Επιθεώρηση Δημοσίου & Διεθνούς Δικαίου

Φοιτητικό Επιστημονικό Περιοδικό Δημοσίου & Διεθνούς Δικαίου της Νομικής Σχολής του Πανεπιστημίου Αθηνών

ΤΕΥΧΟΣ 1 | ΕΤΟΣ Α΄ | ΟΚΤΩΒΡΙΟΣ

ΑΡΘΡΟ

Η Αποκεντρωμένη Τεχνητή Νοημοσύνη υπό το Πρίσμα του Δημοσίου Διεθνούς Δικαίου: Ρυθμιστικές προκλήσεις, Παραβίαση θεμελιωδών δικαιωμάτων και Αστική ευθύνη Δημοσίου για Αυτόματα Οπλικά Συστήματα

Βασιλεία Τριανταφύλλου[1]
Αναστάσιος Βουτζαλής[2]

Abstract. Η Τεχνητή Νοημοσύνη (ΤΝ) παρά την πρόσφατη εμφάνισή της, την τελευταία δεκαετία, έχει αναμφισβήτητα σημειώσει σημαντική εξέλιξη επηρεάζοντας όλους τους τομείς της καθημερινότητας και κατά συνέπεια το δίκαιο και την νομοθεσία. Το παρόν άρθρο πραγματεύεται την σημασία της Αποκεντρωμένης μορφής της *(Decentralised AI)* και τις νομικές προκλήσεις που ανακύπτουν εξαιτίας του διαχωρισμού της από την μέχρι τώρα κρατούσα και μοναδική Κεντρικοποιημένη μορφή της ΤΝ. Η παρακάτω μελέτη δεν θα αρκεστεί σε μια κοινότυπη ανάλυση της Αποκεντρωμένης Τεχνητής Νοημοσύνης αλλά σε μια εξακρίβωση του ζητήματος: «Είναι εφικτό ένα δικανικό σύστημα σχεδιασμένο για την ρύθμιση της Κεντρικοποιημένης ΤΝ, το οποίο αποδίδει ευθύνες και κρατάει υπόλογα συγκεκριμένα φυσικά και νομικά πρόσωπα, να εφαρμόζεται το ίδιο αποτελεσματικά στην Αποκεντρωμένη, χαρακτηριστικό της οποίας είναι η έλλειψη ενός σαφούς «κέντρου», χωρίς την ταυτόχρονη καταπάτηση των θεμελιωδών ανθρωπίνων δικαιωμάτων;». Η πλειοψηφία ειδικών που έχει απασχοληθεί με το ανακύπτον ζήτημα έχει αποφανθεί αρνητικά και έχουν διατυπωθεί διαφόρων ειδών ανησυχίες για καταπάτηση θεμελιωδών

[1]Η Βασιλεία Τριανταφύλλου είναι προπτυχιακή φοιτήτρια της Νομικής Αθηνών.
[2]Ο Αναστάσιος Βουτζαλής είναι προπτυχιακός φοιτητής της Νομικής Αθηνών

ανθρωπίνων δικαιωμάτων λόγω αδυναμίας ανάλογης εφαρμογής κανονισμών στο καινούριο αυτό μοντέλο ΤΝ που έχει έρθει για να αλλάξει ριζικά τα δεδομένα που υπήρχαν μέχρι σήμερα.[3] Στην συνέχεια θα αναφερθούν παραδείγματα των μεταβολών που σημειώνονται σε διάφορους τομείς με δυνατότητα προσβολής θεμελιωδών δικαιωμάτων. Η μελέτη τοποθετείται με την κρατούσα άποψη για τον ασαφή και τον ατελή νομικό έλεγχο ενός διαρκώς αναπτυσσόμενου συστήματος τεχνολογίας που επηρεάζει ουσιωδώς από πολλές πτυχές την ζωή μας και απειλεί άμεσα ορισμένα βασικά δικαιώματα ενώ παράλληλα προστατεύει άλλα πιο αποτελεσματικά. Ιδίως, στα ζητήματα προστασίας της ιδιωτικότητας η Αποκεντρωμένη ΤΝ μέσω της χρήσης "federated learning" δεν χρειάζεται να αποχωρήσει τα δεδομένα από την κατοχή του υποκειμένου με σκοπό την εκπαίδευση του συστήματος όπως στα παραδοσιακά νέφη ελέγχου, κάτι που εξασφαλίζει μεγαλύτερη προστασία της ιδιωτικότητας και των προσωπικών δεδομένων του κατόχου.[4]

[3] Blaine Deolindo, "Decentralized AI: A Regulatory Escape Hatch or the Future of Compliant Innovation," LinkedIn, 23.09.2025, https://www.linkedin.com/pulse/decentralized-ai-regulatory-escape-hatch-future-blaine-deolindo-taasf.

[4] Edward Somgal, "The Rise of Decentralized AI: A New Era of Privacy Protection?," Maya Data Privacy, 09.07.2025, https://www.mayadataprivacy.com/post/the-rise-of-decentralized-ai-a-new-era-of-privacy-protection.

Πίνακας περιεχομένων

Εισαγωγή **246**

Δομή και Λειτουργία **246**

Συμβατότητα Αποκεντρωμένης Τεχνητής Νοημοσύνης με Κανονισμούς - «EU AI ACT 2024» ΚΑΙ «GDPR» **249**

Παραβίαση Θεμελιωδών Αρχών και Διεθνείς Πρωτοβουλίες **256**

Κρατική Ευθύνη **258**

Συμβατότητα με Αρχές Διεθνούς Ανθρωπιστικού Δικαίου **260**

Συμπέρασμα **262**

Βιβλιογραφία **264**

Εισαγωγή

Η Τεχνητή Νοημοσύνη έχοντας εμφανιστεί τα τελευταία μόλις χρόνια με την μορφή της Κεντρικοποιημένης τεχνολογίας, αλλάζει το προσκήνιο με την έντονη παρουσία της Αποκεντρωμένης ΤΝ. Οι διάφορες μορφές με τις οποίες εμφανίζεται διέπονται κατά κύριο λόγο από κοινό νομοθετικό σύστημα ρύθμισης και λειτουργούν σύμφωνα με μία συγκεκριμένη ηλεκτρονική βάση δεδομένων. Η βασική διαφορά στις μορφές αυτές έγκειται στον εκάστοτε ελεγκτικό φορέα που διαχειρίζεται την αντίστοιχη βάση δεδομένων οδηγώντας στην διάκριση μεταξύ της Κεντρικοποιημένης (Centralised AI) και Αποκεντρωμένης ΤΝ (Decentralised AI) αλλά και στο γεγονός ότι η δεύτερη συναντάται στον ιδιωτικό κυρίως τομέα όπου τα δεδομένα είναι πιο ευαίσθητα[5]. Από την πλευρά της Κεντρικοποιημένης ΤΝ η διαχείριση πραγματοποιείται από έναν ενιαίο φορέα, όπως μια εταιρεία ή μια κυβέρνηση, ενώ στην Αποκεντρωμένη ΤΝ ο φορέας διαχείρισης δεν περιορίζεται σε έναν μόνο κεντρικό έλεγχο αλλά σε ένα δίκτυο υπολογιστών και κόμβων με την χρήση σύγχρονων τεχνολογιών *«blockchain»* και *«smart contracts»* και καθίσταται με αυτόν τον τρόπο δυνατή η επεξεργασία των πληροφοριών από πολλούς χρήστες και μέσω *«edge devices».*

Δομή και Λειτουργία

Η Αποκεντρωμένη ΤΝ αποτελείται από τα *δίκτυα κατανεμημένης ισχύος* που εκπαιδεύονται με *ομόσπονδη εκπαίδευση (federated learning)*, το σύστημα «*blockchain*» και τα «*smart contracts*» και την *αποκεντρωμένη διακυβέρνησή* τους.[6] Η σχέση μεταξύ των παραπάνω είναι οργανική όπως αναδεικνύεται και από τον ρόλο που έχει το κάθε συστατικό στην λειτουργία αυτής της

[5] Mia Lysikova, "Decentralized AI: What It Is and How It Differs from Centralized AI? [*sic*]," nexos.ai, 16.01.2026, https://nexos.ai/blog/de-centralized-ai/.
[6] UltraEdge, "Decentralized AI: How It Works and the Benefits," 07.07.2025, https://www.ultraedge.com/en/blog/decentralized-ai.

