βλ. <https://eur-lex.europa.eu/content/welcome/about.html?locale=el>, τελευταία πρόσβαση 26/12/2025.

πράξεων και οι περιλήψεις της νομοθεσίας, οι οποίες περιγράφουν με κατανοητό τρόπο τις νομοθετικές πράξεις.¹¹

1.2.3 N-Lex

Το N-Lex είναι μια κοινή διαδικτυακή πύλη, η οποία ανακατευθύνει τον χρήστη μέσω συνδέσμων στις βάσεις δεδομένων του εθνικού δικαίου κάθε κράτους μέλους της ΕΕ, από τις οποίες και εξαρτάται πλήρως, χωρίς να αποτελεί το ίδιο βάση δεδομένων, αφού δεν περιέχει νομικά έγγραφα¹². Το N-Lex δημιουργήθηκε από την Υπηρεσία Εκδόσεων της ΕΕ σε συνεργασία με τις εθνικές κυβερνήσεις και τέθηκε σε δοκιμαστική εφαρμογή τον Απρίλιο του 2006, αποτελώντας συμπλήρωμα στο EUR-Lex, τον ιστότοπο που παρέχει πρόσβαση στο δίκαιο της ΕΕ. Ουσιαστικά, το ως άνω εργαλείο επιτρέπει στους χρήστες να έχουν πρόσβαση στους εθνικούς νόμους των χωρών της Ένωσης, επιλέγοντας την γλώσσα που οι ίδιοι επιθυμούν¹³.

1.2.3. eu-LISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης (eu-LISA) είναι ένας αποκεντρωμένος οργανισμός της ΕΕ, ο οποίος ιδρύθηκε το 2011 με τον κανονισμό (ΕΕ) αριθ. 1077/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (πλέον έχει αντικατασταθεί από τον κανονισμό (ΕΕ) αριθ. 26/20 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου) και ξεκίνησε τη δραστηριότητά του τον Δεκέμβριο του 2012. Οι αποκεντρωμένοι οργανισμοί της ΕΕ επικουρούν τα θεσμικά όργανα της Ένωσης στη χάραξη πολιτικών και τελούν τεχνικό, επιστημονικό ή διοικητικό έργο, αφού διακατέχονται από τεχνικές και εξειδικευμένες γνώσεις.¹⁴ Σκοπός του οργανισμού είναι η παροχή τεχνολογικής υποστήριξης, ώστε να εξασφαλιστεί η αδιάκοπη και αποτελεσματική λειτουργία μεγάλων συστημάτων πληροφορικής εντός του χώρου ελευθερίας, ασφάλειας και δικαιοσύνης. Τα συστήματα αυτά αφορούν την εσωτερική

¹¹ Βλ. <https://eur-lex.europa.eu/content/welcome/about.html?locale=el> τελευταία πρόσβαση 26/12/2025.

¹² Βλ. <https://n-lex.europa.eu/n-lex/about/about?lang=el> τελευταία πρόσβαση 26/12/2025.

¹³ Βλ. Casanovas P., Biasiotti M. A., Francesconi E., Sagri M. T. (Eds.), (2007) Proceedings of LOAIT '07, "2nd Workshop on Legal Ontologies and Artificial Intelligence Techniques" σελ. 141-142.

¹⁴Βλ. https://employment-social-affairs.ec.europa.eu/policies-and-activities/international-partners-and-agencies/decentralised-agencies_el τελευταία πρόσβαση 26/12/2025.

ασφάλεια και τη διαχείριση των συνόρων στις χώρες Σένγκεν, την ανταλλαγή στοιχείων σχετικών με τις θεωρήσεις, την ελεύθερη διακίνηση των πολιτών εντός της Ένωσης και τον καθορισμό του αρμόδιου κράτους μέλους για τον έλεγχο μιας αίτησης ασύλου. Με αυτό το τρόπο, επιτυγχάνεται η ασφαλής ανταλλαγή πληροφοριών μεταξύ των χωρών, με αποτέλεσμα να καθίσταται η Ευρώπη ασφαλέστερη, αφού συγχρόνως ο οργανισμός εγγυάται την διασφάλιση των πληροφοριών και την προστασία των δεδομένων¹⁵. Πέραν των ανωτέρω, ο eu-LISA αναπτύσσει, επίσης, νέες τεχνολογίες με σκοπό τη δημιουργία πιο ασφαλών συστημάτων διαχείρισης, όπως για παράδειγμα το ECRIS-TCN (Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου για υπηκόους τρίτων χωρών) και το e-CODEX, τα οποία συμβάλλουν στο τομέα της δικαιοσύνης.¹⁶

1.2.4. e-CODEX

Πρόκειται για ένα σύστημα τεχνολογίας πληροφοριών που δημιουργήθηκε το 2010, σε ενωσιακό επίπεδο, με σκοπό την ταχεία, άμεση και ασφαλή επικοινωνία των κρατών μελών στον τομέα της ηλεκτρονικής δικαιοσύνης, μέσω της διασυνοριακής ηλεκτρονικής ανταλλαγής δεδομένων σχετικών με αστικές και ποινικές υποθέσεις. Με το σύστημα e-CODEX καθίσταται δυνατή η αποτελεσματική συνεργασία των συστημάτων δικαιοσύνης με ψηφιακό τρόπο και διασφαλίζεται παράλληλα, ο σεβασμός του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα¹⁷. Αυτό το εργαλείο, το οποίο αποτελεί το κυριότερο του είδους που έχει θεσπιστεί μέχρι σήμερα, διευκολύνει την εκτέλεση νομικών ενεργειών που έχουν διασυνοριακό χαρακτήρα, συμβάλλοντας με αυτό το τρόπο σημαντικά στο έργο των εθνικών δικαστηρίων, αφού μέσω του e-CODEX παρέχεται πρόσβαση σε δικαστικές πληροφορίες, η οποία υπό άλλες συνθήκες θα ήταν δυσχερέστερη λόγω των καθυστερήσεων και του υψηλού κόστους της χρήσης των δικαστικών συστημάτων¹⁸. Σκοπός αυτού του εγχειρήματος είναι, επίσης, η

¹⁵ Βλ. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-operational-management-large-scale-it-systems-area-freedom-security-and_el, τελευταία πρόσβαση 27/12/2025.

¹⁶ Βλ. Gogić K., (2022) *“The Impact of Covid-19 on the Digitalisation of Justice in the European Union”*, CIFILE Journal of International Law, Vol. 3, No. 6, 1-11, σελ. 5.

¹⁷ Βλ. Ευρωπαϊκή Επιτροπή (2020) *“Η ψηφιοποίηση της δικαιοσύνης στην Ευρωπαϊκή Ένωση. Μια εργαλειοθήκη ευκαιριών*, COM (2020) 710 final”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, σελ. 18.

¹⁸ Βλ. Κανονισμός (ΕΕ) 2022/850, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, σκέψη 2.

ευκολότερη πρόσβαση των πολιτών και των επιχειρήσεων στη δικαιοσύνη, ώστε να μπορούν να ανταλλάσσουν ψηφιακά έγγραφα και αποδεικτικά στοιχεία με δικαστικές αρχές¹⁹.

Το e-CODEX λειτούργησε την περίοδο 2010-2016, ενώ το 2022, στο πλαίσιο της επιτάχυνσης της διαδικασίας της ψηφιοποίησης, δόθηκε ιδιαίτερη έμφαση στην ολοκλήρωση νομοθετικών πρωτοβουλιών και μεταξύ άλλων, ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, ο κανονισμός 2022/850 που αφορά την διασυνοριακή ηλεκτρονική ανταλλαγή δεδομένων στον τομέα της δικαστικής συνεργασίας σε αστικές και ποινικές υποθέσεις (σύστημα e- CODEX). Σύμφωνα με τον ως άνω Κανονισμό, το σύστημα e-CODEX τελεί υπό την διαχείριση του Ευρωπαϊκού Οργανισμού για τη λειτουργική διαχείριση μεγάλων πληροφοριακών συστημάτων στον τομέα της ελευθερίας, της ασφάλειας και της δικαιοσύνης (eu-LISA).²⁰ Βέβαια, παρά όλες τις προσπάθειες που έχουν γίνει για την προώθηση του αποκεντρωμένου συστήματος e-CODEX²¹, κρίνεται αναγκαία η περαιτέρω ανάπτυξή του τα επόμενα έτη, τόσο στο πεδίο της διαλειτουργικότητας, όσο και στο πεδίο της ασφαλείας.²²

1.2.5. ECRIS

Το Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου (ECRIS) αποτελεί ένα αποκεντρωμένο σύστημα τεχνολογίας πληροφοριών, το οποίο στοχεύει στην ηλεκτρονική ανταλλαγή πληροφοριών που αφορούν προηγούμενες καταδίκες πολιτών και βασίζεται στις εθνικές βάσεις δεδομένων ποινικού μητρώου κάθε κράτους μέλους της ΕΕ. Η ανταλλαγή των πληροφοριών, δηλαδή, πραγματοποιείται μόνο μεταξύ των κρατών μελών και αφορούν μόνο υπηκόους της ΕΕ. Το εν λόγω εργαλείο δημιουργήθηκε για τη διευκόλυνση κυρίως των εθνικών δικαστηρίων, τα οποία υποχρεούνται, σύμφωνα με το δίκαιο της ΕΕ, να επιβάλλουν ποινές σε ποινικές υποθέσεις, αφού πρώτα λάβουν

¹⁹ Βλ. Κανονισμός (ΕΕ) 2022/850, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, σκέψη 3.

²⁰ Ο.π. υποσημ. 19, σκέψη 7.

²¹ Βλ. Συμβούλιο της Ε.Ε., 2020 "Συμπεράσματα του Συμβουλίου «Πρόσβαση στη δικαιοσύνη – αξιοποίηση των ευκαιριών της ψηφιοποίησης» (2020/C 342 I/01)", Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, §§ 25,26.

²² Βλ. Vicoli D. (2024) "Editorial of Dossier "Digitalisation and Criminal Justice: Procedural Aspects" - An Introductory Overview", 10 Rev Brasileira de Direito Processual Penal 1.

υπόψη τους τις καταδίκες του υπό κρίση προσώπου τόσο σε άλλες χώρες της Ένωσης, όσο και στη χώρα που διενεργείται η δίκη. Στην ουσία, δεν επιδιώκεται η δημιουργία μιας συγκεντρωτικής βάσης δεδομένων ποινικού μητρώου σε ευρωπαϊκό επίπεδο, αφού όλα τα δεδομένα ποινικού μητρώου διαφυλάσσονται σε εθνικές βάσεις δεδομένων και ένα κράτος μέλος δεν διαθέτει πρόσβαση στις αντίστοιχες βάσεις των υπόλοιπων κρατών μελών.²³

Το ECRIS θεσπίστηκε μέσω της απόφασης πλαισίου 2009/315/ΔΕΥ του Συμβουλίου, η οποία τέθηκε σε εφαρμογή τον Απρίλιο του 2009 και τροποποιήθηκε με την οδηγία 2019/884 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Η τροποποιητική οδηγία άρχισε να εφαρμόζεται από τον Ιούνιο του 2022 σε όλα τα κράτη μέλη εκτός από την Ιρλανδία και τη Δανία, για τις οποίες συνεχίζει να ισχύει η απόφαση πλαίσιο, ενώ οι αλλαγές που πραγματοποιήθηκαν αφορούν τη συμπλήρωση του ECRIS με την προσθήκη ενός κεντρικού συστήματος εντοπισμού των κρατών μελών που διαθέτουν πληροφορίες για καταδίκες υπηκόων τρίτων χωρών, ανιθαγενών και ατόμων αγνώστου ιθαγένειας (ECRIS-TCN). Η απόφαση πλαίσιο 2009/315/ΔΕΥ θέτει τους κανόνες και τις γενικές αρχές για την ανταλλαγή των πληροφοριών ποινικού μητρώου, η οποία καθίσταται δυνατή μέσω της δημιουργίας του ηλεκτρονικού συστήματος ECRIS και υποχρεώνει μ' αυτό το τρόπο τα κράτη μέλη να διαβιβάζουν τις σχετικές πληροφορίες στο κράτος μέλος του οποίου ο καταδικασθείς είναι υπήκοος.²⁴ Υπεύθυνος για την συντήρηση και την περαιτέρω βελτίωση του λογισμικού εφαρμογής του ECRIS καθίσταται ο eu-LISA.

Συνοψίζοντας, το σύστημα ECRIS επιτελεί τους ακόλουθους σκοπούς: 1) καθιστά δυνατή την ανταλλαγή πληροφοριών που αφορούν προηγούμενες καταδίκες πολιτών μεταξύ των κρατών μελών με γρήγορο τρόπο, 2) διευκολύνει τους δικαστές, τους εισαγγελείς και τις αρμόδιες διοικητικές αρχές, με την παροχή εύκολης πρόσβασης στις πληροφορίες και 3) προλαμβάνει την περίπτωση οι δράστες εγκληματικών πράξεων να

²³ Ο.π. υποσημ. 5, σελ 42.

²⁴ Βλ. Ευρωπαϊκή Επιτροπή, 2020, *“Η ψηφιοποίηση της δικαιοσύνης στην Ευρωπαϊκή Ένωση. Μια εργαλειοθήκη ευκαιριών, COM(2020) 710 final”*, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, σελ.16.

προσπαθήσουν να αποφύγουν τις συνέπειες των προηγούμενων καταδικαστικών αποφάσεων τους, διαφεύγοντας σε άλλο κράτος μέλος της ΕΕ.

1.2.6 Το Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων (ΟΣΔΔΥ-ΔΔ)

Το Ολοκληρωμένο Σύστημα Διαχείρισης Δικαστικών Υποθέσεων για τη Διοικητική Δικαιοσύνη (ΟΣΔΔΥ-ΔΔ) αποτελεί το κεντρικό βάθρο πάνω στο οποίο οικοδομείται ο ψηφιακός μετασχηματισμός των διοικητικών δικαστηρίων της χώρας. Η αρχιτεκτονική του συστήματος έχει σχεδιαστεί με τρόπο που να υποστηρίζει τον πλήρη κύκλο ζωής μιας δικαστικής υπόθεσης, από την εισαγωγή της έως την οριστική αρχειοθέτηση της απόφασης. Στην πράξη, το ΟΣΔΔΥ-ΔΔ λειτουργεί ως ένας ενιαίος ψηφιακός κόμβος που διασυνδέει το Συμβούλιο της Επικρατείας, τα Διοικητικά Εφετεία και τα Διοικητικά Πρωτοδικεία, εξασφαλίζοντας την ομοιομορφία των διαδικασιών και την ακεραιότητα των δεδομένων.

Η ενσωμάτωση των νέων τεχνολογιών σε όλη τη Διοικητική Δικαιοσύνη πραγματοποιήθηκε μέσω του Ολοκληρωμένου Συστήματος Διαχείρισης Δικαστικών Υποθέσεων Διοικητικής Δικαιοσύνης, γνωστού ως ΟΣΔΔΥ- ΔΔ. Το Υπουργείο Δικαιοσύνης Διαφάνειας και Ανθρωπίνων Δικαιωμάτων κατέληξε το 2014 στο συμπέρασμα ότι η περιορισμένη εφαρμογή των ΤΠΕ στη Δικαιοσύνη οφείλεται στην έλλειψη μιας ενοποιημένης στρατηγικής για την εισαγωγή τους στον τομέα αυτό. Ως αποτέλεσμα, εφαρμόστηκε μια νέα στρατηγική που περιλαμβάνει τη δημιουργία ενός ομογενοποιημένου περιβάλλοντος πληροφορικής, στο οποίο συμπεριλαμβάνονται τα ήδη υπάρχοντα Πληροφοριακά Συστήματα και ενσωματώνονται επίσης τα δικαστήρια που δεν διέθεταν Πληροφοριακά Συστήματα, με στόχο την αναβάθμιση της ποιότητας και της ταχύτητας στη διαχείριση της Διοικητικής Δικαιοσύνης.

1.2.7 Ηλεκτρονική κατάθεση δικογράφων στην Ελλάδα

Η ηλεκτρονική κατάθεση στην Ελλάδα (portal.olomeleia) αποτελεί την πρώτη ουσιαστική επαφή του νομικού κόσμου με την ψηφιοποίηση και το θεμέλιο λίθο του «Έξυπνου Δικαστηρίου» (Smart Court). Σε αντίθεση με την παραδοσιακή διαδικασία, η ηλεκτρονική κατάθεση επιτρέπει την εισαγωγή δικογράφων και αποδεικτικών μέσω ασφαλών διαδικτυακών πυλών, οι οποίες λειτουργούν σε 24ωρη βάση. Αυτή η υποδομή δεν περιορίζεται μόνο στην αποθήκευση εγγράφων, αλλά περιλαμβάνει

προηγμένα συστήματα οπτικής αναγνώρισης χαρακτήρων (OCR) και αυτόματης ταξινόμησης, τα οποία προετοιμάζουν το έδαφος για την εφαρμογή αλγορίθμων τεχνητής νοημοσύνης στο επόμενο στάδιο της δικαστικής επεξεργασίας

Η λειτουργία του portal olomeleia ενσωματώνει προηγμένα μέτρα κυβερνοασφάλειας, καθώς η είσοδος στο σύστημα απαιτεί αυστηρή ταυτοποίηση μέσω της χρήσης ψηφιακών πιστοποιητικών και της Σύγχρονης Υποδομής Δημοσίου Κλειδιού (PKI). Η χρήση εγκεκριμένων ηλεκτρονικών υπογραφών μέσω της πλατφόρμας εγγυάται την αυθεντικότητα και την ακεραιότητα των κατατιθέμενων εγγράφων, αποτρέποντας την αλλοίωση του περιεχομένου τους κατά τη διαβίβαση στο ΟΣΔΔΥ-ΔΔ ή το ΟΣΔΔΥ-ΠΝ. Με αυτόν τον τρόπο, η ηλεκτρονική κατάθεση δεν περιορίζεται μόνο στην αποθήκευση εγγράφων, αλλά περιλαμβάνει υποδομές που προετοιμάζουν το έδαφος για την εφαρμογή αλγορίθμων τεχνητής νοημοσύνης, όπως συστήματα οπτικής αναγνώρισης χαρακτήρων (OCR) και αυτόματης ταξινόμησης.

1.2.8 Εφαρμογή παρακολούθησης Δικών

Η ψηφιακή υπηρεσία παρακολούθησης των εκθεμάτων και των πινακίων²⁵ αποτελεί ένα σύγχρονο εργαλείο πληροφόρησης, το οποίο επιτρέπει στους ενδιαφερόμενους να παρακολουθούν την πορεία των τρεχουσών δικαστικών υποθέσεων από απόσταση. Το κύριο πλεονέκτημα της εφαρμογής είναι η παροχή πληροφοριών σε πραγματικό χρόνο (real-time), γεγονός που διευκολύνει τον προγραμματισμό των νομικών παραστατών και των διαδικών. Ταυτόχρονα, η υπηρεσία λειτουργεί με αυστηρή προσήλωση στις αρχές του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), διασφαλίζοντας ότι όλα τα δημοσιοποιημένα στοιχεία παραμένουν ανώνυμα, ώστε να αποτρέπεται η ταυτοποίηση φυσικών προσώπων και να προστατεύεται η ιδιωτικότητά τους.

Ωστόσο, παρά τις σημαντικές τεχνολογικές προοπτικές, η εφαρμογή φαίνεται να βρίσκεται ακόμη σε πρώιμο στάδιο, καθώς παρουσιάζει συγκεκριμένες λειτουργικές προκλήσεις. Παρατηρείται συχνά ότι η κατάσταση των υποθέσεων ενδέχεται να μην είναι πλήρως ενημερωμένη· ενώ δηλαδή η υπηρεσία προορίζεται για λειτουργία σε

²⁵ Βλ. Παρακολούθηση Δικών <https://pinakio.e-diki.justice.gov.gr/guest/home>, τελευταία πρόσβαση 28-12-2025.

πραγματικό χρόνο, στην πράξη η ροή της πληροφορίας μπορεί να υστερεί (time lag), με αποτέλεσμα η εικόνα που λαμβάνει ο χρήστης να μην ανταποκρίνεται στην τρέχουσα κατάσταση εντός της αίθουσας. Επιπλέον, τα πινάκια που αφορούν μελλοντικές δικασίμους έχουν καθαρά ενδεικτικό χαρακτήρα, καθώς η τελική τους μορφή υπόκειται σε αλλαγές μέχρι την ημέρα της συνεδρίασης. Αυτές οι αποκλίσεις και η έλλειψη οριστικότητας στην προβολή των στοιχείων μπορούν να προκαλέσουν σύγχυση στους πολίτες και τους δικηγόρους, αναδεικνύοντας την ανάγκη για περαιτέρω τεχνική ωρίμανση και ακρίβεια του συστήματος.

ΚΕΦΑΛΑΙΟ II : ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΗ ΔΙΚΑΣΤΙΚΗ ΛΕΙΤΟΥΡΓΙΑ

2.1. Η ιστορία της TN

Η TN (εφεξής Τεχνητή Νοημοσύνη) συνιστά μια ολιστική, παγκόσμια και ταυτόχρονα αφηρημένη έννοια, που συμπεριλαμβάνει πολλούς και διαφορετικούς τρόπους λειτουργίας και πολλές και διαφορετικές εκδοχές, ο πυρήνας των οποίων δεν μπορεί να οριστεί ακόμη επιστημονικά²⁶. Η δυσκολία ορισμού της TN οφείλεται κυρίως στην πολυπλοκότητα των συστημάτων που περιλαμβάνει, στην ταχύτητα με την οποία εξελίσσεται και στο γεγονός ότι η έννοια καλύπτει τόσο τη μηχανική μάθηση όσο και πιο εξελιγμένα συστήματα γενετικής τεχνητής νοημοσύνης. Η TN περιλαμβάνει συστήματα που «μπορούν να προσαρμόζουν τη συμπεριφορά τους, βασισμένα στην ανάλυση δεδομένων, ώστε να επιτυγχάνουν συγκεκριμένους στόχους με ένα δεδομένο επίπεδο αυτονομίας»²⁷.

Αντίστοιχα, η Ευρωπαϊκή Επιτροπή, στο πλαίσιο της πρότασης Κανονισμού για την Τεχνητή Νοημοσύνη (γνωστού και ως AI Act), ορίζει την TN ως «ένα σύστημα που έχει σχεδιαστεί για να λειτουργεί με στοιχεία αυτονομίας και που, για συγκεκριμένους σκοπούς, μπορεί να παράγει προβλέψεις, συστάσεις ή αποφάσεις που επηρεάζουν

²⁶ Βλ. Μήτρου Λ., (2023) *Μπορεί ο αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να είναι διαφανής, να δικάζει και να διοικεί;*, Πανεπιστημιακές Εκδόσεις Κρήτης, σελ 13.

²⁷ Βλ. OECD, Recommendation of the Council on Artificial Intelligence, 2024, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>, τελευταία πρόσβαση 28/12/2025.

φυσικά ή νομικά πρόσωπα»²⁸. Αναμφίβολα η ΤΝ έχει δημιουργηθεί για να διευκολύνει τον άνθρωπο τόσο στην καθημερινότητα του όσο και στην εργασία του.

Η εξάπλωση της Τεχνητής Νοημοσύνης (ΤΝ) αποτελεί πλέον μια πραγματικότητα την οποία βιώνουμε όλοι από πρώτο χέρι, αναγνωρίζοντας την αυξανόμενη επιρροή και δύναμή της στην καθημερινότητα. Αν και η ουσιαστική "επανάσταση" της ΤΝ άρχισε να γίνεται αισθητή πριν από περίπου μια δεκαετία, ενώ οι μηχανικοί και οι ερευνητές εργάζονται πάνω στην ανάπτυξη αυτών των συστημάτων εδώ και πολλές δεκαετίες, με τους Warren McCulloch και Walter Pitts να έχουν αναγνωριστεί πλέον ότι εκείνοι είχαν την πρώτη επαφή με την έννοια της ΤΝ το μακρινό 1943.²⁹

Τον Νοέμβριο του 2022, ένας σημαντικός σταθμός στην ιστορία της τεχνολογίας σημειώθηκε με την κυκλοφορία του ChatGPT από την εταιρεία OpenAI. Η εφαρμογή αυτή, βασισμένη στην Τεχνητή Νοημοσύνη, απέδειξε ότι μέσω μιας σύντομης προτροπής κειμένου (text prompt), μπορεί να παράγει συγκροτημένα έγγραφα και να απαντά σε σύνθετα ερωτήματα με εντυπωσιακή διαύγεια. Η εξέλιξη αυτή επαναφέρει στο προσκήνιο το περίφημο "Παιχνίδι της Μίμησης" (Imitation Game) του Άλαν Τιούρινγκ³⁰. Ο Τιούρινγκ είχε ισχυριστεί ότι αν μια μηχανή καταφέρει να εξισωθεί με έναν άνθρωπο κατά τη διάρκεια μιας συνομιλίας, τότε θα πρέπει να θεωρηθεί ευφυής, ένα ορόσημο που, με τα σημερινά δεδομένα, φαίνεται πιο κοντά από ποτέ.

2.1.1. Ο ορισμός της ΤΝ

Ως Τεχνητή Νοημοσύνη ορίζεται το πεδίο εκείνο της επιστήμης των υπολογιστών που επιδιώκει τον σχεδιασμό και την ανάπτυξη συστημάτων ικανών να προσομοιώνουν ανθρώπινες γνωστικές δεξιότητες. Στην ουσία, πρόκειται για τη δυνατότητα των υπολογιστικών μηχανών να επεξεργάζονται εξωτερικά ερεθίσματα³¹, να αφομοιώνουν πληροφορίες μέσω της μάθησης και να προβαίνουν σε σύνθετους σχεδιασμούς ή

²⁸ Ο.π. υποσημ. 1, άρθρο 3 παρ. 1.