μορφής Τεχνητής Νοημοσύνης και η σύγκλισή τους ευθύνεται για την διαρκή και εύκολη εξέλιξη της εκπαίδευσης και διαχείρισης μοντέλων ανοίγοντας τον δρόμο για ένα πιο ασφαλές και δημοκρατικό οικοσύστημα χωρίς τον περιορισμό εξουσίας στα αρχικά, συγκεντρωτικά υπολογιστικά νέφη *(centralised clouds).*[7] Καταρχήν, τα δίκτυα της κατανεμημένης ισχύος αποτελούν το υποδομικό υπόστρωμα του συνολικού συστήματος *(infrastructure layer).* Σε αντίθεση με το πρωταρχικό σύστημα της κεντρικοποιημένης ΤΝ που χρησιμοποιεί μονολιθικές βάσεις δεδομένων *(data bases),* τα δίκτυα στην προκειμένη περίπτωση μετατρέπουν την ανδρανή επεξεργαστική ισχύ *(idle CPU/GPU/TPU)* διαφόρων ηλεκτρονικών συσκευών «στην άκρη του διαδικτύου» *(Edge Devices)* όπως είναι οι προσωπικής χρήσης ηλεκτρονικοί υπολογιστές όλων των μορφών, οι έξυπνες οικιακές συσκευές, οι έξυπνες κάμερες ασφαλείας, τα αυτόνομα οχήματα αλλά και οι βιομηχανικοί αισθητήρες. Εξασφαλίζεται, με αυτό το νέο μοντέλο ΤΝ, η μείωση κόστους για την αναβάθμιση των κεντρικών υποδομών εφόσον η υπολογιστική ικανότητα αυξάνεται με οριζόντια κλιμακωσιμότητα *(horizontal scalability)* με μόνη την προσθήκη νέων κόμβων.[8] Επιπλέον, καταργείται η ανάγκη για διαμεσολάβηση και οι χρονοτριβές που παρουσιάζονται για την ολοκλήρωση της επικοινωνίας και της μεταφοράς δεδομένων σε μία βάση δεδομένων, αφού γίνεται απευθείας μεταξύ των κόμβων ακολουθώντας το γνωστό σύστημα *Peer-to-Peer* (P2P).[9] Επιπροσθέτως, παρατηρείται διευρυμένη ανοχή σε σφάλματα λόγω απουσίας ενός ενιαίου σημείου αποτυχίας ,σε αντίθεση με την κεντρικοποιημένη ΤΝ όπου ένα σφάλμα λειτουργίας στην βάση δεν επηρεάζει μεμονωμένα ένα μέρος ,αλλά ολόκληρη την βάση πληροφοριών.[10]

---

[7] Ramesh Raskar, "Decentralized AI," MIT Media Lab, https://www.media.mit.edu/projects/decentralized-ai/overview/.
[8] Tom Marshall, *Decentralised Artificial Intelligence* (London: CMS, 2024), https://cms.law/en/gbr/publication/decentralised-artificial-intelligence.
[9] Phillip Shoemaker, "What Is a Peer-to-Peer (P2P) Network?," Identity.org, 18.12.2025, https://www.identity.org/peer-to-peer-network/.
[10] Lysikova, "Decentralised AI," ενότητα "Resilience"

Η εκπαίδευση του αλγοριθμικού συστήματος γίνεται με την μέθοδο της ομόσπονδης, ιδιωτικής και κατανεμημένης μάθησης *«Federated learning».*[11] Υπάρχουν τέσσερα στάδια σε αυτή τη διαδικασία. Πρώτα απ' όλα, είναι το στάδιο της *«initialization»* ή «αρχικοποίησης» , οπού δημιουργείται ένα μοντέλο από τον κεντρικό διακομιστή και διανέμεται σε όλες τις συσκευές όπου ακολουθεί η «τοπική εκπαίδευση» χωρίς αποστολή των προσωπικών δεδομένων εκτός συσκευής. Στην συνέχεια ακολουθεί η συγκέντρωση *«global aggregation»* από διάφορες συσκευές και επανάληψη *«iteration»* της διαδικασίας μέχρι την επίτευξη της επιθυμητής απόδοσης. Ως αποτέλεσμα, εξασφαλίζεται η προστασία των πνευματικών δικαιωμάτων και η ιδιωτικότητα του χρήστη χάρη στην τοπική εκπαίδευση *(on device training)* , την απομόνωση των πρωτογενών δεδομένων *(data soiling)* και την συγκέντρωση παραμέτρων *(gradient aggregation)* που εξασφαλίζει ότι το σύστημα αποκτά μόνο μαθησιακές αναβαθμίσεις κι όχι τα ίδια τα προσωπικά δεδομένα.

Παράλληλα, η χρήση του *blockchain* εγγυάται την πλήρη ασφάλεια και προστασία των δεδομένων με τον έγκαιρο εντοπισμό κακόβουλων κόμβων και αποκλείει την αλλοίωση τους και την πρόσβαση σε αυτά από ανεπιθύμητα λογισμικά. Ταυτόχρονα, η καθιέρωση των smart contracts, που αποτελούν αυτοεκτελούμενους κώδικες στο σύστημα του *blockchain*, εξασφαλίζουν την ποιότητα των πληροφοριών που αποκτώνται και την αμοιβή των κόμβων απ' όπου προήλθαν με ψηφιακά νομίσματα *(tokens).*[12] Τελευταίο χαρακτηριστικό είναι η αποκεντρωμένη διακυβέρνηση που υλοποιείται κυρίως μέσω Αποκεντρωμένων Αυτόνομων Οργανισμών (DAOS-Decentralised Autonomous Organisations),[13]

[11] Rina Diane Caballar και Cole Stryker, "What Is Federated Learning?," IBM Think, 02.04.2025, https://www.ibm.com/think/topics/federated-learning. Υπάρχουν διαφορετικά είδη "Federated Learning": α) cross device β) cross silo γ) horizontal δ) vertical.
[12] J Chen "Blockchain and AI Integration" (2024)
[13] Law Commission, "Decentralised Autonomous Organisations (DAOs)," https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/· Carlos Santana και Laura Albareda, "Blockchain

δημιουργώντας ένα πιο δημοκρατικό, ασφαλές και προσβάσιμο μοντέλο που διέπεται από ηθικούς κανόνες τεθειμένους από τον εκάστοτε ΑΑΟ.

Συμβατότητα Αποκεντρωμένης Τεχνητής Νοημοσύνης με Κανονισμούς - «EU AI ACT 2024» ΚΑΙ «GDPR»

Διαπιστώνεται με βάση την παραπάνω ανάλυση ,η διαφοροποίηση και εξέλιξη ανάμεσα στις δύο αυτές μορφές ΤΝ, η οποία επηρεάζει την αποτελεσματικότητα εφαρμογής των σχετικών νομοθετικών κειμένων που θεσπίστηκαν με βάση το μοντέλο της κεντρικοποιημένης ΤΝ και δημιουργούνται κενά στην προσπάθεια ανάλογης εφαρμογής στην αποκεντρωμένη με επαυξημένο κίνδυνο παραβίασης των ανθρωπίνων δικαιωμάτων.[14] Το EU AI ACT 2024 , από τα πρώτα κιόλας άρθρα φαίνεται να διαμορφώνει την νομοθεσία γύρω από συγκεκριμένα πρόσωπα που θεωρούνται «υπεύθυνοι» χρησιμοποιώντας την ορολογία *«deployer», «provider»*[15] για να ορίσει τα νομικά και φυσικά πρόσωπα που φέρουν νομική ευθύνη (Άρθρο 3 EU AI ACT) και με το άρθρο 16 του ίδιου κειμένου ανατίθενται στο πρόσωπο αυτό συγκεκριμένες υποχρεώσεις αναλόγως τον βαθμό ρίσκου που έχει το εκάστοτε σύστημα.[16] Τα συστήματα ΤΝ ρυθμίζονται στο EU AI ACT 2024 με βάση τον βαθμό ρίσκου που εμφανίζει το καθένα με διαβαθμίσεις «απαράδεκτο ρίσκο»

---

and the Emergence of Decentralized Autonomous Organizations (DAOs): An Integrative Model and Research Agenda," *Technological Forecasting and Social Change* 182 (2022): 121806, https://doi.org/10.1016/j.techfore.2022.121806.

[14] Deolindo "Decentralized AI: A regulatory escape hatch".

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council, 13.06.2024, άρθρο 3 σημεία 3–4, OJ L, 2024/1689, 12.07.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 [AI Act]: "'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge; 'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity".

[16] *Ibid.*, Article 16: Obligations of providers of high-risk AI systems.

(unacceptable risk), «υψηλό ρίσκο» *(high risk)*, «περιορισμένο ρίσκο» *(limited risk)*, «ελάχιστο ρίσκο» *(minimal risk)*.[17] Στην πρώτη βαθμίδα απειλείται εμφανώς η ασφάλεια και τα ανθρώπινα δικαιώματα, όπως γίνεται με την αναγνώριση μέσω χρήσης βιομετρικών στοιχείων και την «κοινωνική πίστωση» ή «*social scoring*». Η δεύτερη αφορά την χρήση ΤΝ για ζητήματα όπως την πρόσληψη ανθρώπινου δυναμικού, καθιστώντας την αμφισβητήσιμη ενώ η δεύτερη και η τρίτη αφορούν την παροχή υπηρεσιών και τις προσωποποιημένες διαφημίσεις που αποτελούν αναπόσπαστο τμήμα της καθημερινότητάς μας. Με βάσει την παραπάνω διαβάθμιση και σύμφωνα με το άρθρο 25 του ίδιου κανονισμού στα μοντέλα υψηλού κινδύνου ένας τρίτος μπορεί να μετατραπεί σε «provider» εφόσον επιφέρει ουσιώδεις τροποποιήσεις, γεγονός που προκαλεί ζήτημα ασφαλείας εφόσον η αποκεντρωμένη ΤΝ λειτουργεί αποκλειστικά σχεδόν με τρίτους, καθιστώντας αδύνατο να αποδοθεί ευθύνη σε συγκεκριμένο πρόσωπο όπως γίνεται και με το άρθρο 26 του κανονισμού ,το οποίο προϋποθέτει την ύπαρξη συγκεκριμένου «*deployer*» που έχει την εξουσία επί του συστήματος. Επομένως, όσον αφορά το EU AI ACT 2024 δεν υπάρχει απευθείας απόκλιση της αποκεντρωμένης ΤΝ από το πεδίο εφαρμογής , αλλά η πρόκληση εντοπίζεται όταν η οργάνωση και το τεχνικό μέρος δεν περιορίζονται σε συγκεκριμένα πρόσωπα κι ο καταλογισμός ευθυνών δυσχεραίνει την αποτελεσματική επιβολή του κανονισμού, όπου και προκύπτουν τα διάφορα ερωτηματικά για το αν είναι εφικτή η αναλογική εφαρμογή του ΓΚΠΔ.

Η έλευση της τεχνολογίας «κατανεμημένου καθολικού» *(Blockchain)* και η «αυτοματοποιημένη εκτέλεση πράξεων μέσω έξυπνων συμβολαίων» *(smart contracts)* έχουν πράγματι επιφέρει μια ριζική μεταβολή στην δομή της πληροφορίας. Με αυτήν την εξέλιξη προσδίδεται η "Αποκεντρωμένη" φύση που δημιουργεί σοβαρά ζητήματα μη συμβατότητας με τον Γενικό

[17] Future of Life Institute, "High-Level Summary of the AI Act," EU Artificial Intelligence Act, 27.02.2024, https://artificialintelligenceact.eu/high-level-summary/.

Κανονισμό Προστασίας των Δεδομένων (GDPR) της Ε.Ε. Το κεντρικό σημείο τριβής εντοπίζεται στον ορισμό του «υπεύθυνου επεξεργασίας» κατά το Άρθρο 4 παρ.7 του ΓΚΠΔ.[18] Σύμφωνα, με την εν λόγω διάταξη ορίζεται ως υπεύθυνος επεξεργασίας ένα νομικό ή φυσικό πρόσωπο που καθορίζει τον τρόπο και τους σκοπούς επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Συνεπώς, σε μια τεχνολογία όπως αυτή της Decentralised AI όπου και δεν υπάρχει η δυνατότητα άσκησης ουσιαστικής και κυρίαρχης επιρροής επί των δεδομένων, το ζήτημα γίνεται πιο περίπλοκο. Μάλιστα, όπως επισημαίνεται από την μελέτη του Ευρωπαϊκού Κοινοβουλίου για το *blockchain* και τον ΓΚΠΔ, η κατανομή των λειτουργιών ανάμεσα σε κόμβους, σε *«digital miners»,*[19] σε προγραμματιστές και σε τελικούς χρήστες διαχέει τον έλεγχο σε τέτοιο βαθμό, ώστε κανένα μεμονωμένο υποκείμενο να μην μπορεί να θεωρηθεί αυτοτελώς υπεύθυνο. Επιπροσθέτως, λόγω αυτής της αμετάβλητης φύσης *(immutability*[20]*)*του καθολικού μετά την εγκατάσταση των *smart contracts* στο δίκτυο, δημιουργείται η τεχνική αδυναμία στους συμμετέχοντες τόσο στο να τροποποιούν όσο και στο να διαγράφουν τα δεδομένα. Αυτό, όπως αποφαίνεται, οδηγεί σε ένα νομικό κενό ευθύνης.

Ποια ήταν η αντίδραση του Ευρωπαϊκού Δικαστηρίου για την κάλυψη των νομικών κενών και την

---

[18] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, 27.04.2016, άρθρο 4 σημείο 7, ΕΕ L 119, 04.05.2016, 1–88, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679 [εφεξής: ΓΚΠΔ]: «"υπεύθυνος επεξεργασίας": το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους».

[19] *«digital miners»* τα εξειδικευμένα μηχανήματα ή άτομα που χρησιμοποιούν ισχυρούς υπολογιστές για την επικύρωση συναλλαγών και τη δημιουργία νέων κρυπτονομισμάτων

[20] Xiang Hui και Catherine Tucker, "Decentralization, Blockchain, Artificial Intelligence (AI): Challenges and Opportunities," *Journal of Product Innovation Management* 42, no. 5 (2025), https://doi.org/10.1111/jpim.12800.

προστασία των υποκειμένων; Η νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ)[21] έχει υιοθετήσει μια ιδιαίτερα ευρεία ερμηνεία του όρου του «υπευθύνου». Κρίθηκε από το αρμόδιο δικαστήριο ότι η συνυπευθυνότητα *(Joint Controllership),* όπως προβλέπεται στο Άρθρο 26 του ΓΚΠΔ,[22] δεν απαιτεί κάποιο είδος ισομερούς ελέγχου ή πρόσβαση στα δεδομένα από τους συμμετέχοντες, αλλά δίνεται η ευχέρεια να καταλήξουν σε μια από κοινού απόφαση για τον τρόπο επεξεργασίας τους. Έτσι, με αυτήν την ρύθμιση το βάρος της ευθύνης στα *"έξυπνα συμβόλαια"* μετακυλίεται σε δύο κατηγορίες δρώντων, τους Δημιουργούς / Προγραμματιστές *«Creators/Developers»* και τους Συμμετέχοντες / Χρήστες *«Participants/Nodes».* Παράλληλα, γαλλική αρχή προστασίας δεδομένων (CNIL),[23] υποστηρίζει ότι την στιγμή που οι *«Creators»* αναπτύσσουν και θέτουν σε εφαρμογή ένα *smart contract* προς δικό τους όφελος ή μιας κοινότητας με χαρακτηριστικό παράδειγμα τα *«DeFi protocols»* αποκτούν ευθύνη. Επομένως, καθορίζονται εκ των προτέρων οι παράμετροι και ο «τρόπος» επεξεργασίας μέσω του αμετάβλητου κώδικα και οι δημιουργοί συμβάλλουν αποφασιστικά στον καθορισμό των μέσων, «εγκλωβίζοντας» το σύστημα σε μια προδιαγεγραμμένη τροχιά επεξεργασίας. Εν συνεχεία, ο κάθε χρήστης, που

[21] Ιδίως στις υποθέσεις *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein κατά Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, EU:C:2018:388, και *Fashion ID GmbH & Co. KG κατά Verbraucherzentrale NRW eV*, C-40/17, EU:C:2019:629.