²⁹ Βλ. Russe S. και Norving P. (1995) *Artificial Intelligence A Modern Approach*, Third edition, σελ. 16.

³⁰ Βλ. Toon N. (2024), *How AI Thinks*, Transworld Publishers Ltd., σελ. 8.

³¹ Βλ. Ανακοίνωση της Ευρωπαϊκής Επιτροπής-Τεχνητή νοημοσύνη για την Ευρώπη, Βρυξέλλες, 25.4.2018 COM (2018) 237 final, <https://eurlex.europa.eu/legalcontent/EL/TXT/HTML/?uri=CELEX:52018DC0237&from=MT> τελευταία πρόσβαση: 26/2/2022 .

δημιουργικές λύσεις που μέχρι πρότινος θεωρούνταν αποκλειστικό προνόμιο της ανθρώπινης διάνοιας. Τα συστήματα αυτά δεν περιορίζονται στην παθητική εκτέλεση εντολών, αλλά αλληλεπιδρούν ενεργά με το περιβάλλον τους, αναλύοντας δεδομένα για την επίλυση προβλημάτων και τη λήψη αποφάσεων που κατατείνουν στην εκπλήρωση προκαθορισμένων στόχων³².

Στο πλαίσιο της δικαιοσύνης, η ικανότητα αυτή μεταφράζεται στην ανάλυση τεράστιου όγκου νομικών δεδομένων και στη χρήση αλγορίθμων που μπορούν να "αντιληφθούν" μοτίβα στη νομολογία, προσφέροντας έτσι εργαλεία που ενισχύουν τη δικαστική κρίση χωρίς να την υποκαθιστούν τον άνθρωπο.

2.1.2. Εκτίμηση αντικτύπου της τεχνητής νοημοσύνης στη δικαιοσύνη

Σύμφωνα με το σύγχρονο ρυθμιστικό πλαίσιο, τα συστήματα Τεχνητής Νοημοσύνης στον τομέα της δικαιοσύνης χαρακτηρίζονται επισήμως ως «υψηλού κινδύνου»³³. Η κατάταξη αυτή οφείλεται στο γεγονός ότι η χρήση τους μπορεί να έχει καθοριστικό αντίκτυπο στις θεμελιώδεις αρχές της δημοκρατίας, στο κράτος δικαίου και στις ατομικές ελευθερίες των πολιτών, ιδιαίτερα στις περιπτώσεις όπου υπάρχει ο κίνδυνος να υποκαταστήσουν τους δικαστές στην τελική λήψη αποφάσεων. Η δικαιοσύνη απαιτεί εξατομικευμένη κρίση, και η τυφλή εμπιστοσύνη σε έναν αλγόριθμο θα μπορούσε να οδηγήσει σε αυθαιρεσίες.

Παρόλο που η χρήση αυτών των συστημάτων επιτρέπεται από τις δικαστικές αρχές για την ενίσχυση της αποδοτικότητάς τους, η λειτουργία τους υπόκειται σε αυστηρούς κανόνες. Οι πάροχοι τέτοιων τεχνολογιών οφείλουν να συμμορφώνονται πλήρως με τις απαιτήσεις των Άρθρων 8-15 του σχετικού Κανονισμού (AI Act). Οι προβλέψεις αυτές διασφαλίζουν ότι τα συστήματα δεν λειτουργούν ανεξέλεγκτα, αλλά εντός ενός πλαισίου που προστατεύει το δημόσιο συμφέρον.

Οι συγκεκριμένες απαιτήσεις εστιάζουν πρωτίστως στη διαρκή διαχείριση κινδύνων, με ιδιαίτερη έμφαση στην αποφυγή των διακρίσεων καθ' όλη τη διάρκεια λειτουργίας των συστημάτων. Επιπλέον, τίθενται αυστηρά πρότυπα για την προστασία

³² Ο.π. υποσημ. 29, σελ. 1-5.

³³ Βλ. Διπλωματική Εργασία της Τερζίδου Κ. (2025), «Η Ψηφιοποίηση της Δικαιοσύνης στην Ευρωπαϊκή Ένωση μέσω της Τεχνητής Νοημοσύνης».

των προσωπικών δεδομένων, τη διαφάνεια των αλγοριθμικών διαδικασιών και, το κυριότερο, τη διατήρηση της ανθρώπινης εποπτείας. Με αυτόν τον τρόπο, διασφαλίζεται ότι η Τεχνητή Νοημοσύνη παραμένει ένα ελεγχόμενο εργαλείο και δεν μετατρέπεται σε έναν αδιαφανή «ψηφιακό δικαστή».

2.1.3 Μηχανική Μάθηση (*Machine Learning*)

Η Μηχανική Μάθηση αποτελεί έναν εξειδικευμένο κλάδο της Τεχνητής Νοημοσύνης, ο οποίος εδράζεται στη θεμελιώδη παραδοχή ότι τα υπολογιστικά συστήματα διαθέτουν τη δυνατότητα αυτόνομης απόκτησης γνώσης μέσω της επεξεργασίας δεδομένων. Η διαδικασία αυτή επιτρέπει στις μηχανές να εντοπίζουν σύνθετα μοτίβα και επαναλαμβανόμενες δομές εντός των πληροφοριών, προκειμένου να καταλήγουν σε συμπεράσματα και να λαμβάνουν αποφάσεις με υψηλό βαθμό αυτονομίας, όπως αυτό πρόκειται να αναλυθεί στα επόμενα κεφάλαια. Κεντρικός στόχος της μηχανικής μάθησης είναι η διαμόρφωση συστημάτων που εκτελούν εξειδικευμένες εργασίες χωρίς να απαιτείται ο εξαντλητικός και λεπτομερής προγραμματισμός κάθε επιμέρους βήματος από τον άνθρωπο.³⁴

Η επίτευξη αυτής της λειτουργίας βασίζεται στην ικανότητα των υπολογιστών να αναγνωρίζουν πρότυπα συμπεριφοράς στα δεδομένα και, μέσω της συνεχούς τροφοδότησης με νέες πληροφορίες, να εξελίσσουν την ακρίβεια των αποτελεσμάτων τους. Ενώ στο τρέχον στάδιο της τεχνολογικής εξέλιξης η πλειονότητα των συστημάτων βασίζεται σε δεδομένα που έχουν προηγουμένως κατηγοριοποιηθεί και επισημανθεί από τον άνθρωπο (*supervised learning*), η εξέλιξη της μηχανικής μάθησης τείνει προς τη σταδιακή ανεξαρτητοποίηση των μηχανών. Η προοπτική αυτή αφορά τη μετάβαση σε μοντέλα όπου η αναγνώριση και η ανάλυση των δεδομένων θα πραγματοποιείται αυτόματα, χωρίς την ανάγκη πρότερης ανθρώπινης παρέμβασης για την ταξινόμηση των πληροφοριών. Η εφαρμογή τέτοιων μοντέλων στον νομικό κλάδο προσφέρει σημαντικές δυνατότητες, όπως η αυτόματη επεξεργασία χιλιάδων δικαστικών αποφάσεων για την εξαγωγή νομικών συμπερασμάτων, εγείροντας ταυτόχρονα κρίσιμα

³⁴ Βλ. <https://bigblue.academy/gr/deep-learning-vs-machine-learning>, τελευταία πρόσβαση 28/12/2025.

ερωτήματα σχετικά με την αξιοπιστία και τη διαφάνεια των παραγόμενων αποτελεσμάτων

2.1.4. Βαθιά Μάθηση (Deep Learning)

Η Βαθιά Μάθηση αποτελεί την εξέλιξη και την περαιτέρω εξειδίκευση της μηχανικής μάθησης, εισάγοντας αλγοριθμικά μοντέλα υψηλής πολυπλοκότητας. Η λειτουργία των συστημάτων αυτών παρουσιάζει αξιοσημείωτες ομοιότητες με τον τρόπο επεξεργασίας πληροφοριών του ανθρώπινου νου, καθώς βασίζεται σε μια αρχιτεκτονική που προσομοιώνει τη δομή του ανθρώπινου εγκεφάλου. Η δομή αυτή ονομάζεται Τεχνητό Νευρωνικό Δίκτυο (Artificial Neural Network - ANN)³⁵ και επιτρέπει στο σύστημα να αναλύει δεδομένα σε πολλαπλά επίπεδα ιεραρχίας, επιτυγχάνοντας έτσι βάθος στην κατανόηση και την επεξεργασία των πληροφοριών.

Η εφαρμογή της βαθιάς μάθησης στην καθημερινή πρακτική γίνεται αντιληπτή μέσα από συστήματα που απαιτούν υψηλή ακρίβεια στην αναγνώριση προτύπων, όπως συμβαίνει στα σύγχρονα συστήματα υποβοήθησης οδήγησης. Χαρακτηριστικό παράδειγμα αποτελούν τα οχήματα που προειδοποιούν τον οδηγό για την ύπαρξη εμποδίων στον δρόμο. Η ικανότητα του συστήματος να ταυτοποιεί διαφορετικά αντικείμενα και κινδύνους σε πραγματικό χρόνο είναι αποτέλεσμα της διαδικασίας του deep learning.

Η εξέλιξη αυτής της ικανότητας είναι σταδιακή και βασίζεται στην εμπειρική μάθηση. Ένας αλγόριθμος που στην αρχική του φάση διέθετε τη δυνατότητα αναγνώρισης ενός περιορισμένου αριθμού αντικειμένων, μέσω της διαρκούς έκθεσης σε νέα δεδομένα και της εκπαίδευσης του νευρωνικού δικτύου, αποκτά σταδιακά την ικανότητα να αναγνωρίζει ένα ευρύ και ικανοποιητικό φάσμα εμποδίων. Αυτή η διαδικασία συνεχούς αυτοβελτίωσης και κλιμακωτής μάθησης καθιστά τη βαθιά μάθηση ένα πανίσχυρο εργαλείο, το οποίο βρίσκει εφαρμογή και στο δικαστικό πεδίο, ειδικά σε περιπτώσεις που απαιτείται η ανάλυση και η κατηγοριοποίηση εξαιρετικά σύνθετων νομικών ή αποδεικτικών δεδομένων.

³⁵ Βλ. <https://www.sciencedirect.com/topics/earth-and-planetary-sciences/artificial-neural-network> τελευταία πρόσβαση 28/12/2025.

2.2. ΕΦΑΡΜΟΓΕΣ ΤΝ

2.2.1. Προώθηση Ψηφιακών Δικαστικών Αιθουσών

Η ενίσχυση της ψηφιακής δικαστικής συνεργασίας³⁶ στην Ευρωπαϊκή Ένωση αποτελεί σημαντικό στόχο για την προώθηση μιας αποτελεσματικής και διαλειτουργικής δικαιοσύνης, με επίκεντρο την ανάπτυξη υπηρεσιών επικοινωνίας σε πραγματικό χρόνο. Οι ψηφιακές δικαστικές αίθουσες διαδραματίζουν καθοριστικό ρόλο, καθώς η βελτίωση της διαλειτουργικότητας των βιντεοδιασκέψεων, μέσω κοινών προτύπων και εργαλείων, διευκολύνει τη διεξαγωγή εξ αποστάσεως ακροάσεων, ενισχύοντας τη διαφάνεια και την προσβασιμότητα στις δικαστικές διαδικασίες.

Επιπλέον, όπως προαναφέρθηκε, η χρήση του συστήματος e - CODEX απλοποιεί την ανταλλαγή πληροφοριών μεταξύ κρατών - μελών σε πραγματικό χρόνο, ενώ η διασύνδεση μητρώων και η εφαρμογή του ECLI (European Case Law Identifier) διασφαλίζουν την εναρμόνιση της πρόσβασης στη νομολογία. Οι πρωτοβουλίες αυτές συνδυάζουν την τεχνολογία με τη δικαιοσύνη, δημιουργώντας ένα σύγχρονο και διαλειτουργικό δικαστικό περιβάλλον, που προάγει την ταχύτερη και ασφαλέστερη επίλυση υποθέσεων σε ολόκληρη την ΕΕ.

Η αξιοποίηση της τεχνητής νοημοσύνης (TN) στις τηλεδιασκέψεις των δικαστικών διαδικασιών αποτελεί ένα σημαντικό βήμα για τον εκσυγχρονισμό και την αποτελεσματικότητα της απονομής δικαιοσύνης. Η TN μπορεί να υποστηρίξει τις ψηφιακές δικαστικές αίθουσες με πολλούς τρόπους, βελτιώνοντας τη διαλειτουργικότητα και τη συνολική εμπειρία των συμμετεχόντων.

Συγκεκριμένα, η TN μπορεί να εφαρμόζεται στην αυτόματη αναγνώριση ομιλίας και τη μεταγραφή των πρακτικών των τηλεδιασκέψεων σε πραγματικό χρόνο, παρέχοντας ακριβείς και έγκυρες αποδόσεις των όσων ειπώθηκαν. Παράλληλα, η χρήση έξυπνων εργαλείων μπορεί να διασφαλίζει την ταυτοποίηση των συμμετεχόντων, ενισχύοντας την ασφάλεια και την αξιοπιστία των διαδικασιών. Επιπλέον, η TN μπορεί να βοηθήσει στη βελτιστοποίηση της επικοινωνίας μέσω αυτοματοποιημένης

³⁶ Συμβούλιο της Ε.Ε., “Ευρωπαϊκή στρατηγική για την ηλεκτρονική δικαιοσύνη για την περίοδο 2024 - 2028 - Έγκριση (15509/2023)”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 17.11.2023, σελ. 2, σκέψη 2.

ανίχνευσης τεχνικών προβλημάτων (π.χ. ήχος, εικόνα, σύνδεση) και στη διαχείριση του λόγου κατά τη διάρκεια της ακροαματικής διαδικασίας, εξασφαλίζοντας ομαλή ροή.

2.2.2. Οι προδικαστικές ενέργειες

Η τεχνητή νοημοσύνη μπορεί να αποτελέσει πολύτιμο εργαλείο για τη βελτιστοποίηση γραφειοκρατικών και διαδικαστικών λειτουργιών. Αρχικά, επιτρέπει μια πιο δίκαιη κατανομή των υποθέσεων στους δικαστές, βασισμένη στην πολυπλοκότητα της κάθε υπόθεσης, αντί για τη μέχρι σήμερα τυχαία ανάθεση. Έτσι, οι υποθέσεις αναλύονται και κατατάσσονται με βάση παράγοντες, όπως ο αριθμός των μαρτύρων, η περιπλοκότητα των νομικών ζητημάτων και ο απαιτούμενος χρόνος εκδίκασης, διασφαλίζοντας ισορροπημένη ανάθεση εργασιών.

Επιπρόσθετα, η τεχνητή νοημοσύνη μπορεί να αξιολογεί αν τα ένδικα μέσα πληρούν τις τυπικές προϋποθέσεις, απορρίπτοντας άμεσα όσα κρίνονται απαράδεκτα, κερδίζοντας πολύτιμο χρόνο στη δικαστική λειτουργία. Παράλληλα, μπορεί να ελέγχει την καθ' ύλην και κατά τόπο αρμοδιότητα του δικαστηρίου, απελευθερώνοντας τους δικαστές από διαδικαστικά ζητήματα και επιτρέποντάς τους να εστιάσουν στην ουσία της υπόθεσης εκεί που προβλέπεται.

Επιπλέον, τα συστήματα τεχνητής νοημοσύνης δίνουν τη δυνατότητα ομαδοποίησης των υποθέσεων βάσει πραγματικών περιστατικών και σχετικών κανόνων δικαίου, μειώνοντας την πιθανότητα έκδοσης αντιφατικών αποφάσεων. Τέλος, η τεχνητή νοημοσύνη μπορεί να βοηθήσει στην ανωνυμοποίηση δικαστικών αποφάσεων, αφαιρώντας δεδομένα που θα μπορούσαν να αποκαλύψουν τις ταυτότητες των διαδίκων³⁷, προστατεύοντας έτσι την ιδιωτικότητά τους.

2.2.3. Τα Smart Courts της Κίνας

Σε μία χώρα που η ανάγκη υπολογισμού και απόδοσης «αξίας» στην ανθρώπινη λειτουργία εντείνει τη χρήση μεθόδων αποτίμησης που μπορεί να περιλαμβάνουν εργαλεία ποιοτικού υπολογισμού (π.χ κριτικές) αλλά και ποσοστού (π.χ βαθμολογίες)

³⁷ Βλ. Bernhardt, W., (2021) *The Use of Artificial Intelligence in the Field of Justice*”, Internet and New Technologies Law. σελ. 173 – 195.

που είθισται να συνδυάζονται³⁸, βλέπουμε τη δικαστική λειτουργία να προοδεύει κρατώντας τα πρωτεία.

Συγκεκριμένα, τον Δεκέμβριο του 2019, το Ανώτατο Λαϊκό Δικαστήριο της Κίνας, αποκάλυψε ότι χρησιμοποιούσε δικαστή τεχνητής νοημοσύνης ήδη από το έτος 2017³⁹. Το πρώτο διαδικτυακό δικαστήριο δημιουργήθηκε το 2017 στην πόλη Χανγκζού και ακολούθησαν άλλα δύο στο Πεκίνο και την πόλη Γκουανγκζού. Τα δικαστήρια αυτά έχουν κεντρική δικαιοδοσία για όλες τις αστικές και διοικητικές υποθέσεις που άπτονται της καθ' ύλην αρμοδιότητας τους, η οποία περιλαμβάνει 11 διαφορετικές κατηγορίες μεταξύ των οποίων βρίσκονται κατά κύριο λόγο οι υποθέσεις που σχετίζονται με την χρήση του διαδικτύου όπως είναι οι διαφορές από συμβάσεις που σχετίζονται με ηλεκτρονικές αγορές και ηλεκτρονικές υπηρεσίες και οι υποθέσεις αδικοπραξιών που σχετίζονται με διαδικτυακή προσβολή δικαιωμάτων προσωπικότητας. Υπάρχει, ωστόσο, ακόμα αβεβαιότητα σχετικά με το αν στα συγκεκριμένα δικαστήρια χρησιμοποιούνται πράγματι δικαστές που βασίζονται στην τεχνητή νοημοσύνη. Ορισμένες πηγές δηλώνουν ξεκάθαρα ότι οι αποφάσεις λαμβάνονται από «δικαστές - ρομπότ», οι οποίοι συμμετέχουν στη διαδικασία μέσω εικονικών άβαταρ, που δημιουργούνται με τη βοήθεια της τεχνητής νοημοσύνης.⁴⁰ Επιπλέον, φαίνεται ότι μια σειρά σημαντικών αλλαγών είχαν ήδη εισαχθεί στα δικαστήρια μέχρι το 2017. Πράγματι, ο Susskind στο βιβλίο του "Online Courts and The Future of Justice" σχολίασε την εμπειρία του επισκεπτόμενος ένα δικαστήριο στην Χανγκζού, Κίνα το 2017: "Εντυπωσιάστηκα με αυτό που είδα: έναν στατικό ρομπότ στην περιοχή υποδοχής που προσφερόταν online νομική βοήθεια για τους χρήστες του δικαστηρίου· εγκαταστάσεις για την ηλεκτρονική υποβολή εγγράφων· ειδικά εικονικά δικαστήρια· αναγνώριση φωνής ανεξάρτητη από τον ομιλητή" (δεν χρειάζονται πλέον στενογράφοι)· και μια επίδειξη του πρώτου "διαδικτυακού δικαστηρίου" της Κίνας, το οποίο επιλύει διαφορές σχετικές με το διαδίκτυο, όπως διαφορές σχετικές με online

³⁸ Βλ. Διπλωματική Εργασία της Σιδέρη Μ. (2025), «Κρατική επιτήρηση και κοινωνική ταξινόμηση στην Κίνα» σελ. 97.

³⁹ Βλ. Διπλωματική Εργασία Ελ. Πολυζώνη, "ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ: Εφαρμογές και προκλήσεις για την εισαγωγή της τεχνητής νοημοσύνης στα δικαστικά συστήματα", Μεταπτυχιακή διπλωματική εργασία, σελ. 41-42.

⁴⁰ Βλ. Chesterman S. (2023), "All Rise for the Honourable Robot Judge? Using Artificial Intelligence to Regulate AI", Technology and Regulation, σελ. 45-47.

δάνεια, ηλεκτρονικό εμπόριο (συμβατικά και θέματα ευθύνης προϊόντων), διαφορές ονομάτων τομέων και θέματα πνευματικών δικαιωμάτων online.⁴¹

2.2.4. Περίπτωση Εσθονίας

Το 2019, αναφορές στα μέσα ενημέρωσης υποστήριζαν ότι το Υπουργείο Δικαιοσύνης της Εσθονίας είχε αναπτύξει ένα καινοτόμο σύστημα τεχνητής νοημοσύνης, ικανό να εκδικάζει υποθέσεις μικροδιαφορών έως 7.000 ευρώ, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Οι πληροφορίες αυτές περιέγραφαν ένα φιλόδοξο πρόγραμμα, όπου τα αντίδικα μέρη θα υπέβαλαν ηλεκτρονικά τα έγγραφα και τα δικόγραφά τους, τα οποία το σύστημα θα αξιολογούσε για να εκδώσει απόφαση. Προβλεπόταν, επίσης, ότι σε περίπτωση ένστασης, η υπόθεση θα εξεταζόταν από ανθρώπινο δικαστή.

Η είδηση αυτή προσέελκυσε διεθνές ενδιαφέρον, δεδομένης της φήμης της Εσθονίας ως πρωτοπόρου στην ενσωμάτωση των νέων τεχνολογιών στον δημόσιο τομέα. Ωστόσο, το φιλόδοξο εγχείρημα δεν προχώρησε ποτέ. Τον Φεβρουάριο του 2022, το Υπουργείο Δικαιοσύνης της Εσθονίας εξέδωσε επίσημη ανακοίνωση διαψεύδοντας τα δημοσιεύματα⁴². Στην ανακοίνωσή του ανέφερε ρητά πως «δεν έχει υπάρξει, ούτε προβλέπεται, η ανάπτυξη οποιουδήποτε συστήματος τεχνητής νοημοσύνης που να υποκαθιστά τους ανθρώπινους δικαστές, είτε για υποθέσεις μικροδιαφορών είτε για άλλες δικαστικές διαδικασίες».

Η διευκρίνιση αυτή υπογράμμισε ότι ο στόχος της Εσθονίας είναι να αξιοποιεί την τεχνολογία για τη βελτίωση της αποδοτικότητας του δικαστικού συστήματος, κυρίως μέσω της μείωσης του διοικητικού φόρτου, χωρίς να αντικατασταθεί ο ρόλος των δικαστών. Το περιστατικό αυτό αποτελεί παράδειγμα της ανάγκης προσεκτικής αξιολόγησης πληροφοριών και διασταύρωσης πηγών, ειδικά όταν πρόκειται για ευαίσθητα ζητήματα, όπως η απονομή δικαιοσύνης.

⁴¹ Βλ. Shi, Changqing and Sourdin, Tania and Li, Bin, (2021), *The Smart Court - A New Pathway to Justice in China?* International Journal for Court Administration, TNPI HEIN, σελ. 8.

⁴² Βλ. ιστότοπο [Estonia does not develop AI Judge | Justitsministeerium](https://www.justitsministeerium.ee/en/press-releases/estonia-does-not-develop-ai-judge), τελευταία πρόσβαση 29/12/2025.

2.2.5 e-Curia: Ηλεκτρονική κατάθεση και επίδοση διαδικαστικών εγγράφων

Μια ακόμη πλατφόρμα που εμπεριέχει στοιχεία Τεχνητής Νοημοσύνης είναι το e-Curia. Το e-Curia είναι μια επίσημη ηλεκτρονική πλατφόρμα του Δικαστηρίου της Ευρωπαϊκής Ένωσης που χρησιμοποιεί ΤΝ, επιτρέποντας την ηλεκτρονική κατάθεση και επίδοση διαδικαστικών εγγράφων μεταξύ των διαδίκων και των δικαστικών αρχών. Από την 1η Δεκεμβρίου 2018, το e-Curia αποτελεί το μοναδικό μέσο ανταλλαγής δικογράφων με το Γενικό Δικαστήριο της ΕΕ, ενισχύοντας την αμεσότητα και την αποδοτικότητα των δικαστικών διαδικασιών.⁴³

Κάθε διαδικαστικό έγγραφο που κατατίθεται μέσω του συστήματος e-Curia λογίζεται ότι αποτελεί το πρωτότυπο του εγγράφου αυτού, υπό την έννοια του άρθρου 57, παράγραφος 1, του κανονισμού διαδικασίας, όταν για τη σχετική κατάθεση χρησιμοποιηθούν ο προσωπικός κωδικός αναγνώρισεως και το προσωπικό συνθηματικό του εκπροσώπου ενός διαδίκου ή του προσώπου που ενεργεί για λογαριασμό δικαστηρίου κράτους μέλους. Η χρήση του προσωπικού κωδικού αναγνώρισεως και του προσωπικού συνθηματικού λογίζεται ως υπογραφή του εγγράφου αυτού. Τα διαδικαστικά έγγραφα, περιλαμβανομένων των αποφάσεων και διατάξεων, επιδίδονται μέσω του e-Curia στους κατόχους λογαριασμού e-Curia οι οποίοι, σε μια υπόθεση, εκπροσωπούν διάδικο ή ενεργούν για λογαριασμό δικαστηρίου κράτους μέλους, καθώς και στους τυχόν βοηθούς τους. Τα διαδικαστικά έγγραφα επιδίδονται επίσης μέσω του e-Curia στα κράτη μέλη, στα λοιπά κράτη που είναι συμβαλλόμενα Μέρη της Συμφωνίας για τον Ευρωπαϊκό Οικονομικό Χώρο και στα θεσμικά και τα άλλα όργανα ή τους οργανισμούς της Ένωσης που έχουν δεχθεί τον τρόπο αυτόν επιδόσεως. Τα διαδικαστικά έγγραφα μπορούν επίσης να επιδίδονται με χρήση των λοιπών τρόπων διαβιβάσεως που προβλέπει ο κανονισμός διαδικασίας, εάν τούτο επιβάλλεται λόγω του όγκου ή της φύσεως του εγγράφου ή όταν η χρήση του e-Curia είναι τεχνικά αδύνατη.⁴⁴

⁴³ Βλ. διαδικτυακό τόπο του Δικαστηρίου της Ευρωπαϊκής Ένωσης σχετικά με τις οδηγίες χρήσης του e-Curia.