[22] Άρθρο 26 παρ. 1 ΓΚΠΔ: «1. Σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της επεξεργασίας, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτοί καθορίζουν με διαφανή τρόπο τις αντίστοιχες ευθύνες τους για συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον παρόντα κανονισμό, ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τα αντίστοιχα καθήκοντά τους για να παρέχουν τις πληροφορίες που αναφέρονται στα άρθρα 13 και 14, μέσω συμφωνίας μεταξύ τους, εκτός εάν και στον βαθμό που οι αντίστοιχες αρμοδιότητες των υπευθύνων επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους στο οποίο υπόκεινται οι υπεύθυνοι επεξεργασίας. Στη συμφωνία μπορεί να αναφέρεται ένα σημείο επικοινωνίας για τα υποκείμενα των δεδομένων.»

[23] Commission nationale de l'informatique et des libertés, "AI System Development: CNIL's Recommendations to Comply with the GDPR," 05.01.2026, https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr.

αλληλεπιδρά με το δημιουργηθέν «*smart contract*», εισάγει δεδομένα ή κόμβους για την επικύρωση των συναλλαγών, επιδιώκοντας κάποιον προσωπικό σκοπό (πχ. οικονομικές συναλλαγές). Αυτή, λοιπόν η σύγκλιση των σκοπών μεταξύ των μέσων που σχεδίασαν οι «*Developers*» και των χρηστών στοιχειοθετεί αυτό που ονομάζεται Συνυπευθυνότητα και ρυθμίζεται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (European Data Protection Board).

Τα νομικά ερωτηματικά, εντούτοις, δεν αίρονται εδώ. Η σύμπλευση της τεχνολογίας του κατανεμημένου καθολικού *(Blockchain)* της Αποκεντρωμένης ΤΝ (Decentralized AI) δημιουργεί μια φαινομενικά αγεφύρωτη νομική ασυμφωνία με το ευρωπαϊκό κανονιστικό πλαίσιο. Το Άρθρο 17 του ΓΚΠΔ (GDPR) κατοχυρώνει το «δικαίωμα στη λήθη» *(right to be forgotten),* επιβάλλοντας την οριστική διαγραφή προσωπικών δεδομένων[24]. Η κανονιστική αυτή επιταγή έρχεται σε σύγκρουση με το δομικό χαρακτηριστικό του «*blockchain*», το «απόλυτο αμετάβλητο» *(immutability).* Πιο συγκεκριμένα, η αρχιτεκτονική δομή του καθολικού βασίζεται στην αρχή του «*append only*» (μόνο για προσθήκη) με αποτέλεσμα η εκ των υστέρων τροποποίηση ή απαλοιφή των δεδομένων να καθίσταται τεχνικά αδύνατη[25]. Αυτή η αδυναμία εκτέλεσης των διαγραφών σε συνδυασμό με την απουσία κεντρικού υπευθύνου επεξεργασίας αιτιολογεί τον χαρακτηρισμό του «*Blockchain*» ως μια «τεχνολογία σε εγγενή ασυμβατότητα με τον «GDPR». Εδώ, αξίζει να αναφερθεί πως το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB), στις Κατευθυντήριες Γραμμές του 2025 για την

[24] ΓΚΠΔ, άρθρο 17 (Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)): «Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση».

[25] Michèle Finck, *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?*, PE 634.445 (Brussels: European Parliamentary Research Service, 2019), https://doi.org/10.2861/535.

επεξεργασία των «*digital data*» μέσω «*Blockchain*», διασαφήνισε πως οι τεχνολογικοί περιορισμοί δεν απαλλάσσουν τους υπευθύνους επεξεργασίας από τις υποχρεώσεις τους, ενώ ταυτόχρονα η νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης επιβεβαιώνει τον αυστηρό χαρακτήρα του Άρθρου 17 του ΓΚΠΔ. Επιπροσθέτως, το ΔΕΕ έκρινε ότι οι εποπτικές αρχές είναι εξουσιοδοτημένες να διατάσσουν τη διαγραφή παράνομα επεξεργασμένων δεδομένων αυτεπάγγελτα.[26]

Με σκοπό, λοιπόν, τη γεφύρωση αυτής της νομικής ασυμφωνίας προκρίνονται τρεις βασικές τεχνικές: «Off-chain Storage», «Crypto-shredding» και «Chameleon Hashes», καθεμία από τις οποίες παρουσιάζει ιδιαίτερα νομικά πλεονεκτήματα και μειονεκτήματα. Στην πρώτη περίπτωση, τα δεδομένα αποθηκεύονται εκτός της αλυσίδας του blockchain, σε εξωτερικά συστήματα, όπως παραδοσιακοί διακομιστές ή αποκεντρωμένα δίκτυα αρχείων (π.χ. IPFS), ενώ στο blockchain καταχωρίζεται μόνο η κρυπτογραφική τους σύνοψη (hash). Η τεχνική αυτή διευκολύνει την άσκηση του δικαιώματος διαγραφής, σύμφωνα με τον ΓΚΠΔ, καθώς επιτρέπει την αφαίρεση των δεδομένων από το εξωτερικό σύστημα χωρίς την τροποποίηση της αμετάβλητης αλυσίδας. Ωστόσο, η διατήρηση του hash ενδέχεται, υπό συγκεκριμένες προϋποθέσεις, να συνιστά επεξεργασία προσωπικών δεδομένων, εφόσον παραμένει δυνατή η ταυτοποίηση του υποκειμένου. Συνεπώς, η διαγραφή των αρχικών δεδομένων δεν συνεπάγεται αυτομάτως την πλήρη συμμόρφωση με τις απαιτήσεις του ΓΚΠΔ. Ύστερα, το «Crypto-shredding» συνίσταται στην οριστική καταστροφή του κλειδιού αποκρυπτογράφησης, καθιστώντας τα κρυπτογραφημένα δεδομένα πρακτικά απροσπέλαστα. Το βασικό νομικό πλεονέκτημα της μεθόδου έγκειται στη δυνατότητα περιορισμού της πρόσβασης στα δεδομένα χωρίς να απαιτείται η φυσική διαγραφή τους από κάθε αποθηκευτικό μέσο. Εντούτοις, η τεχνική αυτή δεν ταυτίζεται κατ'

[26] *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala κατά Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-46/23, EU:C:2024:239.

ανάγκην με τη νομική διαγραφή, καθώς η αποτελεσματικότητά της εξαρτάται από την ισχύ της κρυπτογράφησης, την απουσία αντιγράφων του κλειδιού και τη μη ύπαρξη άλλων μέσων ανάκτησης. Επομένως, η συμμόρφωση με τον ΓΚΠΔ προϋποθέτει αξιολόγηση του κατά πόσον τα δεδομένα καθίστανται πράγματι μη προσβάσιμα και μη επαναταυτοποιήσιμα.Τέλος, τα «Chameleon Hashes» αποτελούν ειδικές συναρτήσεις κατακερματισμού που επιτρέπουν, μέσω ενός μυστικού κλειδιού («trapdoor key»), την τροποποίηση συγκεκριμένων δεδομένων χωρίς μεταβολή της τελικής κρυπτογραφικής σύνοψης. Το σημαντικότερο πλεονέκτημά τους είναι ότι παρέχουν τη δυνατότητα επιλεκτικής αναθεώρησης εγγραφών, περιορίζοντας τη σύγκρουση μεταξύ της αμεταβλητότητας του blockchain και της υποχρέωσης διαγραφής ή διόρθωσης δεδομένων. Παράλληλα, όμως, η ύπαρξη του μυστικού κλειδιού δημιουργεί ζητήματα ασφάλειας, λογοδοσίας και διακυβέρνησης, καθώς η ανεξέλεγκτη χρήση του μπορεί να υπονομεύσει την ακεραιότητα και την αποδεικτική αξιοπιστία της αλυσίδας. Ως εκ τούτου, η νομική αποτελεσματικότητα της τεχνικής εξαρτάται από την ύπαρξη αυστηρών μηχανισμών ελέγχου, διαφάνειας και καταγραφής κάθε τροποποίησης.

Οι νομικές προκλήσεις επεκτείνονται εμφανώς και στα συστήματα *«Federated Learning»*,καθώς όταν εφαρμόζονται στο *«blockchain»*, τα προσωπικά δεδομένα διαχέονται στις παραμέτρους *(weights)* του νευρωνικού δικτύου και τα μοντέλα Αποκεντρωμένης ΤΝ αναπτύσσουν στατιστική μνήμη, επιτρέποντας την αναπαραγωγή των αρχικών πληροφοριών. Η πλήρης επανεκπαίδευση *(retraining)* του μοντέλου αυτού από το μηδέν είναι υπολογιστικά ασύμφορη και έτσι η επιστημονική κοινότητα απαντά μέσω της Μηχανικής Απομάθησης *(Machine Unlearning).*[27] Σύμφωνα με πρόσφατες μελέτες, η τροποποίηση των βαρών επιτυγχάνεται μέσω τριών

[27] Yixiong Wang et al., "Learning to Unlearn in Federated Learning," στο *2024 2nd International Conference on Federated Learning Technologies and Applications (FLTA)* (Piscataway, NJ: IEEE, 2024), https://doi.org/10.1109/FLTA63145.2024.10840121.

μεθοδολογιών:[28] Διαφορική Απομάθηση *(Differential Unlearning)*, την Αρχιτεκτονική SISA *(Sharded, Isolated, Sliced, and Aggregated Learning)* που σχεδιάστηκε κυρίως για να κάνει το *«machine unlearning»* (την αφαίρεση δεδομένων από ένα εκπαιδευμένο μοντέλο) γρήγορο και αποτελεσματικό. Εν κατακλείδι, η διαδικασία «απόσταξης στην απομάθηση» *(Distillation-based Unlearning)* σε συνδυασμό με τις «ενέσεις θορύβου» *(noise injections)*, όπως η μέθοδος «UNDO» *(Unlearn-Noise-Distill-on-Outputs)*, αποτελεί τεχνική αφαίρεσης ικανοτήτων από μοντέλα τεχνητής νοημοσύνης με μειωμένες πιθανότητες για κενά ασφαλείας. Βάσει των παραπάνω δεδομένων, μπορούμε να θεωρήσουμε ασφαλέστερη συνολική προσέγγιση τον συνδυασμό των "Off-chain Storage" και "Crypto-shredding". Η πρώτη τεχνική διευκολύνει τη διαχείριση και τη διαγραφή των δεδομένων, ενώ η δεύτερη προσφέρει ένα πρόσθετο επίπεδο προστασίας της εμπιστευτικότητας. Ο συνδυασμός τους, πάντως, δεν εγγυάται αυτομάτως συμμόρφωση με τον ΓΚΠΔ: απαιτείται αξιολόγηση του κατά πόσον τα δεδομένα που παραμένουν στην αλυσίδα μπορούν ακόμη να συνδεθούν με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Παραβίαση Θεμελιωδών Αρχών και Διεθνείς Πρωτοβουλίες

Η ενσωμάτωση της Αποκεντρωμένης ΤΝ αποκτά ακόμα περισσότερο ενδιαφέρον στην κατασκευή των Φονικών Αυτόματων Οπλικών Συστημάτων (ΑΟΣ), όπως τα *«drones»*, αλλά και το σύστημα εγγύς προστασίας « PHALANX» αναδιαμορφώνοντας τη σύγχρονη στρατιωτική αντίληψη. Αυτή η εξέλιξη, έρχεται σε σύγκρουση με το Δημόσιο Διεθνές Δίκαιο και ειδικότερα τον Ανθρωπιστικό τομέα του (ΔΑΔ), ο οποίος ρυθμίζει και την

[28] Hithem Lamri και Michail Maniatakos, "Fully Decentralized Certified Unlearning," στο *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)* (Piscataway, NJ: IEEE, 2026), https://openaccess.thecvf.com/content/CVPR2026/html/Lamri_Fully_Decentralized_Certified_Unlearning_CVPR_2026_paper.html.

συμπεριφορά των Κρατών και ειδικότερα των ενόπλων δυνάμεων και κυβερνήσεων κατά την διάρκεια ενόπλων συγκρούσεων *(jus in bello).* Η μετάβαση από κεντρικά ελεγχόμενα συστήματα σε αυτοδιοικούμενα και αποκεντρωμένα, δημιουργεί ακούσια νομικά κενά ως προς την τήρηση θεμελιωδών κανόνων του πολέμου δημιουργώντας μεγάλη ανησυχία.

Βάσει των Πρόσθετων Πρωτοκόλλων των Συμβάσεων της Γενεύης (1977), η χρήση οπλισμού στο πεδίο της μάχης, πρέπει να συμμορφώνεται με τρεις βασικές αρχές: την Αρχή της Διακρίσεως,[29] την Αρχή της Αναλογικότητας,[30] και την Αρχή της Προφυλάξεως.[31] Η πρώτη, απαιτεί από τον στρατιωτικό στόλο να διακρίνει τον άμαχο πληθυσμό από τον αντίπαλο στόλο. Για παράδειγμα, μια ομάδα *«drones»* που είναι προγραμματισμένα μέσω συστημάτων *«Federated Learning»,* ενδέχεται χωρίς ανθρώπινη επίβλεψη ή οδηγία να τροποποιήσει τα κριτήρια αναγνώρισης στόχου, γεγονός που, αναμφίβολα μπορεί να οδηγήσει σε τυφλά πλήγματα αμάχων[32]. Με την Αρχή της Αναλογικότητας, απαγορεύονται οι επιθέσεις, κατά την πραγμάτωση των οποίων, η προβλεπόμενη παράπλευρη απώλεια αμάχων είναι δυσανάλογη με το άμεσο στρατιωτικό όφελος. Η αναλογικότητα ρυθμίζεται από την κατ' εξοχήν ανθρώπινη γνωστική λειτουργία, της κριτικής ικανότητας, χαρακτηριστικό που τα συστήματα «Decentralised AI» αδυνατούν να παράξουν, προς το παρόν. Τέλος, το άρθρο 57 πρ.1 με το οποίο καθιερώνεται η αρχή της Προφυλάξεως, επιβάλλει τη λήψη όλων των πρακτικών προλήψεως για την αποφυγή απωλειών αμάχων, συμπεριλαμβανομένης ακόμη και της ακύρωσης μιας σχεδιασμένης επίθεσης. Λόγω της αποκεντρωμένης λήψης αποφάσεων καθίσταται ο συλλογιστικός έλεγχος αδύνατος και αυξάνεται ο κίνδυνος

[29] Συμπληρωματικό Πρωτόκολλο των Συμβάσεων της Γενεύης της 12ης Αυγούστου 1949 που αναφέρεται στην προστασία των θυμάτων των διεθνών ενόπλων συγκρούσεων, Γενεύη, 08.06.1977, άρθρο 48, κυρωθέν στην Ελλάδα με τον Ν. 1786/1988 [εφεξής: Πρωτόκολλο Ι].
[30] *Ibid.,* άρθρο 51.
[31] *Ibid.,* άρθρο 57.
[32] Παντελεήμων Στεργιάννης, «Αυτόνομα οπλικά συστήματα (ΑΟΣ) και κύρια ζητήματα διεθνούς ανθρωπιστικού δικαίου», *Εθνικές Επάλξεις*, άρ. 122 (Οκτώβριος–Δεκέμβριος 2017), https://www.splaw.gr/oas-zitimata-diethnous-anthropistikou-dikaiou/.