⁴⁴ Βλ. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΑΠΟΦΑΣΗ ΤΟΥ ΔΙΚΑΣΤΗΡΙΟΥ της 16ης Οκτωβρίου 2018 σχετική με την κατάθεση και την επίδοση διαδικαστικών εγγράφων μέσω της εφαρμογής e-Curia, άρθρο 6 .

Είναι γεγονός πως όλες οι προαναφερόμενες πτυχές αποκρυστάλλωσης της ψηφιοποιημένης δικαιοσύνης δεν χαρακτηρίζονται από τελειότητα ως προς τη λειτουργία τους, αλλά τείνουν να βελτιώνονται και να αναβαθμίζονται «παράσπρονοντας» στη δίκη τους και εμάς, τους αποδέκτες τους, με αποτέλεσμα να τις αξιοποιούμε ολοένα και περισσότερο. Ας μη ξεχνάμε πως όσο η τεχνολογική εξέλιξη «καλπάζει» ακατάπαυστα, τόσο αυτές οι εφαρμογές ψηφιοποιημένης δικαιοσύνης θα προοδεύουν αποδεικνύοντας μας πως η ψηφιοποίηση της δικαιοσύνης δεν είναι απλώς δυνατή αλλά απολύτως εφικτή.

2.3. ΤΟ ΔΙΚΑΙΩΜΑ ΣΤΗ ΔΙΚΑΙΗ ΔΙΚΗ ΜΕΣΩ ΤΝ

2.3.1 Η επίδραση της Τεχνητής Νοημοσύνης στην αρχή του νόμιμου δικαστή

Η εισαγωγή της Τεχνητής Νοημοσύνης στον χώρο της δικαιοσύνης εκκινεί από την ανάγκη αντιμετώπισης του δυσθεώρητου χρονικού πλαισίου επίλυσης διαφορών, το οποίο στην Ελλάδα μπορεί να φτάσει ακόμη και τα επτά έτη.⁴⁵

Σύμφωνα με μελέτη που διεξήχθη ανάμεσα σε είκοσι δικηγόρους των Ηνωμένων Εθνών, η μέση απόδοση ακρίβειας των δικηγόρων είναι περίπου 85%, ενώ των προγραμμάτων της ΤΝ είναι 94%, παράλληλα ο μέσος χρόνος επιλύσεως της υπόθεσης για έναν μέσο δικηγόρο είναι 92 λεπτά, ενώ το πρόγραμμα της ΤΝ χρειάζεται μόλις κάποια δευτερόλεπτα.⁴⁶

Μπορεί το να εκδίδονται αυτοματοποιημένες αποφάσεις από έναν δικαστή «ρομπότ» να φαντάζεται κάτι το εξωπραγματικό και να εγκυμονεί πολλούς κινδύνους, όπως αυτοί θα αναλυθούν στην παρούσα διπλωματική εργασία, αλλά θα μπορούσε, όπως και είναι, να είναι και πολύ βοηθητική μια τέτοια ιδέα. Η ΤΝ δεν έχει ανθρωπιά να επεξεργαστεί την κάθε μεμονωμένη περίπτωση ξεχωριστά, έχει όμως αντικειμενικότητα και δεν επηρεάζεται από ψυχολογικούς παράγοντες. Μπορεί δηλαδή σε μια ποινική υπόθεση μικροποσότητας ναρκωτικών ουσιών η νομοθεσία να προβλέπει τη καταδίκη

⁴⁵ Βλ. Παναγοπούλου Φ., *Η απονομή της δικαιοσύνης μέσω Τεχνητής Νοημοσύνης. Συνταγματικά ζητήματα δικαστικής προστασίας*, σε : Συλλογικό έργο, Σύ και δικαστής άριστος, σελ 1273, ΤΝΠ: ΣΑΚΚΟΥΛΑΣ.

⁴⁶ Βλ. Stillmann J., *An AI just Outperformed 20 Top Lawyers (and the Lawyers Were Happy)*, A new study highlights a major flaw in much of the usual 'Robots will take all our jobs!', <https://www.inc.com/jessica-stillman/an-ai-just-outperformed-20-top-lawyers-and-lawyers-were-happy.html> τελευταία πρόσβαση 03/02/2026

του δράστη ακόμη και για λίγα μόλις γραμμάρια, στην πραγματικότητα όμως και σύμφωνα με πάγια νομολογία⁴⁷ «ο δράστης μπορεί να κριθεί ατιμώρητος, εάν το δικαστήριο εκτιμώντας τις περιστάσεις τέλεσης της πράξης και την προσωπικότητα του δράστη, κρίνει ότι η αξιόποινη πράξη ήταν εντελώς περιστασιακή και δεν είναι πιθανό να επαναληφθεί». Γίνεται λοιπόν αντιληπτό πως ένα μηχάνημα δεν θα μπορούσε σε μια τέτοια περίπτωση να κρίνει τους παραπάνω παράγοντες αφού όπως αναλύθηκε, δεν επηρεάζεται από ψυχολογικούς παράγοντες και δεν μπορεί να λυπηθεί » τον δράστη.

2.3.2 Η αρχή του «ανθρώπινου ελέγχου» και η διαφύλαξη της δικαστικής ανεξαρτησίας

Η διαπίστωση ότι τα συστήματα Τεχνητής Νοημοσύνης αδυνατούν να προσμετρήσουν υποκειμενικούς και ψυχολογικούς παράγοντες, όπως η μεταμέλεια ή η προσωπικότητα του κατηγορουμένου, καθιστά επιτακτική την εφαρμογή της αρχής του «ανθρώπινου ελέγχου». Σύμφωνα με την αρχή αυτή, η λήψη οποιασδήποτε δικαστικής απόφασης που παράγει έννομα αποτελέσματα δεν μπορεί να επαφίεται αποκλειστικά σε έναν αλγόριθμο, αλλά πρέπει να διέρχεται υποχρεωτικά από την κρίση ενός φυσικού δικαστή. Ο δικαστής οφείλει να διατηρεί την απόλυτη εξουσία να επικυρώνει, να τροποποιεί ή και να απορρίπτει την αλγοριθμική εισήγηση, διασφαλίζοντας ότι η δικαιοσύνη παραμένει μια ανθρωποκεντρική διαδικασία.⁴⁸

Η ανάγκη αυτή πηγάζει από την προστασία της δικαστικής ανεξαρτησίας και αμεροληψίας. Υπάρχει ο ορατός κίνδυνος της λεγόμενης «αλγοριθμικής συμμόρφωσης», όπου ο δικαστής, υπό το βάρος του τεράστιου φόρτου εργασίας, ενδέχεται να υιοθετεί άκριτα τα αποτελέσματα της μηχανής. Μια τέτοια εξέλιξη θα οδηγούσε στην ουσιαστική υποκατάσταση του νόμιμου δικαστή από ένα «μαύρο κουτί» (black box) αλγορίθμων, του οποίου η λειτουργία δεν είναι πάντα διαφανής. Για να αποφευχθεί αυτό, τα συστήματα Τεχνητής Νοημοσύνης πρέπει να σχεδιάζονται ως εργαλεία υποστήριξης (Decision Support Systems) και όχι ως αυτόνομοι λήπτες αποφάσεων, επιτρέποντας στον δικαστή να ασκεί την αξιολογική του κρίση και να αιτιολογεί την απόφασή του με βάση τις

⁴⁷ Βλ. Ν.4139/2023, αρ. 29 παρ. 2.

⁴⁸ Βλ. Terzidou K. (2023), *The Use of Artificial Intelligence in the Judiciary and Its Compliance with the Right to a Fair Trial*, SSRN, σελ. 158.

ιδιαιτερότητες της κάθε περίπτωσης. Όλα αυτά γιατί, σύμφωνα και με τον Campbell ⁴⁹ η κατασκευή του υπολογιστικού συστήματος βασίστηκε στη θεωρία ότι το μυαλό λειτουργεί σαν μια λογική μηχανή, ενώ το υπολογιστικό σύστημα χρησιμοποιεί συγκεκριμένους κανόνες και δεδομένα.

Η πλέον ευρεία χρήση της τεχνητής νοημοσύνης είτε κατά τη διάρκεια της προδικασίας είτε σε μεταγενέστερο στάδιο, εγείρει δικαιολογημένα πλήθος ερωτημάτων κυρίως ως προς τη συνταγματική ερμηνεία αυτών των πρακτικών.

Το άρθρο 8 του Συντάγματος καθιερώνει το θεμελιώδες δικαίωμα του νόμιμου δικαστή, σύμφωνα με το οποίο κανένας δεν μπορεί να στερηθεί χωρίς τη θέλησή του τον δικαστή που του έχει ορίσει ο νόμος. Η συστηματική και γραμματική ερμηνεία της διάταξης οδηγεί στο συμπέρασμα ότι ως δικαστής εννοείται φυσικό πρόσωπο, κάτι που αποκλείει καταρχήν την λήψη δικαστικών αποφάσεων με χρήση τεχνητής νοημοσύνης, εν τη απουσία δηλαδή φυσικού προσώπου και μάλιστα δικαστή⁵⁰ Η χρήση αλγορίθμων και κατ'επέκταση η χρήση τεχνητής νοημοσύνης στην ποινική δίκη εγείρει ζητήματα συμβατότητας με το άρθρο 6 παρ. 1 της ΕΣΔΑ, όπου κατοχυρώνει το δικαίωμα της δίκαιης δίκης, όπως και του αντίστοιχου άρθρου 47 παρ. 2 του ΧΘΔΕΕ. Συνηθέστερη περίπτωση συνιστά η επικουρική - πληροφοριακή χρήση της τεχνητής νοημοσύνης από τον δικαστή κατά την προετοιμασία της απόφασης, οπότε και συμβάλλει στην εκτίμηση των πραγματικών ή και νομικών περιστατικών της υπό διερεύνηση υπόθεσης.⁵¹

Ιδίως τώρα, όσον αφορά στη διαδικασία της ποινικής δίκης- και σε περίπτωση αυτοματοποιημένης απόφασης από αλγορίθμους, όπως αυτό θα αναλυθεί περαιτέρω, είναι ιδιαίτερα κρίσιμο, ο ποινικός δικαστής, τηρώντας την επιταγή του άρθρου 177 ΚΠΔ, σύμφωνα με το οποίο ο δικαστής αποφασίζει κατά την πεποίθησή του ακολουθώντας τη φωνή της συνείδησής του, να μη βασίζεται ετέρου αποκλειστικά σε αλγοριθμικές προγνώσεις προκειμένου να εκφέρει κρίση σε συγκεκριμένη υπόθεση. Εξάλλου, όταν ο αλγόριθμος τροφοδοτείται κατά βάση από μια νομική τράπεζα αποφάσεων, εντείνεται ο

⁴⁹ Βλ. Campbell J., (1989). *The improbable machine: What the upheavals in Artificial Intelligence research reveal about how the mind really works.*

⁵⁰ Βλ. Enders P., *Einsatz Kunstlicher Intelligenz bei juristischer Entscheidungsfindung*, JA 2018, σελ 723.

⁵¹ Βλ. Φιλόπουλος Π., *Η χρήση των αλγορίθμων στη μετεξέλιξη του Ποινικού Δικαίου*, ΕΛΛΔνη 5/2024, σ. 1337.

κίνδυνος επιρροής του από υποκειμενικές αντιλήψεις, κάτι που οδηγεί αναπόφευκτα σε υποβάθμιση του ρόλου του δικαστή. Έχει παρατηρηθεί, μάλιστα, ότι ο δικαστής κινδυνεύει να αναλάβει τον ρόλο του “φυγόποινου κριτή”, δηλαδή ενός δικαστή ο οποίος θα παραμείνει προσκολλημένος στην πρόταση του αλγόριθμου, αδυνατώντας να αναλάβει την αυθεντική, προσωπική του κρίση για την υπόθεση που μελετά.⁵²

Όσον αφορά στη χρήση αλγορίθμων για την πρόληψη του κινδύνου υποτροπής του δράστη, η τεχνητή νοημοσύνη ενδέχεται να θεωρηθεί χρήσιμο εργαλείο. Στο ουσιαστικό ποινικό δίκαιο ο κίνδυνος υποτροπής του καταδικασθέντος πρωταγωνιστεί κυρίως κατά το στάδιο της επιμέτρησης της ποινής, σύμφωνα με το άρθρο 79 παρ. 5 περ. α' του ΠΚ και περιορίζεται στην κατ'επάγγελμα τέλεση της πράξης. Αντίστοιχα, λαμβάνεται υπόψη και κατά την απόφαση αναστολής ή μη της εκτέλεσης της ποινής, όπως προβλέπεται στο άρθρο 99 παρ. 1 εδ. β' ΠΚ ή κατ'άρθρο 302 παρ. 7 εδ. β' ΚΠΔ στη διαδικασία συνδιαλλαγής ή σύμφωνα με το άρθρο 303 παρ. 4 εδ. δ' ΚΠΔ στην ποινική διαπραγμάτευση. Βέβαια, ακόμα και στην περίπτωση χρήσης της τεχνητής νοημοσύνης για την διαπίστωση υποψίας διάπραξης ενός εγκλήματος θα πρέπει σε κάθε περίπτωση να συντρέχουν οι προϋποθέσεις που απαιτούνται ώστε να διαπιστωθεί η ύπαρξη κινδύνου.⁵³

Σε κάθε περίπτωση η χρήση της τεχνητής νοημοσύνης στην ποινική δικαιοσύνη πρέπει να θεμελιώνεται σε ουσιώδεις συνταγματικές και δικονομικές εγγυήσεις οι οποίες θα διασφαλίζουν την αρχή του νόμιμου δικαστή, της διαφάνειας, του τεκμηρίου αθωότητας, της δίκαιης δίκης, της αμεσότητας και της ισότητας των όπλων. Ιδίως όσον αφορά στην τήρηση της ισότητας των όπλων, η ψηφιοποίηση εγείρει σημαντικούς κινδύνους όταν χρησιμοποιούνται μεγάλοι όγκοι δεδομένων (big data), όπως συμβαίνει και στην τεχνητή νοημοσύνη. Τα εμπλεκόμενα μέρη απαιτείται να έχουν ισότιμη πρόσβαση στα ίδια προγράμματα ανάλυσης δεδομένων στα οποία έχουν πρόσβαση δικωτικές αρχές και δικαστήρια.

⁵² Ο.π. υποσημ. 51, σελ. 1343.

⁵³ Ο.π. υποσημ. 52.

2.3.3. Το πλαίσιο της Αλγοριθμικής Δικαιοσύνης: Διανεμητική και Διαδικαστική προσέγγιση

Η ενσωμάτωση της Τεχνητής Νοημοσύνης στη δικαστική πρακτική φέρνει στο προσκήνιο την ανάγκη ορισμού της «αλγοριθμικής δικαιοσύνης». Η έννοια αυτή δεν είναι μονοδιάστατη, αλλά απαιτεί τη σύζευξη των υπαρχόντων νομικών κανόνων με τις κανονιστικές αντιλήψεις περί δικαίου. Σύμφωνα με τη θεωρία του Rawls,⁵⁴ η δικαιοσύνη βασίζεται σε μια κοινή δημόσια αντίληψη, όπου τα κοινωνικά θεσμικά όργανα αποδέχονται και εφαρμόζουν ενιαίες αρχές. Στο πλαίσιο των αλγορίθμων, η αντίληψη αυτή αναλύεται σε δύο βασικούς άξονες: τη διανεμητική και τη διαδικαστική δικαιοσύνη.

Η διανεμητική δικαιοσύνη (distributive justice) εστιάζει στο αποτέλεσμα της απόφασης και στον τρόπο με τον οποίο κατανέμονται τα οφέλη ή οι επιβαρύνσεις. Σε ένα αλγοριθμικό σύστημα, η δικαιοσύνη αυτού του τύπου κρίνεται από το αν το τελικό αποτέλεσμα θεωρείται δίκαιο βάσει του εκάστοτε πλαισίου, όπως λ.χ. μπορεί να είναι ο καθορισμός προστίμου ανάλογα με την οικονομική δυνατότητα του εκάστοτε παραβάτη. Αντίθετα, η διαδικαστική δικαιοσύνη (procedural justice) αφορά την αντιληπτή ορθότητα της ίδιας της διαδικασίας λήψης της απόφασης. Είναι αξιοσημείωτο ότι οι πολίτες τείνουν να αποδέχονται ακόμα και δυσμενείς αποφάσεις, αρκεί να πειστούν ότι η διαδικασία που ακολουθήθηκε ήταν δίκαιη, αμερόληπτη και βασισμένη στον σεβασμό και την εμπιστοσύνη.

2.3.4. Τήρηση των θεμελιωδών δικαιωμάτων και αρχών

Οι προσπάθειες που καταβάλλονται, τόσο σε επίπεδο Ευρωπαϊκής Ένωσης, όσο και εγχώρια, για την προαγωγή της ψηφιοποίησης στον τομέα της δικαιοσύνης, απαιτούν ταυτόχρονα και την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων που κατοχυρώνονται στην ΕΣΔΑ και τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, αφού ελλοχεύει πάντα ο κίνδυνος παραβίασής τους στο πλαίσιο της ψηφιακής ανάπτυξης, όπως επισημαίνει και το Συμβούλιο στα Συμπεράσματά του.⁵⁵

⁵⁴ Βλ. Kinchin N., “Voiceless”: the procedural gap in algorithmic justice, *International Journal of Law and Information Technology*, Volume 32, 2024, σελ. 2.

⁵⁵ Βλ. Συμβούλιο της Ε.Ε., “Συμπεράσματα του Συμβουλίου «Πρόσβαση στη δικαιοσύνη – αξιοποίηση των ευκαιριών της ψηφιοποίησης» (2020/C 342 I/01)”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2020, παραρ. 5.

Πιο συγκεκριμένα, είναι επιβεβλημένο να δοθεί ιδιαίτερη σημασία στην διασφάλιση των δικαιωμάτων που αφορούν την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων (άρθρο 8 ΕΣΔΑ), διότι η χρήση ψηφιακών τεχνολογιών ενέχει το κίνδυνο παραβίασης των συσκευών και των δεδομένων που αποθηκεύονται σ' αυτές στα πλαίσια της ψηφιοποίησης. Εκτός αυτού, η χρήση προγραμμάτων τεχνητής νοημοσύνης στο τομέα της δικαιοσύνης θέτει προκλήσεις όσον αφορά τη πιθανότητα “χακαρίσματος” αυτών των συστημάτων για οικονομικούς ή άλλους λόγους. Γι' αυτό το λόγο, κρίνεται απαραίτητη η δημιουργία ενός αξιόπιστου συστήματος κυβερνοασφάλειας που θα αποτρέπει τέτοιους κινδύνους.⁵⁶ Ανησυχία μάλιστα προκαλεί το γεγονός της δυνατότητας ταυτοποίησης ενός ατόμου, μέσω της δημοσίευσης των δικαστικών αποφάσεων, ακόμη κι αν αυτές είναι ανωνυμοποιημένες, διότι με τη διάδοση τέτοιων δεδομένων προσβάλλεται η ανθρώπινη αξιοπρέπεια και είναι δυνατές οι καταρτίσεις προφίλ, οδηγώντας έτσι σε διακριτική μεταχείριση.⁵⁷

Επίσης, η εισαγωγή της ΤΝ θέτει σε δοκιμασία τη συνταγματική αρχή της ισότητας, η οποία επιτάσσει την ίση μεταχείριση ενώπιον του νόμου. Και αυτό διότι ελλοχεύει ο κίνδυνος της μεροληψίας των αλγορίθμων υπέρ ή κατά συγκεκριμένων ομάδων. Σε κάποιες χώρες δηλαδή, όπως στις Η.Π.Α πολλά προγράμματα-μηχανήματα έχουν στοχοποιήσει κατά το παρελθόν συγκεκριμένες ομάδες όπως αυτές των έγχρωμων ανθρώπων έναντι των λευκών κατηγορούμενων, με τους πρώτους να έχουν διπλάσιο κίνδυνο ταξινομήσεως τους σε ομάδα υψηλού κινδύνου βίαιης υποτροπής. Αντιθέτως, οι λευκοί βίαιοι υπήκοοι είχαν μόλις 63% περισσότερες πιθανότητες να έχουν ταξινομηθεί εσφαλμένα σε ομάδα χαμηλού κινδύνου βίαιης υποτροπής, σε σύγκριση με τους βίαιους έγχρωμους υποτροπιάζοντες.⁵⁸

Αξιοσημείωτο είναι και το γεγονός ότι σύμφωνα με την ΑΙ ΑCT, τον πρώτο Ευρωπαϊκό Κανονισμό για την ΤΝ, τα συστήματα ΤΝ που προορίζονται για χρήση από δικαστική αρχή με σκοπό την παροχή συνδρομής σε δικαστικές αρχές και έρευνες των

⁵⁶ Βλ. Razmetaeva Y. & Razmetaev Se., (2021) *Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities*, Access to Just E Eur 104, σελ. 113.

⁵⁷ Ο.π. υποσημ. 5, σελ. 80.

⁵⁸Βλ. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> τελευταία πρόσβαση: 23/02/26.

πραγματικών περιστατικών και του νόμου και κατά την εφαρμογή του νόμου σε συγκεκριμένο σύνολο πραγματικών περιστατικών, πρέπει να χαρακτηριστούν ως υψηλού κινδύνου, λαμβανομένου υπόψη του δυνητικά σημαντικού αντικτύπου τους στη δημοκρατία, το κράτος δικαίου, τις ατομικές ελευθερίες, καθώς και το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου.⁵⁹

2.3.5 Τηλεδιασκέψεις (ΕΔΔΑ. *Sakhnovski κατά Ρωσίας*, Αριθμ. 21272/03, 2 Νοεμβρίου 2010; *Marcello Viola κατά Ιταλίας*, Αριθμ. 45106/04, 5 Οκτωβρίου 2006)

Για να γίνουν αντιληπτά όλα τα παραπάνω, αξίζει να αναφερθούν δύο πολύκροτες υποθέσεις του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) που αφορούν στο επίκαιρο ζήτημα της νομιμότητας των τηλεδιασκέψεων, την *Sakhnovski κατά Ρωσίας* της 2.11.2010 και *Marcello Viola*⁶⁰ κατά Ιταλίας της 5.10.2006 έκρινε συμβατή με τις απαιτήσεις του άρθρου 6 της ΕΣΔΑ τη βιντεοδιάσκεψη στο πλαίσιο ποινικών διαδικασιών, ως προδήλως μείζονος σημασίας διακύβευμα⁶¹, καθώς ο μηχανισμός αυτός συμβάλλει στην επιτάχυνση της διαδικασίας και υπό τον όρο διασφάλισης των δικαιωμάτων των διαδίκων και της εμπιστευτικότητας. Συγκεκριμένα, στην υπόθεση *Sakhnovski κατά Ρωσίας*⁶², το ΕΔΔΑ εξέτασε τη χρήση τηλεδιάσκεψης στις δικαστικές διαδικασίες και το κατά πόσο αυτή παραβίασε το δικαίωμα σε δίκαιη δίκη, όπως προβλέπεται στο άρθρο 6 της ΕΣΔΑ. Ο αιτών, ο οποίος είχε καταδικαστεί για σοβαρό ποινικό αδίκημα, κατήγγειλε ότι η συμμετοχή του στη διαδικασία αναίρεσης πραγματοποιήθηκε μέσω τηλεδιάσκεψης από το χώρο της κράτησής του, χωρίς να του επιτραπεί να παραστεί φυσικά στη δικαστική αίθουσα. Υποστήριξε ότι αυτό εμπόδισε τη σωστή επικοινωνία με τον δικηγόρο του και την ουσιαστική συμμετοχή του στη διαδικασία. Το ΕΔΔΑ έκρινε ότι η χρήση τηλεδιάσκεψης από μόνη της δεν συνιστά παραβίαση του δικαιώματος δίκαιης δίκης, εφόσον πληρούνται ορισμένες εγγυήσεις. Ωστόσο, στη συγκεκριμένη υπόθεση διαπιστώθηκε ότι ο αιτών δεν είχε επαρκή πρόσβαση σε νομική εκπροσώπηση και η δυνατότητα ουσιαστικής συμμετοχής του στη

⁵⁹ Βλ. Σωτηριάδου Φ., *Τεχνητή Νομοσύνη και Δικαιοσύνη: Διερεύνηση ή συρρίκνωση του δικαιώματος δικαστικής προστασίας*, σελ 400.