κατευθύνσεως επίθεσης σε λανθασμένο στόχο, είναι αδύνατον ένας διοικητής να παρέμβει και να αναστείλει την επίθεση προγραμματισμένων μηχανημάτων (λ.χ. drones) για την αποτροπή του αποτελέσματος εγκαίρως.

Κρατική Ευθύνη

Το Διεθνές Δίκαιο βασίζεται στην αρχή ότι η νομική ευθύνη αποδίδεται πάντα στους ανθρώπους και όχι στις μηχανές. Συνεπώς, δημιουργείται ένα κενό λογοδοσίας που απευθύνεται στους Διοικητές και τις Κυβερνήσεις. Από την μία πλευρά, το Διεθνές Ποινικό Δίκαιο (καταστατικό της Ρώμης) προβλέπει την ευθύνη των διοικητών για εγκλήματα πολέμου. Όταν, όμως, οι αποφάσεις λαμβάνονται συνεργατικά και αποκεντρωμένα από εκατοντάδες κόμβους ΤΝ δημιουργείται το εν λόγω κενό λογοδοσίας *(accountability void)* καθώς κανένας άνθρωπος δεν έδωσε έγκριση για την τελική απόφαση. Από την πλευρά της Κρατικής Ευθύνης, σύμφωνα με το Άρθρο 36 Πρωτόκολλο Ι της Σύμβασης της Γενεύης, τα κράτη είναι υποχρεωμένα να εξετάζουν κάθε όπλο πριν την χρήση του, γεγονός στην περίπτωση που μελετάται αδύνατο, δεδομένου ότι οι αλγόριθμοι αλλάζουν την προκαθορισμένη συμπεριφορά τους και αυτοεξελίσσονται κατά την διάρκεια της ανάπτυξης στο πεδίο, η προκαταρκτική νομική εξέταση καθίσταται πρακτικά αδύνατη.

Η Ρήτρα «Martens», η οποία είναι και κωδικοποιημένη στο ΔΑΔ, ορίζει ότι σε περιπτώσεις που δεν καλύπτονται από γραπτούς κανόνες, οι πολίτες και οι μαχόμενοι παραμένουν υπό την προστασία των αρχών του ανθρωπισμού και των επιταγών της δημόσιας συνείδησης.[33] Η εκχώρηση

[33] International Committee of the Red Cross, *ICRC Position on Autonomous Weapon Systems* (Geneva: ICRC, 2021), https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems· *Report of the 2023 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, CCW/GGE.1/2023/2 (Geneva: United Nations, 2023), https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW-GGE.1-2023-2_English.pdf.

αποφάσεων ζωής και θανάτου σε αποκεντρωμένους αλγορίθμους, κρίνεται από πολλούς νομικούς ως παράβαση αυτής της ρήτρας. Για τον λόγο αυτό, στο πλαίσιο του Οργανισμού Ηνωμένων Εθνών και της Σύμβασης για Ορισμένα Συμβατικά Όπλα (CCW), διεξάγονται πολλές συζητήσεις με σκοπό την δημιουργία μιας διεθνούς δεσμευτικής συνθήκης που είτε θα απαγορεύει είτε θα ρυθμίζει με τέτοια αυστηρότητα τα «LAWS», διασφαλίζοντας τον «ουσιαστικό ανθρώπινο έλεγχο» (meaningful human control).[34]

Σε πρόσθετο πρωτόκολλο στις Συμβάσεις της Γενεύης επιβάλλεται στα Κράτη η υποχρέωση να καταστήσουν σαφές αν η μελέτη, η ανάπτυξη, η απόκτηση ενός νέου μέσου ή μεθόδου πολέμου αντικρούει τις διατάξεις για την προστασία του Διεθνούς Ανθρωπιστικού Δικαίου . Όταν το εν λόγω αντικείμενο ανήκει στην κατηγορία των οπλικών συστημάτων, η λειτουργία των οποίων βασίζεται στην Αποκεντρωμένη ΤΝ (DeAI), η διαδικασία νομικής αξιολόγησης έρχεται αντιμέτωπη σε σημαντικές δοκιμασίες. Στα DeAI συστήματα *(Swarm Intelligence ή Federated Learning),* επειδή η λήψη αποφάσεων δεν προέρχεται από έναν κεντρικό διακομιστή ή αλγόριθμο αλλά από την αλληλεπίδραση πολλών αυτόνομων κόμβων η αξιολόγηση δεν γίνεται με βάση έναν κώδικα στατικό, αλλά ένα διαρκώς εξελισσόμενο σύστημα, καθιστώντας τις προσπάθειες για οποιονδήποτε προληπτικό έλεγχο ανούσιες. Έργο της αξιολόγησης είναι η πιστοποίηση ότι το συγκεκριμένο σύστημα πληροί τις απαραίτητες προδιαγραφές για την διατήρηση των θεμελιωδών αρχών άθικτων. Για την αποτελεσματική λειτουργία των παραπάνω κρίνεται αναγκαία η εξασφάλιση αξιόπιστης ανταλλαγής δεδομένων μεταξύ αισθητήρων ώστε ο στόχος να παραμένει αμετάβλητος και να μην υπάρχουν παράπλευρες απώλειες ακόμη και σε περίπτωση βλάβης του συστήματος (π.χ απώλεια επικοινωνίας). Σε κάθε περίπτωση ένα προγραμματισμένο για οπλικό σύστημα DeAI πρέπει να

[34] Anna-Katharina Ferl, "Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare," *Global Society* 38, no. 1 (2024), https://doi.org/10.1080/13600826.2023.2233004.

περιλαμβάνει στον προγραμματισμό του αυτόματη ματαίωση της επίθεσης *(auto-abort)* σε κάθε περίπτωση μεταβολής δεδομένων αλλά και δικλείδες ασφαλείας που επιτρέπουν στον εκάστοτε χειριστή να διακόψει τη λειτουργία του κατανεμημένου δικτύου όποτε εκείνος κρίνει αναγκαίο. Τα πρωτόκολλα του Άρθρου 36 αναφέρονται και βασίζονται στην πρόβλεψη της χρήσης του όπλου συνήθεις συνθήκες . Στη DeAI, λόγω της αυτοματοποιημένης διαδικασίας και της μειωμένης ανθρώπινης επιρροής, εντείνεται ο κίνδυνος απρόβλεπτης συμπεριφοράς και αποτελέσματος. Η αξιολόγηση προκειμένου να είναι ακριβής και αξιόπιστη απαιτεί επανάληψη προσομοιώσεων και τοποθέτηση μηχανισμών εξήγησης για την ελεγχόμενη δράση του οπλικού μηχανισμού. Επομένως, στο πλαίσιο της διαδικασίας δεν αξιολογείται μόνο το τελικό αποτέλεσμα σαν προϊόν αλλά και η λειτουργία και η δομή του δικτύου, και τα περιθώρια αυτονομίας με βάσει τα πρωτόκολλα και Ουσιαστικό ανθρώπινο έλεγχο, χωρίς τον οποίο δεν είναι δυνατή η έγκριση.

Συμβατότητα με Αρχές Διεθνούς Ανθρωπιστικού Δικαίου

Στη σύγχρονη μάχη στις κατανεμημένες δομές διοίκησης, όπως τα αλγοριθμικά συστήματα «C2» ή τα αυτόνομα όπλα, για την διασφάλιση των αρχών του ΔΑΔ απαιτούν μετατόπιση νομικής ευθύνης από τον στιγμιαίο διοικητή στους σχεδιαστές, προγραμματιστές και ανώτερους στρατηγικούς διοικητές που θέτουν τα όρια λειτουργίας τους[35]. Με γνώμονα, την Αρχή της Διάκρισης, οι αλγόριθμοι τροφοδοτούνται με πολυφασματικά δεδομένα (αισθητήρες, υπέρυθρες) ώστε να ταυτοποιήσουν τους στόχους. Η χρήση των κατανεμημένων αυτόνομων

[35] Neil Davison, "A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law," στο *Perspectives on Lethal Autonomous Weapon Systems*, UNODA Occasional Papers 30 (New York: United Nations, 2017), 12, https://doi.org/10.18356/29a571ba-en.

συστημάτων εγκρίνεται μόνο σε γεωγραφικά απομονωμένες περιοχές όπου η παρουσία αμάχου είναι ελάχιστη έως μηδενική. Η Αρχή της Αναλογικότητας, στο κατανεμημένο δίκτυο υπολογίζεται εκ των προτέρων με τους ανώτερους διοικητές να καθορίζουν μέσω του αλγορίθμου τα ανώτατα όρια αποδεκτού ρίσκου. Εάν οι αισθητήρες εντοπίσουν απρόσμενη συγκέντρωση αμάχων που υπερβαίνει το προκαθορισμένο όριο, το σύστημα ενεργοποιείται ώστε να ματαιωθεί η επίθεση.[36] Όσον αφορά, την Αρχή της Στρατιωτικής Αναγκαιότητας, η κατανεμημένη λήψη αποφάσεων πρέπει να συμβαδίζει με τον στρατηγικό στόχο ο κατόπιν εγκρίσεως από ανθρώπινο σύνολο. Το σύστημα δεν έχει την δικαιοδοσία να παίρνει αυθαίρετες αποφάσεις για τον σκοπό αλλά βελτιστοποιεί την τακτική εκτέλεσης εντός συγκεκριμένου πλαισίου ορισμένου ειδικά για την αποστολή.

Με ποιές μεθόδους λοιπόν είναι εφικτό να διασφαλιστεί η προστασία των θεμελιωδών αρχών του ΔΑΔ; Αρχικά, μέσω του «Meaningful Human Control», διατηρείται ο ανθρώπινος παράγοντας στο στάδιο του σχεδιασμού, της ενεργοποίησης και του καθορισμού των κανόνων εμπλοκής «ROE». Επιπλέον, το Πρόσθετο Πρωτόκολλο[37] «CCW» υποχρεώνει τα κράτη να αξιολογούν νομικά κάθε νέο μέσο ή μέθοδο πολέμου πριν τη χρήση του, ώστε να διαπιστώνεται η συμβατότητα με το ΔΑΔ. Τέλος, χάρη στην Αλγοριθμική Διαφάνεια και στην ιχνηλασιμότητα διευκολύνεται η καταγραφή δεδομένων *(black box)* ώστε να επιτυγχάνεται η απόδοση ποινικής ευθύνης σε ανθρώπους (προγραμματιστές και ανώτερη διοίκηση) σε περιπτώσεις παραβάσεων ακριβώς όπως προβλέπουν τα σχετικά νομοθετικά κείμενα.[38]

[36] "Auto abort Protocol"
[37] Πρωτόκολλο Ι άρθρο 36.
[38] Gerald Mako, "Legal Accountability for AI-Driven Autonomous Weapons," *Articles of War*, Lieber Institute West Point, 09.03.2026, https://lieber.westpoint.edu/legal-accountability-ai-driven-autonomous-weapons/.

Συμπέρασμα

Από την παραπάνω μελέτη συμπεραίνεται ότι η Αποκεντρωμένη Τεχνητή Νοημοσύνη αποτελεί μια μεταβολή μεγάλου μεγέθους και σημασίας, η ραγδαία πρόοδος της οποίας οδηγεί σε ιδιαίτερες κανονιστικές προκλήσεις, επαναπροσδιορίζοντας τα όρια της καινοτομίας στη σύγχρονη ψηφιακή εποχή αλλά και την δύναμη και τον έλεγχο του Νόμου επί της τεχνολογίας. Παρά το γεγονός ότι αποτελεί λύση στα περισσότερα ελαττώματα που χαρακτηρίζουν την Κεντρικοποιημένη Τεχνητή Νοημοσύνη, όπως οι συγκρούσεις που αφορούν την πνευματική ιδιοκτησία, οι παραβιάσεις δικαιώματος της ιδιωτικότητας και τα κενά στην ασφάλεια, οι δυσκολίες που έχουν παρουσιαστεί εξαιτίας της απαιτούν μια ολιστική και πολυεπίπεδη προσέγγιση ως προς τη ρύθμιση και τη διακυβέρνησή της. Καθώς τα συστήματα της ΤΝ εξελίσσονται περαιτέρω, οι νομικοί οφείλουν να ακολουθήσουν διαφορετική προσέγγιση και να μεριμνήσουν για την σταθερή και ολοκληρωμένη ρύθμιση των ζητημάτων που ανακύπτουν λόγω κενών στη νομοθεσία η οποία κρίνεται ανεπαρκής, μη δυνάμενη να ανταποκριθεί στους ταχύτατους ρυθμούς εξέλιξης της τεχνολογίας . Κρίνεται αναγκαία η εναρμόνιση των Κανονισμών «GDPR» και «EU AI ACT 2024» με το μοντέλο της Αποκεντρωμένης ΤΝ ή η θέσπιση νομοθετικού πλαισίου για την κάλυψη των κενών που έχουν δημιουργηθεί ακουσίως ώστε να μην υπάρξουν σοβαρές παραβιάσεις θεμελιωδών δικαιωμάτων ,η οποίες θα μείνουν ατιμώρητες χωρίς «υπεύθυνο» να αναλάβει την ευθύνη. Τα Αυτόματα Οπλικά Συστήματα ως μορφή Αποκεντρωμένης ΤΝ επρόκειτο τα επόμενα χρόνια να παραμείνουν στο προσκήνιο χάρη στην ευαίσθητη φύση του απόλυτου δικαιώματος στην ζωή το οποίο απειλείται από την «αναισθησία» και την έλλειψη κριτικής σκέψης της τεχνητής νοημοσύνης με την ευθύνη για παραβιάσεις της νομοθεσίας να αποδίδεται αδιακρίτως και ημιτελώς στον ανώτερο στρατηγό υπεύθυνο ή ακόμα και τον κατασκευαστή του οπλισμού. Πρόκειται για μία ξεχωριστή τεχνολογία με ατελείωτες δυνατότητες που θα αλλάξει ριζικά την πορεία του ανθρώπινου είδους. Είναι στο χέρι

του ανθρώπου και τον τρόπο διαχειρίσεως της κατάστασης που θα επιλέξει, εάν θα δουλεύει υπέρ αυτού και της προστασίας των δικαιωμάτων του ή εάν θα αποτελέσει βασικό καταλύτη των ανθρωπίνων δικαιωμάτων.

Βιβλιογραφία

Νομοθεσία και διεθνή κείμενα

- European Parliament and Council. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence [...] (Artificial Intelligence Act). OJ L, 2024/1689, 12.07.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.
- Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο. Κανονισμός (ΕΕ) 2016/679, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα [...] (Γενικός Κανονισμός για την Προστασία Δεδομένων). ΕΕ L 119, 04.05.2016, 1–88. https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32016R0679.
- Συμπληρωματικό Πρωτόκολλο των Συμβάσεων της Γενεύης της 12ης Αυγούστου 1949 που αναφέρεται στην προστασία των θυμάτων των διεθνών ενόπλων συγκρούσεων (Πρωτόκολλο Ι). Γενεύη, 08.06.1977. Κυρώθηκε με τον Ν 1786/1988.

Νομολογία

- ΔΕΕ. *Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala κατά Nemzeti Adatvédelmi és Információszabadság Hatóság*. C-46/23, EU:C:2024:239, 14.03.2024.
- ΔΕΕ. *Fashion ID GmbH & Co. KG κατά Verbraucherzentrale NRW eV*. C-40/17, EU:C:2019:629, 29.07.2019.
- ΔΕΕ. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein κατά Wirtschaftsakademie Schleswig-Holstein GmbH*. C-210/16, EU:C:2018:388, 05.06.2018.