⁶⁰ Βλ. ΕΔΔΑ, *Marcello Viola κατά Ιταλίας* 45106/04 της 5.10.2006, §67.

⁶¹ Βλ. Παπαπαναγιώτου Α. και Ζάχου Χ. (2021), *Συστήματα Τεχνητής Νομοσύνης στον τομέα της Δικαιοσύνης. Τα ηθικά διλήμματα και τα όρια του Ευρωπαϊκού Χάρτη*, αναφορά των Προέδρων Ελεγκτικού Συνεδρίου, , ΤΝΠ Google scholar, σελ 25.

⁶² Βλ. ΕΔΔΑ, *Sakhnovski κατά Ρωσίας* 21272/03, της 2ας Νοεμβρίου 2010.

διαδικασία είχε περιοριστεί. Η υπόθεση υπογραμμίζει την ανάγκη προσεκτικής εφαρμογής τεχνολογιών στις δικαστικές διαδικασίες, με στόχο τη διατήρηση της δικαιοσύνης και της προστασίας των δικαιωμάτων των διαδίκων.

Περαιτέρω, στην υπόθεση Marcello Viola κατά Ιταλίας ο προσφεύγων, καταδικασθείς για πλήθος ανθρωποκτονιών και συμμετοχή στην ιταλική μαφία, ισχυρίστηκε ότι η μη φυσική παρουσία του ενώπιον του ποινικού εφετείου παραβίασε το δικαίωμα του σε δίκαιη δίκη. Το ΕΔΔΑ έκρινε ότι η παρουσία του κατηγορουμένου σε δίκη που θα κρίνει την ενοχή ή την αθωότητα του είναι αναγκαία, πλην όμως τούτο διασφαλίζεται και μέσω τηλεδιάσκεψης, η οποία προβλέπεται από το ιταλικό δίκαιο. Και τούτο διότι δια του τρόπου αυτού ο κατηγορούμενος μπορούσε τόσο να ακούει και να βλέπει όσο και να ακούγεται και να τον βλέπουν όλοι οι συμμετέχοντες στη δίκη (δικαστές, μάρτυρες κ.λπ.). Επίσης, διέθετε τη δυνατότητα να επικοινωνεί με τους συνηγόρους του υπό συνθήκες εμπιστευτικότητας, με συνέπεια τη μη χειροτέρευση της θέσης του εξαιτίας της μη φυσικής του παρουσίας του στο δικαστήριο. Αντιθέτως με τον τρόπο αυτό διασφαλίστηκαν η δημόσια τάξη, στον βαθμό που υπήρχαν υπόνοιες απόδρασής του, καθώς και τα δικαιώματα των μαρτύρων και της πολιτικής αγωγής, και επιτεύχθηκαν η πρόληψη αδικημάτων και η περάτωση της δίκης εντός ευλόγου χρόνου. Συνεπώς ο κατηγορούμενος έτυχε δίκαιης δίκης και δεν παραβιάστηκε το κατοχυρωμένο στο άρθρο 6 της ΕΣΔΑ δικαίωμά του.

2.4 ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ

2.4.1 Τεχνητή Νοημοσύνη στο Αστικό και Ποινικό Δίκαιο

Η αυτοματοποίηση της νομικής πληροφορίας έχει οδηγήσει στη σκέψη της αυτοματοποιημένης απονομής δικαιοσύνης μέσω συστημάτων ΤΝ. Η ιδέα του δικαστή «ρομπότ» είναι παλαιότερη από τον τομέα της ΤΝ και δικαίου.⁶³ Οι προσδοκίες που υπήρχαν στην αρχή δεν αποδείχθηκαν επαρκείς, με αποτέλεσμα η ΤΝ να παραμένει ακόμη αναξιόπιστη στον τομέα της δικαιοσύνης. Ωστόσο, η ΤΝ προσφέρει νέες λύσεις ως προς την ηλεκτρονική ανακάλυψη και τη συνδρομή των φυσικών δικαστών στην

⁶³ Βλ. Ronkainen A., *From Spelling Checkers to Robot Judges? Some Implications of Normativity in Language Tech and AI & Law*, σελ. 1.

προετοιμασία και μελέτη του μεγάλου όγκου επεξεργασίας δεδομένων των υπό κρίση υποθέσεων.

Το φαινόμενο ότι μια μηχανή μπορεί να κατανοήσει πιο γρήγορα ένα κείμενο από τον άνθρωπο δημιουργεί ελπίδες ότι στο άμεσο μέλλον θα καταστεί δυνατό, τουλάχιστον στις πιο απλές και καθημερινές υποθέσεις, η επίλυση και η έκδοση αυτοματοποιημένης απόφασης από δικαστές «ρομπότ». Εξάλλου ο στόχος της δικαιοσύνης δεν είναι να αντικατασταθούν οι φυσική δικαστές από τις μηχανές, αλλά να καταστούν «δεξί τους χέρι» μέσω της αναδιατάξεως του τρόπου διαχείρισεως του χρόνου και της πιθανότητας λάθους.

Παράλληλα, η έννοια της πρόσβασης στη δικαιοσύνη αποκτά πλέον ευρύτερο περιεχόμενο στο ψηφιακό περιβάλλον. Η πρόσβαση αυτή δεν περιορίζεται μόνο στη φυσική δυνατότητα προσφυγής ενώπιον των δικαστηρίων, αλλά περιλαμβάνει και την παροχή διαδικτυακής πληροφόρησης σχετικά με τα δικαιώματα των πολιτών, τη δημοσίευση της νομολογίας, καθώς και την ανάπτυξη ψηφιακών μηχανισμών επίλυσης διαφορών, όπως η ηλεκτρονική νομική βοήθεια, η διαδικτυακή διαμεσολάβηση και άλλες μορφές εξωδικαστικής επίλυσης διαφορών.⁶⁴

Η σημασία της αξιοποίησης των ψηφιακών τεχνολογιών για την ενίσχυση της πρόσβασης στη δικαιοσύνη έχει αναγνωριστεί και σε ευρωπαϊκό επίπεδο. Κοινοβουλευτική Συνέλευση του Συμβουλίου της Ευρώπης έχει επισημάνει ότι η πρόσβαση στη δικαιοσύνη αποτελεί θεμελιώδη προϋπόθεση για τη λειτουργία του κράτους δικαίου και για την αποτελεσματική προστασία των ανθρωπίνων δικαιωμάτων, ενώ παράλληλα έχει ενθαρρύνει τη χρήση σύγχρονων τεχνολογιών πληροφορικής με στόχο την επιτάχυνση και την απλούστευση των δικαστικών διαδικασιών.⁶⁵

Παρά τις δυνατότητες αυτές, η ενσωμάτωση της τεχνητής νοημοσύνης στον νομικό τομέα εξελίσσεται με σχετικά αργούς ρυθμούς. Μεταξύ των βασικών παραγόντων που επιβραδύνουν την υιοθέτησή της συγκαταλέγονται η περιορισμένη

⁶⁴ Βλ. Resolution 2081 (2015), «Access to justice and the Internet: potential and challenges», para. 1, 27 November 2015, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=22283&lang=en> τελευταία πρόσβαση 23/02/2026.

⁶⁵ Βλ. Διπλωματική εργασία της Μάρα Α. Γιώργα (2022), «ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΠΡΟΣΒΑΣΗ ΣΤΗ ΔΙΚΑΙΟΣΥΝΗ» του Πανεπιστημίου Πειραιώς, σελ 23.

τεχνική εξοικείωση πολλών νομικών επαγγελματιών με τις σχετικές τεχνολογίες, η έλλειψη διαφάνειας ως προς τον τρόπο λειτουργίας των αλγοριθμικών συστημάτων, καθώς και οι επιφυλάξεις σχετικά με την αξιοπιστία των αποτελεσμάτων και τη δικαστική αποδοχή τους.

Κάνοντας μια μικρή εισαγωγή, αφού αυτά θα αναλυθούν στο επόμενο κεφάλαιο, το Ποινικό Δίκαιο έχει «ανθήσει» εξαιτίας της ΤΝ-και γενικότερα εξαιτίας των νέων και εξελιγμένων τεχνολογιών. Έχουν δημιουργηθεί πολλά νέα αδικήματα με τη χρήση της ΤΝ και γενικότερα με τη χρήση διαδικτύου. Συγκεκριμένα, το κυβερνοέγκλημα αναπτύσσεται ραγδαία, «προλαβαίνοντας» πολλές φορές την νομοθετική του κάλυψη. Παρά το γεγονός ότι η χρήση της ΤΝ στις προδικαστικές διαδικασίες στέκεται επάξια ως βοηθός της δικαιοσύνης, κατά τη διάρκεια της δίκης, η ΤΝ, στα περισσότερα δικαστήρια της Ευρώπης είναι ασυνήθιστη. Κανένα είδος ΤΝ δεν χρησιμοποιείται, καθώς το νομολογιακό καθεστώς στις περισσότερες χώρες της Ευρώπης προβλέπει ότι οι αποφάσεις θα πρέπει να εκδίδονται αποκλειστικά και μόνο από τους δικαστές.

2.4.2 Έκδοση αποφάσεων

Το ελληνικό Υπουργείο Δικαιοσύνης στην παρουσίαση περί εφαρμογών ΤΝ στον τομέα της δικαιοσύνης τον Μάρτιο του 2024 έθεσε ήδη ως στόχο την χρήση συστημάτων ΤΝ στην επίλυση μικροδιαφορών μέχρι, φυσικά, ένα συγκεκριμένο ποσό⁶⁶ ακολουθώντας το μοντέλο της Εσθονίας. Στην Εσθονία ήδη από το 2019 βλέπουμε να έχει αναπτυχθεί ένα πιλοτικό σύστημα επίλυσης μικροδιαφορών με αξία έως 7.000€ με την χρήση συστημάτων ΤΝ, με τον Διευθύνων Σύμβουλο Δεδομένων, Ott Velsberg, να φημολογείται πως δηλώνει ότι αυτό το σύστημα θέλει «να εξαλείψει το ανθρώπινο στοιχείο» και ότι η εφαρμογή της ΤΝ στη συγκεκριμένη περίπτωση, θα είναι λειτουργική στην Εσθονία, δεδομένου ότι η χώρα βασίζεται σε ένα δικαστικό σύστημα που «είναι τώρα ήδη κατά το ήμισυ αυτοματοποιημένο».⁶⁷

Η ηλεκτρονική επίλυση διαφορών (εφεξής «ΗΕΔ») χρησιμοποιείται δειλά δειλά ήδη από πολλές χώρες της Ευρώπης αφού ορισμένοι το θεωρούν συμπληρωματική βοήθεια στην πιο γρήγορη επίλυση διαφορών.

⁶⁶ <https://ministryofjustice.gr/?p=13929> , τελευταία πρόσβαση 24/02/2026

⁶⁷ Βλ. J. Park, “Your Honor, AI”, 2020, Harvard international Review, σελ 64

Εάν ήθελε ληφθεί δεδομένο ως υπόθεση εργασίας ότι επικρατεί ένα καθολικό μοντέλο ηλεκτρονικής επίλυσης διαφορών με την χρήση αλγορίθμων και συστημάτων TN, ανακύπτουν ορισμένοι προβληματισμοί. Αρχικά, η ανθρώπινη επέμβαση κυριαρχεί στο στάδιο της δημιουργίας του εκάστοτε αλγορίθμου καθώς και της μηχανικής μάθησης του εκάστοτε συστήματος TN, χωρίς να ισχύει το ίδιο για το στάδιο κατά το οποίο έχουν τεθεί σε λειτουργία τα συστήματα αυτά. Έτσι, φαίνεται να παραγκωνίζεται το δικαίωμα στον φυσικό δικαστή⁶⁸, η επέμβαση του οποίου ενδεχομένως να περιορίζεται σε μία απλή επαλήθευση της κρίσης στην οποία κατέληξε κάποιος αλγόριθμός ή ένα σύστημα TN. Υπό αυτήν την τελευταία οπτική, το δικαίωμα στον φυσικό δικαστή φαίνεται να αποκτά μία ακόμη έκφανση, εκείνη του δικαιώματος στην ανθρώπινη παρέμβαση (human-in-the-loop). Άλλωστε, η ίδια η Ευρωπαϊκή Πράξη για την TN συμπεριέλαβε την δικαιοσύνη στους τομείς υψηλού κινδύνου. Αντιστοίχως, το Γαλλικό Γραφείο Επιτρόπου Πληροφοριών αναγνωρίζει το δικαίωμα σε ανθρώπινη παρέμβαση και επεξήγηση.⁶⁹ Πρόκειται, φυσικά, για το λεγόμενο ζήτημα του μαύρου κουτιού, το οποίο παραμένει, άρρηκτα συνδεδεμένο με τα συστήματα TN και έχει σοβαρό αντίκτυπο στην συνταγματικά κατοχυρωμένη ανάγκη αιτιολογίας των εκδοθησομένων δικαστικών αποφάσεων. Τούτη η έλλειψη επεξηγησιμότητας θέτει προσκόμματα στον εντοπισμό της ακριβούς νοητικής διαδρομής, του δικανικού συλλογισμού, στον οποίο στηρίχθηκε το εξαχθέν συμπέρασμα.⁷⁰ Η ανάγκη επεξηγησιμότητας εντείνεται και υπό το φως της εγγενούς προκατάληψης των συστημάτων TN, η οποία είναι εμφανής και στην ανάπτυξη αλγορίθμων στο πεδίο της προβλεπτική δικαιοσύνης.

Η προβλεπτική δικαιοσύνη βασίζεται στην εξέταση προηγούμενων δικαστικών αποφάσεων με την χρήση αλγορίθμων και την πρόβλεψη βάσει αυτών και της εκάστοτε δικογραφίας της εκδοθησομένης δικαστικής απόφασης σε κάθε νέα περίπτωση. Σημειώνεται ότι, όπως αναφέρεται και στον Ευρωπαϊκό Χάρτη Δεοντολογίας για την χρήση συστημάτων TN στα δικαστικά συστήματα και στο περιβάλλον τους (sic): «η αξιοπιστία του μοντέλου που δημιουργείται εξαρτάται σημαντικά από την ποιότητα των

⁶⁸ Ο.π υποσημ 22.

⁶⁹Βλ. Βόρρας σε Μήτρου, (2023) *“Μπορεί ο αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να δικάζει και να διοικεί;”*, Πανεπιστημιακές Εκδόσεις Κρήτης, σελ. 171.

⁷⁰ Βλ. Quattrocolo S. (2019) *“An Introduction to AI and Criminal Justice in Europe”*, 5 Rev Brasileira de Direito Processual Penal, σελ. 1519.

δεδομένων που χρησιμοποιούνται και από την επιλογή της τεχνικής της μηχανικής μάθησης».⁷¹ Έτσι, η μεταφορά προκαταλήψεων στο μοντέλο που δημιουργείται αποτελεί τον πλέον σοβαρό κίνδυνο στην ανάπτυξη και λειτουργία αντιστοίχων συστημάτων.

Στην έκδοση αποφάσεων έχουμε και τη κατηγορία της «αυτοματοποιημένης λήψης αποφάσεων», στα πεδία της τεχνητής νοημοσύνης, ιδίως στον δημόσιο τομέα. Σε αρκετές ευρωπαϊκές χώρες έχουν ήδη ενσωματωθεί σε διοικητικές διαδικασίες, υποστηρίζοντας ή ακόμη και αντικαθιστώντας σε ορισμένες περιπτώσεις την ανθρώπινη αξιολόγηση. Ενδεικτικά, χρησιμοποιούνται για την κατανομή υπηρεσιών στο δημόσιο σύστημα υγείας, για την κατηγοριοποίηση ανέργων στις υπηρεσίες απασχόλησης ή για τον εντοπισμό ευάλωτων κοινωνικών ομάδων.

Οι αυτοματοποιημένες αποφάσεις βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω αλγοριθμικών συστημάτων, τα οποία λειτουργούν χωρίς άμεση ανθρώπινη παρέμβαση.⁷² Η χρήση τέτοιων τεχνολογιών δημιουργεί νέες προοπτικές αλλά και προκλήσεις για την πρόσβαση στη δικαιοσύνη, καθώς επηρεάζει τον τρόπο λήψης αποφάσεων, την προστασία των θεμελιωδών δικαιωμάτων και την τήρηση των εγγυήσεων της δίκαιης διαδικασίας.

2.4.5. Προγνωστική Αστυνόμευση

Μέσω της προγνωστικής αστυνόμευσης, επιδιώκεται η «προγνωστική χαρτογράφηση» ενός πιθανού εγκλήματος λαμβάνοντας υπόψη μια ανάλυση συνολικού επιπέδου⁷³. Παράδειγμα τέτοια πρακτικής συνιστά η εφαρμογή “PredPol”, βασικό χαρακτηριστικό της οποίας είναι η ικανότητά της να προβαίνει σε προβλέψεις για μελλοντικές εστίες εγκλήματος. Αξίζει σε αυτό το σημείο να αναφερθεί, ότι πηγή έμπνευσης της εν λόγω εφαρμογής αποτελεί η επιστήμη της σεισμολογίας. Όπως έχει αποδειχθεί επιστημονικά ότι μετά από έναν πρώτο σεισμό συχνά ακολουθούν μετασεισμοί, έτσι και η εφαρμογή “PredPol” εδραζόμενη στο μοντέλο της «σχεδόν

⁷¹ Βλ. Ευρωπαϊκή Επιτροπή για την αποτελεσματικότητα της Δικαιοσύνης (2018), *Ευρωπαϊκός Χάρτης Δεοντολογίας για την χρήση συστημάτων ΤΝ στα δικαστικά συστήματα και στο περιβάλλον τους*, σελ. 43.

⁷² Βλ. Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων» 2019, σελ.292.

⁷³ Ο.π υποσημ 51, σελ 1329.

επαναλαμβανόμενης θεωρίας», εντοπίζει εγκλήματα που διαπράττονται σε γρήγορη διαδοχή. Πιο συγκεκριμένα, χρησιμοποιούνται τρεις μεταβλητές δεδομένων: ο τύπος του εγκλήματος, η τοποθεσία του εγκλήματος και η ημερομηνία/ώρα.⁷⁴

Οι εφαρμογές προγνωστικής αστυνόμευσης μπορούν να φανούν χρήσιμες και στη λήψη αποφάσεων ταυτοποίησης σχετικά με πραγματικούς ή πιθανούς παραβάτες. Η κατηγορία αυτή επικεντρώνεται στον εντοπισμό της εγκληματικής συμπεριφοράς είτε σε ομαδικό είτε σε ατομικό επίπεδο, αναζητώντας τις πιθανότητες τις οποίες ένα άτομο έχει προκειμένου να διαπράξει ένα έγκλημα ή είναι επιρρεπές προς παραβατική συμπεριφορά. Παράδειγμα τέτοιου συστήματος έχει εφαρμοστεί στο Ηνωμένο Βασίλειο, όπου αναπτύχθηκε το σύστημα HART (Harm Assessment Risk Tool). Το σύστημα αυτό αποσκοπεί στην αξιολόγηση κινδύνου μελλοντικής παράβασης και δίνει την ευκαιρία σε παραβάτες που αξιολογούνται ως «μέτριου κινδύνου» να συμμετάσχουν σε προγράμματα αποκατάστασης της αστυνομίας.⁷⁵

Σε αυτό το σημείο αξίζει βέβαια να αναφερθεί ότι στην επιστημονική κοινότητα έχει εκφρασθεί προβληματισμός σχετικά με την αποτελεσματικότητα πρακτικών προγνωστικής αστυνόμευσης. Πιο συγκεκριμένα, τέτοιες μέθοδοι τείνουν να υπεραπλουστεύουν το έγκλημα, δίνοντας περισσότερη έμφαση σε δευτερεύουσες παραμέτρους, όπως λόγου χάρη η γεωγραφική περιοχή στην οποία συμβαίνει ένα έγκλημα, αψηφώντας την βαθύτερη αιτία πίσω από την παραβατική συμπεριφορά των ανθρώπων⁷⁶. Ως εκ τούτου, η πολυπλοκότητα του εγκλήματος, το οποίο, αν μη τι άλλο, συνιστά και ιδιαίτερο κοινωνικό φαινόμενο, δεν μπορεί να αναπαρασταθεί επιτυχώς με τεχνικές προγνωστικής αστυνόμευσης.

2.4.6 Προγνωστική Ταυτοποίηση

Πριν διαταχθεί η ποινική δίωξη οι αρμόδιες αρχές εκκινούν μια έρευνα με άτομα ή ομάδα ανθρώπων που πρέπει να παρακολουθούνται και γενικότερα, τους υπόπτους. Τα συστήματα προγνωστικής ταυτοποίησης ουσιαστικά κατηγοριοποιούν συγκεκριμένα

⁷⁴ Ο.π, υποσημ 51, σελ 1334.

⁷⁵ Ο.π σελ 1335.

⁷⁶ Βλ. T. Singelsstein, *Predictive Pricing; Algorithmenbasierte Strafprognosen zur vorausschauenden Kriminalintervention*, NSTZ 2018, 1.

άτομα προσδιορίζοντας ποια άτομα είναι υψηλού κινδύνου.⁷⁷ Όλα τα παραπάνω εφαρμόζονται με αλγόριθμο βάσει των οποίων θα έπρεπε να μπορούν να εξεταστούν. Αυτό, εφαρμόζεται κυρίως σε τεχνολογικά ανεπτυγμένες χώρες όπως λ.χ. η Αμερική η οποία έχει υιοθετήσει αυτό το σύστημα μέσω της εφαρμογής Intrado Beware η οποία λειτουργεί μέσω της πλατφόρμας Intelligent Data Portal (IDP), της Motorola Solutions.

2.4.7 Ανωνυμοποίηση αποφάσεων μέσω TN

Η ανωνυμοποίηση των δικαστικών αποφάσεων μέσω τεχνητής νοημοσύνης παρουσιάζει σημαντικές προκλήσεις, ειδικά όταν πρόκειται για μαζική επεξεργασία δεδομένων, όπως συμβαίνει με τα σύνολα μεγάλων δεδομένων (big data)⁷⁸. Η διαδικασία της ψευδωνυμοποίησης είναι σύνθετη και απαιτητική, καθώς απαιτεί την αφαίρεση κάθε πληροφορίας που θα μπορούσε να αποκαλύψει την ταυτότητα των εμπλεκόμενων μερών. Αυτό εγείρει νομικά και τεχνικά ζητήματα σχετικά με το ποιος θα είναι υπεύθυνος για την υλοποίηση της διαδικασίας, καθώς και για τις ευθύνες που απορρέουν από την προστασία των προσωπικών δεδομένων.

Ιδιαίτερα κρίσιμο είναι το ζήτημα του φορέα που θα αναλάβει να διασφαλίσει την ανωνυμοποίηση. Ο φορέας αυτός θα πρέπει να διαχειρίζεται τις δικαστικές αποφάσεις με τρόπο που να συμμορφώνεται με το ισχύον νομικό πλαίσιο, ελαχιστοποιώντας τους κινδύνους για την προστασία των δεδομένων. Το έργο αυτό, ωστόσο, ενέχει σημαντικές ευθύνες, δεδομένων των τεχνικών δυσκολιών και των πιθανών συνεπειών από τυχόν παραλείψεις ή λάθη στη διαδικασία.

Ένα ακόμα κρίσιμο ερώτημα αφορά το εύρος της υποχρέωσης για ανωνυμοποίηση και αν αυτή θα πρέπει να επεκτείνεται στους δικαστές και τους δικηγόρους. Από τη μία πλευρά, η δημοσιότητα της δίκης και η διαφάνεια της δικαιοσύνης αποτελούν θεμελιώδεις αρχές που πρέπει να προστατεύονται. Από την άλλη, η δυνατότητα κατάρτισης προφίλ των εμπλεκόμενων επαγγελματιών μέσω αυτοματοποιημένων μεθόδων εγείρει ανησυχίες για την ιδιωτικότητά τους και τις συνέπειες που μπορεί να έχει κάτι τέτοιο στη δημόσια εικόνα και την επαγγελματική τους υπόσταση. Ακόμη

⁷⁷ Ο.π. υποσημ. 65, σελ. 32.

⁷⁸ Βλ. Καρκατζούνης Β., *Ο ρόλος των δεδομένων στο οικοσύστημα της Νομικής Τεχνολογίας (Legal Tech)*, ΤΝΠ QUALEX, ΣΥΝ, 4/2020, σελ.35.

περισσότερο μια τέτοια ευρεία χρήση ανωνυμοποίησης των δικαστικών αποφάσεων ενέχει τον κίνδυνο παραβίασης των προσωπικών δεδομένων των εμπλεκόμενων μερών, τόσο των δικαστικών λειτουργών, όσο και των διαδίκων, υπό το πρίσμα του άρθρου 9^Α του Σ, σύμφωνα με το οποίο «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει». Πιο συγκεκριμένα ακόμη και αν αντικατασταθούν τα ονόματα των μερών με αρχικά, η απόφαση ενδέχεται να περιγράφει μια νομική κατάσταση μοναδική ή ευρέως γνωστή⁷⁹. Σε αυτή την περίπτωση μπορεί να στοιχειοθετηθεί παραβίαση προσωπικών δεδομένων.

Η ανάγκη για ισορροπία μεταξύ της προστασίας των δεδομένων και της διαφάνειας καθιστά το ζήτημα εξαιρετικά περίπλοκο, απαιτώντας λεπτομερή ανάλυση και προσεκτική στάθμιση των αντικρουόμενων συμφερόντων.