Βιβλία, άρθρα και εκδέσεις

Ελληνικά

- Στεργιάννης, Παντελεήμων. «Αυτόνομα οπλικά συστήματα (ΑΟΣ) και κύρια ζητήματα διεθνούς ανθρωπιστικού δικαίου». *Εθνικές Επάλξεις*, άρ. 122

(Οκτώβριος–Δεκέμβριος 2017). https://www.splaw.gr/oas-zitimata-diethnous-anthropistikou-dikaiou/.

Ξενόγλωσσα

- Bazoobandi, Sara. *How Autonomous Weapon Systems Threaten International Humanitarian Law*. GIGA Focus Global 4. Hamburg: German Institute for Global and Area Studies (GIGA), 2026. https://doi.org/10.57671/gfgl-26042.
- Boulanin, Vincent, και Maaike Verbruggen. *Mapping the Development of Autonomy in Weapon Systems*. Solna: Stockholm International Peace Research Institute (SIPRI), 2017. https://www.sipri.org/publications/2017/policy-reports/mapping-development-autonomy-weapon-systems.
- Caballar, Rina Diane, και Cole Stryker. "What Is Federated Learning?" IBM Think, 02.04.2025. https://www.ibm.com/think/topics/federated-learning.
- Casey-Maslen, Stuart. "Autonomous Weapons Systems under International Law." Στο *Artificial Intelligence in Military Technology: Sociological, Cultural and Ethical Perspectives*, επιμ. Kairi Talves και Dierk Spreen, 161–179. Artificial Intelligence, Simulation and Society. Cham: Springer, 2025. https://doi.org/10.1007/978-3-031-95578-5_10.
- Commission nationale de l'informatique et des libertés (CNIL). "AI System Development: CNIL's Recommendations to Comply with the GDPR." 05.01.2026. https://www.cnil.fr/en/ai-system-development-cnils-recommendations-to-comply-gdpr.
- Davison, Neil. "A Legal Perspective: Autonomous Weapon Systems under International Humanitarian Law." Στο *Perspectives on Lethal Autonomous Weapon Systems*, 5–18. UNODA Occasional Papers 30. New York: United Nations, 2017. https://doi.org/10.18356/29a571ba-en.
- Deolindo, Blaine. "Decentralized AI: A Regulatory Escape Hatch or the Future of Compliant Innovation." LinkedIn, 23.09.2025. https://www.linkedin.com/pulse/decentralized-ai-

regulatory-escape-hatch-future-blaine-deolindo-taasf.
- Derosiaux, Stéphane. "Crypto Shredding for Kafka: GDPR-Compliant Data Deletion." Conduktor, 16.10.2026. https://www.conduktor.io/glossary/crypto-shredding-for-kafka.
- Ferl, Anna-Katharina. "Imagining Meaningful Human Control: Autonomous Weapons and the (De-) Legitimisation of Future Warfare." *Global Society* 38, no. 1 (2024): 139–155. https://doi.org/10.1080/13600826.2023.2233004.
- Finck, Michèle. *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* PE 634.445. Brussels: European Parliamentary Research Service, 2019. https://doi.org/10.2861/535.
- Future of Life Institute. "High-Level Summary of the AI Act." EU Artificial Intelligence Act, 27.02.2024. https://artificialintelligenceact.eu/high-level-summary/.
- Hui, Xiang, και Catherine Tucker. "Decentralization, Blockchain, Artificial Intelligence (AI): Challenges and Opportunities." *Journal of Product Innovation Management* 42, no. 5 (2025): 947–957. https://doi.org/10.1111/jpim.12800.
- Human Rights Watch και International Human Rights Clinic (Harvard Law School). *A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making*. New York: Human Rights Watch, 28.04.2025. https://www.hrw.org/report/2025/04/28/a-hazard-to-human-rights/autonomous-weapons-systems-and-digital-decision-making.
- International Committee of the Red Cross (ICRC). *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*. Geneva: ICRC, 2006. https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf.
- International Committee of the Red Cross (ICRC). *ICRC Position on Autonomous Weapon Systems*. Geneva: ICRC, 2021. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.
- Lamri, Hithem, και Michail Maniatakos. "Fully Decentralized Certified Unlearning." Στο *Proceedings*

of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 24577–24586. Piscataway, NJ: IEEE, 2026. https://openaccess.thecvf.com/content/CVPR2026/html/Lamri_Fully_Decentralized_Certified_Unlearning_CVPR_2026_paper.html.

- Law Commission. "Decentralised Autonomous Organisations (DAOs)." https://lawcom.gov.uk/project/decentralised-autonomous-organisations-daos/.
- Lysikova, Mia. "Decentralized AI: What It Is and How It Differs from Centralized AI? [*sic*]." nexos.ai, 16.01.2026. https://nexos.ai/blog/decentralized-ai/.
- Mako, Gerald. "Legal Accountability for AI-Driven Autonomous Weapons." *Articles of War*, Lieber Institute West Point, 09.03.2026. https://lieber.westpoint.edu/legal-accountability-ai-driven-autonomous-weapons/.
- Marshall, Tom. *Decentralised Artificial Intelligence*. London: CMS, 2024. https://cms.law/en/gbr/publication/decentralised-artificial-intelligence.
- Perrin, Benjamin. "Lethal Autonomous Weapons Systems & International Law: Growing Momentum towards a New International Treaty." *ASIL Insights* 29, no. 1 (24.01.2025). https://www.asil.org/insights/volume/29/issue/1.
- Raskar, Ramesh. "Decentralized AI." MIT Media Lab. https://www.media.mit.edu/projects/decentralized-ai/overview/.
- *Report of the 2023 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*. CCW/GGE.1/2023/2. Geneva: United Nations, 2023. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW-GGE.1-2023-2_English.pdf.
- Santana, Carlos, και Laura Albareda. "Blockchain and the Emergence of Decentralized Autonomous Organizations (DAOs): An Integrative Model and Research Agenda." *Technological Forecasting and Social Change* 182 (2022): 121806. https://doi.org/10.1016/j.techfore.2022.121806.

- Sassòli, Marco. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Cheltenham: Edward Elgar Publishing, 2019.
- Schmitt, Michael N., επιμ. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.
- Sergeev, Miron. "Lethal Autonomous Weapon Systems (LAWS): Accountability, Collateral Damage, and the Inadequacies of International Law." Institute for Law, Innovation & Technology (iLIT), Temple University, 08.11.2024. https://law.temple.edu/ilit/lethal-autonomous-weapon-systems-laws-accountability-collateral-damage-and-the-inadequacies-of-international-law/.
- Shoemaker, Phillip. "What Is a Peer-to-Peer (P2P) Network?" Identity.org, 18.12.2025. https://www.identity.org/peer-to-peer-network/.
- Somgal, Edward. "The Rise of Decentralized AI: A New Era of Privacy Protection?" Maya Data Privacy, 09.07.2025. https://www.mayadataprivacy.com/post/the-rise-of-decentralized-ai-a-new-era-of-privacy-protection.
- UltraEdge. "Decentralized AI: How It Works and the Benefits." 07.07.2025. https://www.ultraedge.com/en/blog/decentralized-ai.
- Wang, Yixiong, Jalil Taghia, Selim Ickin, Konstantinos Vandikas και Masoumeh Ebrahimi. "Learning to Unlearn in Federated Learning." Στο *2024 2nd International Conference on Federated Learning Technologies and Applications (FLTA)*, 259–266. Piscataway, NJ: IEEE, 2024. https://doi.org/10.1109/FLTA63145.2024.10840121.
- Zhu, Tianqi, Yuxiang Huang, Zhihong Liang, et al. "Research on an On-Chain and Off-Chain Collaborative Storage Method Based on Blockchain and IPFS." *Future Internet* 18, no. 2 (2026): 92. https://doi.org/10.3390/fi18020092.