ΚΕΦΑΛΑΙΟ ΙΙΙ Κυβερνοασφάλεια στο Ψηφιακό Δικαστικό Σύστημα

3.1 Ορισμός πληροφοριακού συστήματος

Ο ορισμός του «πληροφοριακού συστήματος» (ή συστήματος πληροφοριών) εδράζεται στο Άρθρο 2 της Οδηγίας 2013/40/ΕΕ, η οποία ενσωματώθηκε και στο ελληνικό δίκαιο (Άρθρο 13 ΠΚ). Ως τέτοιο νοείται κάθε συσκευή ή ομάδα διασυνδεδεμένων συσκευών που εκτελούν αυτόματη επεξεργασία ψηφιακών δεδομένων. Είναι κρίσιμο να επισημανθεί ότι ο ορισμός περιλαμβάνει όχι μόνο το υλικό (hardware) αλλά και τα ίδια τα ψηφιακά δεδομένα που αποθηκεύονται, επεξεργάζονται ή διαβιβάζονται, εφόσον αυτά είναι κατάλληλα διαμορφωμένα για επεξεργασία από το σύστημα.

Κατά μία έννοια, μπορεί να πει κανείς, ότι η ύπαρξη της κυβερνοασφάλειας εξασφαλίζει την «παράνομη και χωρίς δικαίωμα πρόσβαση» σ' ένα πληροφοριακό σύστημα, όπως αυτό ορίζεται και τιμωρείται στο άρθρο 3 του παραπάνω Νόμου. Η τελευταία πράξη τιμωρείται από τον ΠΚ κατ' άρθρο 370Δ παρ 2,3 (πρώην 370 Γ/2019 ΠΚ), όπως αυτό θα αναλυθεί περαιτέρω, και θεωρείται έγκλημα διακινδύνευσης και όχι

⁷⁹ Βλ. Jouglaux P., Γενικός Κανονισμός προσωπικών δεδομένων στον τομέα της δικαιοσύνης Μέσο Δημοσίευσης, ΤΝΠ QUALEX, ΔιΜΕΕ, 4/2022, σελ 480.

βλάβης όπως πολλοί θεωρούν. Εδώ, αξίζει να σημειωθεί ότι ακόμη και αν η πρόσβαση σε ένα πληροφοριακό σύστημα γίνεται χωρίς πρόθεση τότε τιμωρείται και πάλι.

Η κυβερνοασφάλεια των δικαστικών συστημάτων συνδέεται άρρηκτα με την προστασία των ζωτικής σημασίας αγαθών και των κρίσιμων υποδομών της χώρας. Σύμφωνα με το Άρθρο 292 παρ. 2 του ΠΚ, ως τέτοια νοούνται αγαθά που αφορούν την εθνική άμυνα, την υγεία και τις επικοινωνίες. Οι δικαστικές υποδομές, ως μέρος της κρατικής λειτουργίας, εντάσσονται στις εγκαταστάσεις κοινής ωφέλειας και στις κρίσιμες υποδομές, ανάλογα με εκείνες της ενέργειας, των μεταφορών και των χρηματοπιστωτικών ιδρυμάτων. Οποιαδήποτε κυβερνοεπίθεση που στοχεύει στην παρακώλυση της λειτουργίας αυτών των συστημάτων (π.χ. μέσω του διαδικτύου) δεν αποτελεί απλή προσβολή δεδομένων, αλλά απειλή κατά της εύρυθμης λειτουργίας του κράτους και της κοινωνικής σταθερότητας.

3.2. Περί Κυβερνοασφάλειας

Με τους όρους κυβερνοασφάλεια και κυβερνοάμυνα ορίζουμε την προστασία συστημάτων που υποστηρίζουν επεξεργασία πληροφορίας και επικοινωνία, συνήθως μέσω του Διαδικτύου. Η κυβερνοασφάλεια έχει ως στόχο να αντιμετωπίσει μια ενδεχόμενη μελλοντική κυβερνοεπίθεση ή και μια κυβερνοεπίθεση που λαμβάνει χώρα σε πραγματικό χρόνο (real time cyberattack). Για να γίνει σαφές το τι είναι κυβερνοεπίθεση (cyberattack) αρκεί να αναφερθεί ότι είναι η οποιαδήποτε κακόβουλη ενέργεια που λαμβάνει χώρα σε ένα πληροφοριακό σύστημα, όπως αναλύθηκε παραπάνω. Με άλλα λόγια πρόκειται για την χωρίς δικαίωμα πρόσβαση σε ένα υπολογιστικό σύστημα ή αλλιώς η μη εξουσιοδοτημένη πρόσβαση, τροποποίηση, καταστροφή, υποκλοπή και γενικά πλήρης πρόκληση βλάβης σε ένα πληροφοριακό σύστημα.⁸⁰

Τα είδη των κυβερνοεπιθέσεων είναι αμέτρητα, κάποια εκ των οποίων θα αναφερθούν στην παρούσα διπλωματική εργασία περισσότερο για να γίνει πλήρως κατανοητή η έννοια της κυβερνοεπίθεσης, της κυβερνοασφάλειας και η υποχρεωτική εφαρμογή σωστής δικαστικής λειτουργίας. Από την παράνομη εγκατάσταση

⁸⁰ Βλ. Εισήγηση του Βασίλειου Θ. Αραβαντινού, Δ.Ν Συμβούλου Επικράτειας, σε επιμορφωτικό σεμινάριο Δικαστικών Λειτουργών (17-18/3/2022) με γενικό θέμα: «Δίκαιο και Πληροφορική».

προγραμμάτων που βλάπτουν τον υπολογιστή ή το σύστημα, την υποκλοπή πληροφοριών και στοιχείων, μέχρι και την οριστική αχρήστευση τους. Συναφής με την κυβερνοασφάλεια όρος θα μπορούσε να είναι η «ασφάλεια πληροφοριακών συστημάτων και δικτυακών υποδομών τους», ένας όρος που περιέχεται και στη σχετική Οδηγία και ευρίσκεται και στον τίτλο του νόμου 4577/2018.

Στο δικαστικό σύστημα η συνεχής ανταλλαγή πληροφοριών, email και λεπτομερειών που σχετίζονται σε μια υπόθεση συνάδουν με την έννοια των προσωπικών δεδομένων, η προστασία των οποίων πρέπει να είναι ξεκάθαρα προτεραιότητα της δικαιοσύνης.

3.2.1. Η Κυβερνοασφάλεια ως εγγύηση της Ψηφιακής Δικαιοσύνης

Η μετάβαση στο μοντέλο της ηλεκτρονικής δικαιοσύνης (e-Justice) και η ενσωμάτωση αλγοριθμικών συστημάτων Τεχνητής Νοημοσύνης, όπως αναλύθηκαν στα προηγούμενα κεφάλαια, μεταφέρουν τον πυρήνα της δικαστικής λειτουργίας στον κυβερνοχώρο. Αυτή η εξάρτηση από τις ψηφιακές υποδομές δημιουργεί μια νέα, κρίσιμη ανάγκη: τη διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δικαστικών δεδομένων. Η κυβερνοασφάλεια δεν αποτελεί πλέον ένα δευτερεύον τεχνικό ζήτημα, αλλά μια θεμελιώδη προϋπόθεση για την προστασία του δικαιώματος στη δίκαιη δίκη. Χωρίς ένα θωρακισμένο περιβάλλον, η ψηφιοποίηση της δικαιοσύνης παραμένει εκτεθειμένη σε απειλές που θα μπορούσαν να αλλοιώσουν αποδεικτικά στοιχεία ή να παραβιάσουν το δικαστικό απόρρητο⁸¹

Η σύνδεση της κυβερνοασφάλειας με την Τεχνητή Νοημοσύνη είναι αμφίδρομη. Από τη μία πλευρά, η ΤΝ προσφέρει προηγμένα εργαλεία για τον εντοπισμό και την πρόληψη κυβερνοεπιθέσεων στα δικαστικά συστήματα, λειτουργώντας ως "ψηφιακός φρουρός". Από την άλλη πλευρά, τα ίδια τα συστήματα ΑΙ αποτελούν νέους στόχους επιθέσεων, καθώς η παραποίηση των δεδομένων εκπαίδευσής τους (data poisoning) μπορεί να οδηγήσει σε εσφαλμένες ή μεροληπτικές δικαστικές κρίσεις. Συνεπώς, η μελέτη των μηχανισμών προστασίας των πληροφοριακών συστημάτων είναι αναπόσπαστο κομμάτι της ανάλυσης για τη σύγχρονη δικαιοσύνη, καθώς η οποιαδήποτε

⁸¹ Βλ. D. Djurayev (2024), *Cybersecurity and Data Protection in Modern Electronic Justice Ecosystems*, σελ. 4.

κυβερνοαπειλή στρέφεται άμεσα κατά του κύρους των θεσμών και της ασφάλειας δικαίου.

Η κυβερνοασφάλεια είναι μία πολυδιάστατη και συνεχώς εξελισσόμενη έννοια, χωρίς έναν ευρέως αποδεκτό ορισμό. Σύμφωνα με τον ENISA⁸², δεν υπάρχει ένας καθολικός ορισμός, καθώς εξαρτάται από το πλαίσιο εφαρμογής της. Η έκθεση παραπέμπει στο πρότυπο ISO/IEC 27032:2012, το οποίο ορίζει την κυβερνοασφάλεια ως την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών στον κυβερνοχώρο, ο οποίος αποτελεί το περιβάλλον που προκύπτει από την αλληλεπίδραση ανθρώπων, λογισμικού και δικτύων.

3.2.2 Το Ευρωπαϊκό Κανονιστικό Πλαίσιο: Υπο την Οδηγία NIS στην NIS 2

Η θωράκιση των ψηφιακών υποδομών της δικαιοσύνης δεν επαφίεται μόνο στην τεχνική πρωτοβουλία των κρατών μελών, αλλά καθορίζεται πλέον από ένα αυστηρό ευρωπαϊκό κανονιστικό πλαίσιο. Η αρχή έγινε με την Οδηγία (ΕΕ) 2016/1148 (NIS 1), που στην Ελλάδα κατοχυρώθηκε με τον Ν.4577/2018, η οποία έθεσε τις βάσεις για ένα κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. Η Οδηγία αυτή επέβαλε στα κράτη μέλη την υποχρέωση να υιοθετήσουν εθνικές στρατηγικές κυβερνοασφάλειας και να ορίσουν φορείς εκμετάλλευσης κρίσιμων υπηρεσιών που οφείλουν να λαμβάνουν κατάλληλα μέτρα ασφαλείας. Αρχικά, σκοπός του νόμου ήταν η ενσωμάτωση της Οδηγίας στην ελληνική νομοθεσία, με την οποία ως στόχος ήταν η θέσπιση μέτρων για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

Η ραγδαία αύξηση των κυβερνοαπειλών και ο επιταχυνόμενος ψηφιακός μετασχηματισμός οδήγησαν στην αντικατάσταση της παραπάνω Οδηγίας από τη, νέα και ισχύουσα πλέον, Οδηγία (ΕΕ) 2022/2555, γνωστή και ως NIS2. Η τελευταία διευρύνει σημαντικά το πεδίο εφαρμογής της, εντάσσοντας περισσότερους τομείς ως «κρίσιμους» και επιβάλλοντας αυστηρότερες απαιτήσεις διαχείρισης κινδύνου και αναφοράς περιστατικών. Για το δικαστικό σύστημα, η συμμόρφωση με την NIS 2 σημαίνει ότι οι

⁸² Βλ. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el τελευταία πρόσβαση 13/02/2026.

υποδομές, όπως λ.χ. το ΟΣΔΔΥ-ΔΔ, πρέπει να υιοθετούν προηγμένες πρακτικές, όπως η κρυπτογράφηση, η πολυπαραγοντική ταυτοποίηση και η διασφάλιση της εφοδιαστικής αλυσίδας λογισμικού, προκειμένου να προστατεύονται από επιθέσεις που θα μπορούσαν να θέσουν σε κίνδυνο τη δημόσια ασφάλεια και την απονομή του δικαίου.

Η μετάβαση στην NIS 2 αντανακλά τη στροφή από την απλή «ασφάλεια πληροφοριών» στην «ψηφιακή ανθεκτικότητα». Στο πλαίσιο της παρούσας μελέτης, η NIS 2 λειτουργεί ως το νομικό εχέγγυο ότι οι τεχνολογίες Τεχνητής Νοημοσύνης που εισάγονται στη δικαιοσύνη θα λειτουργούν μέσα σε ένα περιβάλλον ελεγχόμενο και προστατευμένο, μειώνοντας τις πιθανότητες συστημικών καταρρεύσεων ή μαζικών διαρροών προσωπικών δεδομένων όπως αυτό θα αναλυθεί περαιτέρω.

3.2.3. Το νομοθετικό πλαίσιο στην Ελλάδα και την Ευρωπαϊκή ένωση

Ο Ν.4070/2012 ρυθμίζει τις υποχρεώσεις των παρόχων δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, σχετικά με την προστασία και την σωστή λειτουργία τους.⁸³ Σύμφωνα με το άρθρο 37 του ίδιου Νόμου, οι πάροχοι είναι αυτοί που έχουν την υποχρέωση να λαμβάνουν όλα τα μέτρα προστασίας προκειμένου να διασφαλιστεί η ασφάλεια των δεδομένων και όχι μόνο γίνεται με τον καλύτερο και ασφαλέστερο τρόπο.⁸⁴ Ιδίως στη δικαστική λειτουργία η προστασία και η ασφάλεια των παραπάνω είναι το πάν, κι αυτό διότι είναι πολύ λεπτά τα όρια μεταξύ του να διασφαλιστεί εκτός των άλλων και η ανωνυμοποίηση των δικαστικών αποφάσεων, να μη διαρρεύσουν δηλαδή προσωπικά δεδομένα καταδικασθέντων ή μη. Εκτός όμως από το παραπάνω παράδειγμα, οτιδήποτε σχετίζεται με το δικαστικό σύστημα, όπως λ.χ. καταθέσεις δικογράφων από διαδίκους, δικογραφίες και εξελίξεις των υποθέσεων πρέπει να καταστεί σαφές ότι πρέπει να παραμείνει προστατευμένο.

Σε περιπτώσεις παραβίασης των παραπάνω (και όχι μόνο) παραδειγμάτων, θα πρέπει οι πάροχοι να λαμβάνουν τα αναγκαία μέτρα που θα εξασφαλίσουν την αριότητα των δικτύων, ώστε η παροχή των υπηρεσιών αυτών των δικτύων που επηρέασε

⁸³ Βλ. Νόμο 4070/2012 - ΥΕΚ 82 Α/10-4-2012: Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις *Διαδίκτυο+ Διαθέσιμο στο: <https://www.e-nomothesia.gr/kat-epikoinonies-telepikoinonies-telephonia/n-4070-2012.html> , τελευταία πρόσβαση 12/02/2026.

⁸⁴ Βλ. Μεταπτυχιακή Διπλωματική Εργασία της Ιωάννας Μπάλντα, (2022), *Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΣΥΓΧΡΟΝΗ ΨΗΦΙΑΚΗ ΕΠΟΧΗ*, σελ. 44.

τη λειτουργία τους να αναφέρεται στην ΕΕΤ, η οποία ακολούθως θα πρέπει να αναφέρει κάθε παραβίαση στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών.

Ορόσημο για τη δράση της ΕΕ στον τομέα της κυβερνοασφάλειας θεωρείται η ψήφιση της Οδηγίας 2016/1148 με την Ελλάδα να τον εφαρμόζει με τον Ν.4577 (Α'199/3.12.2018) αναφορικά με κοινώς αποδεκτά μέτρα ασφάλειας υψηλού επιπέδου για συστήματα δικτύου και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση. Χαρακτηριστικοί τομείς είναι η Προστασία των Προσωπικών Δεδομένων, η Τεχνητή Νοημοσύνη και η κυβερνοασφάλεια.⁸⁵

Το ισχύον κανονιστικό πλαίσιο θεσπίζει δεσμευτικούς κανόνες για τους τομείς που κρίνονται ζωτικής σημασίας για τη λειτουργία του κράτους, οι οποίοι στην ευρωπαϊκή νομοθεσία και στον Ν. 4577/2018 αναφέρονται ως «φορείς εκμετάλλευσης βασικών υπηρεσιών». Παρόλο που αρχικά το δικαστικό σύστημα δεν συμπεριλαμβανόταν στους τομείς εφαρμογής του εν λόγω νόμου, η κατάσταση αυτή μεταβλήθηκε ουσιαστικά με την υιοθέτηση της «Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025» (Άρθρο 7 παρ. 1) από το Υπουργείο Ψηφιακής Διακυβέρνησης.

Η συγκεκριμένη στρατηγική, η οποία επικυρώθηκε με την απόφαση 34368/7-12-2020 του Υπουργού Επικρατείας, ενέταξε για πρώτη φορά τα Δικαστήρια στους κρίσιμους τομείς κρατικής λειτουργίας. Κατά συνέπεια, ο χώρος της Δικαιοσύνης αναγνωρίζεται πλέον και σε νομικό επίπεδο ως κρίσιμη υποδομή. Η υπαγωγή αυτή συνεπάγεται την υποχρέωση τήρησης αυστηρών προτύπων ασφαλείας, καθώς η εύρυθμη λειτουργία των δικαστηρίων θεωρείται πλέον ισότιμη με άλλους ζωτικούς τομείς για τη σταθερότητα και τη λειτουργία του κοινωνικού συνόλου.⁸⁶

Ο εθνικός μηχανισμός για την κυβερνοασφάλεια στην Ελλάδα εδράζεται σε τρία κύρια νομοθετικά θεμέλια που καθορίζουν τη στρατηγική και την επιχειρησιακή του

⁸⁵ Βλ. Η εξέλιξη της κυβερνοασφάλειας στην Ε.Ε <https://odeth.eu/%CE%B7-%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CF%84%CE%B7%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5/> , τελευταία πρόσβαση 18/02/2026.

⁸⁶ Ο.π υποσημ. 80.

δομή. Κεντρικό ρόλο διαδραματίζει ο Ν. 4577/2018 (Α' 199), ο οποίος ενσωμάτωσε στην εθνική έννομη τάξη την ευρωπαϊκή Οδηγία 2016/1148/ΕΕ (NIS 1) για την επίτευξη υψηλού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών. Το πλαίσιο αυτό εξειδικεύεται περαιτέρω από την Υ.Α. 1027/2019, που ρυθμίζει τις διαδικασίες εφαρμογής του νόμου, και την Υ.Α. για την «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020 – 2025», η οποία θέτει τους στρατηγικούς στόχους και τις προτεραιότητες της χώρας.

Επιπροσθέτως, το νομικό αυτό οπλοστάσιο συμπληρώνεται από συμπληρωματικά κείμενα και νομοθετήματα, όπως το Εγχειρίδιο Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης (2021)⁸⁷ και ο Ν. 4727/2020 για την Ψηφιακή Διακυβέρνηση και τις Ηλεκτρονικές Επικοινωνίες. Καθοριστική είναι επίσης η συμβολή της Βίβλου Ψηφιακού Μετασχηματισμού 2020-2025 (ΦΕΚ 2894/Β/5-7-2021), η οποία χαράζει την πορεία της δημόσιας διοίκησης προς την ψηφιακή ανθεκτικότητα. Δεν θα μπορούσε να μην αναφερθεί και η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης κατέχοντας τον ρόλο του στρατηγικού συντονιστή και επόπτη.

3.2.4. Η συμβολή της Τεχνητής Νοημοσύνης στην Κυβερνοασφάλεια στη δικαστική χρήση κατά τον Κανονισμό AI ACT

Η κυβερνοασφάλεια θεωρείται ο κλάδος που μπορεί να ωφεληθεί περισσότερο από την εισαγωγή της Τεχνητής Νοημοσύνης (TN). Ενώ τα παραδοσιακά συστήματα ασφαλείας είναι συχνά αργά και ανεπαρκή, οι τεχνικές TN μπορούν να βελτιώσουν τη συνολική απόδοση και να προσφέρουν καλύτερη προστασία από εξελιγμένες απειλές. Οι παραδοσιακές μέθοδοι βασίζονται σε σταθερούς αλγορίθμους και γνωστά πρότυπα, ενώ η TN επιτρέπει στις μηχανές να μαθαίνουν και να προσαρμόζονται αυτόματα στις αλλαγές του περιβάλλοντος

Οι παραδοσιακές μέθοδοι βασίζονται σε σταθερούς αλγορίθμους και γνωστά πρότυπα, ενώ η TN επιτρέπει στις μηχανές να μαθαίνουν και να προσαρμόζονται

⁸⁷ Βλ. Εγχειρίδιο Κυβερνοασφάλειας - Cybersecurity Handbook - Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων - Υπουργείο Ψηφιακής Διακυβέρνησης - Ιούνιος 2021, <https://mindigital.gr/wpcontent/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf> τελευταία πρόσβαση 18/02/2026.

αυτόματα στις αλλαγές του περιβάλλοντος. Στο πλαίσιο μιας Ολοκληρωμένης Προσέγγισης Ασφάλειας (Integrated Security Approach - ISA), η TN μπορεί να συμβάλει σ' ένα από τα πιο σημαντικά πράγματα όπως αυτό της πρόληψης (prevent) ⁸⁸ μιας επίθεσης.

Μία εκ των θεμελιωδών προβλέψεων του Κανονισμού για την Τεχνητή Νοημοσύνη είναι η κατάταξη των συστημάτων TN με γνώμονα τον σκοπό τους και τους πιθανούς κινδύνους που απορρέουν από τη χρήση τους. Ειδικότερα, στην αιτιολογική σκέψη 61 του Κανονισμού, επισημαίνεται ότι συστήματα TN που σχετίζονται με τις δημοκρατικές διαδικασίες και την απονομή της δικαιοσύνης πρέπει να ταξινομούνται ως «υψηλού κινδύνου» (βλ. και Παράρτημα III), λόγω της σοβαρής επίδρασης που μπορεί να έχουν στο κράτος δικαίου, τις ατομικές ελευθερίες και το δικαίωμα σε αμερόληπτο δικαστήριο.

Για τον περιορισμό φαινομένων αδιαφάνειας, σφαλμάτων ή προκαταλήψεων, ο χαρακτηρισμός του υψηλού κινδύνου αποδίδεται σε συστήματα που χρησιμοποιούνται από δικαστικές αρχές για την ερμηνεία πραγματικών περιστατικών, την εφαρμογή του νόμου και τη λήψη αποφάσεων. Το ίδιο ισχύει και για φορείς εναλλακτικής επίλυσης διαφορών, εφόσον τα αποτελέσματα των διαδικασιών τους παράγουν έννομες συνέπειες. Ο Κανονισμός υπογραμμίζει ότι η TN μπορεί να επικουρεί τη δικαστική ανεξαρτησία, αλλά σε καμία περίπτωση δεν πρέπει να υποκαθιστά τον άνθρωπο, ο οποίος οφείλει να διατηρεί τον τελικό έλεγχο της απόφασης. Αντιθέτως, κατά το άρθρο 6 παρ. 3 του Κανονισμού, βοηθητικές διοικητικές εργασίες που δεν επηρεάζουν την ουσία των υποθέσεων (όπως η ανωνυμοποίηση αποφάσεων ή η εσωτερική επικοινωνία) δεν θεωρούνται υψηλού κινδύνου, καθώς δεν ενέχουν ουσιαστική απειλή για τα θεμελιώδη δικαιώματα.

Η ένταξη ενός συστήματος στην κατηγορία υψηλού κινδύνου συνεπάγεται την υποχρεωτική συμμόρφωση με αυστηρές απαιτήσεις, όπως προβλέπεται στο Τμήμα 2 του Κανονισμού άρθρα 8 έως 15 του Κανονισμού⁸⁹. Οι πάροχοι οφείλουν να εφαρμόζουν

⁸⁸ Βλ. Wirkuttis N. και Klein H., *"Artificial Intelligence in Cybersecurity"*, σελ. 111, TNPI HEIN ONLINE.

⁸⁹ Βλ. Βάγιας Ι., *Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΟ ΔΙΚΑΙΟΔΟΤΙΚΟ ΕΡΓΟ ΤΟΥ ΕΛΕΓΚΤΙΚΟΥ ΣΥΝΕΔΡΙΟΥ: ΤΑ ΠΡΩΤΑ ΒΗΜΑΤΑ ΚΑΙ Η ΠΡΟΟΠΤΙΚΗ*, σελ 10.

συστήματα διαχείρισης κινδύνου καθ' όλο τον κύκλο ζωής του προϊόντος, να χρησιμοποιούν ελεγχμένα σύνολα δεδομένων για την εκπαίδευση των μοντέλων και να καταρτίζουν αναλυτικό τεχνικό φάκελο πριν τη διάθεσή τους στην αγορά. Επιπλέον, επιβάλλεται η τεχνική δυνατότητα αυτόματης καταγραφής συμβάντων για την εξασφάλιση της ιχνηλασιμότητας, η διασφάλιση της διαφανούς λειτουργίας ώστε οι χρήστες να ερμηνεύουν ορθά τα αποτελέσματα, καθώς και ο σχεδιασμός που επιτρέπει την αποτελεσματική εποπτεία από φυσικά πρόσωπα. Τέλος, το σύστημα πρέπει να εγγυάται υψηλά επίπεδα ακρίβειας, στιβαρότητας και κυβερνοασφάλειας. Η ρυθμιστική αυτή παρέμβαση κρίνεται καθοριστική, καθώς η τεχνολογική εξέλιξη υπερβαίνει συχνά τη νομοπαραγωγική ταχύτητα, καθιστώντας τους μη δεσμευτικούς κανόνες ηθικής λιγότερο αποτελεσματικούς έναντι της δεσμευτικής νομοθεσίας. Πρέπει να γίνει σαφές ότι η τεχνολογία εξελίσσεται ταχύτερα από τη νομοπαραγωγική διαδικασία, ενώ η προσπάθεια ρύθμισης μέσω μη δεσμευτικών ηθικών αρχών και κανόνων ήπιου δικαίου δεν μπορεί να θεωρηθεί αποτελεσματική.⁹⁰

Στην ελληνική δικαστική πραγματικότητα έχει γίνει κατανοητό ότι αν χρησιμοποιηθεί σωστά, η ΤΝ μπορεί να βελτιώσει κατά ένα πολύ μεγάλο ποσοστό την ποιότητα της δικαιοσύνης. Από το 2020 και με τη «Βίβλο Ψηφιακού Μετασχηματισμού»⁹¹ έγινε έντονη η ανάγκη για την άμεση ψηφιοποίηση της Δικαιοσύνης με την βοήθεια της ΤΝ ως προς την επεξεργασία αρχείων, την προετοιμασία αποφάσεων και την ανωνυμοποίηση και ψευδονυμοποίηση των δικαστικών αποφάσεων.

ΚΕΦΑΛΑΙΟ IV Κυβερνοέγκλημα και Ποινική Δικαιοσύνη

4.1.1 Ορισμός κυβερνοεγκλήματος

Ξεχωριστή αναφορά αξίζει να γίνει για το κυβερνοέγκλημα και την προσπάθεια αντιμετώπισης του από πλευράς δικαιοσύνης, ήτοι από το Ποινικό Δίκαιο, αφού η ΤΝ όπως αναφέρθηκε παραπάνω ευθύνεται για τα αδικήματα με χρήση Η/Υ. Το δικαστικό σύστημα εκτός από το ότι πρέπει να χρησιμοποιήσει την ΤΝ ως όπλο για την

⁹⁰ Ο.π υποσημ 69 Α. σελ 23

⁹¹ Βλ. Βίβλο Ψηφιακού Μετασχηματισμού 2020-2025 , https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_strategy.pdf τελευταία πρόσβαση 21/02/2026.

ψηφιοποίησή του, πρέπει να γνωρίζει και να μπορεί να καταπολεμήσει τους κινδύνους που εγκυμονούν από αυτή.

Ως κυβερνοέγκλημα ή έγκλημα στον κυβερνοχώρο νοούνται οι εγκληματικές πράξεις που τελούνται μέσω ή με τη βοήθεια συστημάτων πληροφορικής και δικτύων ηλεκτρονικών επικοινωνιών. Στις περιπτώσεις αυτές ο υπολογιστής ή γενικότερα οι ψηφιακές τεχνολογίες αποτελούν είτε το βασικό μέσο τέλεσης της παράνομης πράξης είτε το αντικείμενο της προσβολής. Η ύπαρξη λοιπόν κυβερνοασφάλειας είναι αναγκαία. Η διάδοση του διαδικτύου και η ευρεία χρήση ψηφιακών υπηρεσιών έχουν συμβάλει σημαντικά στην αύξηση των σχετικών μορφών εγκληματικότητας, καθιστώντας αναγκαία την ανάπτυξη εξειδικευμένων νομικών και τεχνολογικών μηχανισμών πρόληψης και καταστολής.

4.1.2 Είδη ηλεκτρονικού εγκλήματος

Το ηλεκτρονικό ψάρεμα (phising)

Πρόκειται για την πιο γνωστή σε όλους τεχνική εξαπάτησης κατά την οποία οι δράστες επιχειρούν να αποσπάσουν ευαίσθητες πληροφορίες από τους χρήστες του διαδικτύου, όπως κωδικούς πρόσβασης, στοιχεία τραπεζικών λογαριασμών ή προσωπικά δεδομένα. Η εξαπάτηση πραγματοποιείται συνήθως μέσω παραπλανητικών ηλεκτρονικών μηνυμάτων, ιστοσελίδων ή άλλων ψηφιακών μέσων επικοινωνίας που εμφανίζονται ως αξιόπιστες πηγές, όπως τράπεζες, δημόσιες υπηρεσίες ή γνωστές εταιρείες. Ο όρος αυτός ανήκει κατά κύριο λόγο στον διάσημο χάκερ με το όνομα Khan C Smith⁹² ο οποίος έγινε ευρέως γνωστός περίπου αρχές του 1990.

Ηλεκτρονικό Ψάρεμα (pharming)

Εδώ ο δράστης παρεμβαίνει στη λειτουργία του συστήματος ονοματοδοσίας του διαδικτύου (DNS) ή σε άλλες ρυθμίσεις του υπολογιστή του χρήστη, με αποτέλεσμα ο τελευταίος να ανακατευθύνεται αυτόματα σε ψεύτικες ιστοσελίδες που μιμούνται νόμιμους οργανισμούς, όπως τράπεζες ή ηλεκτρονικές υπηρεσίες. Έχει πολλές

⁹² Βλ. H. George, (2021), «*Phising Emails are Homeland Security's Most Feared Cyber Threat*» <https://www.homelandsecurityedu.org/2017/01/phishingemails-are-homeland-securitys-most-feared-cyber-threat/> , τελευταία πρόσβαση 26/02/2026.

ομοιότητες με το phishing κι αυτό διότι ο δράστης έχει ως όπλο εν απαράπληντικό email η μήνυμα κατά το θύμα του.

Hacking

Μία ακόμη σημαντική μορφή κυβερνοεγκλήματος είναι το hacking, δηλαδή η μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα, δίκτυα ή ηλεκτρονικές βάσεις δεδομένων. Σκοπός είναι κυρίως να προσπορίσουν, οι δράστες, με παράνομο τρόπο ένα περιουσιακό όφελος αλλά και να εγκαταστήσουν προγράμματα σε ξένους Η/Υ αποκτώντας πρόσβαση σε αυτούς εξ αποστάσεως. Ο όρος hacking εμφανίστηκε για πρώτη φορά τη δεκαετία του 1970, ωστόσο άρχισε να γίνεται ευρύτερα γνωστός κατά τη δεκαετία του 1980. Ενδεικτικά, σε άρθρο που δημοσιεύθηκε το 1980 στο περιοδικό *Psychology Today* με τίτλο «The Hacker Papers»⁹³ εξετάστηκε το φαινόμενο της έντονης ενασχόλησης των χρηστών με τους υπολογιστές και η αυξανόμενη κουλτούρα των λεγόμενων «hackers». Λίγα χρόνια αργότερα, η έννοια του hacking έγινε ακόμη πιο γνωστή στο ευρύ κοινό μέσω της ποπ κουλτούρας, ιδίως με την κυκλοφορία των ταινιών *Tron* και *WarGames*, στις οποίες οι πρωταγωνιστές αποκτούν παράνομη πρόσβαση σε πληροφοριακά συστήματα. Οι ταινίες αυτές συνέβαλαν σημαντικά στη διάδοση της έννοιας του hacking και παράλληλα ανέδειξαν τους πιθανούς κινδύνους που μπορεί να δημιουργήσει για την ασφάλεια των πληροφοριακών συστημάτων και ακόμη και για την εθνική ασφάλεια.

4.1.3 Deepfakes ως μέσο παραπλάνησης της δικαιοσύνης

Ξεχωριστή αναφορά πρέπει να γίνει για την έννοια του deepfake στη δικαιοσύνη. Εκτός λοιπόν από τη μικρή αναφορά στα είδη ηλεκτρονικού εγκλήματος που έλαβαν χώρα παραπάνω, υπάρχουν συστήματα με χρήση της ΤΝ που μπορούν εύκολα να επηρεάσουν τη σωστή λειτουργία της Δικαιοσύνης, της ορθής κρίσης των Δικαστών και γενικότερα των συλλειτουργών της.

⁹³ Βλ. <https://www.fortinet.com/resources/cyberglossary/what-is-hacking> , τελευταία πρόσβαση 26/02/2026.

Ένα απτό παράδειγμα είναι τα συστήματα των deepfakes. Τα deepfakes αποτελούν μία σύγχρονη μορφή ψηφιακής παραποίησης περιεχομένου, η οποία βασίζεται στη χρήση τεχνητής νοημοσύνης και ειδικότερα τεχνικών βαθιάς μάθησης (deep learning). Με τη χρήση αυτών των τεχνολογιών καθίσταται δυνατή η δημιουργία ή η αλλοίωση οπτικοακουστικού υλικού, όπως εικόνων, βίντεο ή ηχητικών αρχείων, με τρόπο που να εμφανίζονται ως αυθεντικά, ενώ στην πραγματικότητα έχουν κατασκευαστεί ή τροποποιηθεί ψηφιακά.⁹⁴

Η τεχνολογία αυτή δημιουργεί σημαντικές προκλήσεις για τη λειτουργία της δικαιοσύνης, καθώς μπορεί να χρησιμοποιηθεί για την παραπλάνηση των δικαστικών αρχών, όπως αναφέρθηκε, μέσω της παραγωγής ψευδών αποδεικτικών στοιχείων. Ειδικότερα, ένα παραποιημένο βίντεο ή ηχητικό αρχείο θα μπορούσε να παρουσιαστεί ως αποδεικτικό μέσο σε μια δικαστική διαδικασία, με σκοπό την ενοχοποίηση ή την απαλλαγή ενός προσώπου. Η αυξανόμενη ποιότητα των deepfakes καθιστά πολλές φορές δύσκολη τη διάκριση μεταξύ γνήσιου και παραποιημένου υλικού, γεγονός που ενδέχεται να επηρεάσει την αξιολόγηση των αποδεικτικών στοιχείων.

Η προβληματική αυτή συνδέεται άμεσα με την αξιοπιστία των ψηφιακών πειστηρίων και την ανάγκη ανάπτυξης προηγμένων μεθόδων ανίχνευσης παραποιημένου υλικού. Παράλληλα, ανακύπτουν ζητήματα που αφορούν την προστασία της δικαστικής διαδικασίας, την ασφάλεια των αποδεικτικών μέσων και την ανάγκη προσαρμογής του νομικού πλαισίου ώστε να αντιμετωπιστούν αποτελεσματικά οι κίνδυνοι που συνεπάγεται η χρήση τέτοιων τεχνολογιών.

Για τον λόγο αυτό, η αντιμετώπιση των deepfakes αποτελεί πλέον σημαντικό ζήτημα τόσο για την κυβερνοασφάλεια όσο και για την ορθή απονομή της δικαιοσύνης, απαιτώντας τη συνεργασία νομικών, τεχνικών εμπειρογνομόνων και δικαστικών αρχών

⁹⁴ Περιοδικό της Νομικής Βιβλιοθήκης, 2025, με θέμα: Deepfakes και ποινική δικαιοσύνη: Η νέα απειλή της Τεχνητής Νοημοσύνης, <https://daily.nb.org/arthrografia/periodika-nb/deepfakes-kai-poiniki-dikaivosyni-i-nea-apeili-tis-technitis-noimosynis/> τελευταία πρόσβαση 28/02/2026.

4.1.4 Η ποινική προστασία των δεδομένων προσωπικού χαρακτήρα και η αντιμετώπιση τους από τη Δικαιοσύνη

Η ΤΝ, τα κυβερνοεγκλήματα και οι νέες τεχνολογίες μας φέρνουν αντιμέτωπους με πολλές παραβιάσεις στην καθημερινότητά μας. Η παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι μια από αυτές που ποινικοποιείται και αντιμετωπίζεται από το δικαστικό σύστημα. Συγκεκριμένα, το άρθρο 38 του ειδικού νόμου υπ' αριθμ. 4624/2019, ο οποίος αντικατέστησε το προγενέστερο καθεστώς του νόμου 2472/1997 και, ιδίως, το άρθρο 22 αυτού⁹⁵. Ο Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ΕΕ 679/2018, γνωστός και ως GDPR (General Data Protection Regulation) καθώς και η οδηγία ΕΕ 690/2016 περί επεξεργασίας προσωπικών δεδομένων από τις αρμόδιες αρχές για την ανίχνευση αδικημάτων και εκτέλεση ποινικών κυρώσεων, ενσωματώθηκαν στην ελληνική νομοθεσία με τον Ν. 4624/2019.

Ειδικότερα, η διάταξη του άρθρου 38 τυποποιεί τα βασικά αδικήματα που σχετίζονται με παράνομη επεξεργασία δεδομένων, προβλέποντας ποινές φυλάκισης ή κάθειρξης, ανάλογα με τη βαρύτητα της πράξης, το είδος των δεδομένων και το δόλο του δράστη όπως αυτό αναλύεται παρακάτω. Η εν λόγω ποινική προστασία αφορά τόσο τις περιπτώσεις επεξεργασίας χωρίς νόμιμη βάση όσο και τις περιπτώσεις κατά τις οποίες παραβιάζεται ο σκοπός ή η αρχή της ελαχιστοποίησης των δεδομένων, όπως προβλέπονται από τον ΓΚΠΔ. Συγκεκριμένα «Όποιος, χωρίς δικαίωμα: α) επεμβαίνει με οποιονδήποτε τρόπο σε σύστημα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, και με την πράξη του αυτή λαμβάνει γνώση των δεδομένων αυτών· β) τα αντιγράφει, αφαιρεί, αλλοιώνει, βλάπτει, συλλέγει, καταχωρεί, οργανώνει, διαρθρώνει, αποθηκεύει, προσαρμόζει, μεταβάλλει, ανακτά, αναζητεί πληροφορίες, συσχετίζει, συνδυάζει, περιορίζει, διαγράφει, καταστρέφει (αρ 38 παρ 1) ή Όποιος χρησιμοποιεί, μεταδίδει, διαδίδει, κοινολογεί με διαβίβαση, διαθέτει, ανακοινώνει ή καθιστά προσιτά σε μη δικαιούμενα πρόσωπα δεδομένα προσωπικού χαρακτήρα, τα οποία απέκτησε σύμφωνα με την περίπτωση α' της παραγράφου 1 ή επιτρέπει σε μη δικαιούμενα πρόσωπα να λάβουν γνώση των δεδομένων αυτών(αρ 38 παρ 2) τιμωρείται». Αξίζει επίσης να αναφερθεί, ότι η εφαρμογή του άρθρου 38 Ν. 4624/2019 από τη νομολογία αναδεικνύει ως

⁹⁵ Βλ. <https://lawnet.gr/law-news/i-poiniki-prostasia-ton-dedomenon-prosopikou-charaktira-ypo-to-n-4624-2019>, τελευταία πρόσβαση 26/02/2026

κρίσιμο στοιχείο για τη θεμελίωση του αδικήματος την ύπαρξη «συστήματος αρχειοθέτησης». Δικαστικές αποφάσεις έχουν κρίνει ότι, εάν τα προσωπικά δεδομένα δεν τηρούνται ή δεν αποδεικνύεται πως τηρούνται σε τέτοιο σύστημα, δεν πληρούνται το στοιχείο της αντικειμενικής υπόστασης.

ΚΕΦΑΛΑΙΟ V ΠΡΟΚΛΗΣΕΙΣ ΚΑΙ ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ ΤΗ ΣΤΗ ΔΙΚΑΙΟΣΥΝΗ

Η αξιοποίηση της τεχνητής νοημοσύνης στη λειτουργία της δικαιοσύνης δημιουργεί σημαντικές δυνατότητες βελτίωσης της αποδοτικότητας και της ταχύτητας απονομής της. Παράλληλα, όμως, εγείρει μια σειρά από νομικές, ηθικές και τεχνικές προκλήσεις που σχετίζονται με την προστασία των θεμελιωδών δικαιωμάτων, τη διαφάνεια των αλγοριθμικών συστημάτων και την αξιοπιστία των αποτελεσμάτων που αυτά παράγουν.

5.1 Κίνδυνοι Προγνωστικής Δικαιοσύνης

Η χρήση συστημάτων τεχνητής νοημοσύνης για την πρόβλεψη της έκβασης δικαστικών υποθέσεων, γνωστή ως προγνωστική δικαιοσύνη (predictive justice), δημιουργεί σημαντικούς προβληματισμούς ως προς τη λειτουργία του κράτους δικαίου. Ένας από τους βασικούς κινδύνους είναι η πιθανότητα η χρήση τέτοιων συστημάτων να οδηγήσει σε υποκατάσταση της δικαστικής κρίσης από έναν μηχανιστικό κανόνα εφαρμογής, ο οποίος βασίζεται κυρίως στη στατιστική ανάλυση προηγούμενων αποφάσεων.⁹⁶

Στο πλαίσιο αυτό, έχει υποστηριχθεί ότι τα λογισμικά πρόβλεψης που αναλύθηκαν παραπάνω και βασίζονται στην τεχνητή νοημοσύνη ενδέχεται να ενισχύσουν υπέρμετρα τον ρόλο της υφιστάμενης νομολογίας, μετατρέποντάς την σε βασικό σημείο αναφοράς για τη λήψη μελλοντικών αποφάσεων. Ωστόσο, η εξέλιξη αυτή δεν θα πρέπει να οδηγήσει στην υποβάθμιση του κανόνα δικαίου που θεσπίζεται από τον νομοθέτη ή ερμηνεύεται από τον δικαστή, καθώς μια τέτοια εξέλιξη θα μπορούσε να ανατρέψει την ιεραρχία των πηγών του δικαίου.

⁹⁶ Βλ. T. Lewis, «Don't Let Artificial Intelligence Take Over, Top Scientists Warn» (2015) τελευταία πρόσβαση 28/02/2026, <https://www.livescience.com/49419-artificial-intelligence-dangers-letter.html>

Παράλληλα, τίθεται το ζήτημα του τρόπου με τον οποίο τα συστήματα τεχνητής νοημοσύνης επεξεργάζονται τα νομικά δεδομένα. Στο πλαίσιο της ανάλυσης μεγάλων δεδομένων (big data), ο νόμος, η νομολογία και τα πραγματικά περιστατικά μιας υπόθεσης αντιμετωπίζονται συχνά ως απλά δεδομένα προς επεξεργασία, γεγονός που ενδέχεται να οδηγήσει σε εξίσωση ποιοτικά διαφορετικών στοιχείων της δικαστικής διαδικασίας.

Ένας ακόμη σημαντικός κίνδυνος που αναφέρεται είναι το λεγόμενο «φαινόμενο της αγέλης» (herd effect). Τα εργαλεία τεχνητής νοημοσύνης, αναλύοντας εκτεταμένα τη νομολογία, μπορεί να επηρεάσουν έμμεσα τη δικαστική κρίση, δημιουργώντας πίεση προς τους δικαστές να ευθυγραμμιστούν με τις κυρίαρχες τάσεις των προηγούμενων αποφάσεων. Μια τέτοια εξέλιξη θα μπορούσε να επηρεάσει την ανεξαρτησία και την αμεροληψία των δικαστικών λειτουργιών, οδηγώντας σε φαινόμενα ομοιομορφίας ή «ομαδικού κομπορμιισμού» κατά τη λήψη δικαστικών αποφάσεων.⁹⁷

5.1.1. Τήρηση των θεμελιωδών δικαιωμάτων και αρχών

Οι προσπάθειες που καταβάλλονται, τόσο σε επίπεδο Ευρωπαϊκής Ένωσης, όσο και εγχώρια, για την προαγωγή της ψηφιοποίησης στον τομέα της δικαιοσύνης, απαιτούν ταυτόχρονα και την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων που κατοχυρώνονται στην ΕΣΔΑ και τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, αφού ελλοχεύει πάντα ο κίνδυνος παραβίασής τους στο πλαίσιο της ψηφιακής ανάπτυξης, όπως επισημαίνει και το Συμβούλιο στα Συμπεράσματά του.⁹⁸

Πιο συγκεκριμένα, είναι επιβεβλημένο να δοθεί ιδιαίτερη σημασία στην διασφάλιση των δικαιωμάτων που αφορούν την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων (άρθρο 8 ΕΣΔΑ), διότι η χρήση ψηφιακών τεχνολογιών ενέχει το κίνδυνο παραβίασης των συσκευών και των δεδομένων που αποθηκεύονται σ' αυτές στα πλαίσια της ψηφιοποίησης. Πέραν αυτού, η χρήση προγραμμάτων τεχνητής νοημοσύνης στο τομέα της δικαιοσύνης θέτει προκλήσεις όσον αφορά τη πιθανότητα “χακαρίσματος” αυτών των συστημάτων για λόγους οικονομικούς ή άλλου είδους των δραστών. Γι' αυτό το λόγο, κρίνεται απαραίτητη η δημιουργία ενός αξιόπιστου συστήματος

⁹⁷ Ο.π. υποσημ. 71, σελ. 65.

⁹⁸ Βλ. υποσ. 56 σελ 108

κυβερνοασφάλειας που θα αποτρέπει τέτοιους κινδύνους⁹⁹. Ανησυχία μάλιστα προκαλεί το γεγονός της δυνατότητας ταυτοποίησης ενός ατόμου, μέσω της δημοσίευσης των δικαστικών αποφάσεων, ακόμη κι αν αυτές είναι ανωνυμοποιημένες, διότι με τη διάδοση τέτοιων δεδομένων προσβάλλεται η ανθρώπινη αξιοπρέπεια και είναι δυνατές οι καταρτίσεις προφίλ, οδηγώντας έτσι σε διακριτική μεταχείριση.¹⁰⁰

Υψίστης σημασίας, ακόμη, κρίνεται η ανάγκη προστασίας της αρχής της απαγόρευσης των διακρίσεων (άρθρο 14 ΕΣΔΑ), η οποία είναι πιθανό να προσβληθεί μέσω της ψηφιοποίησης της δικαιοσύνης, αφού πολλοί άνθρωποι δεν διαθέτουν ψηφιακές δεξιότητες ή ψηφιακά εργαλεία, με συνέπεια να παρεμποδίζεται η άσκηση του δικαιώματός τους για πρόσβαση στη δικαιοσύνη και να δημιουργούνται ανισότητες. Απαραίτητη είναι, λοιπόν, η εξασφάλιση ίσων ευκαιριών για όλους τους πολίτες, ώστε να ωφελούνται από τις ψηφιακές δυνατότητες χωρίς διακρίσεις¹⁰¹.

Από την άλλη πλευρά, ο κίνδυνος προσβολής της αρχής της απαγόρευσης των διακρίσεων αναδύεται και από την εισαγωγή συστημάτων τεχνητής νοημοσύνης στη δικαιοσύνη. Αυτό συμβαίνει, διότι οι αλγόριθμοι συχνά εκπαιδεύονται με δεδομένα της αστυνομίας και προηγούμενων δικαστικών αποφάσεων που αποτυπώνουν προκαταλήψεις και ρατσιστικά στερεότυπα, με αποτέλεσμα στη συνέχεια να εκδίδουν μεροληπτικές αποφάσεις και να διαιωνίζουν τις υφιστάμενες διακρίσεις. Παράλληλα με την παραπάνω αρχή προσβάλλεται και το δικαίωμα της ανεξαρτησίας και του αμερόληπτου δικαστηρίου (άρθρο 6 ΕΣΔΑ), αφού η χρήση εργαλείων τεχνητής νοημοσύνης που θα διατυπώνουν προτάσεις στους δικαστές, είναι δυνατό να επηρεάσουν την κρίση και την ανεξαρτησία τους, κατευθύνοντάς τους στην έκδοση μεροληπτικών αποφάσεων¹⁰².

5.1.2. Η προκατάληψη ως κίνδυνος έκδοσης μεροληπτικών αποφάσεων και διαιώνισης υφιστάμενων διακρίσεων

Μία από τις σημαντικότερες προκλήσεις που συνδέονται με τη χρήση συστημάτων τεχνητής νοημοσύνης στη δικαιοσύνη είναι ο κίνδυνος εμφάνισης αλγοριθμικής

⁹⁹ Ο.π υποσημ. 56 σελ 113.

¹⁰⁰ Ο.π. υποσημ. 5 σελ. 80.

¹⁰¹ Βλ. υποσ. 56 σελ 108

¹⁰² Ο.π. υποσημ. 39, σελ. 61.

μεροληψίας (algorithmic bias). Οι αλγόριθμοι που χρησιμοποιούνται σε τέτοια συστήματα εκπαιδεύονται συνήθως με βάση μεγάλα σύνολα δεδομένων, τα οποία προέρχονται από αστυνομικά αρχεία, ποινικές βάσεις δεδομένων ή προηγούμενες δικαστικές αποφάσεις. Ωστόσο, τα δεδομένα αυτά ενδέχεται να αντικατοπτρίζουν ήδη υπάρχουσες κοινωνικές προκαταλήψεις ή ανισότητες.¹⁰³

Στην περίπτωση αυτή, υπάρχει ο κίνδυνος τα συστήματα τεχνητής νοημοσύνης να αναπαράγουν και να ενισχύουν τις υφιστάμενες διακρίσεις, αντί να συμβάλλουν στην αντικειμενική και ουδέτερη απονομή της δικαιοσύνης. Ειδικότερα, εάν τα δεδομένα εκπαίδευσης περιλαμβάνουν προκαταλήψεις που σχετίζονται με παράγοντες όπως η φυλή, η κοινωνικοοικονομική κατάσταση ή ο τόπος κατοικίας, οι αλγόριθμοι ενδέχεται να οδηγηθούν σε μεροληπτικές προβλέψεις ή αξιολογήσεις κινδύνου.

Η χρήση τέτοιων συστημάτων μπορεί να οδηγήσει σε διαίωνιση των υφιστάμενων κοινωνικών ανισοτήτων και να επηρεάσει την αρχή της ίσης μεταχείρισης ενώπιον του νόμου. Για τον λόγο αυτό, η ανάπτυξη και χρήση αλγοριθμικών εργαλείων στη δικαιοσύνη απαιτεί ιδιαίτερη προσοχή ως προς την ποιότητα και την αντιπροσωπευτικότητα των δεδομένων που χρησιμοποιούνται για την εκπαίδευσή τους, καθώς και τη θέσπιση κατάλληλων μηχανισμών ελέγχου και διαφάνειας.

Χαρακτηριστικό παράδειγμα των προβληματισμών που ανακύπτουν με την αλγοριθμική μεροληψία αποτελεί το σύστημα COMPAS (Correctional Offender Management Profiling for Alternative Sanctions). Το COMPAS είναι ένα σύστημα που λειτουργεί στις Ηνωμένες Πολιτείες της Αμερικής και ουσιαστικά χρησιμοποιείται από τους δικαστές επιβοηθητικά κατά τη λήψη απόφασης για την υφ' όρο απόλυσή ή μη ενός καταδικασθέντος προσώπου βάσει μίας πρόγνωσης για τη μελλοντική πιθανότητα υποτροπής του προσώπου αυτού.¹⁰⁴

¹⁰³ Βλ. ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΓΙΑ ΑΞΙΟΠΙΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ, (ΟΕΥΕ για την ΤΝ), 2019, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf τελευταία πρόσβαση 28/02/2026.

¹⁰⁴ Βλ. <https://edblogs.medium.com/compas-an-ai-tool-sending-or-keeping-people-in-jail-d9228df3a2c6> τελευταία πρόσβαση 28/02/2026

Σκοπός του COMPAS είναι να εκτιμήσει την πιθανότητα υποτροπής ενός ατόμου, δηλαδή τον κίνδυνο να διαπράξει εκ νέου αξιόποινή πράξη. Για τον σκοπό αυτό, το σύστημα αναλύει μεγάλο αριθμό δεδομένων που αφορούν το άτομο, όπως το ποινικό του ιστορικό, κοινωνικοοικονομικούς παράγοντες, προσωπικά χαρακτηριστικά και απαντήσεις σε ειδικά ερωτηματολόγια. Με βάση την επεξεργασία αυτών των δεδομένων, ο αλγόριθμος παράγει μια βαθμολογία κινδύνου (risk score), η οποία χρησιμοποιείται από τους δικαστές ως εργαλείο υποστήριξης κατά τη λήψη αποφάσεων, για παράδειγμα σχετικά με την προφυλάκιση, την επιβολή ποινής ή την αποφυλάκιση υπό όρους. Εν συνεχεία, η πρόγνωση αυτή γίνεται μέσω της κατάρτισης ενός προφίλ του υπό εξέταση καταδικασθέντος προσώπου, το οποίο συγκρίνεται με τα προφίλ άλλων δραστών που είχαν κατά το παρελθόν τελέσει παρόμοια εγκλήματα και το ιστορικό τους.¹⁰⁵

Η χρήση του COMPAS έχει προκαλέσει έντονη επιστημονική και νομική συζήτηση. Από τη μία πλευρά, υποστηρίζεται ότι τέτοια συστήματα μπορούν να συμβάλουν στην αντικειμενικότερη αξιολόγηση κινδύνου και στην αποτελεσματικότερη διαχείριση των σωφρονιστικών πόρων. Από την άλλη πλευρά, έχουν διατυπωθεί σοβαρές ανησυχίες σχετικά με τη διαφάνεια των αλγορίθμων, την πιθανή ύπαρξη αλγοριθμικών προκαταλήψεων (algorithmic bias) και τις επιπτώσεις τους στα θεμελιώδη δικαιώματα των κατηγορουμένων, ιδίως ως προς την αρχή της δίκαιης δίκης που αναφέρθηκε παραπάνω και της ίσης μεταχείρισης. Συγκεκριμένα ανεξάρτητοι οργανισμοί που εξέτασαν το σύστημα COMPAS διαπίστωσαν ότι το σύστημα λειτουργούσε με προκατάληψη και ουσιαστικά είχε λανθασμένη πρόγνωση κι αυτό διότι υπήρχε προκατάληψη σε φυλετικές ομάδες, ενώ ξεχώριζε έντονα τους λευκούς.

5.1.3. Έλλειψη διαφάνειας των αλγοριθμικών συστημάτων

Ένα από τα σημαντικότερα ζητήματα που ανακύπτουν από την ενσωμάτωση συστημάτων τεχνητής νοημοσύνης στη λειτουργία της δικαιοσύνης είναι η ανάγκη διασφάλισης της αρχής της διαφάνειας. Η διαφάνεια αποτελεί βασική προϋπόθεση για την αποφυγή αρνητικών επιπτώσεων από τη χρήση αλγοριθμικών εργαλείων στη δικαστική διαδικασία και συνδέεται άμεσα με τη δυνατότητα κατανόησης και ελέγχου του τρόπου λειτουργίας των συστημάτων αυτών.

¹⁰⁵ Ο.π υποσημ. 89 σελ 5

Ειδικότερα, η αρχή της διαφάνειας προϋποθέτει τη δυνατότητα πρόσβασης τόσο στα δεδομένα που χρησιμοποιούνται για την εκπαίδευση των αλγορίθμων όσο και στη μεθοδολογία και τον τρόπο με τον οποίο τα συστήματα τεχνητής νοημοσύνης καταλήγουν σε συγκεκριμένα αποτελέσματα. Στο πλαίσιο αυτό, τίθεται το ζήτημα της πρόσβασης στον πηγαίο κώδικα των αλγοριθμικών συστημάτων, ο οποίος συχνά προστατεύεται από κανόνες διανοητικής ιδιοκτησίας. Για την εξασφάλιση ουσιαστικής διαφάνειας, έχει υποστηριχθεί ότι θα πρέπει να προβλέπονται κατάλληλοι περιορισμοί ή μηχανισμοί ελέγχου, ώστε να καθίσταται δυνατή η τεχνική αξιολόγηση των συστημάτων αυτών από τις αρμόδιες αρχές αλλά και από τα πρόσωπα που επηρεάζονται από τις αποφάσεις τους.¹⁰⁶

Παράλληλα, κρίνεται σημαντικό να παρέχονται πληροφορίες σχετικά με τα δεδομένα που χρησιμοποιήθηκαν για την εκπαίδευση του αλγορίθμου, όπως ο αριθμός των αποφάσεων που αναλύθηκαν, η αντιπροσωπευτικότητά τους και οι πηγές από τις οποίες προέρχονται. Η πρόσβαση σε τέτοιου είδους πληροφορίες επιτρέπει τόσο στις δικαστικές και αστυνομικές αρχές όσο και στους διαδίκους να αξιολογήσουν την αξιοπιστία και την εγκυρότητα των αποτελεσμάτων που παράγονται από τα συστήματα τεχνητής νοημοσύνης.¹⁰⁷

5.1.4. Πλεονεκτήματα της χρήσης ΤΝ στη Δικαιοσύνη

Παρά τις επιφυλάξεις που εκφράζουν, ιδίως τα ευρωπαϊκά δικαστήρια, σχετικά με την ενσωμάτωση συστημάτων τεχνητής νοημοσύνης στις δικαστικές διαδικασίες, και ιδιαίτερα σε εφαρμογές όπως η προγνωστική αστυνόμευση που αναλύθηκε παραπάνω, δεν μπορεί να παραγνωριστεί ότι οι τεχνολογίες αυτές έχουν τη δυνατότητα να συμβάλουν ουσιαστικά στην απονομή της δικαιοσύνης. Ειδικότερα στον τομέα της εγκληματολογίας διαπιστώνεται ότι οι αλγόριθμοι μπορούν να λειτουργήσουν υποστηρικτικά προς τις αρμόδιες αρχές και τους ερευνητές, διευκολύνοντας την ανάλυση μεγάλου όγκου δεδομένων και επιταχύνοντας την εξαγωγή χρήσιμων συμπερασμάτων. Με τον τρόπο αυτό, τα συστήματα τεχνητής νοημοσύνης μπορούν να βελτιώσουν την

¹⁰⁶ Ο.π υποσ 97 σελ 14

¹⁰⁷ Ο.π υποσ 97 σελ 64

αποτελεσματικότητα των υφιστάμενων διαδικασιών, αυτοματοποιώντας ορισμένα στάδια της έρευνας και συμβάλλοντας στην ταχύτερη επίτευξη αποτελεσμάτων.¹⁰⁸

Μάλιστα, η ορθή λειτουργία ενός συστήματος πρόληψης τέλεσης νέων εγκλημάτων αποτελεί ιδιαιτέρως σημαντική πτυχή των συστημάτων τεχνητής νοημοσύνης, αφού η χρήση τους θα μπορούσε ενδεχομένως να ελαχιστοποιήσει τους παράγοντες κινδύνου που σχετίζονται με εγκληματική-παρατακτική συμπεριφορά και να βελτιώσει την συμβίωση των πολιτών.¹⁰⁹ Θα βοηθούσε επίσης και μετά την φυλάκιση ενός δράστη καθώς δεν αποκλείεται η χρήση τους να συμβάλλει στην αποτροπή τέλεσης νέων εγκλημάτων.¹¹⁰

Η τεχνητή νοημοσύνη μπορεί να προσφέρει σημαντικά πλεονεκτήματα στη λειτουργία της δικαιοσύνης, συμβάλλοντας κυρίως στην ταχύτερη και αποτελεσματικότερη επεξεργασία μεγάλου όγκου νομικών δεδομένων. Μέσω της ανάλυσης νομολογίας, εγγράφων και αποδεικτικών στοιχείων, τα συστήματα ΤΝ μπορούν να υποστηρίξουν τους δικαστικούς λειτουργούς στο έργο τους, διευκολύνοντας την έρευνα και την προετοιμασία των υποθέσεων. Παράλληλα, η αυτοματοποίηση ορισμένων διαδικασιών μπορεί να μειώσει τον χρόνο απονομής της δικαιοσύνης και να συμβάλει στην αποσυμφόρηση των δικαστηρίων. Επιπλέον, η χρήση τέτοιων τεχνολογικών εργαλείων μπορεί να περιορίσει ορισμένα ανθρώπινα λάθη που οφείλονται στον μεγάλο φόρτο εργασίας, ενισχύοντας έτσι την αποτελεσματικότητα και την οργάνωση του δικαστικού συστήματος.

5.2 Προτεινόμενες λύσεις

Απέναντι στις πολυεπίπεδες προκλήσεις που αναλύθηκαν στην προηγούμενη ενότητα, η ακαδημαϊκή κοινότητα και τα ευρωπαϊκά θεσμικά όργανα έχουν αρχίσει να χαράσσουν ένα πλαίσιο αντίδρασης, το οποίο κινείται σε τρεις αλληλένδετους άξονες: τον κανονιστικό, τον τεχνικό και τον θεσμικό.

¹⁰⁸ Βλ. Γ. Καρανταΐδης, *Cyber Security Month*, (2018) *Η Τεχνητή Νοημοσύνη στην υπηρεσία της Εγκληματολογίας*.

¹⁰⁹ Διπλωματική Εργασία της Ζωής Λουλούδη (2022) *ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ* Υπό το πρίσμα των Θεμελιωδών Δικαιωμάτων του Ανθρώπου, σελ 77.

¹¹⁰ Βλ. J. Bachner (2013), *Predictive Policing: Preventing Crime with Data and Analytics*, IBM Center for The Business of Government, Washington, DC, σελ. 86

Πρώτον, σε κανονιστικό επίπεδο, ο Κανονισμός (ΕΕ) 2024/1689 για την Τεχνητή Νοημοσύνη (AI Act) θέτει ήδη δεσμευτικές υποχρεώσεις για τα συστήματα ΤΝ υψηλού κινδύνου που χρησιμοποιούνται στη δικαιοσύνη, επιβάλλοντας αυστηρές απαιτήσεις διαφάνειας, ιχνηλασιμότητας και ανθρώπινης εποπτείας κατά το άρθρο 14 του Κανονισμού.¹¹¹ Η ανθρώπινη εποπτεία δεν αποτελεί απλώς τυπική επιταγή, αλλά ουσιαστική εγγύηση: ο δικαστής οφείλει να διατηρεί την τελική εξουσία να επικυρώνει, τροποποιεί ή απορρίπτει οποιαδήποτε αλγοριθμική εισήγηση, διότι μόνο έτσι διασφαλίζεται η συμβατότητα με το άρθρο 8 του Συντάγματος για το δικαίωμα στον νόμιμο δικαστή.¹¹²

Δεύτερον, σε τεχνικό επίπεδο, κεντρική θέση κατέχει η αρχή της «επεξηγησιμότητας» (explainability), σύμφωνα με την οποία κάθε αλγοριθμικό σύστημα που επηρεάζει δικαστική κρίση οφείλει να παράγει κατανοητή αιτιολόγηση της λειτουργίας του, ώστε να μπορεί να ελεγχθεί τόσο από τον δικαστή όσο και από τα αντίδικα μέρη, διασφαλίζοντας την αρχή της ισότητας των όπλων.¹¹³ Στο ίδιο πλαίσιο, η Οδηγία NIS 2 (2022/2555/ΕΕ) επιβάλλει στις δικαστικές υποδομές υψηλά πρότυπα κυβερνοασφάλειας, κρυπτογράφηση, πολυπαραγοντική ταυτοποίηση και έλεγχο της εφοδιαστικής αλυσίδας λογισμικού, ως αναγκαία συμπλήρωμα κάθε εφαρμογής ΤΝ στο δικαστικό σύστημα¹¹⁴.

Τρίτον, σε θεσμικό επίπεδο, ο Ευρωπαϊκός Χάρτης Δεοντολογίας της CEPEJ για τη χρήση ΤΝ στα δικαστικά συστήματα προτείνει την εφαρμογή πέντε θεμελιωδών αρχών: σεβασμό των θεμελιωδών δικαιωμάτων, αρχή της μη διάκρισης, ποιότητα και ασφάλεια δεδομένων, διαφάνεια και ουδετερότητα, και τέλος τη διατήρηση του ελέγχου εκ μέρους του χρήστη.¹¹⁵ Η αποτελεσματική εφαρμογή των λύσεων αυτών στην ελληνική πραγματικότητα προϋποθέτει, ωστόσο, και τη συστηματική επιμόρφωση των δικαστικών λειτουργών στις νέες τεχνολογίες, καθώς η ΤΝ δεν μπορεί να λειτουργήσει ως αξιόπιστο

¹¹¹ Ο.π. υποσημ. 1, άρθρο 14.

¹¹² Ο.π. υποσημ. 45, σελ. 1273.

¹¹³ Ο.π. υποσημ. 70, σελ. 1519.

¹¹⁴ Βλ. Οδηγία (ΕΕ) 2022/2555 (NIS 2), άρθρο 21

¹¹⁵ Ο.π. υποσημ. 97, σελ. 9-10.

εργαλείο δικαιοσύνης αν ο χειριστής της αγνοεί τόσο τις δυνατότητες όσο και τους εγγενείς περιορισμούς της.¹¹⁶

5.2.1 Ο ανθρώπινος έλεγχος ως θεμελιώδης εγγύηση της δικαστικής ανεξαρτησίας

Η πλέον θεμελιώδης λύση στους κινδύνους που αναλύθηκαν δεν είναι τεχνολογικής αλλά ανθρωποκεντρικής φύσεως: η αρχή του «ανθρώπινου ελέγχου» (human-in-the-loop). Σύμφωνα με την αρχή αυτή, η οποία κατοχυρώνεται ρητώς στο άρθρο 14 του AI Act, κανένα σύστημα ΤΝ που παράγει έννομα αποτελέσματα δεν μπορεί να λειτουργεί χωρίς τη δυνατότητα ουσιαστικής παρέμβασης φυσικού προσώπου.¹¹⁷ Στο δικαστικό πεδίο, η αρχή αυτή αποκτά συνταγματική υπόσταση: το άρθρο 8 του Συντάγματος, που κατοχυρώνει το δικαίωμα στον νόμιμο δικαστή, ερμηνευόμενο συστηματικά, οδηγεί στο συμπέρασμα ότι ως «δικαστής» νοείται αποκλειστικά φυσικό πρόσωπο, γεγονός που καθιστά συνταγματικά ανεπίτρεπτη τη λήψη δικαστικών αποφάσεων από αλγόριθμο εν απουσία φυσικού δικαστή.¹¹⁸

Η εφαρμογή deep της αρχής αυτής στην πράξη σημαίνει ότι τα συστήματα ΤΝ πρέπει να σχεδιάζονται και να λειτουργούν αποκλειστικά ως «Συστήματα Υποστήριξης Αποφάσεων» (Decision Support Systems), και όχι ως αυτόνομοι λήπτες αποφάσεων.¹¹⁹ Ο δικαστής οφείλει να διατηρεί την απόλυτη εξουσία να επικυρώνει, τροποποιεί ή ολοκληρωτικά απορρίπτει κάθε αλγοριθμική εισήγηση, και μάλιστα να αιτιολογεί την τελική του κρίση με βάση τις ιδιαιτερότητες της υπόθεσης, σύμφωνα με την επιταγή του άρθρου 177 ΚΠΔ.¹²⁰ Ο ορατός κίνδυνος, που επισημαίνεται εύστοχα στη θεωρία ως «αλγοριθμική συμμόρφωση», συνίσταται ακριβώς στην αντίθετη πρακτική: ο δικαστής, υπό το βάρος του τεράστιου φόρτου εργασίας, ενδέχεται να υιοθετεί άκριτα τα αποτελέσματα του συστήματος, μετατρέπόμενος ουσιαστικά σε «φυγόποινο κριτή» που παραμένει προσκολλημένος στην πρόταση του αλγορίθμου αδυνατώντας να αναλάβει αυθεντική, προσωπική κρίση.¹²¹

¹¹⁶ Ο.π υποσημ. 69, σελ 9-10.

¹¹⁷ Βλ. Κανονισμός (ΕΕ) 2024/1689 (AI Act), άρθρο 14 «Ανθρώπινη εποπτεία»

¹¹⁸ Ο.π. υποσημ. 50, σελ. 723

¹¹⁹ Ο.π υποσημ 48, σελ 158.

¹²⁰ Ο.π υποσημ 5, σελ. 1343

¹²¹ Ο.π υποσημ 22, σελ 3

Η αντιμετώπιση του κινδύνου αυτού απαιτεί συνδυασμό δύο μέτρων. Αφενός, σε επίπεδο σχεδιασμού, τα συστήματα ΤΝ πρέπει να παρέχουν στον δικαστή όχι μόνο αποτελέσματα αλλά και επεξηγήσεις της μεθοδολογίας τους, ώστε να είναι τεχνικά δυνατός ο έλεγχος του δικανικού συλλογισμού που οδήγησε σε κάθε αλγοριθμικό συμπέρασμα.¹²² Αφετέρου, σε επίπεδο εκπαίδευσης, κρίνεται απολύτως αναγκαία η συστηματική επιμόρφωση των δικαστικών λειτουργών τόσο στις δυνατότητες όσο και στους εγγενείς περιορισμούς των συστημάτων ΤΝ, ώστε ο δικαστής να μπορεί να αξιολογεί κριτικά κάθε αλγοριθμική εισήγηση και να μην της αποδίδει αυθεντία που δεν της ανήκει. Η λύση αυτή δεν αντιτίθεται στην αξιοποίηση της ΤΝ στη δικαιοσύνη· αντίθετα, αποτελεί την αναγκαία προϋπόθεση για να γίνει η αξιοποίηση αυτή ουσιαστική, ασφαλής και συνταγματικώς ανεκτή. Διότι, όπως εύστοχα επισημαίνεται, ο στόχος δεν είναι να αντικατασταθούν οι φυσικοί δικαστές από τις μηχανές, αλλά να καταστούν οι μηχανές «δεξί τους χέρι».

5.2.2 Αρχές δεοντολογίας (Χάρτης CEPEJ)

Όπως προελέχθη, η ταχέως εξελισσόμενη χρήση της τεχνητής νοημοσύνης στα δικαστικά συστήματα οδήγησε στην υιοθέτηση του “ Ευρωπαϊκού Χάρτη Δεοντολογίας για τη χρήση της Τεχνητής Νοημοσύνης και στο περιβάλλον τους” από την Ευρωπαϊκή Επιτροπή για την Αποτελεσματικότητα της Δικαιοσύνης (CEPEJ).¹²³

Μια από τις βασικότερες αρχές που προβλέπονται στον εν λόγω Χάρτη είναι η αρχή του σεβασμού των θεμελιωδών δικαιωμάτων, ιδίως υπό το πρίσμα της διασφάλισης ότι ο σχεδιασμός και η εφαρμογή των εργαλείων και υπηρεσιών της τεχνητής νοημοσύνης σέβονται τα θεμελιώδη δικαιώματα. Πιο συγκεκριμένα, σε περίπτωση που εφαρμογές τεχνητής νοημοσύνης χρησιμοποιούνται για την επίλυση μιας διαφοράς ή για τη λήψη μιας δικαστικής απόφασης, είναι σημαντικό να διασφαλίζεται ότι μια τέτοια χρήση σέβεται το δικαίωμα πρόσβασης σε δικαστήριο και το δικαίωμα στη δίκαιη δίκη¹²⁴. Ωστόσο, προκειμένου να επιτευχθεί αυτός ο σκοπός, έμφαση πρέπει να δοθεί ήδη κατά το στάδιο σχεδιασμού των εν λόγω αλγοριθμικών εφαρμογών, έτσι ώστε να ακολουθηθεί

¹²² Ο.π υποσημ 71, σελ 64

¹²³ Βλ. <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>, τελευταία πρόσβαση 16/03/2026

¹²⁴ Ο.π. υποσημ. 71, σελ. 11.

μια “ethical-by-design” προσέγγιση, η οποία προβλέπει την ενσωμάτωση κανόνων που σέβονται τα ανθρώπινα δικαιώματα, όπως αυτά προβλέπονται στις Συνθήκες¹²⁵

Δεύτερη αρχή που προβλέπει ο Χάρτης είναι η αρχή της μη διακριτικής μεταχείρισης, υπό την έννοια της αποφυγής πρόκλησης ή ενίσχυσης διακριτικής μεταχείρισης μεταξύ ατόμων ή ομάδων ατόμων.¹²⁶

Σε αυτό το σημείο αξίζει να σημειωθεί ότι τα συστήματα τεχνητής νοημοσύνης δεν μπορούν να θεωρηθούν αντικειμενικά και ουδέτερα, καθώς ήδη από το στάδιο της εκμάθησης είναι δυνατή η αναπαραγωγή στερεοτύπων και διακρίσεων εις βάρος μειονοτικών ομάδων. Κρίσιμος παράγοντας στην αντιμετώπιση αυτής της κατάστασης είναι η επιλογή μηχανισμών εποπτείας όπου ο άνθρωπος είναι εκείνος που παρεμβαίνει (human-in-the-loop), εκείνος που εποπτεύει (human-on-the-loop) ή εκείνος που ελέγχει (human-in-command).¹²⁷ Συναφώς κρίνεται απαραίτητο οι μέθοδοι επεξεργασίας των δεδομένων να είναι προσβάσιμες και κατανοητές, κάτι που συνάδει με την αρχή της διαφάνειας που πρέπει να διακατέχει τα συστήματα τεχνητής νοημοσύνης.¹²⁸

Επιπρόσθετα, εξίσου σημαντική είναι η αρχή της ποιότητας και της ασφάλειας, σύμφωνα με την οποία η επεξεργασία των δικαστικών αποφάσεων και δεδομένων πρέπει να γίνεται με τη χρήση πιστοποιημένων πηγών και άυλων δεδομένων λαμβάνοντας υπόψη μοντέλα που έχουν δημιουργηθεί με διεπιστημονικό τρόπο μέσα σε ένα ασφαλές τεχνολογικό περιβάλλον.

Ιδίως όταν πρόκειται για χρήση της τεχνητής νοημοσύνης στον τομέα της δικαιοσύνης εν γένει, οι σχεδιαστές των αλγορίθμων πρέπει να αξιοποιούν τις ειδικές γνώσεις των δικηγόρων, δικαστών, εισαγγελέων κ.ο.κ. Αυτό θα μπορούσε να επιτευχθεί μέσω της δημιουργίας μικτών ομάδων εργασίας, κάτι που θα ενισχύσει την διεπιστημονική προσέγγιση.

¹²⁵ Ο.π. υποσημ. 124.

¹²⁶ Ο.π. υποσημ. 71, σελ. 12

¹²⁷ Ανεξάρτητη ομάδα εμπειρογνομόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη (2018) *ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΓΙΑ ΑΞΙΟΠΙΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ*, σελ. 20.

¹²⁸ Ο.π. υποσημ. 71, σελ. 14.

Τέλος, θεμελιώδης είναι και η αρχή του ελέγχου από τον χρήστη. Πιο συγκεκριμένα, καθίσταται υψίστης σημασίας η αποφυγή τυποποιημένων προσεγγίσεων και η προτεραιοποίηση της αυτονομίας του χρήστη. Είναι αυτονόητο, δε, ότι οι επαγγελματίες του συστήματος απονομής δικαιοσύνης πρέπει να διατηρούν τον έλεγχο της προσωπικής τους κρίσης και ανεξαρτησίας χωρίς να δεσμεύονται από δεδομένα και εφαρμογές που τους προσφέρει ο αλγόριθμος. Στο ίδιο πλαίσιο, ακόμα και αν πρόκειται για διάδικο, πρέπει να ενημερώνεται με σαφή τρόπο ως προς το αν έχει τυχόν προηγηθεί επεξεργασία κάποιας υπόθεσης μέσω τεχνητής νοημοσύνης, αλλά και να απολαμβάνει το δικαίωμα εναντίωσης έτσι ώστε η υπόθεσή του να εκδικασθεί άμεσα από δικαστήριο, κατά της επιταγές του άρθρου 6 της ΕΣΔΑ.¹²⁹

Οι Αρχές αυτές, όπως παρουσιάζονται στον Χάρτη Δεοντολογίας, θέτουν τα ηθικά θεμέλια για τη χρήση των συστημάτων τεχνητής νοημοσύνης στη δικαιοσύνη. Ωστόσο, δεν μπορεί να παραλειφθεί το γεγονός ότι η ανάγκη δημιουργίας ενός αυστηρότερου και δεσμευτικότερου δεοντολογικού πλαισίου είναι αδήριτη. Η παγκόσμια κοινότητα οφείλει να στρέψει την προσοχή της στη διαμόρφωση αυστηρών κατευθυντήριων γραμμών, απευθυνόμενων τόσο σε εταιρίες που ασχολούνται με την δημιουργία συστημάτων τεχνητής νοημοσύνης, όσο και στα ίδια τα Κράτη Μέλη, ώστε να προωθηθούν και στα δικαστικά συστήματα.

ΚΕΦΑΛΑΙΟ VI ΣΥΜΠΕΡΑΣΜΑ

Η ραγδαία εξέλιξη της τεχνολογίας τα τελευταία χρόνια έχει επηρεάσει σημαντικά πολλούς τομείς της ανθρώπινης δραστηριότητας, μεταξύ των οποίων και τη λειτουργία της δικαιοσύνης. Η τεχνητή νοημοσύνη αποτελεί πλέον ένα από τα πιο σημαντικά εργαλεία της ψηφιακής εποχής και σταδιακά αρχίζει να ενσωματώνεται και στα δικαστικά συστήματα. Η αξιοποίηση τέτοιων τεχνολογιών δημιουργεί νέες δυνατότητες για την οργάνωση και τη λειτουργία της δικαιοσύνης, αλλά ταυτόχρονα προκαλεί και προβληματισμούς σχετικά με τις επιπτώσεις που μπορεί να έχει στην εφαρμογή του δικαίου και στην προστασία των θεμελιωδών δικαιωμάτων.

¹²⁹ Ο.π. υποσημ. 71, σελ. 16.

Στο πλαίσιο της παρούσας εργασίας εξετάστηκε ο ρόλος της τεχνητής νοημοσύνης στη διαδικασία ψηφιοποίησης της δικαιοσύνης, καθώς και οι προκλήσεις που προκύπτουν από την εφαρμογή της. Όπως προκύπτει από την ανάλυση που προηγήθηκε, η τεχνητή νοημοσύνη μπορεί να συμβάλει σημαντικά στη βελτίωση της λειτουργίας των δικαστικών συστημάτων. Ιδιαίτερα σε περιπτώσεις όπου απαιτείται η επεξεργασία μεγάλου όγκου δεδομένων, τα συστήματα τεχνητής νοημοσύνης μπορούν να λειτουργήσουν ως χρήσιμα εργαλεία υποστήριξης για τους δικαστές και τους νομικούς επαγγελματίες.

Ένα από τα βασικά πλεονεκτήματα της χρήσης τέτοιων τεχνολογιών είναι η δυνατότητα επιτάχυνσης της επεξεργασίας πληροφοριών και νομικών δεδομένων. Τα δικαστικά συστήματα πολλών χωρών αντιμετωπίζουν σημαντικές καθυστερήσεις λόγω του μεγάλου αριθμού εκκρεμών υποθέσεων. Στο πλαίσιο αυτό, η τεχνητή νοημοσύνη μπορεί να συμβάλει στην καλύτερη οργάνωση και διαχείριση των υποθέσεων, καθώς είναι σε θέση να αναλύει γρήγορα μεγάλο όγκο εγγράφων, νομολογίας και αποδεικτικών στοιχείων. Με τον τρόπο αυτό μπορεί να διευκολυνθεί το έργο των δικαστών και των δικηγόρων, μειώνοντας τον χρόνο που απαιτείται για την προετοιμασία και την εξέταση μιας υπόθεσης.

Παράλληλα, η τεχνητή νοημοσύνη μπορεί να λειτουργήσει ως ένα εργαλείο που υποστηρίζει τη δικαστική κρίση. Μέσω της ανάλυσης προηγούμενων δικαστικών αποφάσεων και νομικών δεδομένων, τα συστήματα αυτά μπορούν να εντοπίζουν μοτίβα και τάσεις στη νομολογία, προσφέροντας χρήσιμες πληροφορίες στους νομικούς επαγγελματίες. Σε ορισμένες περιπτώσεις μάλιστα έχουν αναπτυχθεί συστήματα που επιχειρούν να προβλέψουν την πιθανή έκβαση μιας υπόθεσης με βάση προηγούμενες αποφάσεις, κάτι που μπορεί να συμβάλει στην καλύτερη κατανόηση της δικαστικής πρακτικής.

Ωστόσο, η χρήση της τεχνητής νοημοσύνης στη δικαιοσύνη δεν είναι απαλλαγμένη από κινδύνους. Ένας από τους σημαντικότερους προβληματισμούς αφορά το ενδεχόμενο να περιοριστεί ο ρόλος της ανθρώπινης κρίσης στη διαδικασία λήψης αποφάσεων. Η δικαιοσύνη αποτελεί έναν θεμελιώδη θεσμό του κράτους δικαίου και βασίζεται σε αρχές όπως η ανεξαρτησία των δικαστών και η εξατομικευμένη αξιολόγηση

κάθε υπόθεσης. Για τον λόγο αυτό, η πλήρης αυτοματοποίηση της δικαστικής λειτουργίας θα μπορούσε να δημιουργήσει σοβαρά προβλήματα, καθώς οι αλγόριθμοι δεν είναι σε θέση να λαμβάνουν υπόψη όλες τις κοινωνικές και ανθρώπινες παραμέτρους που συχνά επηρεάζουν μια δικαστική κρίση.

Ένα ακόμη σημαντικό ζήτημα που αναδείχθηκε είναι ο κίνδυνος εμφάνισης αλγοριθμικών προκαταλήψεων. Τα συστήματα τεχνητής νοημοσύνης εκπαιδεύονται συνήθως με βάση δεδομένα που προέρχονται από προηγούμενες αποφάσεις ή από αστυνομικά και διοικητικά αρχεία. Εάν τα δεδομένα αυτά περιλαμβάνουν ήδη κοινωνικές ανισότητες ή προκαταλήψεις, υπάρχει ο κίνδυνος τα συστήματα τεχνητής νοημοσύνης να αναπαράγουν αυτές τις ανισότητες. Αυτό θα μπορούσε να οδηγήσει σε αποφάσεις που επηρεάζονται από διακρίσεις, γεγονός που έρχεται σε αντίθεση με τις θεμελιώδεις αρχές της δικαιοσύνης και της ισότητας.

Επιπλέον, σημαντικός προβληματισμός δημιουργείται και από το ζήτημα της διαφάνειας των αλγοριθμικών συστημάτων. Πολλά από τα συστήματα τεχνητής νοημοσύνης λειτουργούν με ιδιαίτερα σύνθετους αλγορίθμους, οι οποίοι δεν είναι εύκολο να κατανοηθούν από τους χρήστες τους. Αυτό δημιουργεί δυσκολίες ως προς την αξιολόγηση του τρόπου με τον οποίο λαμβάνονται οι αποφάσεις ή παράγονται τα αποτελέσματα των συστημάτων αυτών. Στο πλαίσιο της δικαιοσύνης, η διαφάνεια αποτελεί ιδιαίτερα σημαντική προϋπόθεση, καθώς οι πολίτες πρέπει να μπορούν να γνωρίζουν και να ελέγχουν τον τρόπο με τον οποίο λαμβάνονται αποφάσεις που επηρεάζουν τα δικαιώματά τους.

Σημαντικό είναι επίσης το ζήτημα της ευθύνης σε περίπτωση που ένα σύστημα τεχνητής νοημοσύνης οδηγήσει σε λανθασμένο αποτέλεσμα. Η πολυπλοκότητα των αλγοριθμικών συστημάτων καθιστά συχνά δύσκολο τον εντοπισμό του υπεύθυνου σε περίπτωση σφάλματος. Για τον λόγο αυτό, είναι απαραίτητο να υπάρχουν σαφείς κανόνες και ρυθμίσεις που να καθορίζουν ποιος φέρει την ευθύνη για τις αποφάσεις που επηρεάζονται από τη χρήση τέτοιων τεχνολογιών.

Παρά τους κινδύνους και τις προκλήσεις που αναφέρθηκαν, η τεχνητή νοημοσύνη δεν πρέπει να αντιμετωπίζεται αποκλειστικά ως απειλή για τη λειτουργία της δικαιοσύνης. Αντίθετα, μπορεί να αποτελέσει ένα ιδιαίτερα χρήσιμο εργαλείο για τον

εκσυγχρονισμό των δικαστικών συστημάτων, εφόσον χρησιμοποιείται με προσοχή και υπό κατάλληλες εγγυήσεις. Η τεχνητή νοημοσύνη μπορεί να συμβάλει στην καλύτερη οργάνωση των δικαστικών διαδικασιών, στην ταχύτερη επεξεργασία των υποθέσεων και στη βελτίωση της πρόσβασης των πολιτών στη δικαιοσύνη.

Συνεπώς, το μέλλον της τεχνητής νοημοσύνης στη δικαιοσύνη δεν θα πρέπει να βασίζεται στην πλήρη αντικατάσταση του ανθρώπινου παράγοντα, αλλά στη συνεργασία μεταξύ ανθρώπου και τεχνολογίας. Ο ρόλος των δικαστών και των νομικών επαγγελματιών παραμένει καθοριστικός, καθώς η απονομή της δικαιοσύνης απαιτεί όχι μόνο τεχνική ανάλυση δεδομένων αλλά και ανθρώπινη κρίση, εμπειρία και κατανόηση των κοινωνικών συνθηκών κάθε υπόθεσης.

Τελικά, η αξιοποίηση της τεχνητής νοημοσύνης στη δικαιοσύνη αποτελεί μια σημαντική πρόκληση για τα σύγχρονα νομικά συστήματα. Η τεχνολογία αυτή μπορεί να προσφέρει σημαντικά οφέλη, αρκεί η χρήση της να γίνεται με τρόπο που να σέβεται τις βασικές αρχές του κράτους δικαίου και την προστασία των θεμελιωδών δικαιωμάτων. Η σωστή ισορροπία μεταξύ τεχνολογικής καινοτομίας και νομικών εγγυήσεων θα αποτελέσει καθοριστικό παράγοντα για το πώς θα διαμορφωθεί στο μέλλον η σχέση μεταξύ τεχνητής νοημοσύνης και δικαιοσύνης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Αραβαντινός Β. Θ., «Δίκαιο και Πληροφορική» σε επιμορφωτικό σεμινάριο Δικαστικών Λειτουργών (17-18/3/2022).

Βόρρας σε Μήτρου, (2023) “Μπορεί ο αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να δικάζει και να διοικεί;”, Πανεπιστημιακές Εκδόσεις Κρήτης.

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΑΠΟΦΑΣΗ ΤΟΥ ΔΙΚΑΣΤΗΡΙΟΥ της 16ης Οκτωβρίου 2018 σχετική με την κατάθεση και την επίδοση διαδικαστικών εγγράφων μέσω της εφαρμογής e-Curia.

Ευρωπαϊκή Επιτροπή για την αποτελεσματικότητα της Δικαιοσύνης (2018), Ευρωπαϊκός Χάρτης Δεοντολογίας για την χρήση συστημάτων ΤΝ στα δικαστικά συστήματα και στο περιβάλλον τους
Ιγγλεζάκης Ι. (2021), Δίκαιο Πληροφορικής, Δ' Έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 449.

Καρανταΐδης Γ. (2018) Η Τεχνητή Νοημοσύνη στην υπηρεσία της Εγκληματολογίας.

Καρκατζούνης Β., Ο ρόλος των δεδομένων στο οικοσύστημα της Νομικής Τεχνολογίας (Legal Tech), ΤΝΠ QUALEX, ΣΥΝ, 4/2020.

Μήτρου Λ., (2023) Μπορεί ο αλγόριθμος να είναι ηθικός, να είναι δίκαιος, να είναι διαφανής, να δικάζει και να διοικεί; Πανεπιστημιακές Εκδόσεις Κρήτης.

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων» 2019.

Παναγοπούλου Φ., Η απονομή της δικαιοσύνης μέσω Τεχνητής Νοημοσύνης. Συνταγματικά ζητήματα δικαστικής προστασίας, σε : Συλλογικό έργο, Σύ και δικαστής άριστος. ΤΝΠ: ΣΑΚΚΟΥΛΑΣ.

Παπαπαναγιώτου Α. και Ζάχου Χ. (2021), Συστήματα Τεχνητής Νοημοσύνης στον τομέα της Δικαιοσύνης. Τα ηθικά διλήμματα και τα όρια του Ευρωπαϊκού Χάρτη.

Συμβούλιο της Ε.Ε. (2020) “Συμπεράσματα του Συμβουλίου «Πρόσβαση στη δικαιοσύνη – αξιοποίηση των ευκαιριών της ψηφιοποίησης» (2020/C 342 I/01)”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.
Σωτηριάδου Φ., Τεχνητή Νοημοσύνη και Δικαιοσύνη: Διερεύνηση ή συρρίκνωση του δικαιώματος δικαστικής προστασίας;

Φιλόπουλος Π., Η χρήση των αλγορίθμων στη μετεξέλιξη του Ποινικού Δικαίου, ΕΛΛΔνη 5/2024.

Bernhardt W., (2021) *The Use of Artificial Intelligence in the Field of Justice*”, Internet and New Technologies Law

Campbell J. (1989). *The improbable machine: What the upheavals in Artificial Intelligence research reveal about how the mind really works.*

Casanovas P., Biasiotti M. A., Francesconi E., Sagri M. T. (Eds.), (2007) *Proceedings of LOAIT '07, "2nd Workshop on Legal Ontologies and Artificial Intelligence Techniques"*

Chesterman S. (2023), *All Rise for the Honourable Robot Judge? Using Artificial Intelligence to Regulate AI, Technology and Regulation.*

D. Djurayev (2024), *Cybersecurity and Data Protection in Modern Electronic Justice Ecosystems.*

Enders P., *Einsatz Kunstlicher Intelligenz bei juristischer Entscheidungsfindung*, JA 2018.

Gogić K., (2022) *"The Impact of Covid-19 on the Digitalisation of Justice in the European Union"*, CIFILE *Journal of International Law*, Vol. 3, No. 6, 1-11.

J. Park (2020) *Your Honor, AI*, Harvard international Review.

Jougleux P. (2022) *Γενικός Κανονισμός προσωπικών δεδομένων στον τομέα της δικαιοσύνης Μέσο Δημοσίευσης*, ΤΝΠ QUALEX.

Kinchin N., *"Voiceless": the procedural gap in algorithmic justice*, *International Journal of Law and Information Technology*, Volume 32, 2024.

Loveday B., (2000) *Address to EGPA Conference, Cape Sounion, Greec'*, σε M. Fabri et al. (eds.), *"The Challenge of Change for Judicial Systems"*

Quattrocchio S. (2019) *An Introduction to AI and Criminal Justice in Europe*, 5 Rev Brasileira de Direito Processual Penal.

Razmetaeva Y. & Razmetaev Se., (2021) *Justice in the Digital Age: Technological Solutions, Hidden Threats and Enticing Opportunities*, Access to Just E Eur 104.

Ronkainen A., *From Spelling Checkers to Robot Judges? Some Implications of Normativity in Language Tech and AI & Law.*

Russe S. και Norving P. (1995) *Artificial Intelligence A Modern Approach"*, Third edition.

Shi, Changqing and Sourdin, Tania and Li, Bin, (2021), *The Smart Court - A New Pathway to Justice in China?* *International Journal for Court Administration*, ΤΝΠ HEIN.

T. Singelsnstein, *Predictive Pricing; Algorithmenbasierte Strafprognosen zur vorausschauenden Kriminalintervention*, NStZ 2018, 1.

Terzidou K. (2023), *The Use of Artificial Intelligence in the Judiciary and Its Compliance with the Right to a Fair Trial.*

Toon N. (2024), *How AI Thinks*, Transworld Publishers Ltd.

Vicoli D. (2024) *"Editorial of Dossier "Digitalisation and Criminal Justice: Procedural Aspects" - An Introductory Overview"*, 10 Rev Brasileira de Direito Processual Penal 1.

Wirkuttis N. και Klein H., *Artificial Intelligence in Cybersecurity*, ΤΝΠ HEIN ONLINE.

ΔΙΠΛΩΜΑΤΙΚΕΣ ΕΡΓΑΣΙΕΣ

Ανδρεάδου Χ. (2025) *Αξιοποίηση του κειμένου της δικαστικής απόφασης στο Ολοκληρωμένο Σύστημα Διαχείρισης Διοικητικής Δικαιοσύνης (ΟΣΔΔΥ-ΔΔ) με σύγχρονες εφαρμογές ανάλυσης και επεξεργασίας κειμένου*, Παν. Μακεδονίας.

Βιδάκη Α. Ν. (2022) *Ψηφιοποίηση της δικαιοσύνης: Κανονιστικό πλαίσιο, ζητήματα δεοντολογίας και μελλοντικές προκλήσεις* Διώνη.

Γιώρκα Μ. Α. (2022), *ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΠΡΟΣΒΑΣΗ ΣΤΗ ΔΙΚΑΙΟΣΥΝΗ*, Παν. Πειραιώς.

Λουλούδη Ζ. (2022) *ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ Υπό το πρίσμα των Θεμελιωδών Δικαιωμάτων του Ανθρώπου*, Διώνη.

Μπάλντα Ι. (2022), *Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΣΥΓΧΡΟΝΗ ΨΗΦΙΑΚΗ ΕΠΟΧΗ*, Παν. Πειραιώς.

Πολυζώη ΕΛ., *ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ ΔΙΚΑΙΟΣΥΝΗ: Εφαρμογές και προκλήσεις για την εισαγωγή της τεχνητής νοημοσύνης στα δικαστικά συστήματα*

Σιδέρη Μ. (2025), *Κρατική επιτήρηση και κοινωνική ταξινόμηση στην Κίνα*, Διώνη.

Σουλδάτου Μ. (2024) *Τεχνητή Νοημοσύνη και Δικαιοσύνη* Παν. Μακεδονίας.

Τερζίδου Κ. (2025), *Η Ψηφιοποίηση της Δικαιοσύνης στην Ευρωπαϊκή Ένωση μέσω της Τεχνητής Νοημοσύνης*, Διώνη.

Ευρωπαϊκή και ελληνική Νομοθεσία

Ευρωπαϊκή Επιτροπή (2020) *“Η ψηφιοποίηση της δικαιοσύνης στην Ευρωπαϊκή Ένωση. Μια εργαλειοθήκη ευκαιριών*, COM (2020) 710 final”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1689 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Ιουνίου 2024 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη).

Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση, ΕΕ L 194/1.

Συμβούλιο της Ε.Ε., “Ευρωπαϊκή στρατηγική για την ηλεκτρονική δικαιοσύνη για την περίοδο 2024 - 2028 - Εγκριση (15509/2023)”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 17.11.2023.

Συμβούλιο της Ε.Ε., “Συμπεράσματα του Συμβουλίου «Πρόσβαση στη δικαιοσύνη – αξιοποίηση των ευκαιριών της ψηφιοποίησης» (2020/C 342 I/01)”, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2020.

Συμβούλιο της Ε.Ε., Ευρωπαϊκή στρατηγική για την ηλεκτρονική δικαιοσύνη για την περίοδο 2024 - 2028 - Εγκριση (15509/2023), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

Νομολογία

ΕΔΔΑ, *Marcello Viola κατά Ιταλίας* 45106/04 της 5.10.2006.

ΕΔΔΑ, *Sakhnovski κατά Ρωσίας* 21272/03, της 2ας Νοεμβρίου 2010.

Ιστοσελίδες- Ιστότοποι

[Estonia does not develop AI Judge | Justitiisministeerium](#), τελευταία πρόσβαση 29/12/2025

H. George, (2021), «Phising Emails are Homeland Security’s Most Feared Cyber Threat» <https://www.homelandsecurityedu.org/2017/01/phishingemails-are-homeland-securitys-most-feared-cyber-threat/> , τελευταία πρόσβαση 26/02/2026.

<https://bigblue.academy/gr/deep-learning-vs-machine-learning>, τελευταία πρόσβαση 28/12/2025.

<https://edblogs.medium.com/compas-an-ai-tool-sending-or-keeping-people-in-jail-d9228df3a2c6>

https://employment-social-affairs.ec.europa.eu/policies-and-activities/international-partners-and-agencies/decentralised-agencies_el τελευταία πρόσβαση 26/12/2025.

<https://eur-lex.europa.eu/content/welcome/about.html?locale=el> τελευταία πρόσβαση 26/12/2025.

<https://eur-lex.europa.eu/content/welcome/about.html?locale=el>, τελευταία πρόσβαση 26/12/2025.

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-operational-management-large-scale-it-systems-area-freedom-security-and_el , τελευταία πρόσβαση 27/12/2025.

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_el τελευταία πρόσβαση 13/02/2026.

<https://ministryofjustice.gr/?p=13929> τελευταία πρόσβαση 24/02/2026

<https://lawnet.gr/law-news/i-poiniki-prostasia-ton-dedomenon-prosopikou-charaktira-ypo-to-n-4624-2019>, τελευταία πρόσβαση 26/02/2026

<https://n-lex.europa.eu/n-lex/about/about?lang=el> τελευταία πρόσβαση 26/12/2025.

<https://pinakio.e-diki.justice.gov.gr/guest/home>

<https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>, τελευταία πρόσβαση 16/03/2026

<https://www.fortinet.com/resources/cyberglossary/what-is-hacking>, τελευταία πρόσβαση 26/02/2026.

<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> τελευταία πρόσβαση: 23/02/26.

<https://www.sciencedirect.com/topics/earth-and-planetary-sciences/artificial-neural-network> τελευταία πρόσβαση 28/12/2025.

OECD, Recommendation of the Council on Artificial Intelligence, 2024, <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>, τελευταία πρόσβαση 28/12/2025.

Resolution 2081 (2015), «Access to justice and the Internet: potential and challenges», para. 1, 27 November 2015, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=22283&lang=en> τελευταία πρόσβαση 23/02/2026.

Stillmann J., *An AI just Outperformed 20 Top Lawyers (and the Lawyers Were Happy)*, A new study highlights a major flaw in much of the usual 'Robots will take all our jobs!', <https://www.inc.com/jessica-stillman/an-ai-just-outperformed-20-top-lawyers-and-lawyers-were-happy.html> τελευταία πρόσβαση 03/02/2026

T. Lewis, «Don't Let Artificial Intelligence Take Over, Top Scientists Warn» (2015) τελευταία πρόσβαση 28/02/2026, <https://www.livescience.com/49419-artificial-intelligence-dangers-letter.html>

Ανακοίνωση της Ευρωπαϊκής Επιτροπής-Τεχνητή νοημοσύνη για την Ευρώπη, Βρυξέλλες, 25.4.2018 COM (2018) 237 final, <https://eurlex.europa.eu/legalcontent/EL/TXT/HTML/?uri=CELEX:52018DC0237&from=MT> τελευταία πρόσβαση: 26/2/2026.

Βίβλο Ψηφιακού Μετασχηματισμού 2020-2025, https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_strategy.pdf τελευταία πρόσβαση 21/02/2026.

Εγχειρίδιο Κυβερνοασφάλειας - Cybersecurity Handbook - Βέλτιστες πρακτικές για την προστασία και την ανθεκτικότητα των πληροφοριακών συστημάτων - Υπουργείο Ψηφιακής Διακυβέρνησης - Ιούνιος 2021, <https://mindigital.gr/wpcontent/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%B>

[D%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf](#)

τελευταία πρόσβαση 18/02/2026.

Η εξέλιξη της κυβερνοασφάλειας στην Ε.Ε <https://odeth.eu/%CE%B7-%CE%B5%CE%BE%CE%AD%CE%BB%CE%B9%CE%BE%CE%B7-%CF%84%CE%B7%CF%82-%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82-%CF%83%CF%84%CE%B7%CE%BD-%CE%B5/> ,

τελευταία πρόσβαση 18/02/2026.

KATEYΘYNTHPIEΣ ΓPAMMEΣ ΔEONTOΛOΓIAC ΓIAC AΞIOPICTH TEXNHITH NOHMOCYTHH, (OEYE για την TN), 2019, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf

Περιοδικό της Νομικής Βιβλιοθήκης, 2025, με θέμα: Deepfakes και ποινική δικαιοσύνη: Η νέα απειλή της Τεχνητής Νοημοσύνης, <https://daily.nb.org/arthrografia/periodika-nb/deepfakes-kai-poiniki-dikaiosyni-i-nea-apeili-tis-technitis-noimosynis/> τελευταία πρόσβαση 28/02/2026,

Υπουργείο Δικαιοσύνης (2025) « Ψηφιοποίηση αρχείων δεδομένων του Υπουργείου Δικαιοσύνης» Διαθέσιμο στο: https://ministryofjustice.gr/?page_id=14882 τελευταία πρόσβαση 27/12/2025.

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Άρθρο	Άρ.
Βλέπετε	Βλ.
Νόμος	N.
Τράπεζα Νομικών Πληροφοριών	TNP
Σελίδα	Σελ.
Υποσημείωση	Υποσημ.
Όπως προηγουμένως	Ό.π.